Enhanced Cyber-Physical Security in Internet of Things Through Energy Auditing

Fangyu Li, Yang Shi, *Graduate Student Member, IEEE*, Aditya Shinde, Jin Ye, *Senior Member, IEEE*, and Wenzhan Song, *Senior Member, IEEE*

***Abstract*—Internet of Things (IoT) are vulnerable to both cyber and physical attacks. Therefore, a cyber-physical security system against different kinds of attacks is in high demand. Traditionally, attacks are detected via monitoring system logs. However, the system logs, such as network statistics and file access records, can be forged. Furthermore, existing solutions mainly target cyber attacks. This paper proposes the first energy auditing and analytics-based IoT monitoring mechanism. To our best knowledge, this is the first attempt to detect and identify IoT cyber and physical attacks based on energy auditing. Using the energy meter readings, we develop a dual deep learning (DL) model system, which adaptively learns the system behaviors in a normal condition. Unlike the previous single DL models for energy disaggregation, we propose a disaggregation-aggregation architecture. The innovative design makes it possible to detect both cyber and physical attacks. The disaggregation model analyzes the energy consumptions of system subcomponents, e.g., CPU, network, disk, etc., to identify cyber attacks, while the aggregation model detects the physical attacks by characterizing the difference between the measured power consumption and prediction results. Using energy consumption data only, the proposed system identifies both cyber and physical attacks. The system and algorithm designs are described in detail. In the hardware simulation experiments, the proposed system exhibits promising performances.**

***Index Terms*—Cyber and physical attack detection, deep learning (DL), energy audit, Internet of Things (IoT).**

I. Introduction

INTERNET of Things (IoT) face complex and complicated security challenges. IoT devices are exposed to both cyber and physical worlds, so attacks and threats may come from both cyber and physical channels [1]. With diversified and numerous applications, IoT systems require the adaptive adjustment ability to solve not only cyber threats but also physical attacks [2], [3]. However, because of the limited processing, storage, and communication resources as well as the unpredictable physical environment, traditional security software solutions are too heavy for IoT devices and often cannot detect physical threats [1], [4]. Thus, the IoT security system design is always challenging.

In an IoT system, the perception and application layers have the physical attack vulnerabilities, while the network layer is facing possible cyber attacks [2]. Typically, the IoT system performance data can be used for analyzing the system behavior [5], such as network parameters [6], but those anomaly detection approaches are usually targeting for cyber attacks [7]. When IoT systems carry ubiquitous computing, IoT devices are physically reachable [8], thus physical threats and attacks become possible [9], which should be considered.

However, as system logs are also attack targets and can be forged, IoT security should depend on a more "reliable" system monitoring mechanism. Energy auditing has been investigated in the emerging smart grids [10], but has not been known as a major attack target. In addition, energy auditing is widely available in the IoT devices, for example, Jiang *et al.* [11] embedded wireless power meters in smart appliances to continuously measure the voltage and current. And smartphones [12] as well as energy-aware smart home systems [13] also have energy auditing functions nowadays. Thus, we adopt the energy consumption reading as the source of the proposed security system. In addition, to further improve the data fidelity and secrecy, the data can be obtained from a side-channel energy audit sensor, which is separated from the communication channel of IoT system. Furthermore, the energy auditing channel can be encrypted, if needed [14]. It is a new monitoring mechanism and can be generally applied to most IoT devices and systems. The hypothesis is that cyber or physical attacks leave a trace in the energy profile. If an attack does not affect energy profile at all, it would perhaps be negligible. In a real system implementation, if the energy auditing is not available in the application program interface (API) of the IoT device, a low-cost energy meter can be designed and attached to an IoT device, performing continuous energy auditing and analytics to enhance security.

Because of the complexity and uncertainty, energy analytics has been an active application of the artificial intelligence [15], [16]. Machine learning (ML), especially deep learning (DL), changes the energy analytics from programmatically to intelligently [17], [18]. Thanks to the multilayered architecture, DL learns complex data patterns between inputs and outputs [19]. Assuming the normal system behavior patterns are modeled by DL models, the error between the real energy consumption data and prediction results can be used to detect anomalous events based on statistical analysis [6].

Manuscript received September 12, 2018; revised November 25, 2018 and December 29, 2018; accepted February 11, 2019. Date of publication February 14, 2019; date of current version June 19, 2019. The research was partially supported by NSF-1663709 and Southern Company. *(Corresponding author: Fangyu Li.)*

The authors are with the Center for Cyber-Physical Systems, University of Georgia, Athens, GA 30602 USA (e-mail: fangyu.li@uga.edu; adityas@uga.edu; yang.atrue@uga.edu; jin.ye@uga.edu; wsong@uga.edu).

Digital Object Identifier 10.1109/JIOT.2019.2899492

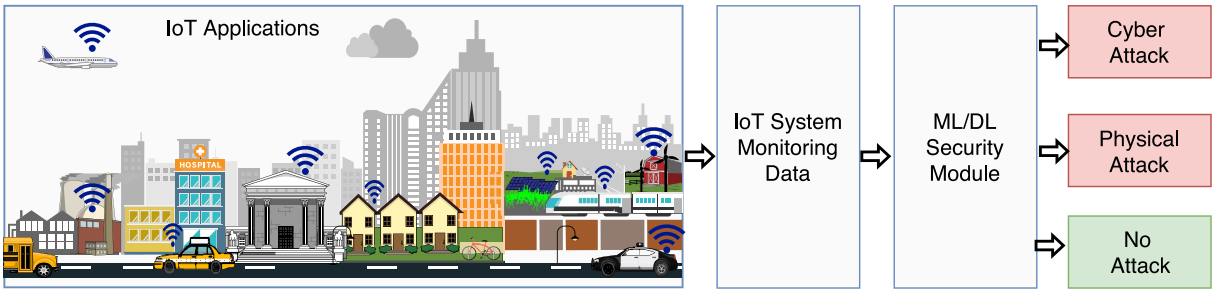

Fig. 1. Big picture of the general learning-based IoT security system.

Fig. 1 shows the big picture of the proposed IoT security mechanism. Based on the monitoring data, ML/DL intelligently learn "normal" behaviors from how IoT components operate and interact with one another, and to detect "abnormal" behaviors. Moreover, learning-based methods can intelligently predict unknown new attacks by learning from existing normal system behaviors.

In this paper, we propose a DL-based IoT energy audit analytics for detecting and identifying not only cyber but also physical attacks. Using the proposed DL models, a system is built to detect anomalies in power consumption, which indicate characteristics of certain types of attacks. The contributions of this paper are as follows.

1) To our best knowledge, this is the first attempt to use energy audit data in the IoT security system to detect both cyber and physical threats and attacks.
2) We propose a dual DL model system. Unlike the previous DL applications, our system has two DL models, the disaggregation model and aggregation model.
3) Our system detects operation anomalies based on only the energy audit readings without other sources. The dual DL models are pretrained based on the performance metrics and energy consumption of an IoT device.
4) Based on the disaggregated system performance metrics and energy consumption prediction, the attacks can not only be detected but also identified.

II. Related Work

The proposed energy audit and analytics-based security mechanism for IoT security is original and has not been attempted before. In this section, we first introduce some typical cyber and physical attacks and discuss their characteristics, then the most related works, power disaggregation and prediction, are presented.

A. Cyber and Physical Attacks

Recently, Abdul-Ghani *et al.* [3] made a comprehensive IoT attack survey, including both cyber and physical attacks. Cyber attacks affect system statistics. For example, unauthorized access which tries to manipulate sensitive data would generate abnormal network traffic [20]. Similarly, if the attackers use a port scan tool to look for weak ports [21], network properties would be abnormal. In addition, virus services may send out sensitive data or run suspicious processes [22], where system performances are related to the specific types viruses. A typical denial of service (DoS) attack sends a huge amount of packages to make the device unreachable [23], where a large amount of received packages are reflected in the network traffic. Physical attacks damage the IoT devices deployed in unattended environments [24]. Generally speaking, IoT functionality is threatened by physical layer damages [25].

B. Power Disaggregation and Prediction

Power disaggregation aims to disaggregate the whole house energy measurement to identify individual appliance's energy consumption, which is always referred to as a nonintrusive load monitoring problem. Kolter and Jaakkola [15] used additived factorial hidden Markov models (HMMs), an extension to HMMs for power disaggregation. Kolter *et al.* [26] proposed to use dictionary learning for energy disaggregation. With the recent DL developments, various neural network architectures, such as recurrent neural networks with convolution layers, auto encoders, and another regression networks, have been used to disaggregate the power consumption to individual devices in a household [27]. However, those algorithms cannot directly apply to IoT devices for disaggregation, because the state transition in IoT software is far more dynamic and fast.

Power prediction has applications in optimizing energy consumption and scheduling in high-performance computing domains. Contreras and Martonosi [28] used a linear model to predict power consumption from hardware counter values. The model has a relatively low complexity, however, it relies on data from hardware counters during operations, which may be difficult to obtain. In addition, Economou *et al.* [29] used the same principles to model power utilization in a server environment. They used utilization metrics of various components, such as CPU, memory, and network to get the total power utilization.

III. Algorithm and System Design

Threat Model: Our system is designed to be sensitive to the abnormal energy pattern changes caused by physical and cyber attacks. In terms of physical attacks, energy changes due to tempering, physical damage, jamming, etc., can be detected and identified. Speaking of cyber attacks, network and software attacks [30] are our targets, including DoS, unauthorized access, virus and worms, Trojan horse, etc. Energy anomaly is the evidence of attacks, furthermore, different energy patterns indicate the attack types.

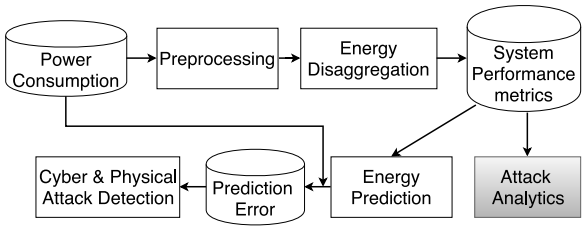

Fig. 2. Workflow of the proposed IoT security system. The block in gray indicates the possible attack analytics when the system performance metrics are measured.

Algorithm 1 Proposed IoT Security System

1: **Input:** Energy audit reading of the IoT device.
2: **Output:** Whether the device is compromised.
3: Preprocessing (Section III-A).
4: Energy disaggregation (Section III-C).
5: *If applicable,* the disaggregated performance metrics are compared with the ground truth to indicate which IoT component is not behaving normal.
6: System performance metrics aggregation for energy prediction (Section III-D).
7: Anomaly detection based on the prediction error (Section III-E).

Algorithm Design: The proposed IoT security analytics system is shown in Fig. 2, which is an end-to-end system. The device power consumption data are organized into a time series. First, a preprocessing step is applied to maintain the waveforms and condition data samples. Next, the energy consumption data are fed into the disaggregation model. The disaggregation model generated the modeled CPU usage, network TX[1] throughput and the disk usage using the input power sequences. (If applicable, these individual performance metrics can be used separately outside the system for finer analytics.) If cyber attacks happen, the disaggregated system subcomponents from energy auditing will differ from the measured system statistics. Because the DL models are trained based on known system behaviors, only the normal system responses will be reflected. Then, the predicted power consumption and the true power consumption will be compared to generate a prediction error. In the end, a time series anomaly detection method is applied to detect the possible attacks. If either cyber or physical attack happens, the abnormal prediction error will be detected. Algorithm 1 and Fig. 2 show the whole end-to-end system operation workflow. To be noted, in the training phase the ground truth of system performance metrics are required, but in the real operations, based on the pretrained models, only the energy audit data are needed.

A. Preprocessing

The power consumption, as well as the performance metrics, are time series data. Because the energy meter could accidentally lose some data samples, a conditioning step to maintain a stable sampling frequency is very important for the further analysis. Typically, an interpolation step is implemented.

[1]In the network chart, TX and RX are the abbreviations of transmit and receive, which may refer to packet or bytes.

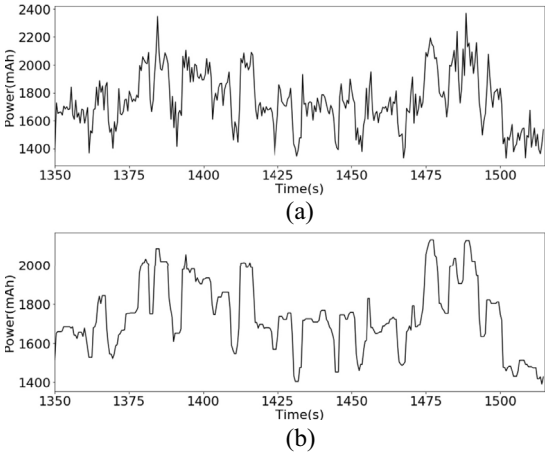

Fig. 3. Preprocessing power data to remove the high frequency noises without damaging the edges. (a) Raw power data. (b) Power data after filtering.

Next, energy meter readings and collected system performance data are susceptible to noise. This is more likely for the energy consumption reading as it is read from an input/output port on the device. Noisy data may have a negative effect on the model training. The edges caused by the sharp rise in CPU and disk usage could be useful features in the models. Hence, the data need to be smoothed whilst still maintaining edges. The median filtering is an edge preserving noise removal technique [31]. Fig. 3 shows the edge-preserving filtering results on power data, which retain the main power consumption patterns. After filtering, the data are normalized to lie between 0 and 1 before feeding into the DL model. The scaler is fit only to the training set. In the later stage, the validation and testing sets are rescaled for real-world interpretation based on the values from the training set.

B. Deep Learning Model Components

1) Convolutional Neural Network: The convolutional neural network (CNN) is a popular DL algorithm which has been successfully applied to time series classification and prediction [17]. Hence, we use CNN-based models to learn power disaggregation and prediction. Formally, extracting a feature map using a 1-D convolution operation is given by

$$a_j^{(l+1)}(\tau) = \sigma\left(b_j^l + \sum_{f=1}^{F^l} K_{jf}^l(\tau) * a_f^l(\tau)\right) \tag{1}$$

where F^l is the number of feature maps in layer l, a_f^l denotes the feature map f in layer l, σ is a nonlinear function, K_{jf}^l is the kernel convolved over feature map f in layer l to create the feature map j in layer $(l+1)$ as $a_j^{(l+1)}$. A designed DL model can consist of more than one convolutional layers, thus it is effective to learn complex feature patterns.

2) Activation Function: In the proposed models, convolution layers with rectified linear unit activations $y = \max(0, b + W * x)$, are used, where x is the input sequence, W is the set of 1-D kernels used for convolution. The final layers of both models predict the value of the time series at a single point.

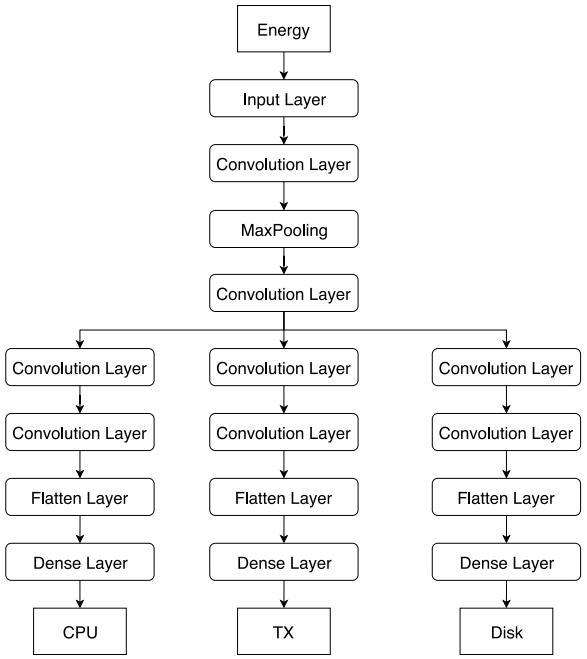

Fig. 4. Architecture of power disaggregation model.

A sigmoid activation function given by $\sigma(x) = (1/1 + e^{-x})$ is used for the last layer.

C. Disaggregation Model

Energy disaggregation is unidentifiable and thus a difficult prediction problem because more than one sources are extracted from a single observation. A typical regression model resulting in a deterministic prediction does not take into account the uncertainty factors. The proposed disaggregation model is a modified seq2point model [17]. The midpoint x_τ of the output is mapped from a neural network F based on the input $Y_{t:t+w-1}$ as $x_\tau = F_p(Y_{t:t+w-1}) + \epsilon$, where w denotes the analysis window length. The loss function describes the difference between the approximate and posterior distribution of the midpoint value as $L = \sum_{t=1}^{T-w+1} \log p(x_\tau | Y_{t:t+w-1}, \theta_p)$, where θ_p are the DL parameters, which are selected by trials.

In this paper, we disaggregate the power consumption to three components, and we will discuss the reason in Section IV-C. Note that, since the CPU, TX, and disk performances are all time series as well as the energy reading, 1-D features are adequate to represent the inherent relations. So we adopt 1-D convolution operators. In addition, as our application is for IoT systems, the computation burden is also in consideration, which means if a model uses smaller memory space and less computation resources but achieves a similar performance, it should be adopted. Simply speaking, to characterize the time series properties, a convolution operator should have certain length, but it should be as short as possible, which benefits the computation cost and improves the system sensitivity. The architecture of the disaggregation model is shown in Fig. 4, where the input layer size is [51 × 1].

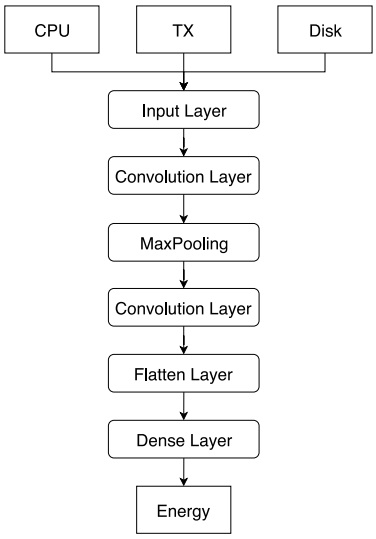

Fig. 5. Architecture of the power prediction model.

D. Aggregation-Based Prediction Model

Unlike the traditional energy consumption study, where the total power consumption is the direct summation of all associated appliances [28], the power consumption and IoT system performance metrics have a nonlinear relationship. We propose to use a DL-based aggregation model to predict the power consumption, whose architecture is shown in Fig. 5, where the input layer size is [21 × 3]. The model uses performance metrics, such as CPU usage, network TX data, and disk usage patterns to predict the power consumption at certain instant. The input is a sequence of high dimensional vectors. Each dimension corresponds to one performance metric. Since energy consumption readings are time series data, 1-D convolutions are performed. The input is passed to the first convolution layer which transforms the vector using 20 kernels. Unlike popular CNN models which use smaller kernels, we use longer kernels in the first layer for capturing features like edges which extend over a longer time. The transformed vectors are passed on to a "max pooling" layer to reduce the vector lengths while still capturing significant features, which is followed by another convolution layer containing ten kernels with sigmoid activations. Once the convolutional operations are performed, the extracted features are forwarded to the last dense layer, which is a regression machine predicting a single number representing the power value for the corresponding input. The loss function is the mean square error (MSE) between the predication result and ground truth for N time steps, expressed as $(1/N) \sum_{t=1}^{N} [y(t) - \tilde{y}(t)]^2$.

E. Anomaly Detection

The anomaly detection for time series data is usually based on statistical analysis. A classic threshold for normal distribution data is 3σ, where σ denotes the standard deviation. We commonly use $\mu \pm 3\sigma$, where μ denotes the mean of time series, to represent a normal data, which means if a data sample is out of this range, it is statistically likely to be an anomaly. In the real-time IoT security system, the μ and σ

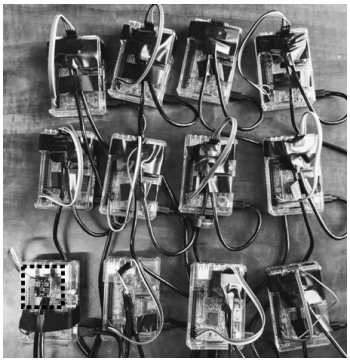

Fig. 6. Energy meter labeled by a dashed frame is implanted to monitor the Raspberry Pi board. The 12 Raspberry Pi form a local network.

vary from time to time, thus, an online estimation is used based on the Welford's algorithm [32]

$$\mu_n = \frac{(n-1)\mu_{n-1} + x_n}{n} = \mu_{n-1} + \frac{x_n - \mu_{n-1}}{n} \tag{2}$$

$$\sigma_n^2 = \frac{M_{2,n}}{n} = \frac{M_{2,n-1} + (x_n - \mu_{n-1})(x_n - \mu_n)}{n} \tag{3}$$

where, $M_{2,n}$ is the second-order moment. Based on the online time series statistics, the system anomaly detection can be implemented in a real time style for the IoT applications. Note, in the online security system, the analysis window length determines the system sensitivity, which means short analysis window would be more sensitive but also more willingly generate false alarms.

IV. Experiments and Evaluations

Simulating a real IoT system operation, we run a program, which samples random data with a fixed interval and carries variety of signal processing, storage, compression, and transmission operations. The system consists of 12 Raspberry Pi wireless boards connected to a router in a mesh network style. An energy meter [33] is implanted to monitor the power consumption of the IoT device, shown in Fig. 6. These nodes simulate the IoT devices running various applications. In this section, we describe how the system components work. And the system performance is evaluated in specially designed experiments with both cyber and physical attacks simulated.

A. Data Collection

The DL models for power disaggregation and prediction are pretrained on real data. In the training phase, the performance metrics and energy audit data are needed. In order to get performance metrics, the statistics are collected using the `/proc` file system on Linux. The energy consumption reading is collected using the API of Raspberry Pi, where the energy meter is attached to. The model can be trained for any device as long as its performance metrics and power consumption can be recorded. For this task, the performance metrics for CPU usage, network usage, and disk usage are monitored and stored while the device is running an application. Streaming the data continuously to the collection database is taxing on the embedded devices. In addition, to minimize the influence on the power consumption, the system performance statistics are sampled every 5 s. As the smart energy meter used in the system can be viewed as a side-channel sensor, the power consumption reading is separately extracted and saved.

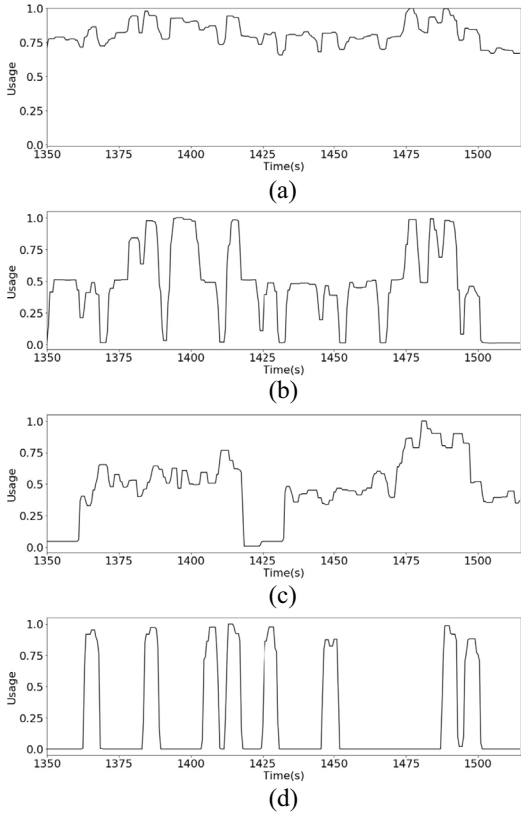

Fig. 7. Collected data after preprocessing. From the top to the bottom are (a) power, (b) CPU, (c) TX, and (d) disk.

B. Data Preprocessing

The system is designed to detect volume attacks, such as network floods, and physical tampering, such as heating the device. None of these attacks cause transient anomalies. As discussed in Section III-A, a median filter acting as an edge preserving filter is used to preprocess the raw data collected from the sensor and the device. Then a normalization step is applied. Fig. 7 shows a data segmentation after both filtering and normalization. Note that the power segment does not lie exactly between 0 and 1, because the normalization is applied on the whole data not only on this segment.

C. Feature Selection

It is intuitive to claim that for a complex system operating complicated applications, more system performance metrics should be collected. However, typically, IoT devices are specially designed for certain purposes, so limited system performance metrics could be adequate for system monitoring and attack detection tasks. From Fig. 7, the CPU usage is highly correlated with the power consumption. In order to quantitatively analyze the importance of each performance metrics in the power consumption, a correlation matrix is computed, shown in Table I. CPU has the highest correlation with

TABLE I
CORRELATIONS AMONG POWER CONSUMPTION AND SYSTEM PERFORMANCE METRICS, CPU, TX, RX, AND DISK

	CPU	TX	RX	Disk	Power
CPU	1	-0.66	0.022	0.34	0.95
TX	-0.66	1	-0.018	-0.26	-0.66
RX	0.022	-0.018	1	0.016	0.04
Disk	0.34	-0.26	0.016	1	0.5
Power	0.95	-0.66	0.04	0.5	1

the power consumption, while the correlation coefficients show that the network RX feature has a very low relation with power consumption. This is likely specific to the application we are running. One possible explanation is that due to greater data transmission than receiving, the power consumption is affected more by the TX and the effect of RX is masked out. Since the correlation is very low, the RX feature is dropped. Thus, in our system, no matter the aggregation or the disaggregation model, only CPU usage, disk usage, and TX throughput are employed for analytics.

D. Model Training

For training both disaggregation and aggregation models, the dataset is split into training, validation, and testing sets based on the fivefold cross-validation rule. The total dataset contains 88 650 samples, out of which 40 000 points are used for training, while 10 000 are used for validation, and the rest are used for testing. The data samples are shuffled after windowing them into smaller subsequences/segments. For training and evaluation, MSE is used as a metric. To determine if the model has fitted the data, the MSE on the validation dataset is tracked. Early stopping is a suitable technique to stop training once a model is fit. If the MSE on the validation set does not decrease over a predetermined set of epochs, it is assumed that the model is fitted and training will be stopped [34]. Early stopping and back propagation are used to train both the disaggregation and prediction models.

E. Disaggregation

In our experiments, only CPU, TX, and disk are considered as system performance metrics. Thus, the energy consumption is disaggregated to these three components. Fig. 8 shows an example of the disaggregation results. Fig. 8(a) is the normalized power consumption plot, while Fig. 8(b)–(d) are the disaggregated CPU, TX, and disk components, respectively. In the training phase, as the model shown in Fig. 4, the loss functions of all the disaggregated components are combined together as the total MSE. So there are some misfits in the individual components, but the total prediction error is acceptable. The inaccurate energy audit reading could cause some problems, and from the results we can observe that certain small energy oscillations are ignored or not reflected in the disaggregation results. In addition, in Fig. 8(d), the predicted TX fails to fit all the detailed system behaviors, but only the general trend is learned. The possible reason can be concluded to the architecture of the DL model, and the hyper parameter selection influences the model performance.

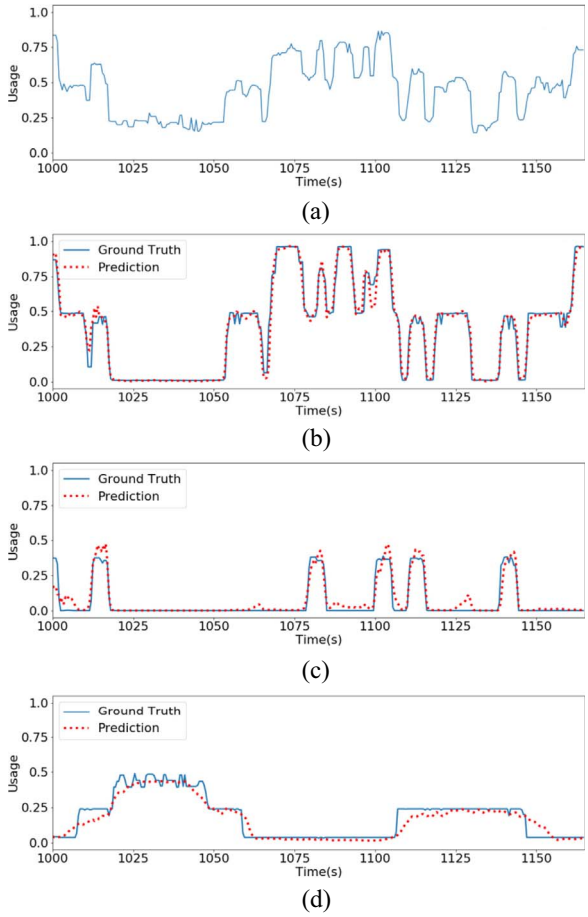

Fig. 8. Disaggregation results. (a) Normalized power consumption with disaggregated. (b) CPU. (c) Disk. (d) TX.

F. Aggregation-Based Energy Prediction

As shown in Fig. 2, the input to the aggregation-based prediction model is a sequence of 3-D vectors. Each dimension corresponds to one of the performance metrics, CPU, TX, and disk. MSE is also adopted in the model training. Fig. 9 shows the prediction results as well as the recorded energy consumption data with different convolution filter sizes. Fig. 9(a) and (b) demonstrate the differences using filter lengths 21 and 101. The MSE of these two models are similar: $\text{MSE}_{21} = 0.032$ and $\text{MSE}_{101} = 0.031$. Because of the random cross-validation, the performances are actually on the same level. Since our system targets at the IoT devices, the filter with 101 samples taking too much memory space is less suitable. (Note that during the training and testing, the computational cost increases nonlinearly with the data size.) Thus, we employ 21 as the convolution filter length.

G. Cyber and Physical Attack Detection

In the previous Figs. 8 and 9, the proposed system performance is shown with normal system behaviors. So both the disaggregation and aggregation models produce prediction results with very small errors. In this section, we simulate the both cyber and physical attacks in the IoT system.

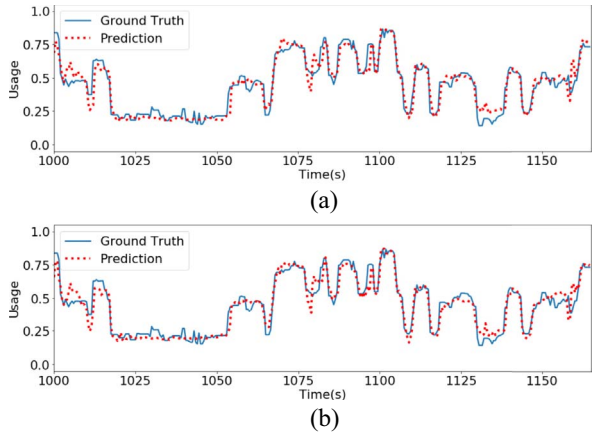

Fig. 9. Power prediction model results with convolution filter length equals (a) 21 and (b) 101.

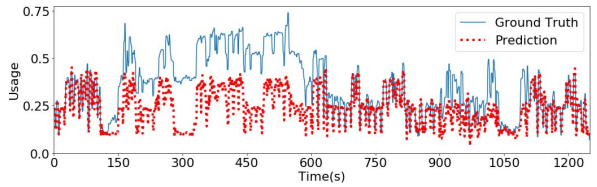

Fig. 10. Cyber and physical attacks are simulated in the experiments. The energy meter data are plotted as ground truth, while the predicted energy consumption is plotted as prediction. The anomalous mismatches indicate the attacks.

First, we simulate a high temperature situation as a physical attack by heating up the Raspberry Pi chip using a heating lamp. Because the easiest physical damage is to directly harm its components [30], heating attack can be viewed as a simple but representative physical attack. If the IoT device is overheated, the system will fail. Second, according to Section II-A, typical cyber attacks affect network statistics. Thus, we simulate a DoS attack on the network throughputs, which generates heavy TX transmission and the associated energy anomalies. Fig. 10 shows the predicted energy consumption and the measured energy consumption. The simulated physical attack is shown between around 150 s and 600 s, while the cyber attack is between around 900 s and 1100 s.

Then, based on differences between actual energy consumptions and prediction results, we apply the anomaly detection to detect and identify the attacks. Fig. 11 shows the prediction error, true attacks and detected anomalies. The anomalies are detected based on the statistical changes of the prediction errors. Both physical and cyber attacks are detected, which proves the effectiveness of the proposed system. Note that the DoS attack is not constant all the time, and there are some breaks during the attack, which can also be identified.

Furthermore, the attack types can be identified. Fig. 12 shows a detailed analysis of the TX statistics. The prediction error is obtained by the comparison between disaggregated TX and measured TX. The detected anomalies have a good correspondence with the true cyber attacks, which indicates this is a network attack reflected on TX. Thus, if the system performance metrics are applicable, not only the cyber attack

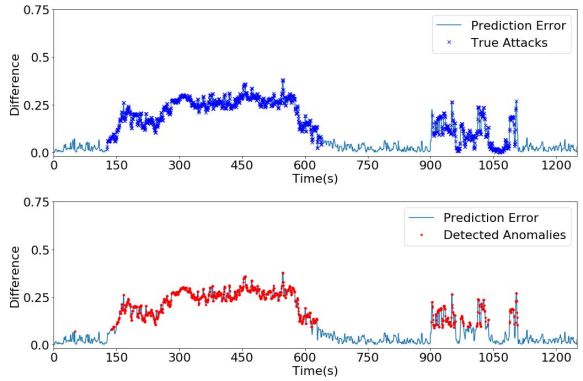

Fig. 11. Power prediction error with true attacks and detected anomalies. It is clear that the proposed system detects both cyber (between 900 s and 1100 s) and physical (between 150 s and 600 s) attacks successfully.

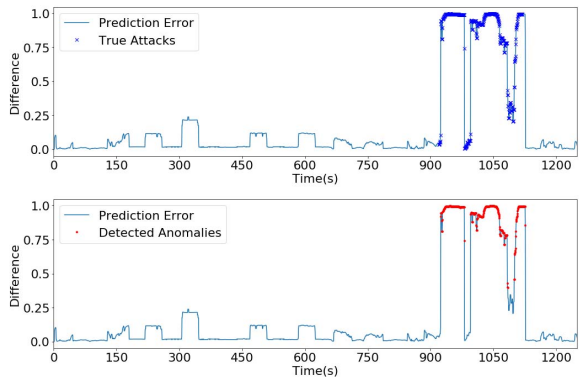

Fig. 12. Cyber attack analysis on the TX statistics.

can be detected, but also the attack types can be identified according to the abnormal system metrics.

V. Conclusion

In this paper, we propose a DL-based IoT security system using energy auditing data. The side-channel energy meter readings enable the proposed system to detect not only cyber but also physical attacks and threats. In addition, the energy auditing data are hard to be compromised compared with other sources. The dual disaggregation and aggregation DL models learn the normal performances of the IoT system, and can also provide detailed analytics of individual system performance metrics, if applicable. The anomaly detection based on the prediction errors tracks both cyber and physical anomalous behaviors. With the proposed approach, IoT system will be better monitored and secured.

References

[1] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani. (2018). *A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security*. [Online]. Available: https://arxiv.org/abs/1807.11023

[2] H. Ning, H. Liu, and L. Yang, "Cyber-entity security in the Internet of Things," *Computer*, vol. 46, no. 4, pp. 46–53, 2013.

[3] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018.

[4] H. Guo, S. Li, B. Li, Y. Ma, and X. Ren, "A new learning automata-based pruning method to train deep neural networks," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3263–3269, Oct. 2018. doi: 10.1109/JIOT.2017.2711426.

[5] F. Li *et al.*, "System statistics learning-based IoT security: Feasibility and suitability," *IEEE Internet Things J.*, to be published. doi: 10.1109/JIOT.2019.2897063.

[6] M. Zou, C. Wang, F. Li, and W. Song, "Network phenotyping for network traffic classification and anomaly detection," in *Proc. IEEE Int. Symp. Technol. Homeland Security (HST)*, Woburn, MA, USA, 2018, pp. 1–6.

[7] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in *Proc. IEEE Int. Workshops Found. Appl. Self* Syst.*, 2016, pp. 242–247.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.

[9] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber-physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 283–299, Jan. 2012.

[10] D. E. Phillips *et al.*, "Supero: A sensor system for unsupervised residential power usage monitoring," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, 2013, pp. 66–75.

[11] X. Jiang, M. Van Ly, J. Taneja, P. Dutta, and D. Culler, "Experiences with a high-fidelity wireless building energy auditing network," in *Proc. 7th ACM Conf. Embedded Netw. Sensor Syst.*, 2009, pp. 113–126.

[12] A. Carroll and G. Heiser, "An analysis of power consumption in a smartphone," in *Proc. USENIX Annu. Techn. Conf.*, vol. 14. Boston, MA, USA, 2010, p. 21.

[13] M. Jahn *et al.*, "The energy aware smart home," in *Proc. IEEE 5th Int. Conf. Future Inf. Technol. (FutureTech)*, 2010, pp. 1–8.

[14] R. Tan, S.-Y. Chiu, H. H. Nguyen, D. K. Y. Yau, and D. Jung, "A joint data compression and encryption approach for wireless energy auditing networks," *ACM Trans. Sensor Netw.*, vol. 13, no. 2, p. 9, 2017.

[15] J. Z. Kolter and T. Jaakkola, "Approximate inference in additive factorial HMMs with application to energy disaggregation," in *Proc. Artif. Intell. Stat.*, 2012, pp. 1472–1482.

[16] L. Ghelardoni, A. Ghio, and D. Anguita, "Energy load forecasting using empirical mode decomposition and support vector regression," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 549–556, Mar. 2013.

[17] C. Zhang, M. Zhong, Z. Wang, N. Goddard, and C. Sutton, "Sequence-to-point learning with neural networks for nonintrusive load monitoring," in *Proc. 32nd AAAI Conf. Artif. Intell. (AAAI)*, New Orleans, LA, USA, Feb. 2018, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8468976

[18] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2923–2960, 4th Quart., 2018.

[19] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, p. 436, 2015.

[20] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: A layered approach for attacks & defenses," in *Proc. Int. Conf. Commun. Technol. (ComTech)*, 2017, pp. 104–110.

[21] *The Five-Layer TCP/IP Model: Description/Attacks/Defense—Computing and Software Wiki*, McMaster Univ., Hamilton, ON, Canada, 2008.

[22] *OWASP Top 10-2013 the Ten Most Critical Web Applications Security Risks*, OWASP Found., Annapolis, MD, USA, 2013.

[23] S. Kumarasamy and A. Gowrishankar. (2012). *An Active Defense Mechanism for TCP SYN Flooding Attacks*. [Online]. Available: https://arxiv.org/abs/1201.2103

[24] M. Abomhara and G. M. Køien, "Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Security*, vol. 4, no. 1, pp. 65–88, 2015.

[25] A. Pandey and R. C. Tripathi, "A survey on wireless sensor networks security," *Int. J. Comput. Appl.*, vol. 3, no. 2, pp. 43–49, 2010.

[26] J. Z. Kolter, S. Batra, and A. Y. Ng, "Energy disaggregation via discriminative sparse coding," in *Proc. Adv. Neural Inf. Process. Syst.*, 2010, pp. 1153–1161.

[27] J. Kelly and W. Knottenbelt, "Neural NILM: Deep neural networks applied to energy disaggregation," in *Proc. 2nd ACM Int. Conf. Embedded Syst. Energy Efficient Built Environ.*, 2015, pp. 55–64.

[28] G. Contreras and M. Martonosi, "Power prediction for Intel XScale® processors using performance monitoring unit events," in *Proc. Low Power Electron. Design (ISLPED)*, 2005, pp. 221–226.

[29] D. Economou, S. Rivoire, C. Kozyrakis, and P. Ranganathan, "Full-system power analysis and modeling for server environments," in *Proc. Workshop MOBS*, 2006, pp. 70–77.

[30] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. I-SMAC (IoT Soc. Mobile Anal. Cloud) (I-SMAC)*, 2017, pp. 32–37.

[31] E. Arias-Castro and D. L. Donoho, "Does median filtering truly preserve edges better than linear filtering?" *Ann. Stat.*, vol. 37, no. 3, pp. 1172–1206, 2009.

[32] D. E. Knuth, *The Art of Computer Programming, 2: Seminumerical Algorithms*. Reading, MA, USA: Addision Wesley, 1998.

[33] A. Hindle *et al.*, "Greenminer: A hardware based mining software repositories software energy consumption framework," in *Proc. 11th ACM Working Conf. Mining Softw. Repositories*, 2014, pp. 12–21.

[34] R. Caruana, S. Lawrence, and C. L. Giles, "Overfitting in neural nets: Backpropagation, conjugate gradient, and early stopping," in *Proc. Adv. Neural Inf. Process. Syst.*, 2001, pp. 402–408.

Fangyu Li received the bachelor's degree in electrical engineering from Beihang University, Beijing, China, the master's degree in electrical engineering from Tsinghua University, Beijing, and the Ph.D. degree in geophysics from the University of Oklahoma, Norman, OK, USA.

He is a Post-Doctoral Fellow with the College of Engineering, University of Georgia, Athens, GA, USA. His current research interests include signal processing, seismic imaging, machine learning, deep learning, distributed computing, Internet of Things, and cyber-physical systems.

Yang Shi (GS'18) received the B.Eng. degree in automation from Central South University, Changsha, China, in 2015, and the M.S. degree in computer science from the University of Georgia, Athens, GA, USA, in 2017, where he is currently pursuing the Ph.D. degree at the Department of Computer Science.

His current research interests include distributed computing, machine learning, and Internet of Things.

Aditya Shinde received the B.E. degree in electronics and telecommunication engineering from the University of Mumbai, Mumbai, India, in 2016. He is currently pursuing the M.S. degree in artificial intelligence at the University of Georgia, Athens, GA, USA.

His current research interests include machine learning and its applications in cyber security and Internet of Things security.

Jin Ye (S'13–M'14–SM'16) received the B.S. and M.S. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2008 and 2011, respectively, and the Ph.D. degree in electrical engineering from McMaster University, Hamilton, ON, Canada, in 2014.

She is currently an Assistant Professor of electrical engineering with the University of Georgia, Athens, GA, USA. Her current research interests include power electronics, electric machines, energy management systems, renewable energy systems, and electrified transportation.

Wenzhan Song (M'05–SM'11) received the B.S. and M.S. degrees from the Nanjing University of Science and Technology, Nanjing, China, in 1997 and 1999, respectively, and the Ph.D. degree in computer science from the Illinois Institute of Technology, Chicago, IL, USA, in 2005.

He is a Chair Professor of electrical and computer engineering with the University of Georgia, Athens, GA, USA. His current research interest includes cyber-physical systems and their applications in energy, environment, and food and health sectors. Dr. Song was a recipient of the NSF CAREER Award in 2010.