Hindawi
Journal of Engineering
Volume 2019, Article ID 4910232, 9 pages
https://doi.org/10.1155/2019/4910232

Research Article

Eliminating Rogue Femtocells for IoT Open Meter System Based on Expert System

Yong Xiao,[1] Bin Qian,[1] Ziwen Cai,[1] Liang Hong,[2] and Sheng Su[2]

[1]*Electric Power Research Institute of China Southern Power Grid, Guangzhou 510080, China*
[2]*College of Electrical & Information Engineering, Changsha University of Science and Technology, Changsha 410004, China*

Correspondence should be addressed to Ziwen Cai; 578119620@qq.com

Received 8 July 2019; Revised 12 September 2019; Accepted 16 October 2019; Published 6 December 2019

Academic Editor: Di He

The Internet of things (IoT), including power meters, water meters, natural gas meters, and meter collectors in an open metering system (OMS), which is dispersed around the user side, relies on wireless virtual private networks (VPNs) to communicate with head end, and thus it is exposed to malicious cyber attacks. The General Packet Radio Service (GPRS), which is vulnerable to rogue femtocells, is widely used for communication among meter collectors and the head end. Because telecommunication fraud related to rogue femtocells is a serious offence, rogue femtocells will be turned on for some time and immediately turned off and moved from here to there to escape from being caught. The signal strength (SS) of rogue femtocells is characterized by abrupt changes. Because meter collectors and lawful femtocells are deployed at the fixed location, there is a notable difference between signal strength profile of lawful and rogue femtocells. Prior knowledge of variation of signal strength is utilized to formulate rules to detect rogue femtocells. An expert system is developed to detect rogue femtocells and prevent meter collectors from attaching to them. Numerical simulation indicates that the proposed approach can detect both stationary and moving rogue femtocells online. Since computation load of the proposed approach is not high, it can be implemented in existing IoT meter collectors with limited computation resource and the proposed approach can harden cyber security of OMS.

1. Introduction

Open metering system (OMS) is an infrastructure integrating natural gas meters, water meters, and electricity meters together with advanced metering infrastructure (AMI) [1]. The natural gas meters and water meters communicate with meter collectors in the same way as electricity meters. The meter collectors collect electricity, water, and gas usage data and upload them to the head end of OMS [2, 3]. IoT electricity/water/gas meters and meter collectors in the OMS are the most visible parts of the smart grid, which plays a key role in communication between customers and the utilities [4]. They send electricity/water/gas consumption to head end, receive tariff data, and update account deposit according to electricity/water/gas charge [1, 5].

In an OMS, while water/gas meters communicate with meter collectors via wireless M-Bus, electricity meters communicate via power line communication (PLC) or RS-485. The meter collectors communicate with the head end of OMS via the General Packet Radio Service (GPRS) [4, 5]. It is required to keep the integrity and privacy of user consumption data when transmitted between dispersed meters and the utilities [6]. Symmetric data encryption/decryption integrated circuits (ICs) are embedded in electricity/water/gas meters to facilitate identity authentication and encrypted communication. Since IoT devices have limited computation resource, light key management protocol for IoT meters is developed in [7, 8]. Because the public shared network is vulnerable to cyber attacks, such as spoofing, eavesdropping, and man-in-the-middle attacks, Internet service providers offer a virtual private network (VPN) for secured communication of OMS [9]. Communication beyond the VPN tunnel remains exposed to malicious adversaries. Because General Packet Radio Service (GPRS) supports only one-way subscriber authentication, it is feasible for a malicious adversary to take control of meter

collectors with rogue femtocells [10]. Once forced to attach to a rogue femtocell, the meter collectors as well as associated meters are in great danger [11]. According to [12], once lots of smart meters are under malicious control, an adversary could cause extensive power outage and dramatic changes in load, which could trigger cascading outage to blackout and result in disorder of society.

Unlike GPRS, both Universal Mobile Telecommunications System (UMTS) and Long-Term Evolution (LTE) support two-way authentication [13]. Hence, it is widely believed that the threat of rogue femtocells can be eliminated once meter collectors are replaced by the ones that communicate with UMTS and LTE mobile network. However, meter collectors are designed to be backward compatible, and many of them can communicate via GPRS, UMTS, and LTE. Malicious adversaries can broadcast an interference signal to disable UMTS and LTE communication. Consequently, meter collectors fall back to communicate by GPRS and can be compromised according to the aforementioned approach. Therefore, threat of rogue femtocells will exist till meter collectors are replaced with the ones that do not support GPRS. Therefore, ways to detect rogue femtocells for IoT meter collectors with limited computational resource are desirable.

Unlike mobile communication terminals such as mobile phones, both meter collectors and lawful femtocells are located in the fixed places. Therefore, signal strength of neighboring lawful femtocells sensed by a meter collector has similar profile, which is notably different from that of a rogue femtocell. The difference in the signal strength (SS) profile of rogue and lawful femtocells is utilized as a radio fingerprint, and an expert system is developed to detect rogue femtocells in this paper.

Our contribution is two-fold. The first consists of presenting similarity of signal strength profile of lawful femtocells and their difference to that of rogue femtocells, which lay the foundation to detect rogue femtocells. The second contribution consists of developing a signal strength profile clustering based on an expert system to detect rogue femtocells.

The remaining part of the paper is organized as follows. The structure of OMS, threat of rogue femtocells, and related work to detect a rogue femtocell are given in Section 2. Differences among SS of lawful and rogue femtocells are investigated in Section 3. A prior knowledge-based expert system is developed in Section 4 to detect rogue femtocells. Numerical simulation of proposed approach is shown in Section 5. Section 6 concludes the paper.

2. Threat of Rogue Femtocells Hijacking

2.1. Structure of OMS. An OMS is composed of electricity/water/gas meters, meter relays, meter collectors, the head end system, and communication system [14] as shown in Figure 1.

The communication system of OMS is composed of 4 parts, i.e., neighborhood area network, wireless access network, data transmission network, and power core network [14]. The function of each part is depicted as follows:

(i) Neighborhood area network: most electricity meters and meter relays communicate with meter collectors via PLC or RS-485 while water/gas meters communicate with the meter collector via wireless M-Bus.

(ii) Wireless access network: meter collectors communicate with the head end of an OMS via public shared networks provided by Internet service providers. Meter collectors are attached to femtocells, and then encrypted meter data are transmitted from meter collectors to the carrier network of the Internet service provider.

(iii) Data transmission network: it is a carrier network provided by the Internet service provider. In order to keep the integrity and privacy of metering data, IPSec VPN is utilized to establish a VPN tunnel. Channel encryption and end-to-end encryption are employed to guarantee security of the data transmitted within VPN tunnel [14].

(iv) Power core network: it is a private network of power utility. Firewall is deployed between the access router device and the head end of OMS to prevent malicious external connection [15].

2.2. Rogue Femtocells Threat. There are usually several femtocells in the neighborhood of a meter collector. The meter collector compares communication parameter of all available femtocells and chooses to attach to the best available femtocell, usually the one with the strongest signal strength. GPRS-Attach initiated by a meter collector has 3 phases as shown in Figure 2.

The first phase is the Radio Resource Control (RRC). A request of a GPRS-Attach initiated by a meter collector will be sent to Serving GPRS Support Node (SGSN) to establish a RRC connection between the meter collector and radio network controller. The second phase is authentication and encryption. The SGSN authenticates the identity of the user and equipment to start ciphered data exchange. In the third phase, SGSN address will be registered with the Home Location Register (HLR), a database containing pertinent data regarding subscribers authorized to use a global system for communications network. Thereafter, SGSN gets the services which the meter collector can use from HLR [16].

It can be observed from Figure 2 that there is only one-way authentication of meter collectors in GPRS while there is no authentication for femtocells towards meter collectors. Therefore, communication over wireless access network is exposed to hijacking of rogue femtocells-based cyber attack.

Malicious adversaries could measure and collect the carrier frequency of the targeted cell as described in [16, 17]. Thereafter, it could broadcast the same carrier frequency using rogue femtocells with higher power. In this case, meter collectors would be forced to detach from the lawful femtocell and attach to the rogue femtocell due to its better communication parameters and stronger SS. Furthermore, malicious adversaries could get International Mobile Subscriber Identity (IMSI) and International Mobile Equipment

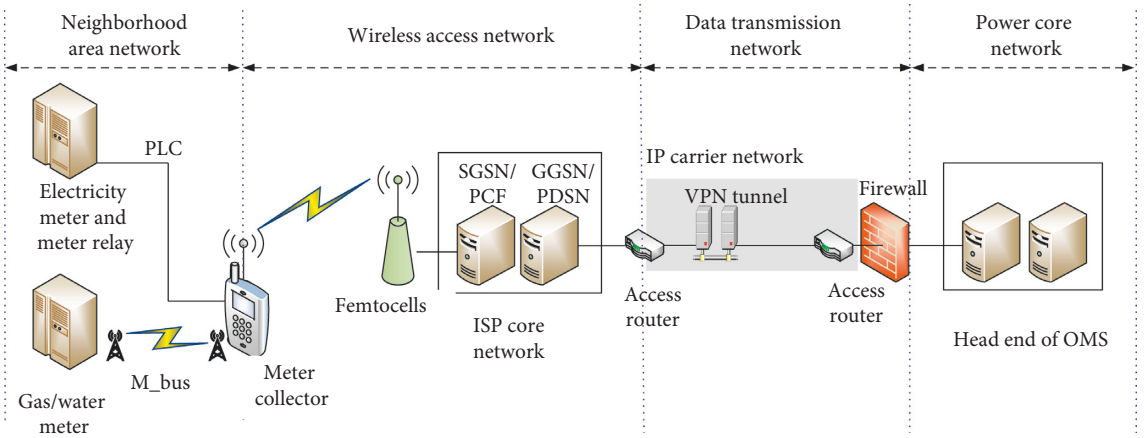

Figure 1: Communication architecture of OMS.

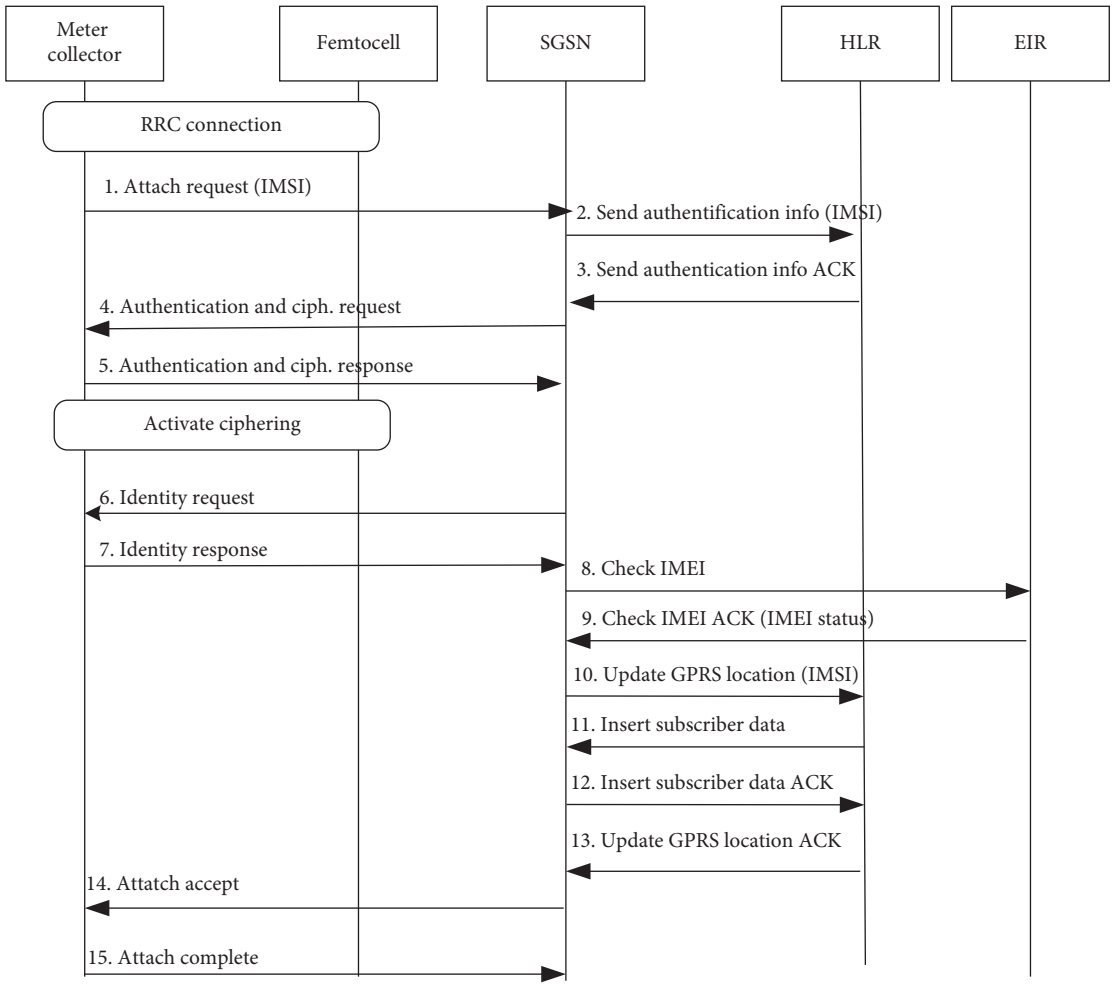

Figure 2: Attach process of a meter collector.

Identity (IMEI) of meter collectors via the rogue femtocells to implement further attack [18]. According to [19], the smart meters using encryption algorithm AES-128 could be cracked and meters can be attacked by bypassing encryption that was designed to secure their communications. Thereafter, the malicious intruder could take full control of the meter and shut down power supply of the user.

2.3. Related Works on Detecting Rogue Femtocells. Since communication security has become increasingly prominent

in modern society, various approaches have been developed to detect rogue femtocells. An observation-based detection technique is proposed in [19] to detect attacks on femtocells. Smart phones are used as observers to provide required information of femtocells. Thereafter, observation management server could identify attack from femtocells including location movement attack, impersonating subscriber attack, etc. However, IoT meters of OMS are notably different from average mobile intelligent terminals. For example, meter collectors usually upload data to the head end system once an hour. Even though a management system in the head end of OMS could detect a rogue femtocell with uploaded data of meter collectors, it is too late. Therefore, IoT meters should identify rogue femtocells by themselves.

Since the signal of a femtocell can cover only a small area and physical location of femtocells can be queried with its Location Area Code (LAC), the distance between femtocells and the user communication device can be estimated. Thereafter, the femtocells with an unreasonable distance can be detected as rogue ones [21]. However, it is rather difficult to identify a rogue femtocell once it duplicates the LAC of neighboring lawful femtocells with rational distance.

In recent years, radio frequency fingerprinting (RFF) is considered as one of the promising techniques to enhance wireless security of IoT devices. Since wireless communication devices have slim differences in their communication signal induced by the variance in component parameters, the RFF is utilized to authenticate identity of a wireless device [13]. Once we establish a database that records RFF of all lawful femtocells, the femtocell that is not in the white list can be identified as a rogue one [22]. However, IoT meter collectors have limited computational resource, and they cannot detect and extract the RFF of IoT devices, currently.

Since the threat of rogue femtocells originates from one-way authentication of GPRS, UMTS and LTE support two-way authentication between communication terminals, and it seems to be possible for meter collectors to prevent hijacking of rogue femtocells [23]. However, meter collectors are designed to be backward compatible. Malicious adversaries can broadcast interference signal to disable UMTS and LTE communication. Therefore, meter collectors that communicate with UMTS and LTE can be compromised with aforementioned approach once they support GPRS communication. Hence, threat of rogue femtocells will exist till meter collectors are replaced with the ones that do not support GPRS.

What is worse, LTE communication may not be as secure as expected, either. Recent investigation indicates that LTE RRC redirection attacks [24], aLTEr attacks, and so on [25] could compromise communication terminals using LTE, too.

3. Differences in SS of Lawful and Rogue Femtocells

With limited computation and memory resources, IoT devices have a computation bottleneck to limit the support for advanced applications involving complex algorithms [4, 9]. Therefore, the aforementioned ways to detect hijacking of rogue femtocells may not fit for resource-constrained IoT meter collectors.

Unlike mobile intelligent terminals, IoT meter collectors locate in the fixed places. A meter collector could detect several femtocells in its neighborhood. It chooses to attach to the one with the best communication parameters, usually the one with the strongest SS. The SS of neighboring femtocells detected by a meter collector could be influenced by the distance, buildings, and meteorological factors at large. The former two are constant and thus will not result in the variation of sensed SS of neighboring femtocells. Therefore, the sensed SS is usually determined by the meteorological factors. Consequently, variations of sensed SS of neighboring lawful femtocells have similar profiles.

The SS around a meter collector is measured with a base station analyzer. The SS profiles measured consecutively for 24 hours is shown in Figure 3. The horizontal axis denotes time span of a day, and the vertical axis denotes signal strength of femtocells in dBm. The SS of neighboring femtocells varies according to their distance from the meter collector. The SS of all neighboring lawful femtocells fluctuates slightly, and they have similar profiles around the clock.

Rogue femtocells-related telecommunication fraud is one of the most serious crimes affecting the safety of people's personal property, which has been heavily cracked down and punished by Chinese courts [26]. In order to provide a secure communication circumstance for their customers, Internet service providers will track, locate, and crack rogue femtocells. In this case, a rogue femtocell will be turned on for some time and immediately turned off, now and then, here and there, to escape from being caught. Once a rogue femtocell is turned on, its SS escalates much higher than that of a lawful femtocell. Consequently, meter collectors near to a rogue femtocell will seamlessly hand over from the lawful femtocell to the rogue femtocell if there is not any approach to stop it.

The SS profiles of a rogue femtocell and several lawful femtocells are plotted in Figure 3. It can be observed that there is notable difference among the SS profiles of lawful femtocells and that of the rogue femtocell. Unlike lawful femtocells in the neighborhood with similar SS profiles, SS of a rogue femtocell is characterized by abrupt changes. Therefore, SS profile of femtocells sensed by a meter collector could be used as a steady-state RFF and clustered to identify rogue femtocells.

4. Expert System to Detect Rogue Femtocells

An expert system is a computer system that emulates the decision-making ability of a human expert and is designed to solve complex problems by reasoning through bodies of knowledge, represented mainly as if-then rules [27, 28]. An expert system is employed to identify rogue femtocells whose SS profile is notably different from that of lawful femtocells.

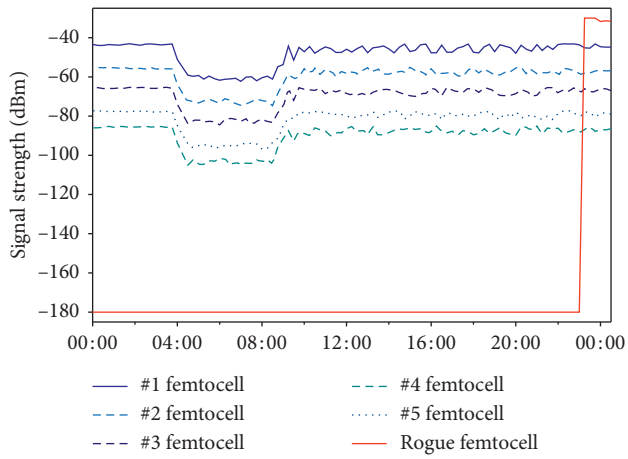

Figure 3: Signal strength profile of lawful and rogue femtocells.

4.1. Rule to Identify a Rogue Femtocell. Once a rogue femtocell appears, it broadcasts stronger signal power to hijack wireless communication devices. When a meter collector communicating by GPRS reselects to attach to a femtocell with higher SS, the identity of the femtocell should be verified.

Unlike lawful femtocells in the fixed location, a rogue femtocell will be turned on and off from time to time or kept moving here and there to prevent the rogue femtocell from being caught. Therefore, its SS profile sensed by a meter collector in the fixed location is fickle and unstable. Difference in SS profile of two femtocells can be reflected with their Euclidean distance. The Euclidean distance between lawful femtocells is small since they have similar SS profiles, whereas the Euclidean distance between lawful and rogue femtocells is much larger. This can be used as prior knowledge to formulate a rule to identify rogue femtocells.

The average Euclidean distances among all sensed femtocells can be used to determine the threshold to detect a rogue femtocell. Once there is a rogue femtocell, it can be picked out since its Euclidean distances to the other femtocells are notably higher than the threshold. Without rogue femtocells, Euclidean distances among lawful femtocells are lower than the threshold, and meter collectors can hand over to the femtocell with higher SS without difficulty. We find that the threshold can be set to 1.5 times the average Euclidean distances of all femtocells by trial and error.

4.2. Length of Time Window. In order to prevent from being cracked, a rogue femtocell will not stay in the same place for a long time. According to reported activity of rogue femtocells related to fraud, most rogue femtocells operate consecutively for several hours [26]. Therefore, we set a 24-hour time window to identify rogue femtocells in this paper. That is, the SS of the past 24 hours would be recorded and calculated to detect rogue femtocells. Once a rogue femtocell does not stay for a day, it can be identified and meter collectors will not attach to it.

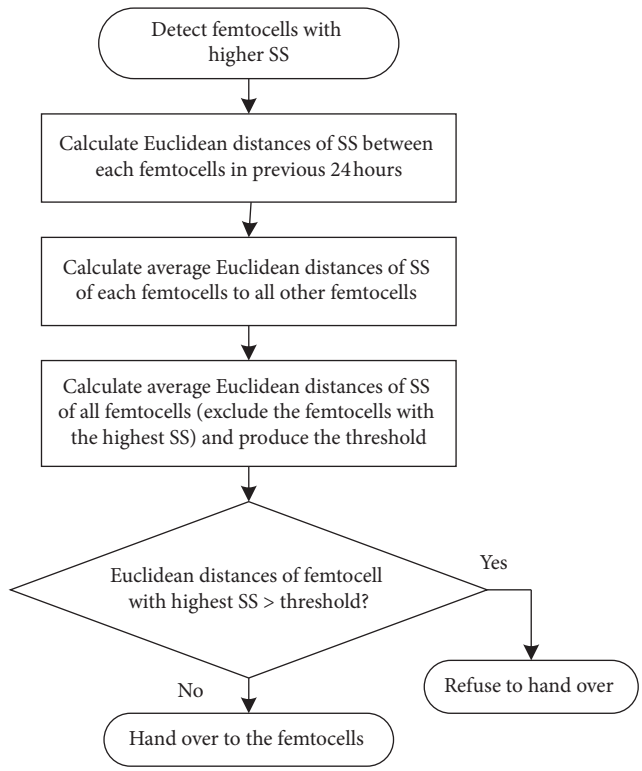

Figure 4: Flowchart to detect a rogue femtocell.

Once a meter collector reselects the femtocell it attaches to, the way to determine its identity can be demonstrated as shown in Figure 4 with the following steps:

Step 1. Calculate Euclidean distances of SS between every two femtocells in the previous 24 hours.

Step 2. Calculate average Euclidean distances of SS of each femtocells to all other femtocells.

Step 3. Calculate average Euclidean distances of SS of all femtocells and then multiply them by 1.5 to obtain the threshold.

Step 4. If the average Euclidean distance to all other femtocells of the femtocells with highest SS is larger than the threshold, it is identified as a rogue one and the meter collector is not allowed to attach to it. Otherwise, it is a lawful femtocell, and the meter collector hands over to it.

5. Numerical Simulation

5.1. Identifying Stationary Rogue Femtocells. A meter collector prefers to attach to the femtocell with stronger SS. Once there is a femtocell with stronger SS than the one that meter collector attaches to for 5 seconds, the meter connector will hand over to it. In order to avoid frequent cell reselection, meter collectors will implement cell reselection with a random time span ranging from 20 seconds to 620 seconds. For simplicity, it is supposed that cell reselection happens every 15 minutes in the paper.

The SS of lawful femtocells and a stationary rogue femtocell with 192 data points in 2 days is shown in Figure 5.

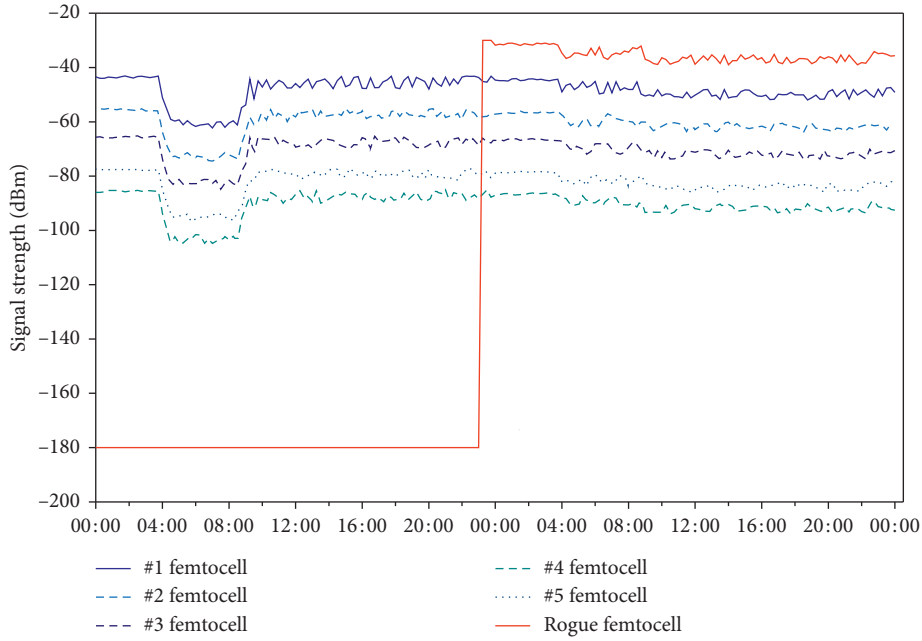

Figure 5: Signal strength profile of stationary rogue and lawful femtocells.

The SS of a femtocell can be normalized according to the following equation:

$$x_i^* = \frac{x_i - \min_i}{\max_i - \min_i}, \quad (1)$$

where x_i denotes SS of ith femtocell; $\min_i$ and $\max_i$ denote the weakest and strongest signals in the current time window of investigated ith femtocell; and x_i^* denotes the normalized SS of ith femtocell.The Euclidean distances between the ith and jth femtocells can be calculated according to the following equation:

$$D_{i,j} = \sqrt{\sum_{k=1}^{96} \left(x_{i,k}^* - x_{j,k}^*\right)^2}, \quad (2)$$

where $D_{i,j}$ denotes Euclidean distances between ith and jth femtocells in the previous 24-hour time window.

According to Figure 5, a stationary rogue femtocell appears at 23:30. The Euclidean distances between SS of all femtocells at that time are calculated according to equation (2) and are listed in Table 1.

It can be observed from Table 1 that the Euclidean distances between 2 lawful femtocells are usually small. For example, the Euclidean distance between the 1st and 2nd femtocells is 0.969 and that among lawful femtocells varies around 0.95. However, the SS of the rogue femtocells is notably far away from those of lawful ones in the state space. Its average Euclidean distance to lawful ones is around 7.7, which is notably larger than those among lawful ones.

Add up Euclidian distance of SS of the 1st femtocell to all other femtocells (i.e., first row of Table 1) to produce the average Euclidian distance of the 1st femtocell to all other femtocells (2.302 of the 1st femtocell at that time). The average Euclidian distances of SS of femtocells are calculated every 15 minutes to get a time series of Euclidian distance of SS in Figure 6.

Table 1: Euclidean distances of SS between femtocells at 23:30.

	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	Rogue	Average distance
$i=1$		**0.969**	0.918	0.898	**1.015**	7.710	2.302
$i=2$	0.969		0.850	0.857	0.859	7.723	2.252
$i=3$	0.918	0.850		0.941	0.809	7.721	2.248
$i=4$	0.898	0.857	**0.941**		0.947	7.676	2.264
$i=5$	**1.015**	0.859	0.809	0.947		7.803	2.287
Rogue	7.710	7.723	7.721	7.676	7.803		7.727

The mean of all average Euclidean distances is 3.180. Multiply it by 1.5 and get the threshold of 4.770. At 23:30, the average Euclidean distances of all lawful femtocells are around 2.25, and the average Euclidean distance of the rogue femtocell is 7.727, which is notably larger than the threshold. Therefore, it can be identified as a rogue femtocell.

Since the rogue femtocell has stronger SS throughout the following 24 hours according to Figure 5, the meter collector will keep on reselecting to attach to the rogue femtocell with stronger SS. The average Euclidean distances of every femtocell to the others in the following day can be calculated and are plotted as shown in Figure 6. The threshold of 4.770 can be used in the following day to detect potential rogue femtocells.

(i) It is obvious that the average Euclidean distances of SS of these lawful femtocells are rather close to each other because their SS has the similar profile. However, the average Euclidean distance of SS of the rogue femtocell is significantly higher than the lawful ones throughout the following day.

(ii) Since the average Euclidean distance of the SS of the rogue femtocell is larger than the threshold, it can be picked out in the following 24 hours.

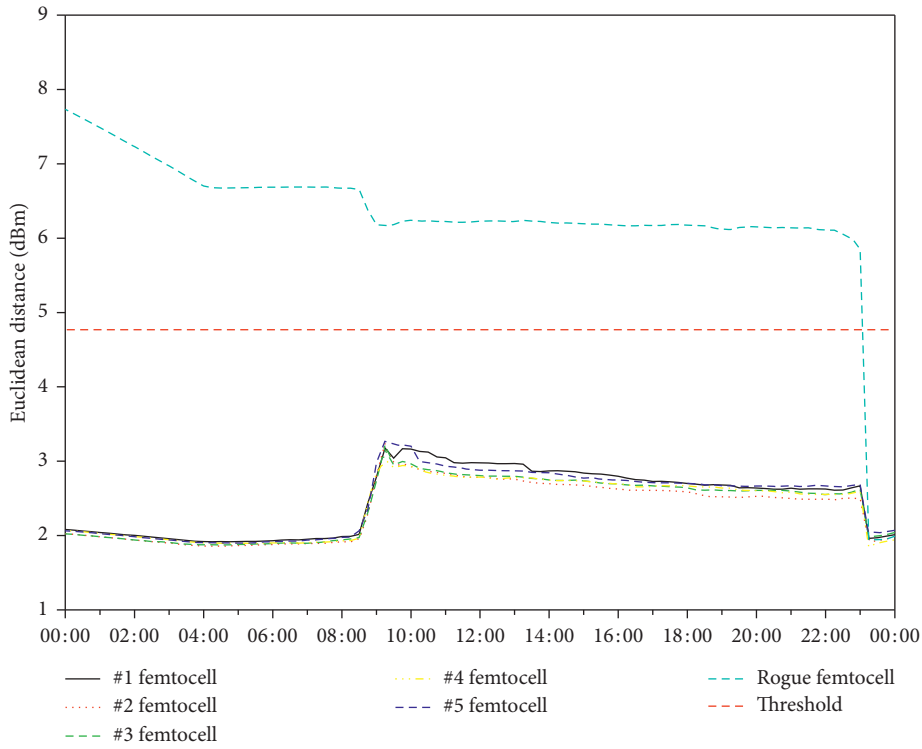

Figure 6: Average Euclidean distances of stationary rogue femtocells.

(iii) Note that there is a notable escalation in the average Euclidean distances of lawful femtocells from 8:00 a.m. to 9:00 a.m., while there is a sag in the average Euclidean distance of the rogue femtocell. It is speculated that this is because the fog dissipates from 8:00 a.m. and disappears at 9:00 a.m.

(iv) There is a turning point of the average Euclidean distance of the rogue femtocell at 4:00 a.m. It is speculated that the turning point is caused by the decline of SS of lawful femtocells when fog appears at this time.

To conclude, average Euclidean distances of SS in the time window of previous 24 hours could be utilized to detect rogue femtocells. When a meter collector reselects to attach to a new femtocell, it will compare the average Euclidean distance of SS of the new femtocell with the threshold to decide whether to attach or not. If it is larger than the threshold, the femtocell is identified as a malicious one and the meter collector will not attach to it. In the following 24 hours, the threshold remains unchanged and collectors will not attach to it even though it has the strongest SS.

5.2. Identification of Moving Rogue Femtocells. Unlike stationary rogue femtocells, moving ones keep changing their locations from time to time. At the beginning, the SS of a moving rogue femtocell is as shown in Figure 7. It can be observed that it emerges at 23:15, and its SS achieves its maximum at 01:00 a.m. and then disappears gradually. The moving rogue femtocell forces the meter collector to attach to it at 01:00 when its SS is higher than that of lawful ones.

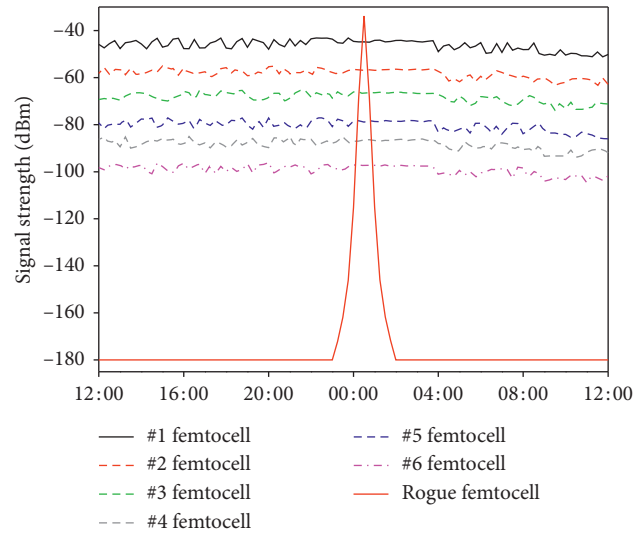

Figure 7: Signal strength profile of moving rogue and lawful femtocells.

Also, the average Euclidean distances between every femtocell at 01:00 a.m. are calculated and are listed in Table 2.

The average Euclidean distances of lawful and rogue femtocells every 15 minutes are calculated and are listed in Table 2. Meter collectors implement cell reselection to attach to the rogue femtocell at 01:00, and the average Euclidean distance of SS of all femtocells is 2.842. Multiply it by 1.5 and then get the threshold of 4.263. The rogue femtocell with an average Euclidean distance of 7.637 can be picked out easily, and the meter collector will not attach to it. Thereafter, SS of

Table 2: Average Euclidean distances of SS of lawful and moving rogue femtocells.

	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	Rogue	Average distance
00:30	2.083	2.023	2.024	2.071	2.067	7.742	2.872
00:45	2.073	2.013	2.015	2.061	2.057	7.684	2.855
01:00	2.066	2.004	2.007	2.053	2.049	7.637	2.842
01:15	2.062	1.998	2.003	2.048	2.044	7.606	2.833
01:30	2.059	1.996	1.999	2.044	2.041	7.586	2.828
01:45	2.056	1.993	1.998	2.041	2.039	7.572	2.823

the moving rogue femtocells declines and then disappears after 2:00.

6. Conclusion

To defend against hijacking of rogue femtocells, a rogue femtocell detection approach for IoT meters in the fixed location is proposed in this paper. Prior knowledge of difference in SS profile among rogue and lawful femtocells is utilized to formulate a rule to identify rogue femtocells. Numerical simulation suggests that the developed expert system can pick out stationary and moving rogue femtocells, and meter collectors will not attach to the malicious rogue femtocell. Moreover, the developed system works on the specific rule and requires limited computation and memory resource, which are fit for resource-constraint IoT device.

Since the developed approach works with the premise that the rogue femtocell does not stay for a long time, malicious adversaries could subvert by sustained attack for more than a day. In this way, the meter collector will attach to the rogue femtocell and malware could mount on it.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the support from the Electric Power Research Institute of China Southern Power Grid (grant no. ZNKJXM20170085), National Natural Scientific Funding of China (51777015), National Key R&D Program of China (2018YFB0904903), and Scientific Research Funding of Hunan Education Department (15A0015).

References

[1] S. Rinaldi, P. Ferrari, A. Flammini, E. Sisinni, and A. Vezzoli, "Uncertainty analysis in time distribution mechanisms for OMS smart meters: the last-mile time synchronization issue," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 3, pp. 693–703, 2019.

[2] A. Montazerolghaem, M. H. Y. Moghaddam, and A. Leon-Garcia, "OpenAMI: software-defined AMI load balancing," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 206–218, 2018.

[3] S. Bohn, M. Agsten, O. Waldhorst et al., "An ICT architecture for managed charging of electric vehicles in smart grid environments," *Journal of Engineering*, vol. 2013, Article ID 989421, 11 pages, 2013.

[4] J. Siryani, B. Tanju, and T. J. Eveleigh, "A machine learning decision-support system improves the internet of things' smart meter operations," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 1056–1066, 2017.

[5] E. Spano, L. Niccolini, S. D. Pascoli, and G. Iannaccone, "Last-meter smart grid embedded in an internet-of-things platform," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 468–476, 2015.

[6] Y. Sun, L. Lampe, and V. W. S. Wong, "Smart meter privacy: exploiting the potential of household energy storage units," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 69–78, 2018.

[7] M. Wolf and D. Serpanos, "Safety and security in cyber-physical systems and internet-of-things systems," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 9–20, 2018.

[8] G. Liu and D. Jiang, "5G: vision and requirements for mobile communication system towards year 2020," *Chinese Journal of Engineering*, vol. 2016, Article ID 5974586, 8 pages, 2016.

[9] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2017.

[10] D. Malone, D. F. Kavanagh, and N. R. Murphy, "Rogue femtocell owners: how Mallory can monitor my devices," in *Proceedings of the IEEE INFOCOM*, pp. 3387–3392, Turin, Italy, April 2013.

[11] G. Nico, R. Kévin, and B. Ravishankar, Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication, 2012, https://www.tu-berlin.de/fileadmin/fg214/Papers/femto_ndss12.pdf.

[12] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT Botnet of high wattage devices can disrupt the power grid," in *Proceedings of the 27th USENIX Security Symposium*, Baltimore, MD, USA, August 2018.

[13] Z. Haddad, M. Mahmoud, S. Taha et al., "Secure and privacy-preserving AMI-utility communications via LTE-A networks," in *Proceedings of the IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 748–755, Abu Dhabi, United Arab Emirates, October 2015.

[14] Halifax Regional Water Commission, *AMI Technology Assessment & Feasibility Study Consolidated Report*, Halifax Regional Water Commission, Excergy, Denver, USA, 2014, https://www.halifax.ca/sites/default/files/documents/home-property/water/AMI-Technology-FianlReport.pdf.

[15] K. Sander and B. Roos, *Security Analysis of Dutch Smart Metering Systems*, University van Amsterdam, Amsterdam, Netherlands, 2008.

[16] C. Xenakis, "Malicious actions against the GPRS technology," *Journal Computer Virology*, vol. 2, no. 2, pp. 121–133, 2006.

[17] D. Zhu, N. Pang, and Z. Fan, "A self-testing approach defending against rogue base station hijacking of intelligent terminal," in *Proceedings of the International Conference on Applied Science and Engineering Innovation*, pp. 929–937, Wuhan, China, April 2015.

[18] J. Martin, I. Tøndel, and G. Køien, "GPRS security for smart meters," in *1st Cross-Domain Conference and Workshop on Availability, Reliability, and Security in Information Systems (CD-ARES), Lecture Notes in Computer Science, LNCS-8127*, A. Cuzzocrea, C. Kittl, D. E. Simos et al., Eds., pp. 195–207, Springer, Regensburg, Germany, 2013.

[19] A. G. Illera and J. V. Vidal, "Lights off! the darkness of the smart meters," in *Proceedings of the Europe Black Hat Conference*, Amsterdam, Netherlands, October 2014, https://www.blackhat.com/eu-14/archives.html#lights-off-the-darkness-of-the-smart-meters.

[20] M. J. Guezguez, S. Rekhis, and N. Boudriga, "Observation-based detection of femtocell attacks in wireless mobile networks," in *Proceedings of the Symposium on Applied Computing, SAC'17*, pp. 529–534, Marrakech, Morocco, April 2017.

[21] C.-M. Chen, Y.-H. Chen, Y.-H. Lin et al., "Eliminating rouge femtocells based on distance bounding protocol and geographic information," *Expert Systems with Applications*, vol. 41, no. 2, pp. 426–433, 2014.

[22] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a secure wireless-based Home area network for metering in smart grids," *IEEE Systems Journal*, vol. 8, no. 2, pp. 509–520, 2014.

[23] H. He and J. Yan, "Cyber-physical attacks and defenses in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[24] S. R. Hussain, O. Chowdhury, S. Mehnaz et al., "LTE inspector: a systematic approach for adversarial testing of 4G LTE," in *Proceedings of the Network and Distributed Systems Security Symposium*, pp. 18–21, San Diego, CA, USA, February 2018.

[25] D. Rupprecht, K. Kohls, T. Holz et al., "Breaking LTE on layer two," in *Proceedings of the IEEE Symposium on Security & Privacy*, San Francisco, CA, USA, May 2019.

[26] C. Daily, Strict Crackdown on Telecommunication Fraud Coming, 2019, http://english.court.gov.cn/2019-03/14/content_37450221.htm.

[27] S. Park, E. Lee, W. Yu, H. Lee, and J. Shin, "State estimation for supervisory monitoring of substations," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 406–410, 2013.

[28] S. Sarkar, T. Sharma, A. Baral, B. Chatterjee, D. Dey, and S. Chakravorti, "An expert system approach for transformer insulation diagnosis combining conventional diagnostic tests and PDC, RVM data," *IEEE Transactions on Dielectrics and Electrical Insulation*, vol. 21, no. 2, pp. 882–891, 2014.