Optimized Federated Learning with Ensemble of Sequential Models for Detecting RPL Routing Attacks for AMI Networks

Puneet Sharma (✉ puneetgrandmaster@gmail.com)  
Amity University ASET: Amity University Amity School of Engineering and Technology  
https://orcid.org/0000-0002-4480-0996

T. Sakthivel  
Firstsoft Technologies Pvt. Ltd.

Ibrahim Ali Alnajjar  
Universiti Utara Malaysia

Research Article

Keywords: AMI, RPL, Federated Learning, Ensemble of Sequential Classifiers, PSO, Local Model Sharing Optimization, and Loss Function

Posted Date: March 21st, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2571557/v1

License: ☒ ☑ This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Optimized Federated Learning with Ensemble of Sequential Models for Detecting RPL Routing Attacks for AMI Networks

Puneet Sharma¹, T. Sakthivel², Ibrahim Ali Alnajjar³

¹Dept. of Computer Science and Engineering, Amity University, Uttar Pradesh, India
²Firstsoft Technologies P Ltd, Chennai, India
³Universiti Utara Malaysia, Malaysia

Abstract

With the rapid expansion of smart applications and services, the Internet of Things (IoT) plays a vital role in enabling changes in the usage of information and communication technology. Advanced Metering Infrastructure (AMI) is the key component of the smart grid which often meets privacy and security threats from the routing layer. The Routing Protocol for Low-Power and Lossy Networks (RPL) is the prominent routing protocol for AMI networks, and securing the RPL is the cornerstone of all security controls in the AMI for successful deployment. Recently, IoT security systems have increasingly adopted privacy-preserving Federated Learning (FL) that trains a local data model across multiple decentralized edge devices and takes global decisions without the need for global data sharing. Relying on a single learning model significantly degrades the FL performance due to the frequent transmission of weights and training on heterogeneous IoT networks. This paper proposes an Optimized FL model for Securing RPL (OFL-SRPL) over AMI devices. By reducing the size of the data transferred from the multiple local models to the server, the OFL-SRPL adopted the Particle Swam Optimization (PSO) algorithm to select the best local model from the Home Area Network (HAN) gateway and build the global model. The proposed OFL-SRPL applies an ensemble of sequential classifiers with its appropriate loss function to improve the decision-making quality and reduce the FL communication burden. Instead of transferring all the local model weights to the global model, the OFL-SRPL iteratively selects the best ensemble model with sequential classifies and only sends the weight of the best model to build the global model. The sequential classifier design improves the ownership weight and handles class imbalance issues. After taking an optimized global model decision, the devices execute ensemble classifiers successfully with
appropriate learning parameters. Thus, the proposed OFL-SRPL achieves 10.6% higher detection accuracy than a centralized setup of the Long Short-Term Memory (LSTM) model without incurring multiple communication rounds like traditional FL.

**Keywords:** AMI, RPL, Federated Learning, Ensemble of Sequential Classifiers, PSO, Local Model Sharing Optimization, and Loss Function.

1. **Introduction**

   Smart meter applications utilize the Advanced Metering Infrastructure (AMI), which is a composite technology of the Smart Grid (SG) infrastructure with bi-directional communication between smart meter devices at homes and servers. AMI composes a set of smart devices for monitoring and estimating utility usage between companies and customers. The Internet of Things (IoT) assists in building bidirectional communication in AMI applications [1]. Owing to the high scalability of the IoT network, providing security during bidirectional communication becomes a primary concern in AMI. At the same time, security controls at the top layers fail without securing the routing protocol. The Routing Protocol for Low-Power and Lossy Networks (RPL) is widely used but often suffers from security issues that impact the next-generation electricity grid and the design of secure two-way communication in AMI [2]. In addition, the design of a reliable RPL protocol for the AMI system is a critically challenging task due to the adversarial activities and constrained resources of the AMI devices. Recently, machine learning-driven IDS solutions have dominated in protecting AMI communication against intelligent attacks [3]. Even though centralized machine learning models deliver very promising solutions for the applications in the AMI, preserving end-user privacy is a key challenge among smart grid devices. Hence, security systems increasingly adopt the Federated Learning (FL) concept to ensure secure communication in the AMI networks without sensitive data exposure.

   FL enables the IoT clients to share only the local training model instead of transmitting their actual data to the global model [4]. The FL model grasps the knowledge of diversified data among IoT clients with independently trained local models. By aggregating the parameters of these local models, the IoT server generates a global model with resilience and greater accuracy to attack detection issues in IoT [5, 6]. Moreover, integrating the FL with the AMI networks guarantees the privacy preservation of each participant and improved communication efficiency
in a large-scale environment. Although aggregation algorithms in the FL iteratively transmit and receive the weights between each local learning model and global model, it significantly impacts the accuracy of the FL in the dynamically changing AMI network environments. The FL models employ the optimization algorithm to optimally fix the global model for selective weights from the local models to overcome this constraint. In addition, applying a single learning model to learn insightful knowledge from the data patterns in the multiple local networks becomes ineffective for the FL. Thus, this research adopts the deep ensemble model with a metaheuristic algorithm to design the optimal FL model to ensure secure communication in the IoT. Thus, the proposed work attempts to design an efficient and secure RPL model using optimized FL for the AMI networks.

1.1. Summary of Contributions

The main contributions of the proposed OFL-SRPL scheme are as follows.

⚫ The OFL-SRPL enables the ML training in Home Area Network (HAN)’s gateway and designs the AMI server with federated learning to ensure routing security at HAN’s end devices.

⚫ Instead of adopting a single learning model for the different networks of the FL, it designs the ensemble learning model with sequential classifiers and optimally selects the data-specific model parameters based on the prediction errors.

⚫ The proposed work iteratively designs the adaptive ensemble model in three stages of federated learning during the local model generation, global model generation, and local model updation with a different set of sequential classifiers for each local model in the HAN gateway.

⚫ The OFL-SRPL designs the FEDAGG with the PSO-based optimal local model sharing and integrates the benefits of class-specific improved ownership weight in the FEDAGG to achieve secure decision-making with reduced communication cost.

⚫ The experimental results exemplify the superiority of the proposed optimized FL utilizing a synthetic dataset generated from multiple runs of the Cooja simulator.

1.2. Paper Organization
Section 2 reviews previous work regarding RPL security utilizing Machine Learning (ML) models and IoT attack detection using FL. Section 3 provides system and attack models for the proposed work. Section 4 discusses ensemble classifier selection, FL local model generation, PSO-based optimization, and global model-sharing processes. Section 5 explains the performance evaluation section with graphs. The final section concludes the proposed work.

2. Related Works

Previously, the works related to RPL security solutions did not utilize the FL concept to improve security at a considerable cost of communication. However, Many upper layer security schemes have included FL for IoT security [7, 8]. Several works have utilized machine/deep learning models for RPL security provisioning. This section reviews RPL security solutions on RPL and FL-based IoT security solutions in other layers.

2.1. RPL Security Solutions using Machine Learning Models

ML algorithms are widely used in numerous RPL security schemes. A security solution in [9] enables the RPL to detect multiple network layer attacks using ML techniques. The security solution is analyzed under various OFs of RPL against combined attacks using ML algorithms under various scenarios. As a result, the ML models provide highly accurate solutions in detecting combined attacks against RPL. However, it is not evaluated under distributed network environment of attacks. Likewise, a GRU-based security scheme is designed [10] to defend the RPL protocol against hello flooding attacks in IoT networks and mitigates the misclassification of attacks. Likewise, Multi-Layer Perceptron (MLP) is used in [11] to detect the rank attack. However, the solutions in [10] and [11] are not scalable because they arise issues when the number of smart meters increases. In addition, the efficiency of security schemes is not evaluated under combined routing attacks, and privacy issues remain. In the work of [12], a Machine Learning based secure RPL routing (MLRP) protocol is proposed in which a complex dataset with malicious and normal network behavior is generated for RPL protocol using the Cooja simulator and adopted SVM model to isolate the attack behaviors. Moreover, it has utilized the Principal Component Analysis (PCA) to improve the performance of SVM by minimizing the dimensionality of features in the dataset.
A machine learning-based framework is proposed in [13] to identify the new insider attack effectively. It has formulated a set of features by analyzing the network traffic information and has modeled the network behavior. It employed a low-complex ML algorithm, such as XGBoost. However, a dynamic network topology needs adaptive and ensemble ML schemes for improved RPL security. In [14], an IDS is developed by combining supervised and semi-supervised deep learning for network traffic classification of normal and malicious RPL instances in the IoT environment. Likewise, several Artificial Intelligence (AI), Deep Learning (DL), and Reinforcement Learning (RL) schemes have been used in the design of secure RPL. Most of the works have improved their efficiency using feature reduction schemes while dealing with a large number of instances. However, most existing works fail to analyze the combined RPL attacks. In addition, analyzing the network traffic on IoT devices is inefficient for resource-restricted AMI, and traffic analysis on selective nodes using a single classifier does not improve the accuracy of the RPL security mechanism design. Moreover, a dynamic network topology needs adaptive and ensemble ML schemes for RPL security. Hence, the proposed work intends to incorporate and optimize the ensemble learning models to improve RPL communication security.

2.2. Federated Learning-Based IoT Security Schemes

The FL-based security schemes have emerged using a distributed collaborative AI approach in several intelligent IoT applications. FL schemes allow classifier training at distributed IoT devices without data sharing. The FL schemes overcome most of the issues in ML schemes on AMI. The ML schemes prerequisite the whole training data set on devices, which is expensive. Moreover, security risks involve transferring the data from end devices to a central server. The FL-based security scheme in [15] has utilized the advantages of combining different layers of Gated Recurrent Unit (GRU) and has attempted to improve the classification accuracy of FL under an IoT environment. Consequently, it preserves data integrity and privacy due to storing the data in its local IoT devices. FL has enabled the devices to share only the weights learned with the global server of the federated model. The FL-based security solution in [16] improves the attack detection accuracy by effectively designing the learning model with a local adaptive optimizer, such as the Adam optimizer and a cross-round learning rate scheduler. The work in [16] is the first attempt to explain various use cases to issues and scopes for future
enhancements. The FLGUARD, a poisoning defense framework, is developed in [17], and it provides data security and privacy without losing the benign performance of the aggregated model. Most of the existing FL scheme is vulnerable to inference attacks, in which a malicious aggregator gathers the information about IoT training data of the devices from their model updates during the process of local model sharing. In [18], the PSO heuristic search approach is used to model and tune the hyperparameters used in deep learning models. Consequently, it assists in the determination of the near-optimal values to deep learning parameters cost-effectively. However, it does not focus on the security and communication cost of local model parameters during sharing.

Several works [19,20] have proposed FL techniques to integrate ensemble methods. The FL scheme in [19] utilizes the advantages of the ensemble method in analyzing the network in multiple aspects. However, it fails to focus on ensemble optimization due to resource-constrained devices and insecurity during local model sharing. The attention Mechanism-based Convolutional Neural Network-LSTM (AMCNN-LSTM) model is developed in [21] to detect the anomalies successfully. The AMCNN-LSTM model uses attention mechanism-based CNN units and identifies the fine-grained features accurately. It has attempted to solve the gradient dispersion problems without losing the advantages of the LSTM unit in predicting time series data. However, it lacks in ensuring the privacy of the local model parameter due to the possibility of the attackers reversing the process of the local model to identify the information about IoT devices [22, 23]. The existing work [23] explores cloud data centers. During the collection of large amounts of data from the data centers with the support of FL, mitigating the communication latency and local model parameter privacy are the major concerns. Hence, edge computing is modeled in the IoT networks [24] to balance the computing resources in the secure model implementation. However, it still raises privacy concerns as devices’ local model parameters are shared with external entities. In addition, IoT devices are resource-constrained devices communicating through wireless technologies with limited battery and memory power. Hence, the frequent transmission of local model parameters to the server from many devices negatively impacts the advantages of FL schemes on IoT devices.

2.3. Problem Statement
Data routing across unprotected smart home devices in the IoT environment becomes vulnerable to RPL attacks. Even though ML algorithms have been designed for AMI, especially to detect the attackers, which are frequently upgrading their attack strategies, such as Denial of Service (DoS) attacks, several shortcomings need to be considered in designing an effective and accurate FL model for AMI.

➢ The performance of the FL heavily relies on the tradeoff between FL accuracy and communication rounds. Hence, sending many messages with a large size during local model sharing tends to cause data loss and inaccurate decision-making.

➢ Most FL schemes apply the FedAvg scheme in a global model generation, increasing the number of communication rounds.

➢ Lack of contemptating the data imbalance issues significantly degrades the efficiency of the FL model and fails to protect the routing of the AMI network.

➢ Increasing the number of training nodes negatively influences the FL model due to the increased global synchronization rounds to meet certain criteria in the local models.

➢ Designing a training model with a single classifier often fails to build a global learning model that supports all the local models with consistent knowledge.

➢ Even though ensemble models have been adopted in the FL model, an improper combination of results from ML techniques violates the decision-making ability of FL for different datasets.

Thus, the proposed work designs the intelligent scheme integrating the ensemble FL model and PSO to decrease the network communication costs during global model construction in FL without compromising the classification accuracy.

3. Network and Attack Model

The proposed network model considers the HANs for implementing the FL-based RPL security scheme, and the HANs is an extension of AMI networks. HAN devices are smart home and electrical appliances. These devices are under the control of the HAN gateway. The role of the gateway is to gather and analyze the power utilization of home appliances and energy loss information. The HAN gateway devices are directly connected to the AMI server to identify any malfunction and monitor the system performance. In Figure 1, multiple HANs are connected to the AMI server. One of the prime technologies used in AMI networks is Wireless mesh
connection. The smart home devices in HAN form a mesh network and follow the multi-hop communication until the gateway is reached. The tools analyzing the data are executed with the collected multi-hop information in the HAN gateway for malicious packet classification. For that, an AMI server executes an optimized federated global model learning, and the Gateway nodes connected with HAN are accountable for running the local models using an ensemble of classifiers. The processes of FL include the following key functions.

![Diagram](image)

**Figure 1: Architecture of AMI Network**

- **System Initialization:** Initially, the AMI server sets up the learning parameter, such as communication rounds, and is denoted as ‘t’.
- **Classifier Selection and Distributed Local Training:** In the proposed OFL-SRPL scheme, three different sequential classifiers are used, such as Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and GRU. After configuring the training parameters, each HAN gateway selects classifiers and starts the learning phase with its dataset, D_k. During the classifier selection, the main aim of the research work is to minimize the loss function F(w_k).

\[ W_k = \arg \min F(W_k)_t \]

The loss function differs for various classifiers; however, the proposed OFL-SRPL model explores the same loss function, such as cross-entropy.
\[ H(D,q) = - \sum_{i=1}^{N} \frac{1}{N} \log_2 q(x_i) \quad (2) \]

Where ‘N’ is the size of the test set (D), ‘i’ represents a particular instance \( i \in D \), and \( q(x) \) is the success of the classifier by the measure of the accuracy of \( i \)th instance. As per the basic FL, each gateway needs to update the result attained from equation (2) to the AMI server. The proposed scheme eases the parameter sharing from the local models with the assistance of the PSO method.

**Model Aggregation and Download:** The fundamental FL process enables the server to collect all the local model updates from gateway devices. In the FL model, the server aggregates them and decides the global model parameters.

\[ \text{Global } W_k = \frac{1}{k(\sum_{i=1}^{k} W_k(i))} \quad (3) \]

However, it tends to have high communication overhead, impacting the FL advantages. Hence, the proposed OFL-SRPL scheme adopts the PSO model and optimizes the global model aggregation. Finally, the AMI server executes the global model, and thus, the selected model is adopted by each HAN gateway.

### 3.1. Attack Model

The dataset in each HAN contains two parts, training and testing sets. The attacks covered by the synthetic dataset are as follows.

1. **Rank Attack:** The malicious nodes send control packets with fake rank values.
2. **Version Attack:** The version number is modified to drain the resources of HAN devices.
3. **Local repair:** It executes the poisoning mechanism for its implementation. The malicious node sets its rank to infinite and broadcasts this message to the whole network.
4. **Hello flooding:** A malicious node sends important route information, i.e., rank, to other nodes in the network.
5. **Puppet Attack [25]:** The intruder selects some nodes as puppets and sends an attack packet to these puppets. The puppet nodes flood control packets unnecessarily.

### 3.2. Overview of the OFL-SRPL Approach
With the rapid adoption of IoT applications, particularly AMI communication networks, securing the network layer has been a primary concern in recent years. To handle large-scale IoT data and ensure the privacy preservation of sensitive end-user data, FL becomes a potential solution for executing on-device training [5] in distributed AMI networks. Thus, the proposed OFL-SRPL work adopts and optimizes the FL with the aid of PSO and appropriately selects the ensemble classifiers with loss functions for the HAN to ensure the RPL security, illustrated in Figure 2. In the OFL-SRPL, the optimized FL leverages the global model updation to HAN devices with low latency. As mentioned in Figure 2, multiple HAN devices are directly connected to Secure Gateways, and multiple HAN gateways are connected to the AMI server. In the routing layer, the RPL is implemented to share the data to the gateway securely. The HAN communication is vulnerable to routing layer attacks, such as Hello Flooding, Local repair, Rank attack, Version, and puppet attack, and the traffic flows. The processes involved in the proposed scheme are outlined as follows.

**Dataset Creation and Feature Reduction at HAN Gateway:** To test the secure RPL scheme for the AMI, this work constructs the synthetic dataset and includes five attacks: Rank, Version, Local repair, Hello Flooding, and Puppet attacks. The dataset is partitioned into multiple files in which each file is loaded in HAN Gateway individually, and each packet has a set of features associated with a label. Irrelevant features in data packets degrade the optimized FL model; hence, in the proposed OFL-SRPL, the HAN gateway node penetrates the relevant features alone to the learning model to detect RPL attacks in AMI with the responsibility of loading the data samples in the network. It is accomplished by feature selection or irrelevant feature elimination, enhancing the FL accuracy with minimal computational time.

**Optimized Local Model Generation at HAN Gateway:** The proposed OFL-SRPL selects the sequential RNN, LSTM, and GRU classifiers for the ensemble model. Instead of running all the classifiers in each HAN, the proposed approach plans to execute selective classifiers in each HAN gateway in an iterative manner. Initially, every HAN gateway selects the appropriate classifier and initializes the parameters by processing the synthetically generated datasets in which each gateway retains its parameters while training its local model. The optimized FL applies the PSO to share only the best FL local model without compromising the FL accuracy instead of sending all the local models to the global model generation. The AMI server accepts the model weights from the gateway that offers the best score and eliminates the need to transmit the
local models from all Gateways to the global model. In the subsequence of identifying whether the HAN’s gateway has the Gbest classifiers, only the parameters from the local model are received from the Gbest classifiers to build the global model, and subsequently, the global model parameters are sent out from the AMI server back to the HAN gateway node for the next iteration. The OFL-SRPL repeats the process above for all iterations to enhance the global model.

![Diagram of the Proposed OFL-SRPL Scheme](image)

**Figure 2: Structure of the Proposed OFL-SRPL Scheme**

**Class-Specific Local Model Aggregation at AMI Server:** In the OFL-SRPL, implementing the local learning and global model with the FL concept contemplates the class imbalance constraint. The class-specific local model aggregation considers the number of instances in every class while estimating the loss function in the local and global model generation. Consequently, it effectively prevents inaccurate FL aggregation, and the server decides the best classifiers for a particular AMI network. Thus, the OFL-SRPL ensures the RPL security of the AMI networks by accurately classifying the attack and legitimate instances.

4. Proposed OFL-SRPL Methodology
Detecting the RPL for AMI networks, this work designs the OFL-SRPL that detects the HAN attackers in the routing layer and supports the provision of secure communication in HAN. The proposed work models the IoT architecture in HAN and connects multiple HANs to the AMI server. In the subsequence of OFL local model deployment on the HAN’s gateway, the local model is responsible for collecting the data from smart devices in HAN and executing the ensemble of classifiers with the collected data. Consequently, the OFL-SRPL builds the global model of the FL on the AMI server with the influence of the knowledge learned from the local models and the adoption of the PSO algorithm. Finally, to detect the attackers at IoT smart devices and secure the AMI network, the AMI server provides the globally learned parameters of the learning model and HAN gateway for the updation of local models.

4.1. Dataset Creation using Simulations

Most of the available IoT attack detection datasets contain various attacks, such as Rank, Version number, and so on. However, benchmark IoT datasets are outdated and exclude the traces of modern normal and attack traffic in the AMI network. Hence, the puppet DoS attack is created by considering the modern network traffic to evaluate AMI networks accurately. The Puppet attack refers that the intruder selecting a set of nodes as puppets and sending an attack packet to the selected puppets in which the puppet nodes ineffectually flood the request packets. Thus, the proposed work intends to build the RPL-IoT attack dataset with Rank, Version number, Local repair, Hello message flooding, and Puppet DoS attacks. This work runs the Cooja simulator on the Contiki operating system to generate such a synthetic dataset. The legitimate and attack smart devices in the simulated IoT environment run with the Contiki platform and generate the traffic patterns for the smart grid AMI network. The synthetic RPL attack detection dataset consists of 13 attributes and 1 target attribute. The RPL features and their value ranges in the synthetic dataset are listed in Table 1.

<table>
<thead>
<tr>
<th>No</th>
<th>Feature</th>
<th>Normal_Range</th>
<th>Modified Range during the attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No: Packet sequence number.</td>
<td>1-12500</td>
<td>1-12500</td>
</tr>
</tbody>
</table>

Table 1: Features of SyntheticRPL Attack Detection Dataset
<table>
<thead>
<tr>
<th></th>
<th>Time: Simulation time</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Source: Source Node IP</td>
<td>1-30</td>
<td>1-30</td>
</tr>
<tr>
<td>4</td>
<td>Destination: Destination Node IP</td>
<td>5-15</td>
<td>5-15</td>
</tr>
<tr>
<td>5</td>
<td>Length: Packet Length</td>
<td>RPL_DIS - 64 Bytes, RPL_DIO - 100 Bytes, 5RPL.DAO - 76 Bytes, ACK - 5Bytes; Data size is varied as per the measured parameter in HAN</td>
<td>RPL_DIS - 64 Bytes, RPL_DIO - 100 Bytes, RPL.DAO - 76 Bytes, ACK - 5Bytes. Data size is varied as per the measured parameter in HAN</td>
</tr>
<tr>
<td>6</td>
<td>Version: DODAG Version</td>
<td>240</td>
<td>&gt;Varied</td>
</tr>
<tr>
<td>7</td>
<td>Rank: Rank Value</td>
<td>255</td>
<td>&gt;256</td>
</tr>
<tr>
<td>8</td>
<td>Packet: Type of packet</td>
<td>RPL_DIS, RPL_DIO, RPL.DAO, DATA, ACK</td>
<td>RPL_DIS, RPL_DIO, RPL.DAO, DATA, ACK</td>
</tr>
<tr>
<td>9</td>
<td>SR: Sending_Rate</td>
<td>10 packets/sec</td>
<td>10 packets/sec</td>
</tr>
<tr>
<td>10</td>
<td>MOP: Mode of Operation</td>
<td>2 Storing Mode</td>
<td>2 Storing Mode</td>
</tr>
<tr>
<td>11</td>
<td>DSTN: Destination Advertisement Trigger Sequence Number</td>
<td>240</td>
<td>≠240</td>
</tr>
<tr>
<td>12</td>
<td>CP: Control Packets</td>
<td>2000 packets during the time</td>
<td>&gt;&gt;2000 packets during the time</td>
</tr>
<tr>
<td>13</td>
<td>ID: RPLInstance ID</td>
<td>1-30</td>
<td>1-30</td>
</tr>
<tr>
<td>14</td>
<td>Label: Benign/Malicious</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The OFL-SRPL utilizes the synthetic dataset to implement the proposed method with the initialization of the data preprocessing. Synthetic data preprocessing involves data cleaning and
normalizing the attribute or feature values, converting the categorical variables into numerical values by the filtration of the relevant features. A few of the features in the constructed dataset, such as ‘No’, ‘Version’, and ‘CP’, comprise a wide range of values, which are scaled into a normalized range of values from their wider value range. To represent the generated dataset with the potential features, the popular Principal Component Analysis (PCA) method [26] enforced the dimensionality reduction of the dataset.

4.2. Optimal Selection of Ensemble Deep Learning Model

The HAN connects the smart appliances and their data in the AMI networks to seamlessly perform smart metering processes. The data generated from the HAN resembles time series data in the network layer because every feature indexes a data point in a packet sequence, number, order, and such sequence of observations needs to be processed for the traffic classification. To work with the sequential patterns of the traffic data in the synthetically constructed RPL dataset, the OFL-SRPL adopts the sequential learning models with the advantage of learning a sequence of observations for predicting a class label. Thus, the proposed OFL-SRPL approach employs the ensemble of sequential classifiers to overcome the constraints in the traditional attack detection system with the OFL ensemble model. The constraints in the traditional attack classification model involve a single best classifier is likely to increase the variance in class prediction, and adopting different classifiers in ensemble-based FL without the facts of the data contradicts the advantage of multiple local model generation and aggregation in FL. Hence, the proposed OFL-SRPL scheme selects sequential learning models [27], such as RNN, LSTM, and GRU, and executes the different combinations of the ensemble models in a single HAN to generate local models in a resource-constrained manner. The OFL-SRPL aggregates the local models generated from different HANs using a different combination of sequential classifiers and significantly reduces the loss value without increasing resource consumption.

4.2.1. FL Training with Improved Ownership Weight

With the maximum likelihood of data imbalance in the RPL traffic patterns, the OFL-SRPL intends to contemplate the class imbalance with the improved ownership weight during the training of the data in the FL model. In OFL-SRPL, each HAN’s gateway selects any one of the ensemble sequential classifiers from the design of RNN, LSTM, and GRU models for the
traffic patterns in each HAN. The RNN is a type of neural network with loops that helps retain feature values from the past. Especially, the loops used in RNN explore the feature values from other packets and produce an accurate output for a particular node in which the class prediction at time ‘t-1’ affects the decision at the time, ‘t’. As a result, the response of the network to the node depends on the current node as well as the output from its parent as well as children in the DODAG structure of RPL. However, RNN often meets the performance degradation in the class prediction due to the gradient vanishing and exploding problems. In addition, the RNN is suffered from short-term memory, particularly when the data sequence is long. Thus, enhanced RNN models, such as LSTM and GRU, have been increasingly adopted to address these constraints in the RNN. The architecture of LSTM considers the gate mechanism to regulate the flow of information with memory cells and maintain the long-term temporal dependencies in the data. However, the LSTM fails to support the control decision on the storage volume of previous memory. Hence, the GRU has become popular among sequential data processing researchers with the advantage of resetting and updating gates. Thus, the OFL-SRPL designs an ensemble model combining these different sequential classifiers to enhance the class prediction accuracy rather than statistically deciding the best single classifier.

4.2.1. Improved Ownership Weight

In the subsequence of PCA-based feature reduction, the OFL-SRPL initiates the implementation of the FL model with the design of the ensemble sequential classifiers for three stages local model generation, global model generation, and local model updation. While executing the sequential classifiers at any of the three stages in the FL, it contemplates the improved ownership weight for handling class imbalance on the reduced feature set. The normal, Rank, Version number, Local repair, Hello message flooding, and Puppet DoS attack are labeled as 0, 1, 2, 3, 4, and 5 categories in the synthetic dataset. Among different categories, the instances in the classes are imbalanced, impacting the OFL performance. For example, if the sequential classifiers such as RNN, LSTM, and GRU categorize all the traffic in the DoS puppet attack as type 0, the accuracy of the model is reduced. Hence, the proposed OFL-SRPL implements the learning algorithm with an improved ownership weight. The computation of class weight eliminates the necessity of updating the ownership weight at every step by appending only the initial weight based on the volume of the data category. The categories with
different instances are assigned different weights, which are assigned according to the number of instances. Equation (4) computes the class weight for each class.

\[ w_i = \frac{N}{c \times n_i} \]  

(4)

In Equation (4), ‘c’ and ‘N’ refers to the number of categories and traffic samples in the dataset, respectively, \( w_i \) represents the class weight of class ‘i’, and \( n_i \) represents the amount of traffic of class ‘i’. A class with the highest weight denotes more emphasis on the class. Without improved ownership weight, few records in a class are modeled as a high-weight class. By adopting the improved ownership weight in the OFL-SRPL, all the sequential classifiers effectually categorize the instances into normal and malicious traffic patterns. Furthermore, the OFL-SRPL shares the local model parameters generated from each HAN in an optimized manner with the help of the PSO algorithm.

4.2.2. Optimized Local Model Sharing using PSO

With the target of alleviating the communication burden in the FL, the OFL-SRPL designs the proposed optimized federated learning with the adoption of the PSO algorithm on multiple HANs regardless of exchanging a large number of weights between the local model and global model. The main concept of OFL is to train local models on a local dataset of HAN and exchange optimal local model parameters based on the loss of sequential learning models between gateway nodes and AMI servers to build a global model optimally. In the FL, the loss value is in a decimal point, taking nearly 16 bytes. The transmission of 16 bytes to a server from several connected HANs for multiple iterations is inappropriate and compromises the advantages of the FL algorithm. Hence, the OFL-SRPL intends to transform the loss value into a weight factor; thus, the gateway devices transmit the optimal parameters of the local model to the AMI server. In the proposed scheme, every HAN gateway sends the weight to the server, and the PSO algorithm identifies the best weight across the multiple local models. Consequently, the AMI server requests the trained local models only from the best weight gateway to build the global model in the FL. The basic FEDAVG and proposed OFL algorithms are presented in Algorithm 1 and Algorithm 2.
Algorithm 1: Conventional FEDAVG

In the PSO algorithm, the components involve the swarm and particles [28], in which a swarm refers to a group of particles, and each particle denotes a possible solution to the problem. Each particle in the solution is set with its position and speed, ‘V’ for the next step. To search for the global optimal value, the particles converse with each other and identify their own particle best (pbest) variable. The gbest value is determined based on \( \max(p_{best}) \). Each particle computes the speed of the particle using the constant parameters representing the inertia weight (a), acceleration constant for the pbest (c1), and acceleration constant for gbest (c2). The values of rand1 and rand2 are in the random value range between 0 and 1.
In the OFL-SRPL scheme, the optimal local model selection for the global model building in the FL is based on the design of Algorithm 2. Algorithm 2 is an enhanced form of Algorithm 1 with the adoption of the cross-entropy measurement and PSO algorithm. In contrast to the conventional FL algorithm, the OFL function AMI_Server_Executes receives only pbest values without receiving the decimal values from the loss function from all the HAN gateway devices on Line 5. Lines 6-8 determine the gateway device with the minimum pbest value among those collected. In lines 10 to 20, the functions of Gateway_Weight Estimation and Gateway_Update estimate the weight factor using cross-entropy and execute any of the selected ensemble sequential classifiers by applying the PSO, respectively. In line 11, ‘N’ is the size of the test set (D), and q(x) is the success of classifier accuracy, i.e., whether the instance x_i is

---

**Algorithm 2: Proposed OFL Algorithm**

//&OFL-Local Model Generation and Sharing &*/

1: function AMI_SERVER_EXECUTES
2: initialize w0, gbest, Global_gbest, gid
3: for each round t = 1, 2, . . . do
4: for each client k in parallel do
5: pbest ← ClientUpdate(k ∈ N, w^g_id_t)
6: if Global_gbest > gbest then
7: Global_gbest ← gbest
8: gid ← k
9: w_{t+1} ← GetBestModel(gid)
10: function GATEWAY_WEIGHT_ESTIMATION(k)
11: Cross Entropy Estimation: − ∑_{i=1}^{N} \frac{1}{N} log_q(x_i)
12: w_k ≈ H(D, q) ∗ 10^1
13: function GATEWAY_UPDATE(k, w^g_id_t)
14: w_k ← GATEWAY_WEIGHT_ESTIMATION(k)
15: initialize V, w, w^{pbest}, a, c1, c2
16: for each client k=1, 2, . . . do
17: V_l ← a * V_l + c1 * rand * (w^{pbest}_l - V_l) + c2 * rand * (w^{gbest}_l - V_l)
18: w_{t+1} ← w_t + V
19: repeat the process for all iterations
20: gbest_k ← max(pbest_k)
21: return gbest_k to server
22: function GET_BEST_MODEL(gid)
23: requests Client(gid) which has gbest value
24: return its corresponding loss value to server
classified correctly or not. The sum is averaged over the size of the dataset. In lines 13–14, Variable ‘V’ is estimated, and the optimal value of w_pbest is shared by the gateway to identify the w_gbest value at the server using the AMI_SERVER_EXECUTES function. This process is carried out for each gateway after all t iterations. Line 18 denotes the addition of Variable ‘V’ and w from the previous round to identify the w used in the current round. Finally, GetBestModel helps the server request the model from the gateway with the best score. It eliminates the necessity of local model sharing from all gateway nodes to the AMI server. Instead, the PSO-based OFL identifies the Global_gbest using PSO by only sending small packets with gbest_k from all the connected gateway devices.

4.3. Ensemble Class-Specific Local and Global Model Generation for FL

The proposed OFL-SRPL approach executes the local and global model with the concept of ensemble modeling. Each sequential classifier model used in OFL has different strengths and weaknesses. The class predictions of every classifier are better than any other in a certain condition. It indicates that the models must perform well in different ways, resulting in different prediction errors. Hence, the OFL-SRPL adopts the ensemble for the local model execution in each HAN gateway and global model generation in the AMI server. In addition, instead of sending all the model weights to the AMI server as the traditional federated learning model, the OFL-SRPL model mitigates the transfer of the collection of weights on the server by utilizing the PSO model. It is because the attackers extract the sensitive data through reverse processing the transmitted model weights in the network. To adaptively implement federated learning, the proposed OFL-SRPL designs the ensemble learning model in three ways: local model generation, global model generation, and local model updation. Initially, it executes each local model that is the HAN gateway with the ensemble modeling of three deep learning models, including RNN, LSTM, and GRU. Secondly, the design of the ensemble learning model in the global model relies on the PSO-based Gbest score of the ensemble model across different HAN gateways. Finally, the OFL designs the ensemble model with performance-based two-learning models for the local model updation in each HAN gateway. Algorithm 2 is executed for different classifiers of HAN gateway devices and optimizes sharing the best local model to the AMI server. The AMI server iteratively executes Algorithm 2 for each HAN gateway separately to select the best ensemble model with a sequential classifier for each HAN gateway among multiple local
models. After identifying the global parameters for each classifier, the AMI server detects two suitable classifiers for each HAN and suggests those classifiers with global parameters to the HAN gateway device. After that, the HAN starts to detect the normal and malicious packets using such suitable classifiers with global best local model parameters based on the class-specific weight model and improves the class prediction accuracy by handling both imbalances and constrained resource issues successfully.
Figure 3: OFL–SRPL Packet Classification
Figure 3 depicts the overall process of the OFL-SRPL methodology. To design the federated setup for the packet classification in the AMI environment, the proposed model focuses on enriching the processes involved in the HAN gateway with multiple local models and the AMI server. Applying the PSO algorithm and ensemble model, the OFL-SRPL optimizes the traditional federated learning in the attack detection model. Let each HAN gateway comprises multiple local models for its HAN gateway devices, executing on the ensemble of different sequential classifiers. To optimally select the ensemble learning model for a particular HAN gateway instead of sending all the local models from each HAN gateway, the proposed model adopts the PSO algorithm and optimizes the global model generation with the combination of different sequential classifiers in the ensemble model iteratively. In subsequence, the OFL-SRPL updates the local models in each HAN gateway based on the iterative selection of an ensemble of two classifiers that are well performed in their data with the knowledge of the global parameters. Thus, the local models accurately distinguish the normal and attack classes in each HAN gateway with its ensemble of sequential classifiers in an iterative manner.

5. Experimental Evaluation

To evaluate the performance of the proposed OFL-SRPL approach, this section compares it with MLP [11], GRU [10], and LSTM [13] models. For experimenting with the federated learning scenario, RNN, GRU, and LSTM models are selected as the proposed deep neural network models. The existing MLP [11], GRU [10], and LSTM [13] models are non-federated learning models trained on a traditional environment setup of centralized training data.

5.1. Experimental Setup

Implementing the proposed and existing models of a secure RPL network for the AMI environment depends on Python programming language experiments. The environment setup is configured with the Intel i3 2.5GHZ CPU and a 16 GB memory server hosted Ubuntu 18.04 LTS operating system. Federated learning is implemented using the Keras API and the deep learning framework.

5.1.1. Dataset Description
An RPL-IoT dataset is simulated from the IoT device communication in the Cooja simulator to implement the proposed approach. The AMI dataset consists of 1 normal and 4 attack scenarios involving Rank, Version, Local Repair, Hello Flooding, and Puppet Attacks. The normal and attack samples are generated with multiple features in the Contiki-ng operating system. To test the secure RPL routing model, three different RPL-IoT datasets have been employed, involving the Smart Grid, Smart Healthcare, and Smart Agriculture datasets in the AMI environment. The learning model utilizes the AMI input data with the reduced features of Version, Rank, DSTN, and CP.

5.1.2. Performance Metrics

To measure the performance of the proposed and comparative secure RPL routing models, the experimental model exploits the True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), F-Score, Accuracy, and Training Time.

**True Positive Rate:** It is the ratio between the number of correctly classified samples in the positive class and the total number of samples in the positive class. It is also termed recall or sensitivity.

\[
TPR = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}}
\]

**True Negative Rate:** It is the ratio between the number of correctly classified samples in the negative class and the total number of samples in the negative class. It is also termed specificity.

\[
TNR = \frac{\text{True Negative}}{\text{True Negative} + \text{False Positive}}
\]

**False Positive Rate:** It is the ratio between the number of incorrectly classified samples in the positive class that actually belongs to the negative class and the total number of samples in the negative class.

\[
FPR = \frac{\text{False Positive}}{\text{False Positive} + \text{True Negative}}
\]

**F-Score:** It is the weighted harmonic mean of the precision and recall of the model.
\[ F - \text{Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \]

**Accuracy**: It is the ratio of correctly classifying positive and negative classes across the total samples.

\[
\text{Accuracy} = \frac{\text{True Positive} + \text{True Negative}}{\text{True Positive} + \text{True Negative} + \text{False Positive} + \text{False Negative}}
\]

Where,

**True Positive (TP)**: Total number of correctly classified samples in a particular target class of AMI recordings.

**True Negative (TN)**: Total number of correctly classified samples in a non-target class of AMI recordings.

**False Positive (FP)**: Total number of incorrectly classified non-target class of AMI samples as the target samples.

**False Negative (FN)**: Total number of the incorrectly classified target class of AMI samples as the non-target samples.

### 5.2. Experimental Results

To validate and compare the proposed and existing approaches, the experimental model conducts the experiments for binary labeling of normal and attack classes and the multi-class labeling of normal, Rank, Version, Local Repair, Hello Flooding, and Puppet Attacks. Also, the performance of the proposed federated learning scenario of OFL–SRPL is compared with the centralized learning scenario of MLP, GRU, and LSTM models. The federated learning with PSO is compared with the federated learning with grid search to exemplify the performance of the PSO-based federated optimization.

#### 5.2.1. Performance of True Positive Rate
Figure 4 illustrates the true positive rate of the proposed OFL–SRPL and the existing LSTM, GRU, and MLP models in different epochs. The OFL-SRPL produces a comparatively higher true positive rate than the centralized model of the LSTM in all the epochs. The higher true positive rate of the OFL-SRPL is 0.884 at 20 epochs, whereas the centralized models of the LSTM and GRU obtain 0.692 and 0.701 only in the same scenario. Adopting the PSO for the best learning model selection enhances the performance of the federated learning model, resulting from optimal convergence and maintaining the true positive rate with minimal fluctuations from early epochs. As a result, the proposed OFL-SRPL approach decreases the variance in class prediction, and yields improved performance on the true positive rate for the normal and multiple attack categories. The execution of GRU individually has the disadvantages of slow convergence and low learning efficiency. Even though LSTM and GRU models provide better performance at 25.76% and 19.6% higher true positive rate or recall than the MLP model at 30 epochs, the individual learning model and the centralized setup tend to perform poorly than the ensemble and federated model associated with the proposed OFL-SRPL model.

5.2.2. Performance of True Negative Rate
Figure 5: Number of Communication Rounds Vs. True Negative Rate

Figure 5 compares the specificity or true negative rate of the proposed OFL-SRPL model with that of the FL-SRPL-Grid search for the binary and multi-class classification problem. FL-SRPL-Grid refers to the proposed federated learning concept with the replacement of grid search for PSO-based optimization. In both the binary and multi-class classification, the performance of the learning model also relies on the result of the true negative rate in addition to accomplishing a higher true positive rate. Compared to the FL-SRPL-Grid, the OFL-SRPL achieves a higher true negative rate within minimal communication rounds. With the assistance of the PSO algorithm and ensemble model, the OFL-SRPL optimizes the traditional federated learning in the attack detection model compared to the grid search. As illustrated in Figure 5, the PSO-based proposed model yields a 0.85 value of true negative rate at 25 communication rounds. However, the comparative FL-SRPL-Grid reaches its maximum true negative rate of 0.824 after completing 35 communication rounds. It is accomplished by the PSO model that restricts the iterations of the local and global model learning through the optimal selection of the classifiers within fewer communication rounds. Also, at the communication rounds of 25, the OFL-SRPL obtains a 7.18% and 9.4% higher true negative rate than the FL-SRPL-Grid model in the binary-class and multi-class scenarios, respectively.

5.2.3. Performance of False Positive Rate
The false-positive rate experimental results of the proposed OFL-SRPL and the comparative analysis of LSTM, GRU, and MLP in the attack detection for the binary class and multi-class are presented in Figure 6. All the existing schemes do not handle class imbalance issues. The unhandled class imbalance issues in the synthetic dataset affect the attack classification accuracy. The OFL-SRPL results in a minimal false positive rate of 0.152 to the comparative models. Even the LSTM and GRU-based attack detection models inherently recognize the attack patterns from the extracted features. The false-positive rate of the OFL-SRPL during binary classification has a negligible difference of 0.017 with the multi-class classification of the proposed model, but the false-positive rate of the GRU and MLP increases to 0.387 and 0.561, respectively, for the multi-class classification problem. The principle behind the obtained results is that the proposed OFL-SRPL learns the multiple attack patterns through the federated learning and use of PSO in the FL model. The categories with different instances are assigned different weights, and the weight is assigned according to the number of records. The PSO and improved ownership weight concepts tend to yield a reduced number of false positives with optimal convergence in fewer epochs.

5.2.4. Performance of F-Score
Figure 7: Models Vs. F-Score

Figure 7 compares the F-score of the proposed model with the comparative models of the LSTM, GRU, and MLP. Among these competing models, the OFL-SRPL is a federated learning-based model, and the rest are centralized models. Even though all the models produce better results in the attack detection applications, knowledge sharing from the trained local models reduces the negative impact on the attack classification and ensures the globally optimized decision. As a result, the OFL-SRPL model obtains 11.86%, 15.05%, and 27.3% higher F-score than the LSTM, GRU, and MLP models, as illustrated in Figure 7. Since individual sequential classifiers may tend to overfit easily, LSTM is sensitive to different random weight initialization. Moreover, the integrated results of the ensemble learning models of RNN, LSTM, and GRU and the optimal selection of the learning model by the PSO leverage the accurate detection of the different types of attack samples in the AMI recordings. Although, the potential advantage of the deep layers in the LSTM and GRU proves its 15.44% and 12.25% better attack detection performance than the MLP model.

5.2.5. Performance of Accuracy
Figure 8 compares the accuracy of the proposed OFL-SRPL model with competing models of FL-SRPL-Grid in a federated setup, LSTM, GRU, and MLP in a centralized setup for attack detection. The experimental result implies that the proposed model accomplishes the highest accuracy of all four comparative methods. The accuracy of the OFL-SRPL model is 89.86% at 20 epochs, which is 18.16% higher than that of the federated setup of the FL-SRPL-Grid at the same number of epochs. The implementation results show that the proposed model has better detection accuracy on multiple attacks. The reason is that the OFL-SRPL employs the ensemble structure of three deep learning models as well as the PSO-based global model training and updation, thereby improving the robustness of the system in the detection of different attack types. Although, the FL-SRPL-Grid outperforms the LSTM, GRU, and MLP by 3.19%, 12.2%, and 21.56% higher accuracy when there are 30 epochs due to the advantage of training the distributed data on the different local models and then updating the global model in the federated setup rather than distinguishing the normal and attack patterns by a centralized training model.

5.2.6. Number of Communication Rounds
Figure 9 depicts the comparison of the OFL-SRPL and FL-SRPL-Grid models in terms of the number of communication rounds to achieve their maximal accuracy in the scenario of binary classification and multi-class classification. To illustrate the potential advantage of the PSO algorithm in federated learning, Figure 9 plots the results obtained from the PSO-based attack detection model of OFL-SRL and the Grid search-based attack detection model of FL-SRPL model. The proposed OFL-SRPL outperforms the comparative FL-SRPL-Grid during the classification of normal and intrusions and the normal and multiple attack categories. In particular, the OFL-SRPL accomplishes 89.99% and 89.86% accuracy during the communication rounds of 18 and 25 binary and multi-class classification. In the same scenario, the FL-SRPL obtains 82.56% and 82.45% accuracy during communication rounds 29 and 38, respectively. It is accomplished by transferring the optimal local models to the global model in the federated learning process through the PSO method instead of aggregating the weights of all the local models. Moreover, the loss value is nearly 16 bytes. The transmission of 16 bytes frequently for local model sharing from several connected HANs for multiple iterations is not inappropriate and may lead to packet loss. It mitigates the proposed system to utilize the advantages of FL entirely. The conversion of loss value into weight factor and utilization of the PSO model helps to improve the efficiency and accuracy of the proposed work.

6. Conclusion
This work presented OFL-SRPL on RPL for the AMI network to model attack detection. The proposed OFL-SRPL utilized a metaheuristic optimization algorithm to select the best local model to build the global model, significantly reducing the data transmission size between the multiple local models to the server. Moreover, OFL-SRPL has iteratively designed the federated learning model with the adaptive ensemble model in three stages: local model generation, global model construction, and local model updation. By applying the PSO-based metaheuristic optimization, the OFL-SRPL has optimized the aggregation process of the global model from the knowledge acquired from different combinations of ensemble sequential classifiers in each HAN gateway. Furthermore, it handled the class imbalance constraint in the AMI dataset by modeling the ensemble classifiers with the improved ownership weight. The results illustrated that the OFL-SRPL outperforms the existing centralized models of the individual deep learning models such as the RNN, LSTM, and GRU. Also, the proposed model obtained 7.41% higher accuracy within comparatively minimal communication rounds than the federated learning model of the FL-SRPL-Grid method.

**Declarations**

- **Funding (information that explains whether and by whom the research was supported)**
  This work was supported by all the authors and there is no funding granted nor required for the preparation of this work.

- **Conflicts of interest/Competing interests (include appropriate disclosures)**
  The authors would like to declare that the manuscript titled “Optimized Federated Learning with Ensemble of Sequential Models for Detecting RPL Routing Attacks for AMI Networks” is submitted for your consideration for publication in the journal of Wireless Personal Communications. We confirm that the work is original and plagiarism free. The manuscript has been approved for submission and has never been published or under consideration for publication elsewhere. To the best of our knowledge, no conflict of interest exists. We hope that the significant contributions of the manuscript in optimized federated learning match the scope of the journal.

- **Availability of data and material (data transparency)**
  The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.
• **Code availability (software application or custom code)**
  The code used for this manuscript can’t be provided at this stage as succession of this work is going on and will be used for publication of another manuscript.

**References**


[18] Qolomany, Basheer, Kashif Ahmad, Ala Al-Fuqaha, and Junaid Qadir, “Particle swarm optimized federated learning for industrial IoT and smart city services”, In GLOBECOM IEEE Global Communications Conference, pp.1-6, 2020.
Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- AuthorsProfile.pdf