Rogue Base Stations Detection for Advanced Metering Infrastructure Based on Signal Strength Clustering

QIAN BIN¹, CAI ZIWEN¹, XIAO YONG¹, HONG LIANG², AND SU SHENG², (Senior Member, IEEE)

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

Corresponding author: Xiao Yong (xiaoyong@csg.cn)

This work was supported in part by the Electric Power Research Institute of China Southern Power Grid under Grant ZNKJXM20170085, in part by the National Natural Scientific Foundation of China under Grant 51777015 and Grant U196620027, and in part by the National Key Research and Development Program of China under Grant 2018YFB0904903.

ABSTRACT The smart meters and meter collectors in Advanced Metering Infrastructure (AMI), which are installed in every home, rely on wireless Virtual Private Network (VPN) for communicating with Head End System (HES). Therefore, they are prone to suffer from malicious cyber-attack. Usually, based on General Packet Radio Service (GPRS) communicated method is the most popular for meter collectors and consequently they are vulnerable to rogue Base Stations (BS) and get compromised by malicious adversaries further. Thus a Density-based spatial clustering of applications with noise (DBSCAN) method is employed to filter rogue BSs out and prevent meter collectors from attaching to them, because there is a notable difference between Signal Strength (SS) profile of legitimate BSs and rogue BSs, Numerical simulation indicates that the proposed approach is capable of detecting both stationary and moving rogue BSs online within fixed time window effectively. Moreover, the method can be implemented in existing meter collectors with limited computation resource. In conclusion, the proposed approach can enhance the level of cyber security of meter collectors.

INDEX TERMS Rogue base station, cyber-attack, clustering analysis, advanced metering infrastructure.

I. INTRODUCTION Smart meters and meter collectors in AMI are the most visible parts of the smart grid in daily life, which play an important role in two-way communications between customers and the utility [1]. They send real-time electricity consumption to Head End System (HES), receive electricity tariffs from HES, and update electricity charge, which facilitate demand response and effective energy management and consumer engagement [2].

Generally speaking, while the communication means between meter collectors and smart meters are Power Line Communication (PLC) or RS-485, meter collectors communicate with HES by GPRS [3]. Hence, it is significantly necessary to keep their data confidential and private when transmitted between dispersed meters and the utility [4], [5].

To solve this problem, data encryption/decryption Integrated Circuits (IC) is embedded in smart meters [6]. Additionally, a light and flexible key management protocol is developed in [7], [8] for smart meters with limited computational resource. Since public network is vulnerable to cyber-attacks, such as spoofing, eavesdropping and man-in-the-middle attacks, Internet Service Providers (ISP) provide a Virtual Private Network (VPN) for secured communication of AMI [3]. However, communication beyond the VPN tunnel remains to be exposed to cyber-attack. For instance, GPRS supports only one-way subscriber authentication. That is to say, there isn’t network authentication, which makes it possible for a malicious adversary to take full control of meter collectors by setting up a rogue BS [9]. Upon being forced to attach to a rogue BS, the meter collectors are in great danger and their data information could be stolen and even tampered by malicious adversaries [10]. What’s worse, if lots of collectors are under malicious control, adversary could cause dramatic

Received July 14, 2019, accepted July 28, 2019, date of publication August 9, 2019, date of current version September 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2934222

IEEE Access
changes in load, which has a negative impact on the stability of the whole power system [11], [12]. Therefore, ways to detect rogue BSs for meter collectors with limited computational resource are highly preferred.

Up to now, various approaches have been developed to identify rogue BSs. For example, Radio Frequency Fingerprinting (RFF), which is designed to enhance the authentication reliability of wireless devices, is able to identify them [13]. More specifically, if we establish a database that records RFF of all legitimate BSs, the rogue BS can be distinguished [14]. However, it is greatly challenging for meter collectors with limited computational resource to detect and extract the RFF of all legitimate BSs. In fact, they are not qualified to perform that task at all. Another example is the eliminating rogue BS based on distance bounding and geographical information [15]. Location Area Code (LAC) of a BS is utilized to inquire its latitude and longitude and its physical location can be estimated. Thereafter, the approximate distance between a subscriber’s device and the BS can be estimated. Since a BS can only cover a small area, the BS with an unreasonable distance can be identified as a rogue BS by a subscriber. Whereas, it is rather difficult to identify a rogue BS once it duplicates LAC of a neighboring legitimate BS with rational distance. Besides, since Universal Mobile Telecommunications System (UMTS) and Long Term Evolution (LTE) support two-way authentication between communication terminals and BSs [16], it is widely believed that application of meter collectors, which communicate with 3rd and 4th generation mobile network, could prevent threat of rogue BSs [17].

Different from mobile communication terminals like cellphones, both meter collectors and legitimate BSs are located in the fixed places. Note that the SS of neighboring BSs sensed by a meter collector is of similar profile and not totally different from that of a rogue BS. Furthermore, a rogue BSs detection approach based on SS profile clustering is proposed in this paper. The contributions of this paper are listed as follows.

- We investigate the threat of rogue BSs towards AMI. We find that if meter collectors are set to be compatible with GPRS, the malicious adversaries can broadcast interference signal to disable 3G (UMTS) and 4G (LTE) communication to force meter collectors to communicate simply by 2G (GPRS), which is one-way authentication. Thus, only until antiquated meter collectors are replaced by the ones that are incompatible with GPRS will the threat disappears, which is much later than expected.
- We propose a rogue BSs detection approach for AMI based on SS profile clustering. Since it is difficult for meter collectors with limited computational resource to detect and extract the RFF of all legitimate BSs, the SS profile is utilized as a steady-state RFF due to fixed location between meter collectors and BSs. The proposed approach can adapt to existing meter collectors with limited computational resource and no retrofit on other parts of the system is required. Numerical simulation demonstrates feasibility of the proposed approach.

The remainder of this paper is organized as follows. Section II gives an overview of background of AMI and potential threat resulted from rogue BSs. In Section III, we propose a rogue BSs detection approach for AMI based on SS profile clustering. Section IV shows the process of the proposed approach to identify both stationary and moving rogue BSs by numerical simulation. Section V concludes the paper.

II. BACKGROUND OF AMI AND POTENTIAL THREAT FROM ROGUE BS

A. STRUCTURE OF AMI

The AMI are usually composed of smart meters, meter relays, HES, and communication system [5], [18] as shown in Fig. 1.

Most smart meters & meter relays communicate with meter collectors via PLC or RS-485 in neighborhood area network. However, meter collectors communicate with HES via shared and public networks provided by ISP [3]. More specifically, the communication system is composed of 3 parts, i.e., wireless access network, data transmission network, and power core network. Function of each part is depicted as follows [3], [5].

- Wireless access network. Through wireless access network, meter collectors are connected to a BS and then encrypted meter data are transmitted from meter collectors to the carrier network of ISP.
- Data transmission network. It is a carrier network provided by the ISP. In order to keep the transmitted data integral and private, Layer 2 Tunneling Protocol is utilized to establish VPN tunnel. Also, channel encryption and end-to-end encryption are employed to guarantee security of the data transmitted within the tunnel [3], [5].
- Power core network. It is a private network of power utility. Firewall is deployed between the access router device and the HES of AMI, which can effectively prevent malicious connection from the external network. Moreover, intrusion detection system can be employed in HES to detect adversary intrusion in time [19], [20]. HES determines encryption key of uploaded data according to the ID of the meter. Thereafter, uploaded data are decrypted for billing service.
B. THREAT FROM ROGUE BSS IN WIRELESS NETWORK

It can be observed from Fig.1 that the communication over wireless access network is exposed to malicious cyber-attack. When a meter collector is going to attach to a BS, it sends an attach request and Serving GPRS Support Node (SGSN) to the BS as shown in Fig.1. Thereafter, it receives an identity request and then sends its International Mobile Subscriber Identification Number (IMSI) and International Mobile Device Identity (IMEI) back to implement identity authentication and Home Location Register. After authentication and location updates are finished, the meter proceeds in attaching to the BS [21].

In GPRS, meter collectors are authenticated towards BSs while there is no authentication for BSs towards meter collectors. That’s, the authentication in GPRS is one-way. As a result, it is likely for an adversary to take control of meter collectors by setting up a rogue BS [22]. What’s more, according to [21], attackers could establish a rogue BS with modest budgets. The malicious adversary could measure and collect carrier frequency of the targeted cell. Thereafter, it could broadcast the same carrier frequency using the rogue BS with higher power. In this case, meter collectors would be forced to attach to it due to its better communication parameters and higher SS. In addition, malicious adversary could get IMSI and IMEI of meter collectors via the rogue BS to implement further attack [21]. Once encryption of a smart meter is cracked, intruders could take full control of it.

Unlike GPRS, both Universal Mobile Telecommunications System (UMTS) and Long Term Evolution (LTE) support two-way authentication towards both communication terminals and BSs [17]. Therefore, it is widely believed that the threat of rogue BSs can be eliminated once antiquated meter collectors are replaced by the ones only communicating through the 3rd and 4th generation mobile network. However, that’s not the whole story. Since meter collectors are designed to be backward-compatible, they can communicate via GPRS, UMTS, and LTE. And malicious adversary can broadcast interference signal to disable UMTS and LTE communication. As a result, meter collectors can be forced to communicate simply by GPRS and compromised according to aforementioned approach. Therefore, threat of rogue BSs will exist till antiquated meter collectors are replaced with the ones that do not support GPRS. What’s worse, LTE communication may not be as secure as expected, either. Recent investigation indicates that LTE RRC redirection attacks [23], alTER attacks, etc. [24] could compromise communication terminals using 4G LTE, too. In that circumstance, it is highly preferred to develop ways to detect rogue BSs for meter collectors with limited computation resource.

III. ROGUE BSS DETECTION BASED ON SS CLUSTERING

A. DIFFERENT SS BETWEEN LEGITIMATE AND ROGUE BSS

Smart meters and meter collectors are usually located in fixed places. A meter collector could detect several BSs in its neighborhood at the same time as shown in Fig.2. Usually, it chooses to connect to the BS with best communication parameters, in particular, the BS with the strongest SS. The SS of neighboring BSs detected by a meter collector is related to the distance, buildings, and meteorological factors (such as fog, rain, and etc.). The former two remain constant and thus won’t result in the variation of sensed SS of neighboring BSs. Therefore, only meteorological factors affect the SS. However, the variations of sensed SS of different BSs are of similar profile. The SS profiles sensed by a meter collector in a day are shown in Fig.3. It can be observed that the SS of all BSs declines at 3:00 a.m. and escalates when the fog melts at 8:00 a.m.. What’s more, the SS of all neighboring legitimate BSs fluctuates slightly and they are of similar profile over the time.

Since telecommunication fraud related to rogue BS is one of the most serious social harms affecting the safety of people’s personal property in China, the Chinese courts have been heavily punishing such offenders [25]. In order to provide a secure communication circumstance for their customers, ISPs will track, locate and crack rogue BSs. Because staffs of ISP need some time, maybe several hours or longer, to reach and crack rogue BSs. During this period, meter collectors are still in danger. In this way, meter collectors should be of ability to identify rogue BSs by themselves instead of relying on ISP.

In order to escape from being caught, a rogue BS will be turned on for some time and immediately turned off, now...
and then, here and there. Once a rogue BS is turned on, its SS escalates to much higher than that of legitimate BSs. As a result, meter collectors nearby will seamlessly hand over from the legitimate BS to it if there isn’t any approach to stop it. The SS profiles of legitimate BSs and a rogue one are plotted as Fig.3. Note that the SS profile of legitimate BSs is of notable difference from that of the rogue one. Unlike legitimate BSs in the neighborhood with similar SS profile, that of a rogue BS is characterized by abrupt changes. Therefore, SS profile of BSs sensed by a meter collector could be used as a steady-state RFF and clustered to pick rogue BSs out according to this kind of notable difference.

According to the rogue BSs detection approach based on distance bounding proposed in [15], a rogue BS can duplicate LAC of a legitimate BS with rational distance to prevent from being identified. Since a rogue BS in the same place could be located and cracked by ISPs, it must change its location from time to time. Consequently, mutation of its SS is an inherent characteristic. Therefore, it is credible to distinguish a rogue BS according to its SS profile.

B. ROGUE BSS IDENTIFICATION BASED ON DBSCAN
Cluster analysis is the process of dividing a set of objects into groups. After that, objects in the same group are very similar, while objects in different groups are very different. As an unsupervised learning method, it is able to classify datasets without class labeling information. The way to determine the number of clusters is crucial. Density Based Spatial Clustering of Applications with Noise (DBSCAN), a classical clustering algorithm, can divide clusters with arbitrary shapes according to the distribution density of samples in the state space with noise. Therefore, the number of clusters can be determined according to density distribution of datasets automatically [26], [27].

Due to its ability to discover groups of arbitrary shape and to distinguish noise in complex state space, DBSCAN has been widely utilized. DBSCAN labels data points that are densely distributed and associated with a single cluster as shown in Fig.4. Density represents the number of points, \( n \), which fall in a small volume \( V \) surrounding a specific point \( P \). \( V \) can be assumed to be a sphere of radius \( E_{ps} \) centered at \( P \). Hence, the threshold density can be specified by a parameter \( N_{min} \) that represents the minimum number of samples to make the sphere \( V \) notable dense. \( E_{ps} \) and \( N_{min} \) are the two key parameters of DBSCAN. Point \( P \) may either be a core point or non-core point. A non-core point may be a border point of a dense region or noise point. In particular:

- A generic point, \( P \), is a core-point if there are more than \( N_{min} \) points included in the sphere \( V \) with radius \( E_{ps} \) and centered at \( P \).
- A point \( Q \) is directly-density reachable from \( P \) if \( Q \) is included in \( V \) and \( P \) is a core-point.
- A point \( R \) is density reachable from \( P \) within \( V \), if there is a series of objects \( p_1, p_2, \ldots, p_n \), where \( p_1 = Q \) and \( p_n = P \), such that, for \( 1 \leq i \leq n \), \( p_i \in D \) and \( p_{i+1} \) is directly-density reachable from \( p_i \).
- A point \( S \) is density-connected to \( P \) in a set of volumes \( V_j \), if there is an object \( T \in V_j \) such that both \( Q \) and \( P \) are densely reachable from \( S \).

A density-based cluster is defined as a set of density-connected points maximized with respect to the density-reachability concept [21]. The points that do not contained by a sufficiently populated cluster are classified as noise.

For any given \( E_{ps}, N_{min} \) value, by selecting an initial random point \( P \), DBSCAN checks if \( P \) is a core-point. If this is found to be the case, it selects the directly reachable points and directly-density reachable points and expands the cluster by merging neighboring dense regions together. Once the border of the first cluster is identified, DBSCAN selects another point \( P' \) in space that does not belong to a previously formed cluster and the aforementioned procedure is repeated [26]. The algorithm collects directly-density reachable points from these core-points iteratively, which may involve the merging of a few density-reachable clusters. The process terminates when no new points can be added to any of the clusters.

The SS of all BSs sensed by a meter collector can be collected first. Thereafter, Euclidean distances between SS profile of each pair BSs are calculated. Since SS of legitimate BSs are of similar profile, they are categorized in a group and the rogue BS with notable different SS profile can be identified as noise point that are far away from that of legitimate ones.

IV. NUMERICAL SIMULATION
In order to cluster SS profile of BSs by the approach based on DBSCAN, to start with, three parameters should be determined, i.e. radius of a neighborhood \( E_{ps} \), minimum point in the neighborhood \( N_{min} \), and the length of time window of historical SS.

- In order to prevent from being cracked, a rogue BS won’t stay in the same place for a long time. What’s more, according to reported activity of rogue BSs related to fraud, most rogue BSs operate consecutively for several hours [28]. Therefore, we set a 24-hour time window to identify rogue BS in this paper. That’s, the SS of past 24 hours would be recorded and clustered to detect rogue BSs. Once a rogue BS does not stay for a day, it can be identified and meter collectors will not attach to it.
The minimum number of points in the neighborhood \( N_{\text{min}} \) could be determined according to total number of available BSs. BSs are usually deployed every 300 to 500 meters and the number of them sensed by a meter collector ranges from 6 to 20 in its neighborhood in the investigated city. However, the proposed approach should be fit for diversified operation condition including both urban area with dense BSs and rural area with sparse BSs. In rural area with sparse BSs, meter collectors might sense signal of a few BSs, higher \( N_{\text{min}} \) is not applicable for meter collectors in these areas. In this paper, we set \( N_{\text{min}} \) 2.

When a meter collector hands over the BS that it attaches to, it will calculate the Euclidean distances between SS of every BSs in previous 24 hours and the mean of all average Euclidean distances. If the \( E_{\text{ps}} \) is set to a larger number, a rogue BS might be identified as a legitimate one. Otherwise, a legitimate BS might be identified as a rogue one. Thereafter, double the mean and set it as neighborhood radius \( E_{\text{ps}} \) by trial and error.

### A. IDENTIFICATION OF STATIONARY ROGUE BSS

A meter collector will seamlessly hand over from the BS it connect with to another one with stronger SS. It is supposed that this action happens every 15 minutes in this paper. In general, according to whether the locations of rogue BSs are fixed, they can be divided into two categories, stationary or moving BSs. In this case, we will discuss these two situations respectively and we will start with the stationary rogue BSs.

The SS of legitimate BSs around a meter collector as shown in Fig.2 are measured with a base station analyzer. In general, the SS of rogue BSs is generated according to pre-determined rule. The SS of stationary rogue BS before 23:15 is set to \(-180\)dB when the rogue BS is turn off, and \(-36\)dB with a random perturbation of \(3\)dB when it is turn on after 23:15. The SS of legitimate BSs and a stationary rogue BS in 2 days with 192 data as shown in Fig.5 can be used to depict the procedure to detect a stationary rogue BS. At first, the SS of a BS can normalized according to Eq. (1).

\[
x^* = \frac{(x - \text{min})}{(\text{max} - \text{min})}
\]

where \(x\) denotes SS, \(\text{min}\) and \(\text{max}\) denote the weakest and strongest signals in the current time window of investigated BS, and \(x^*\) denotes normalized SS.

Obviously, it can be observed that a stationary rogue BS appears at 23:30. Then, the Euclidean distances between SS of all BSs in the time window of previous 24 hours are calculated and listed as Table 1. Note that all the Euclidean distances between legitimate BSs varies around 0.95 and the largest one is 1.086. Whereas, the SS of the rogue BS is notable far away from that of legitimate ones in the state space. And its average Euclidean distance to legitimate ones is around 7.740, which is apparently higher than that of all legitimate ones. What’s more, the mean of all average Euclidean distances is 2.869. Then double it to obtain the threshold of neighborhood radius \(E_{\text{ps}}\), 5.738 in the following 24 hours. If the average Euclidean distance between SS of a BS and the others is longer than the threshold of neighborhood radius \(E_{\text{ps}}\), 5.738, this BS will be seen as a rogue one.

At 23:30, the average Euclidean distances of all legitimate BSs are around 2.030 and their maximum Euclidean distance is 1.086, therefore, all they are directly density reachable points according to DBSCAN and they can be clustered as a group. However, the average Euclidean distance of the rogue BS is 7.740 and its minimum Euclidean distance to legitimate ones is 7.676, which is notable larger than \(E_{\text{ps}}\) of 5.738. Therefore, it is noise point according to DBSCAN and can be thought of as a rogue BS. Since its SS will be always higher than that of legitimate ones, meter collectors will not connect to it in the following time. In addition, the average Euclidean distances between SS of every BSs in the following 24 hours are calculated and plotted as shown in Fig.6.

- It is obvious that the average Euclidean distances of SS of these legitimate BSs are rather close to each other because their SS are of similar profile. However, the average Euclidean distances of SS of the rogue
BS is significantly higher every hour in the following 24 hours.

- If the average Euclidean distance of SS of a rogue BS is larger than $E_{ps}$ of 5.738, the rogue BS will be picked out effectively in the following 24 hours.
- Note that there is a notable escalation in the average Euclidean distances of legitimate BSs from 8:00 a.m. to 9:00 a.m. while a sag in that of the rogue BS. It is speculated that this is because the fog dissipates from 8:00 a.m. and doesn’t disappear until 9:00 a.m..
- Also, there is a turning point of the average Euclidean distance of the rogue BS at 4:00 a.m.. We speculate that the turning point is resulted from the decline of SS of legitimate BSs when fog begins to rise at this time.

In order to investigate the impact of SS of a rogue BS on the proposed approach, a rogue BS with weaker SS is also simulated. In this case, the SS of stationary rogue BS #2 before 23:15 is set to $-180$dB when it is turn off, and $-43$ dB with a random perturbation of 3dB when it is turn on after 23:15, which is slightly higher than that of legitimate BS 1# and lower than that of the former rogue BS as shown in Fig.7. The Euclidean distances between SS of all BSs in the time window of previous 24 hours are calculated and listed as Table 2. It can be observed that the Euclidean distances among legitimate BSs remain unchanged. Although the SS of rogue BS 2# is slightly larger than that of legitimate BS 1# and smaller than that of rogue BS 1#, its SS profile is characterized by abrupt change at 23:15, too. Therefore, as compared to that of Table 1, the Euclidean distances between SS of legitimate BSs and that of rogue BS 2# change slightly as compared to that of rogue BS 1#. Its average Euclidean distance to legitimate ones is around 7.578. The mean of all average Euclidean distances is 2.824. Then double it to obtain the threshold of neighborhood radius $E_{ps}$, 5.648 in the following 24 hours. Since Euclidean distances of rogue BS 2# remain almost the same as those of rogue BS 1# in the following 24 hours, it can be identified with proposed approach, too.

To conclude, the average Euclidean distances of SS in the time window of previous 24 hours could be utilized to detect rogue BSs. More specifically, when a meter collector reselects to attach to a new BS, it will compare the average Euclidean distance of SS of the new BS with the threshold of neighborhood radius $E_{ps}$ to decide whether to connect or not.

### B. IDENTIFICATION OF MOVING ROGUE BS

Unlike stationary rogue BSs, moving ones keep changing their locations from time to time. As shown in the fig.7, the SS of a moving rogue BS before 23:15 is set to $-180$dB. It escalates to its maximum, $-36$dB, at 00:30 a.m., and then diminishes to -180dB at 2:00 a.m.. The moving rogue BS forces the meter collector to attach to it at 00:30 when its SS is higher than that of all legitimate ones. And the average

| $i = 1$ | 0.969 | 0.918 | 0.898 | **1.015** | 0.973 | 7.561 | 2.056 |
| $i = 2$ | 0.969 | 0.850 | 0.857 | 0.859 | 0.885 | 7.613 | 2.006 |
| $i = 3$ | 0.918 | 0.850 | 0.941 | 0.809 | 0.891 | 7.587 | 1.999 |
| $i = 4$ | 0.898 | 0.857 | **0.941** | 0.947 | **1.086** | 7.544 | 2.046 |
| $i = 5$ | **1.015** | 0.859 | 0.809 | 0.947 | 0.944 | 7.564 | 2.023 |
| $i = 6$ | 0.973 | 0.885 | 0.891 | **1.086** | 0.944 | 7.596 | 2.063 |
| rogue | 7.561 | 7.613 | 7.587 | 7.544 | 7.564 | 7.596 | 7.578 |
**TABLE 3.** Euclidean distances of SS of legitimate BSs & A moving rogue bs.

| i  | 00:30 | 00:45 | 01:00 | 01:15 | 01:30 | 01:45 |
|----|-------|-------|-------|-------|-------|-------|
| 1  | 2.083 | 2.073 | 2.066 | 2.062 | 2.059 | 2.056 |
| 2  | 2.023 | 2.013 | 2.004 | 1.998 | 1.996 | 1.993 |
| 3  | 2.024 | 2.015 | 2.007 | 2.003 | 1.999 | 1.998 |
| 4  | 2.071 | 2.061 | 2.053 | 2.048 | 2.044 | 2.041 |
| 5  | 2.067 | 2.057 | 2.049 | 2.044 | 2.041 | 2.039 |
| 6  | 2.092 | 2.083 | 2.076 | 2.070 | 2.068 | 2.065 |
| rogue | 7.742 | 7.684 | 7.637 | 7.606 | 7.586 | 7.572 |
| Average distance | 2.872 | 2.855 | 2.842 | 2.833 | 2.828 | 2.823 |

Euclidean distances between every BS around 00:30 a.m. are calculated and listed as Table 3.

At this time, the average Euclidean distance of SS of all BSs is 2.842, and 5.684 can be set as the neighborhood radius $E_{ps}$. The rogue BS 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 the moving rogue BS declines and will be smaller than the strongest SS of the legitimate BS. After 2:00, it declines to −180dB again.

**C. OUTAGE OF A LEGITIMATE BS**

When a legitimate BS falls outage, meter collectors connected with it should seamlessly attach to another one without difficulty. Specifically, a legitimate BS #1 with highest SS falls outage at 10:00 a.m. and restores at 13:00 as shown in Fig.9. Then the average Euclidean distances between every BS at 10:00 are calculated and listed as Table 3. Note that the mean of the all average Euclidean distance is 1.013 at that time and 2.026 can be utilized as neighborhood radius $E_{ps}$. Since there is not any rogue BS with large Euclidean distance, the meter collector can seamlessly hand over from BS #1 to BS #2, SS of which is second to that of BS #1. Even if BS #1 restores at 13:00, meter collectors will not connect to it for its dramatic variation of SS. Whereas, meter collectors could connect to it after the 24-hour time window.

**V. CONCLUSION**

To secure the communication between meter collectors and BSs, a rogue BSs detection approach for AMI based on SS clustering is proposed in this paper. Since rogue BS is characterized by its abrupt variation in SS profile, the variation of SS profile in a 24-hour time window is clustered with DBSCAN to identify the rogue BS. Numerical simulation indicates that the proposed approach can identify both stationary and moving rogue BSs out effectively. Since DBSCAN related computation load is slight, the proposed approach can be implemented in existing meter collectors with limited computation resource and no retrofit on other parts of AMI is required.

Lastly, it should be pointed out that the proposed approach works within 24-hour-time window. If a rogue BS attacks a meter collector for more than a day, the meter collector will attach to the rogue BS and it would be in great danger.

**REFERENCES**

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, “Smart grid technologies: Communication technologies and standards,” *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[2] Z. Yang, R. Han, Y. Chen, and X. Wang, “Green-RPL: An energy-efficient protocol for cognitive radio enabled AMI network in smart grid,” *IEEE Access*, vol. 6, pp. 18335–18344, 2018.
H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee Security Analysis of an Advanced Metering Infrastructure," Int. J. Crit. Infrastructure Protection, vol. 18, pp. 3–19, Sep. 2017.

S. Keemink and B. Roos, "Security Analysis of Dutch Smart Metering Systems," Univerd Amsterd Amst Amst, The Nethemis, Tech. Rep., Jul. 2008.

H. He and J. Yan, “Cyber-physical attacks and defenses in the smart grid: A survey,” IET Cyber-Phys. Syst., Theory Appl., vol. 1, no. 1, pp. 13–27, Dec. 2016.

S. Liu, S. You, H. Yin, Z. Lin, Y. Liu, W. Yao, and L. Sundaresh, “Model-Free Data Authentication for Cyber Security in Power Systems,” IEEE Trans. Smart Grid, early access, Apr. 8, 2020, doi: 10.1109/TSG.2020.2986704.

R. Ullah, Y. Faheem, and B.-S. Kim, “Energy and Congestion-Aware Routing Metric for Smart Grid AMI Networks in Smart City,” IEEE Access, vol. 5, pp. 13799–13810, 2017.

V. Namboodiri, V. Aravinth, S. N. Mopahatta, B. Karimi, and W. Jewell, “Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids,” IEEE Syst. J., vol. 8, no. 2, pp. 509–520, Jun. 2014.

S. Finster and L. Baumgart, “Privacy-Aware Smart Metering: A Survey,” IEEE Commun. Surveys Tuts., vol. 17, no. 2, pp. 1088–1101, 2nd Quart., 2015.

Y. Guo, C.-W. Ten, S. Hu, and W. W. Weaver, “Preventive Maintenance for Advanced Metering Infrastructure Against Malware Propagation,” IEEE Trans. Smart Grid, vol. 7, no. 3, pp. 1314–1328, May 2016.

S. Soltani, P. Mittal, and H. V. Poor, “BlackIoT: IoT botnet of high wattage devices can disrupt the power grid,” in Proc. 27th USENIX Secur. Symp., Baltimore, MD, USA, Aug. 2018, pp. 1–19.

H. J. Patel, M. A. Temple, and R. O. Baldwin, “Improving ZigBee Device Network Authentication Using Ensemble Decision Tree Classifiers with Frequency Distinct Native Attribute Fingerprinting,” IEEE Trans. Rel., vol. 64, no. 1, pp. 221–233, Mar. 2015.

A. Chouchane, S. Rekhis, and N. Boudriga, “Defending against rogue base station attacks using wavelet based fingerprinting,” in Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl., Rabat, Mar. 2009, pp. 523–530.

C.-M. Chen, Y.-H. Chen, Y.-H. Lin, H.-M. Sun, “Eliminating rogue femtocells based on distance bounding protocol and geographic information,” Expert Syst. Appl., vol. 41, no. 2, pp. 426–433, 2014.

A. Al Mazrooa and M. Arozulillah, “Detection and Remediation of Attack by Fake Base Stations in LTE Networks,” Int. J. Soft Comput. Eng., vol. 5, no. 2, pp. 12–15, May 2015.

Z. Haddad, M. Mahmoud, S. Taha, and I. A. Saroti, “Secure and Privacy-Preserving AMI-Utility Communications via LTE-A Networks,” in Proc. IEEE 11th Int. Conf. Wireless Mobile Commun. Netw. Commun. (WMoN), Abu Dhabi, United Arab Emirates, Oct. 2015, pp. 748–755.

U. Seetha and P. Sharma, “Meter Data Acquisition System in Power Utilities,” J. Innov. Res. Sci., Eng. Technol., vol. 2, no. 4, pp. 970–972, Apr. 2013.

X. Liu, P. Zhu, Y. Zhang, and K. Chen, “A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure,” IEEE Trans. Smart Grid, vol. 6, no. 5, pp. 2435–2443, Sep. 2015.

M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, “Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study,” IEEE Syst. J., vol. 9, no. 1, pp. 31–44, Mar. 2015.

M. G. Jaatun, I. A. Tondel, and G. M. Koenig, “GPRS Security for Smart Meters,” in Proc. 1st Cross-Domain Conf. Workshop Availability, Rel., Secur. Inf. Syst. (CD-ARES), in Lecture Notes in Computer Science, vol. 8127, A. Cuzzocrea, C. Kittl, D. E. Simos, E. Weippl, and L. Xu, Eds. Regensburg, Germany: Springer, Sep. 2013, pp. 195–207.

C. Xenakis, “Malicious Actions Against the GPRS Technology,” J. Comput. Virol., vol. 2, no. 2, pp. 121–133, Aug. 2006.

S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, “LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE,” in Proc. Netw. Distrib. Syst. Secur. Symp., Feb. 2018, pp. 1–15.

D. Rupprecht, K. Kohls, T. Holz, and C. Popper, “Breaking LTE on Layer Two,” in Proc. IEEE Symp. Secure Privacy, May 2019, pp. 1121–1136.

China Daily. (2019). Strict Crackdown on Telecommunication Fraud Coming. [Online]. Available: http://english.chinadaily.com.cn/2019/03/14/content_27450221.htm

B. Jiang, J. Pei, Y. Tao, and X. Lin, “Clustering uncertain data based on probability distribution similarity,” IEEE Trans. Knowl. Data Eng., vol. 25, no. 4, pp. 751–763, Apr. 2013.

J. Lu and Q. Zhu, “An effective algorithm based on density clustering framework,” IEEE Access, vol. 5, pp. 4991–5000, 2017.

China Court. Characteristics of the Existing of Rogue Base Station Crime and Related Recommendations. [in Chinese]. [Online]. Available: https://www.chinacourt.org/article/detail/2017/03/id/2573259.shtml

Qian Bin was born in Xiangyang, Hubei, China, in 1989. He received the B.E. and M.S. degrees in electrical engineering from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 2011 and 2014, respectively. He is currently a Research Scientist with the Electric Power Research Institute (EPRI), China Southern Power Grid, Guangzhou, China. His research interest includes big data analysis and cyber security defense of AMI.

Cai Ziwen was born in Jieyang, China, in 1991. He received the B.S. degree in electronic engineering from Hunan University, Changsha, China, in 2014, and the M.S. degree in electronic engineering from the South China University of Technology, Guangzhou, China, in 2017. He is currently a Research Scientist with EPRI, China Southern Power Grid, Guangzhou. His research interests include big data analysis of AMI and cyber security defense of AMI.

Xiao Yong received the B.S. degree in electronic engineering and the M.S. degree in computer science from the University of Electronic Science and Technology of China, Chengdu, China, in 2002 and 2005, respectively. From 2005 to 2012, he was a Research Scientist with the Electric Power Research Institute (EPRI), Guangdong Southern Power Grid, Guangzhou, China. He is currently with EPRI, China Southern Power Grid, Guangzhou. His research interests include data mining of AMI and cyber security defense.

Hong Liang received the B.S. degree in electrical engineering from Jishou University, Jishou, China, in 2017. He is currently pursuing the M.S. degree in electrical engineering with the Changsha University of Science and Technology (CSUST), Changsha, China. His research interests include big data application of AMI and cyber security defense of AMI.

Su Sheng (Senior Member, IEEE) received the B.S. degree in electrical engineering from the Wuhan University of Hydraulic and Electrical Engineering, Wuhan, China, in 1998, the M.S. degree in electrical engineering from Wuhan University, Wuhan, in 2002, and the Ph.D. degree from HUST, Wuhan, in 2009. He joined CSUST, Changsha, China, in 2002. From 2004 to 2007, he was a Research Assistant with The Hong Kong Polytechnic University, Hong Kong. From 2009 to 2012, he held a postdoctoral position at the Department of Automatic Control Engineering, HUST, Wuhan. He is currently a Professor with CSUST, Changsha, China. His research interests include the cyber security defense of power systems and application of power system big data. He was a recipient of the Outstanding Doctoral Thesis Award at Hubei province.