Deep Learning-based Malicious Energy Attack Detection in Sustainable IoT Network

1st Xinyu Zhang
The Department of Computer Science,
The Unversity of Alabama,
Tuscaloosa, AL 35487 USA
xzhang205@crimson.ua.edu

2nd Long Li
The Department of Computer Science,
The Unversity of Alabama,
Tuscaloosa, AL 35487 USA
lli90@crimson.ua.edu

3rd Lina Pu
The Department of Computer Science,
The Unversity of Alabama,
Tuscaloosa, AL 35487 USA
lina.pu@crimson.ua.edu

4th Jing Yang
The Department of Electrical and Computer Engineering
Mississippi State University
Starkville, MS 39762 USA
jy599@msstate.edu

5th Zichen Wang
School of Electronics & Information Engineering
TianGong University
Tianjin, 300387 China
wzc8090@163.com

6th Rong Fu
The Department of Electrical and Computer Engineering
The Unversity of Alabama
Tuscaloosa, AL 35487 USA
rfu7@crimson.ua.edu

7th Zhipeng Jiang
The Department of Mechanical & Industrial Engineering
New Jersey Institute of Technology
Newark, NJ 07102 USA
zj28@njit.edu

***Abstract*—Through the use of renewable energy, sustainable Internet of Things (IoT) network can significantly enhance its sustainability and scalability. However, it faces a unique security challenge known as malicious energy attack (MEA), which compromises information security by selectively charging nodes to manipulate the routing path in the network. To efficiently counter MEA, we introduce a two-stage deep learning framework to accurately detect the presence of MEA. It is composed of a stacked residual network (SR-Net) for classification and a stacked LSTM network (SL-Net) for prediction. This model is capable of determining whether an IoT network is under MEA attacks and identifying the affected nodes. Our experimental results verify the efficacy of our proposed model, with the SR-Net demonstrating an average binary cross entropy of less than 0.0590, and the SL-Net showcasing an average mean-square error of approximately 0.0215. These results suggest a high degree of accuracy in detecting MEAs, underscoring the potential of our approach in fortifying the security of sustainable IoT networks.**

***Index Terms*—IoT security, deep learning, malicious energy attack**

I. Introduction

The exponential growth of Internet of Things (IoT) presents substantial sustainability challenges, as traditional power solutions like power grids or batteries are not scalable to accommodate the deployment of a vast number of devices over extensive areas. To fulfill these sustainability needs, energy harvesting emerges as a promising solution [1, 2]. It empowers wireless devices by scavenging energy from the environment, such as solar, RF energy, and biothermal energy, allowing nodes to operate semi-perpetually without battery replacements [3, 4]. In this work, we consider the sustainable IoT network where nodes harvest ambient RF energy. Although the energy harvesting feature can greatly enhance the sustainability and scalability of IoT network [5–7], it arises a unique security challenge known as malicious energy attack (MEA) [8].

In our previous work [9], we verified the effectiveness of the MEA and developed a reinforcement learning based method to enhance the attack performance. The MEA attacker manipulates the energy distribution of Energy Harvesting Nodes (EHNs), thereby controlling network traffic to go through a specific node. A typical process of MEA is presented in Fig. 1. It takes advantage of the energy-aware properties of routing protocols within sustainable IoT networks. An adversarial energy source, the energy attacker, selectively charges specific EHNs. Consequently, these targeted EHNs with extra energy, will become more active than other normal nodes to work as data forwarders or information aggregators. By strategically selecting its victims, the attacker can alter the routing path to divert data traffic through a compromised node. The compromised node is a node in the network that was cracked by the attacker and will passively collect and share information with the attacker without inserting any malicious information into the network. The target of the MEA is to manipulate the routing path to the compromised node as much as possible. Although the attacker doesn't directly profit from the energy attack, it can greatly augment the effectiveness of other attack methods, such as eavesdropping, black hole, wormhole, selective forwarding, and Sybil attack.

MEA is an emerging attack method [9] that the counter-

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

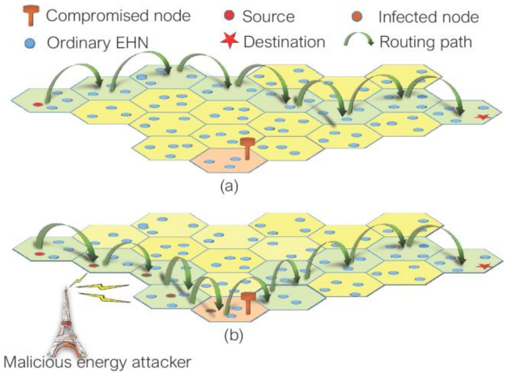


Fig. 1. The Process of MEA [8]

measure has not been sufficiently investigated in the literature. In response to this gap, we propose a two-stage deep learning framework to accurately detect the MEA and identify the infected EHNs. This MEA detection will assist the IoT network in avoiding routing paths through the infected EHNs and further defending against MEA.

The deep learning framework is composed of a stacked residual network (SR-Net) that classifies whether an IoT network is under MEA and a stacked LSTM network (SL-Net) that identifies whether each EHN is infected by energy attack. In this framework, we utilize the residual energy levels (RELs) of all EHNs in the network as the input. The REL is highly relevant to the energy attack and easy to obtain [8]. We divide the time into uniform slots, within which we measure the REL, thereby generating a series of time-related REL values. The MEA detection problem is transformed into a process of extracting and analyzing features from time sequences. Benefiting from its advanced capabilities of nonlinear feature representation and time series sequence prediction, the long short-term memory network (LSTM) adept at learning long-term dependencies, is ideally suited to address our MEA detection problem.

The contributions of this paper can be concluded as follows:

- A two-stage deep learning model is proposed for MEA detection. It can effectively extract the features of REL sequence, judge the state that whether the current network is under MEA and give the prediction results that reveal which nodes are most likely to be attacked.
- We build a MEA dataset by collecting REL information from a network that under energy attack. This dataset can be used to trained the proposed detection model.
- We conduct an evaluation to verify the detection performance of proposed method. .

The rest of the paper is organized as follows: Section II illustrates the IoT network model and the method of generating the dataset. Section III provide more detail about our proposes a two-stage DL detection scheme for the MEA problem, and Section IV presents the evaluation results and analysis. Finally, we give the conclusion of the whole paper in Section V.

II. IoT Network Model and dataset construction

A. IoT Network Model

In this study, we conduct simulations on a large-scale IoT network consisting of 90 Energy Harvesting Nodes (EHNs) deployed in a 700 square meter area, as shown in Fig. 2. The data transmitted by these nodes varies with diverse engineering applications, not confined to the transmission of any particular type of information like underwater communication [10] and solar energy information [11]. Instead, it represents a versatile, non-specific network that operates on RF technology, adaptable to a wide range of scenarios. To simulate a highly dynamic large network, the energy harvest rate of each EHN fluctuates over time.

We assume a node in the original network is been compromised and will share the traffic it forwarded to the attacker. The compromised node has no malicious interaction with the network other than passively sharing information with attacker. The attacker are interested in the traffic originating from a specific source node to a destination node. The source node will continuously send traffic to the destination node every 2 time slots. The blue arrow line illustrates the preferred routing path of the original IoT network without attack. The compromised node we select to verify the effectiveness of the attack is in the lower left corner which has very little opportunity to be selected in the routing path. To assist the MEA, three spy nodes are scattered around the compromised node to monitor the network. As shown in Fig. 2, the spy area for each spy node is marked by a blue dash circle. The spy node will only record the amount of traffic traveling through its spy area and report to the attacker periodically. The attacker will use it to indicate the energy consumption in this spy area. Similar to the compromised node, the spy node does not interact with the network in any way other than passive monitoring. The attacker doesn't know the location of each specific EHN but knows the area of the entire network instead. The attacker will evenly divide the network so that each cell only contains 0-2 EHNs. The energy harvest rate of each cell will be recorded before launching the attack.

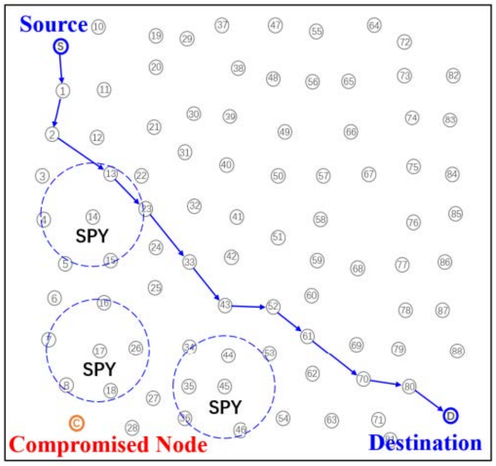


Fig. 2. IoT Network with 90 EHNs [9]

With all the information collected, the attacker can roughly estimate the average energy level of each spy area during the attack. And then train a reinforcement learning model to help select the 5 optimal attack nodes based on the average energy level of all spy areas. After training, the model should accommodate the highly dynamic network environment and select the most appropriate 5 victim nodes in each time slot. By providing extra energy to those 5 victim nodes, the routing path that includes the compromised node is preferred during the attack. To optimize the attack performance, the reinforcement learning-based method we used called PG-IEA that is developed in our previous work [9] to help the attacker intelligently select victim nodes.

To be noticed, the selection of the compromised node is not restricted. The attacker can crack any node as the compromised node. In our simulation, we select a node that most deviated from the main path just to verify the effectiveness of the attack. And the strategy to deploy the spy node is just near the compromised node. With very less information the attacker knows about the network, we believe the energy status near the compromised node is more important.

There is no information interaction with the network during the entire attack process. The spy node is the extra node that is deployed by the attacker. The only interaction with the network is energy, the desired resources of the network, which makes it difficult for the network owner to be aware of.

B. Dataset Construction

To build the dataset, the REL information of the entire network (*1x90*) is recorded at each period. Eventually, the dataset comprises *Nx90* data points, representing the normalized RELs of the network over N consecutive periods. The ground truth is also an *Nx90* binary matrix that indicates the attack behavior for each period by the attacker. In this matrix, value 1 denotes a victim node, while 0 signifies a normal node. For SR-Net, the ground truth can be simplified to an *Nx1* vector, in which 1 represents that the network is under attack in the corresponding period, and 0 indicates no attack.

To train the proposed model, we require datasets for both the attacked network and the normal network. The network owner can collect normal network dataset without attack right after network deployment. Subsequently, the network owner can initiate an attack themselves to collect data from the attacked network. The resulting dataset consists of a total of 40,000 samples, with the training set, validation set, and test set distributed in proportions of 7:2:1, respectively.

III. The Deep Learning Network For MEA Detection

A. MEA Detection Process

The basic process of MEA Detection is depicted in Fig. 3. The input data would be a vector that contains the REL of 90 nodes at each observation period. The output of SR-Net is a binary results in which 1 represent the network is under attack and 0 represent no attack happened. If no MEA detected, the process concludes. Otherwise, input data are further processed through the SL-Net model. A *1x90* binary vector is produced, in which the index of value 1 indicates the corresponding victim node is under attack.

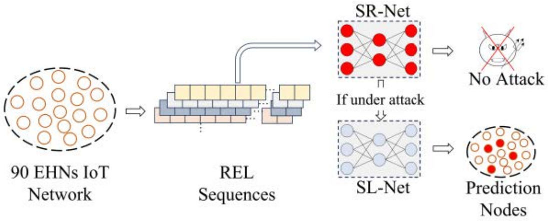


Fig. 3. The Process of MEA Defense

B. Deep Learning Model Design

Fig. 4 depicts the detailed structure of the MEA detection deep learning network, which comprises two sub-networks: an SR-Net that classifies whether an IoT network is under MEA, and an SL-Net that identifies the specific victim nodes.

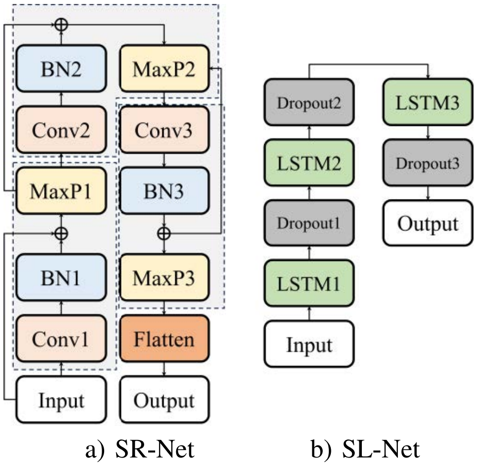


Fig. 4. Deep Learning-based MEA Detection Model

The parameters of each layer in SR-Net are shown in TABLE I. The core component of SR-Net is the residual connection, a powerful skip link method widely recognized for addressing the challenges of gradient dissipation and explosion that occur with increasing network depth [12, 13]. The batch normalization (BN) layer and Max Pooling (MaxP) layer are also included to facilitate easier convergence during training. SR-Net is structured with three blocks using a Pooling-Conv-BN configuration and a flatten layer before the output layer. The convolution layer utilized here is one dimension, meaning that the kernel size height is fixed at 1. The kernel number in TABLE I only reflects width. The 'same' padding strategy is applied to all convolution layers.

As outlined in the prior discussion Section II, following the selection of a compromised node, an attacker typically chooses just one spy node within a very shortly time. For efficiency and convenience, the location of the spy node is generally not too distant from the compromised node, which narrows down

TABLE I
LAYER PARAMETERS OF SR-NET

Layer name	Kernal and Filter	Strides	Padding
Input	*	*	*
Conv1	Kernal = 1 * 3 and Filter = 8	1	same
BN1	*	*	*
MaxP1	Kernal = 1 * 2	2	*
Conv2	Kernal = 1 * 3 and Filter = 16	1	same
BN2	*	*	*
MaxP2	Kernal = 1 * 2	2	*
Conv3	Kernal = 1 * 3 and Filter = 32	1	same
BN3	*	*	*
MaxP3	Kernal = 1 * 2	2	*
Flatten	*	*	*
Output	Dense = 1	*	*

the potential choices for spy nodes. Consequently, variations in energy data collected over a certain period are primarily manifested as increased energy level or high energy level in certain specific nodes. A convolutional neural network can be effectively employed to compress and extract these distinctive changes in energy patterns, subsequently feeding this refined feature to the final classification layer for analysis and classification.

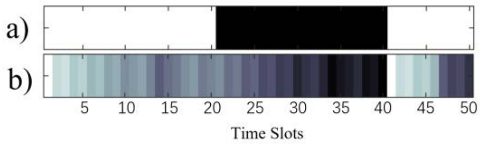
The parameters of each layer in SL-Net are shown in TABLE II. SL-Net is primarily composed of LSTM layers and dropout layers. Compared with ordinary recurrent neural network (RNN), LSTM can better preserve important information from input sequences and solve the issues of gradient disappearance and explosion during training with long sequences [14]. To address potential overfitting, dropout layers are included after each LSTM layer. Additionally, only the first two ‘Return Sequence’ states of the LSTM layers are set to ‘TRUE’.

TABLE II
LAYER PARAMETERS OF SL-NET

Layer name	Units	Dropout Rate	Return Sequence
Input	*	*	*
LSTM1	128	*	TRUE
Dropout1	*	0.3	*
LSTM2	100	*	TRUE
Dropout2	*	0.3	*
LSTM3	90	*	FALSE
Dropout3	*	0.3	*
Output	Dense = 90	*	*

Based on the operational traits of MEA in Section I, it’s observed that it persistently supplies energy to the targeted node, leading to a steady increase in energy over a brief time slot (if a node already occupies the highest energy position, charging will be made to sustain its energy level near this peak position.). Utilizing this distinct behavior, the LSTM layer is designed to monitor and capture the energy fluctuations from time series data within a specified slot, allowing the detection system to recognize and retain the unique pattern, enabling it to identify and confirm which nodes are under attack.

The Fig. 5 present the energy fluctuation of a victim node. We randomly select a victim node from the dataset to monitor its energy fluctuations across 50 time slots. The Fig. 5.(a) indicate the attack pattern dedicated for this node, where white represent attack and black represent no attack. The Fig. 5.(b) shows the energy level fluctuation over 50 slots of this victim node, where the darker the color, the lower the energy level.



a) Attack mode diagram b) Energy change diagram

Fig. 5. Energy Fluctuation of Victim Node Under Attack

As shown, this node is subject to continuous under attack throughout the two periods (slot 0 $\sim$ slot 20 and slot 40 $\sim$ slot 50, which are marked by white), and one period experiences no attack (slot 21 $\sim$ slot 39, which is marked by black). In Fig. 5.(b), darker color slot indicate a decrease trend. The figures clearly show that the energy level of node is predominantly in a high level when it is under attack. In the contrast, the node maintain or stay consistently decrease to the lower energy level when it is not under-attack. By comparing Fig. 5.(a) and Fig. 5.(b), we can observe a strong correlation between these energy trends and the attack status of the node. It’s important to note that the energy level of an individual node is determined by its intrinsic characteristics named harvesting rate. Hence, the criterion for identifying whether a node is under-attack is based on the trend of energy change within a specific time slot.

C. *Training Parameters Setting*

In SR-Net, the activation function used after each layer is Gaussian Error Linear Units (GELU). The learning rate, batch size, and number of epochs are set to 0.001, 8, and 10000, respectively. Considering that the output of SR-Net is binary, the binary cross entropy (BCE) is employed as the loss function.

Regarding SL-Net, the activation function after each LSTM layer is rectified linear unit (ReLU), while sigmoid is used between the last LSTM layer and the Dense layer. The learning rate, batch size, and epochs are configured as 0.0001, 4, and 10000, respectively. Similar to SR-Net, the loss function in SL-Net is BCE.

Both models were developed using Keras 2.11 with Tensorflow-gpu 2.5. The model is trained on a workstation with an Nvidia RTX A6000 GPU.

IV. EXPERIMENTS AND RESULTS

In our evaluation, we utilized the 90 EHNs IoT network introduced in Section II. In this section, we evaluate the detection accuracy of the proposed two-stage detection model in different metrics. The experiment encompassed a total of 4000 test samples for evaluation. The results illustrate the proposed model achieves a high degree of accuracy in detecting MEA.

A. Evaluation Metrics

Due to the differences in the tasks performed by the two models, we employed different evaluation metrics to present the results. These metrics are as follows:

1) Binary cross entropy (BCE): In this study, we use BCE to evaluate the accuracy of SR-Net. BCE is widely used to assess the accuracy of the binary classification model. It can describe the difference between the prediction value and the ground truth label. The lower the BCE, the closer the prediction is to the ground truth. The equation of BCE is shown bellow.

$$Y = -\frac{1}{N}\sum_{1}^{N} y_i * \log\left(p\left(y_i\right)\right) + \left(1 - y_i\right) * \log\left(1 - p(y_i)\right) \tag{1}$$

The $Y$and N represent metrics and the number of samples, respectively. The y_i denotes the label types (it is either 0 or 1 in binary classification), and $p\left(y_i\right)$ is the probability that the output belongs to the label y_i.

2) Mean-square error (MSE): For SL-Net evaluation, the MSE is used to describe the accuracy performance. MSE is commonly used for regression problem to evaluate how well the predicted value aligns with the ground truth. The equation of MSE is as follows:

$$MSE = \frac{1}{N}\sum_{1}^{N}\left(y_i - \widehat{y_i}\right)^2 \tag{2}$$

In this equation, y_i and $\widehat{y_i}$ represents the ground-truth and predicted value, respectively.

B. Evaluation Result

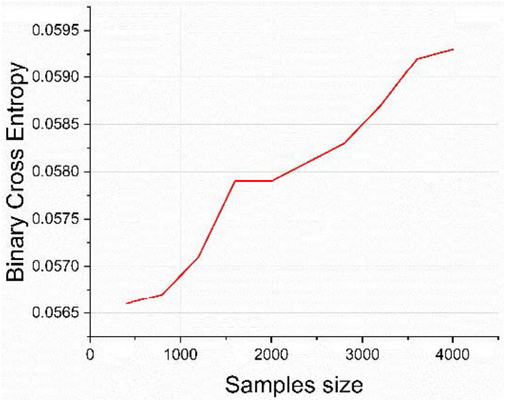


Fig. 6. Numerical Analysis of SR-Net

We evaluate the accuracy against different samples size of both SR-Net and SL-Net, and the result for SR-Net and SL-Net are presented in Fig. 6 and Fig. 7, respectively.

From Fig. 6, it can be observed that the binary cross entropy of SR-Net slightly increases as the sample size expands. This is attributed to the increasing diversity of the test samples with a larger size. However, the overall average BCE remains below 0.0595, indicating that nearly 94% of the test samples were correctly classified. A similar trend is observed for SL-Net, as shown in Fig. 7, where the maximum mean squared error is below 0.0215, indicating that 98% of the EHNs can be accurately predicted as either under attack or not. These results demonstrate that both SR-Net and SL-Net achieve a high level of accuracy in detecting victim nodes in MEA.

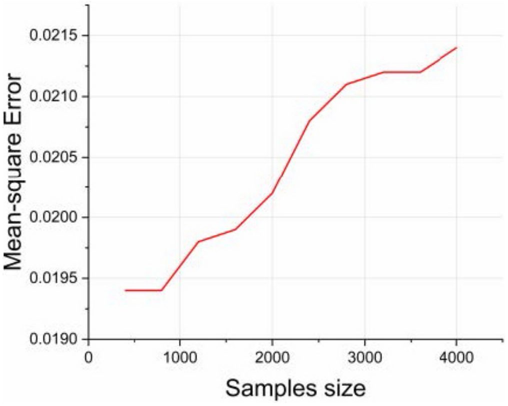
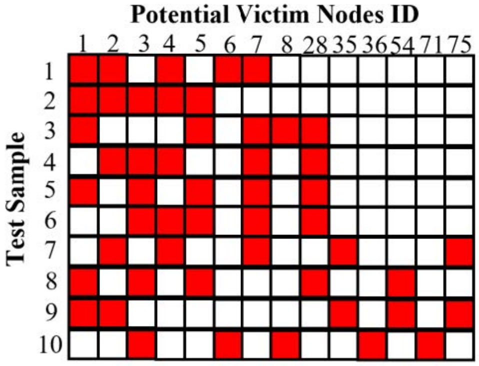


Fig. 7. Numerical Analysis of SL-Net

To provide further insights into the detection performance of the proposed model, the detection results from 10 randomly selected tests are presented in Fig. 8 and Fig. 9. In Fig. 8, the ground truth distribution of 10 samples is depicted, with victim nodes represented by the color red. Fig. 9 shows the prediction results on samples corresponding to Fig. 8, where blue blocks represent the true detected victim nodes and yellow block means falsely detected victim node. Although there were a few instances of misjudgment and incorrect predictions, the global prediction results for the 10 samples demonstrate a relatively high accuracy.



Potential Victim Nodes ID

Test Sample	1	2	3	4	5	6	7	8	28	35	36	54	71	75
1	🟥	🟥	⬜	🟥	⬜	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜
2	🟥	🟥	🟥	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜
3	🟥	⬜	⬜	⬜	🟥	⬜	🟥	🟥	🟥	⬜	⬜	⬜	⬜	⬜
4	⬜	🟥	🟥	🟥	⬜	⬜	🟥	⬜	🟥	⬜	⬜	⬜	⬜	⬜
5	🟥	⬜	🟥	⬜	🟥	⬜	🟥	⬜	🟥	⬜	⬜	⬜	⬜	⬜
6	⬜	⬜	🟥	🟥	🟥	⬜	🟥	⬜	🟥	⬜	⬜	⬜	⬜	⬜
7	⬜	🟥	⬜	🟥	⬜	⬜	🟥	⬜	⬜	🟥	⬜	⬜	⬜	🟥
8	🟥	⬜	🟥	⬜	🟥	⬜	⬜	⬜	🟥	⬜	⬜	🟥	⬜	⬜
9	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟥	⬜	🟥	⬜	🟥
10	⬜	⬜	🟥	⬜	⬜	🟥	⬜	🟥	⬜	⬜	🟥	⬜	🟥	⬜

Fig. 8. The MEA example of ground-truth

V. Conclusion

In conclusion, this two-stage deep learning model proposed in this paper demonstrates a high degree of accuracy in detecting the victim nodes in MEA, underscoring the potential of our approach in fortifying the security of sustainable IoT networks. Furthermore, the proposed model also offers a new

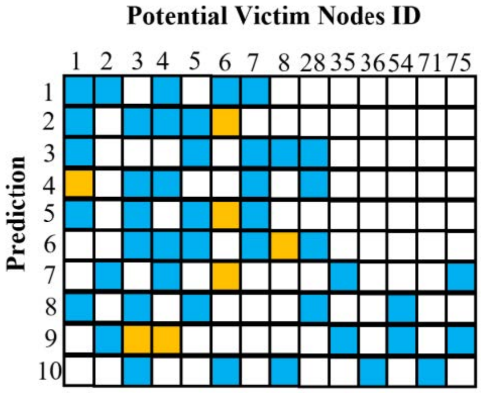


Fig. 9. The MEA example of final detection

direction for MEA detection strategy to preserve the security of sustainable IoT networks.

However, While the effectiveness of two-stage detection method SR-Net and SL-Net contrary to MEA network attack is commendable, the robustness and resistance under external or internal threats need additional empirical validation in future studies. In the future, our group will continuously improve the proposed model and deploy it into a network to evaluate the real-time performance in a more comprehensive experiment.

Acknowledgment

This work is supported by the US National Science Foundation under Grant No. 2051356, No. 2122167, and No. 2122159.

References

[1] F. Akhtar and M. H. Rehmani, "Energy harvesting for self-sustainable wireless body area networks," *IT Professional*, vol. 19, pp. 32–40, 2017.

[2] T. Wu, F. Wu, J.-M. Redouté, and M. R. Yuce, "An autonomous wireless body area network implementation towards iot connected healthcare applications," *IEEE Access*, vol. 5, pp. 11 413–11 422, 2017.

[3] D. In Kim, "Keynote talk #2: Wireless-powered communication networks: Architectures, protocols, and applications," in *2016 International Conference on Advanced Technologies for Communications (ATC)*, 2016, pp. xxxiii–xxxiii.

[4] Q. Liu, K. S. Yildirim, P. Pawełczak, and M. Warnier, "Safe and secure wireless power transfer networks: challenges and opportunities in rf-based systems," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 74–79, 2016.

[5] G. Papadopoulos, "Challenges in the design and implementation of wireless sensor networks: A holistic approach-development and planning tools, middleware, power efficiency, interoperability," in *2015 4th Mediterranean Conference on Embedded Computing (MECO)*, 2015, pp. 1–3.

[6] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Security in energy harvesting networks: A survey of current solutions and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2658–2693, 2020.

[7] Z. Wang, Z. Liu, L. Liu, C. Fang, M. Li, and E. Sun, "Joint optimization design for wireless sensor and actuator networks with energy harvesting," in *2021 7th International Conference on Computer and Communications (ICCC)*, 2021, pp. 272–276.

[8] L. Li, Y. Luo, J. Yang, and L. Pu, "Reinforcement learning enabled intelligent energy attack in green iot networks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 644–658, 2022.

[9] L. Li, Y. Luo, and L. Pu, "Q-learning enabled intelligent energy attack in sustainable wireless communication networks," in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6.

[10] S. Vignesh, R. Sukumaran, T. Subash Ponraj, T. Manikandan, and M. Saravanan, "Analysis on energy harvesting techniques for underwater wireless sensor networks," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2021, pp. 153–156.

[11] M. Hamza, M. U. Rehman, A. Riaz, Z. Maqsood, and W. T. Khan, "Hybrid dual band radio frequency and solar energy harvesting system for making battery-less sensing nodes," in *2021 IEEE Radio and Wireless Symposium (RWS)*, 2021, pp. 116–118.

[12] X. Zhang, Z. Wang, R. Fu, D. Wang, X. Chen, X. Guo, and H. Wang, "V-shaped dense denoising convolutional neural network for electrical impedance tomography," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–14, 2022.

[13] Z. Wang, X. Zhang, R. Fu, D. Wang, X. Chen, and H. Wang, "Electrical impedance tomography image reconstruction with attention-based deep convolutional neural network," *IEEE Transactions on Instrumentation and Measurement*, vol. 72, pp. 1–18, 2023.

[14] H.-D. Do, D.-E. Kim, M. B. Lam, and W.-Y. Chung, "Self-powered food assessment system using lstm network and 915 mhz rf energy harvesting," *IEEE Access*, vol. 9, pp. 97 444–97 456, 2021.