Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 02
Pages: 60-67
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.2.001

Optimal Wireless Smart Grid Networks Using Duo Attack Strategy

Dr. S. Smys,
Department of CSE,
RVS Technical Campus,
Coimbatore, India.
Email id: smys375@gmail.com

Dr. Haoxiang Wang,
Department of Electrical and Computer Engineering,
Cornell University, Ithaca, USA.
Email: wanghaoxiang1102@hotmail.com

Abstract: The Smart Grid Network (SGN) is one of the fastest developing technology and has been widely used because of its high performance, in power governance system and current power supply industry. The restriction over wired infrastructure has been overcome because of Wireless Smart Grid Networks (WSGN) which offers the best solution for power management. The most commonly used wireless networking approaches used is the Cognitive Radio Network (CRN). However, when the WSGN approach used is CRN, there is a lot of concern over communication security. The major attaches faced are fended using spoofing and hamming in CRN. The proposed work using optimal power distribution in order to fence off spoofing and jamming known as Maximum Attacking Strategy. Both jamming and spoofing will be able to interfere with many signal channels in order to ensure proper functioning of the channels. The attack strategy proposed in our work uses Duo-Attack using Jamming and Spoofing to evaluate the experiment and record the observations.

Keywords: Cognitive Radio Network, Wireless Smart Grid Networks, Spoofing, Jamming

1. Introduction

The introduction of smart grid technology has paved way to this flexible solution in order to reach their goals like scalable power offerings, high performance services and green systems. However, there are many approaches used in Smart Grid Network (SGN) for communication and one of the best used approaches is that of Wireless Smart Grid Network (WSGN) [1]. To take the best use of Cognitive Radio Networks (CRN), so that it gives higher security level using advanced wireless solution [2]. To some amount, spoofing and jamming attacks can be used to prevented unwanted interruptions by programmed CRN system. Depending on the level of the potential threat, the Dynamic Spectrum Access (DSA) can be used to protect the system. However, these approaches cannot prevent wireless communication. Hence we propose a novel attack method using CRN in WSGN, that makes use of spoofing and jamming in order to obstruct a simple wireless communication [3]. We have named the Attacking Strategy as Duo-Attack using Jamming and Spoofing which denotes the combination of methods used. This method of approach used is based on the power required for the two attacks will vary based on the frequency used. An optimal power distribution solution is hence used in our proposed work so that the frequency scope of the attack can be maximized. An illustration of the proposed methodology along with the attacking criteria are described in figure Fig. 1. It is observed that the power

ISSN: 2582-3051

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 02
Pages: 60-67
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.2.001

users are connected to the power sources using WCRN as the medium. It is at the spectrum sensing stage that the most important attack operation takes place. Hence this is the place where spoofing and jamming can be used to intrude the system. In [4] and [5], some innovative approaches have been recorded addressing the issue. However, the drawback with their work is the power limitation which restricts the performance of the system.

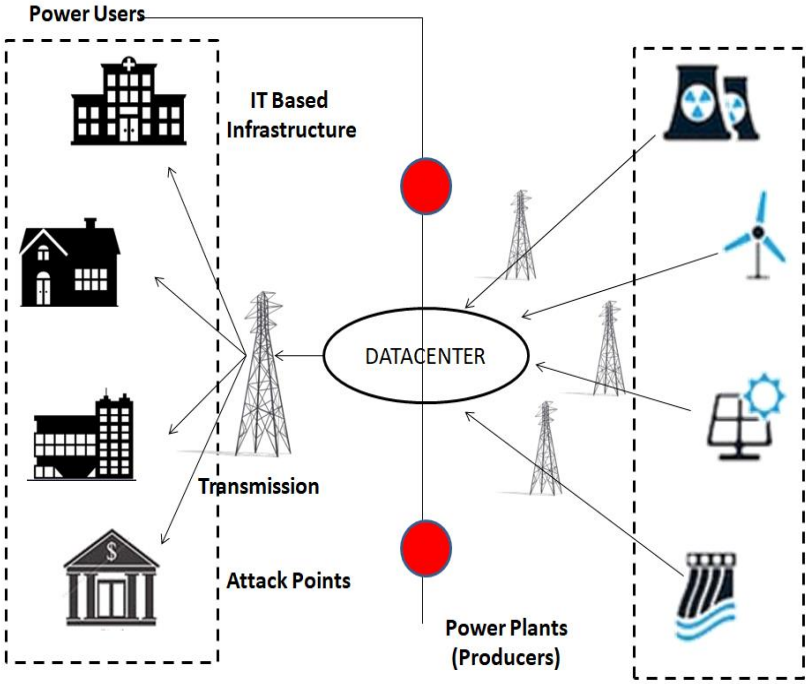


Fig.1. Structure of Duo Attack Strategy

In this paper, we have addressed CRN attack issue using optimal power distribution which is focused on using spectrum adversarial occupations to improve the attack strength. To attain optimum power usage, jamming and spoofing attacks are switched and used dynamically. The secondary users [6] and primary users are the CRN users and our attacking strategy targets the secondary users by attacking them and decreasing the spectrum availability, thereby affecting the transmission performers. There are two main contributions implemented in this work:

- We solve the power distribution optimal problem using dynamic programming
- We propose a novel attack method using CRN in WSGN, that makes use of spoofing and jamming in order to obstruct a simple wireless communication. It takes into account both success probabilities as well as attack return values where there is restriction on power availability.

The paper is organised into the following sections:

ISSN: 2582-3051

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 02
Pages: 60-67
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.2.001

- Section 2 outlines related work and survey of similar approaches.
- Section 3 represents the concept and implementation of the proposed work.
- Section 4 gives a detailed look into the problem addressed and solutions identified while Section 5 illustrates experimental results
- Section 6 concludes the proposed work.

2. Related Works

One of the biggest targets for adversaries are the wireless connections since they rely largely on control signal deliveries during the initiation of IP-based infrastructure resulting in cyber attacks. In general a proper attack will hold both spoofing as well as jamming. However, there have been many research on these two methods and observations show that they work on different frequency spectrums, based on the power used. Spoofing is the process of using fraudulent data within the transmission to give the wrong information over the WSGN system thereby hindering grid control [7]. Jamming is a means of blocking data from being transmitted or intervening in the different channels between signal receiver and sender. When spoofing and jamming attacks take place, the grid operator will be forced to make use of previous data for estimation and analysis purpose. Phasor Measurement Units are used to collect data over the grid and are easily prone to be attacked easily over WSGN. They are used in order to synchronize real-time data [9]. One of the basic requirement for PMU is the collection of data which is essential for evaluating the next WSGN condition and also the system operations and adjustments [10]. Because of wide distribution of grid points and signal senders, defending spoofing and jamming becomes difficult. As an alternative to this, other adversarial approaches have been used to interrupt communications of WSGN such that the overall smart grids performance reduces significantly [11].On the other hand, many researchers have tackled both spoofing and jamming attacks in prior research using many technologies like cognitive radio networks and vehicular networks [13]. In [12] Pei et al observed an external helper for passive eavesdropping and a multi-antenna wire tapped channels. The methodology we have proposed works on two attacks with a power constraint. Moreover, multiple frequency spectrum are also examined in our work. In recent trends, game theory has also been explored for jamming defences and attacks in [8]. The proposed work takes into consideration power constraint instead of the attacks' state analysis resulting in a novel standpoint of adversarial behaviour.

3. Proposed Work

The inputs of the proposed problem definition is made of many parameters such as jamming attack manner (J), attack success probability (P_w), power constraint to a certain level $p(P_w)$, individual frequency (F_i), number of spectrum (N) and spoofing attack manner (S). The output of the work is a well-planned attack strategy. The problem defined proposes finding the best power distribution plan for optimal effect of the attack. We have considered constraint configurations, return values and power costs for spoofing and jamming attacks representing a cluster of variables. A number of frequency spectrums are considered for the attacks. There are two sets of data needed for this process.

ISSN: 2582-3051

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 02
Pages: 60-67
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.2.001

- First, we need to hold parameter data which comprises of the value weight used at a particular power level P_w for the attacker method along with the likelihood of success.
- Second, based on the power constraints that are pre-configured, we will also require the return value and likelihood attainment in alignment with P_w.

Spoofing and Jamming are the attack methodologies chosen such that it formulates into an attack strategy plan which identifies the attack method used in the different frequency spectrum based on spoofing and jamming. Return values or probability can be used to estimate the attack effect and Figure Fig.2 outlines the principles of spoofing and jamming in CRN. It is observed that different frequencies are occupied by different power levels. Here the cube height portrays power level needed for adversaries and represent the spectrums that are being used. The difference in power used can be observed from the difference in heights between the cubes. Under power constrain, CRN faces the vulnerability of periodic sensing wherein spectrums are searched for availability by the secondary users.

$$Max\ [Vw_{total}, Pr_{total}] = Max\ [\sum_{b(i)} Vw(i), \prod_{b(i)} \Pr\ (i)] \quad (1)$$

$$\sum_{b(i)} Vw(i) = \sum_{b(i)=0} Vw(i) + \sum_{b(i)=1} Vw(i) \quad (2)$$

$$\prod_{b(i)} \Pr\ (i)] = \prod_{b(i)=0} \Pr\ (i)\ X\ \prod_{b(i)=1} \Pr\ (i) \quad (3)$$

Where Pr_{total} is the production of probabilities and Vw_{total} is the total attack return value.

Moreover, the proposed work aims to identify the optimal power Pw at a fixed level when it is possible to get the optimal adversarial plan. Equation (1) represents the total return value which is to be considered such that the aim is to find the maximum of the two function within the boundary conditions such that b(i)=0 when spoofing attack is applied and '1' when Jack attack is applied, for a particular power constraint. Here Vw_{total} denotes the total attack return value. To obtain the optimum attack performance, our work uses switching of the attack methods dynamically.

4. Algorithm Used

4.1 Algorithm 1

A D-table is built with the help of the first algorithm such that it represents the range of Vw and Pr values with constraint on power, for every spectrum. In the table, a list of all the possible optimal values for Pr and Vw are predicted, laying out an attack strategy plan. Based on the preferences of the attack, we can choose the best solution which will serve as an optimum attack strategy. The major stages of the proposed algorithm are:

- A set of input is fed from the Basic Table where each input is associated with a particular frequency spectrum and power constraint. Initially, the first frequency of the list of frequency spectrum is used as the first entry in the data sheet.

ISSN: 2582-3051

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 02
Pages: 60-67
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.2.001

- Based on the power constraints set for the frequency spectrums, the values of the calculated pairs are added to the table. The unnecessary pairs are removed using Algorithm 2 such that only the optimal solutions are present for access.
- The second step is repeated for frequency spectrums along with the optimal solution in order to form the D-Table. In the D-Table, every band of frequency spectrum is represented as a row.
- Back Forward methodology is used to produce the right optimal solution.

Algorithm 1:

Requirement: Table B
Result: Table D

1: Begin
2: $D_{1,j} < - B_{i,j}$
3: for F_i, i>do
4: for power j do
5: for Power k in $B_{i,k}$ do
6: if $D_{i-1, j-k}$!= null, then
7: $D_{i,j} = D_{i-1, j-k} . B_{i,k}$
8. end if
9: Algorithm 2
10: end for
11:Return Table

4.2 Algorithm 2

Redundant pair can be removed using Algorithm 2 where $V_{i,j}^k, P_{i,j}^k$ are the input values. The output values will hold only the optimal solutions. Moreover Algorithm 2 is a part of Algorithm 1 and the former's output will be used by the latter. The basic mechanism deals with comparison of the pairs and removal of the unnecessary pairs in the D-Table. Then assessment of return values and probability functions are made. For example, if P2=P3 and V2>V3, then from the table, (P3,V3) will be removed.

Algorithm 2:

Requirement: List of values for $V_{i,j}^k, P_{i,j}^k$
Result: A new list with unnecessary pairs removed

1: In ascending order sort the list using $P_{i,j}^k$
2: Length-1 Is applied when k=1

ISSN: 2582-3051

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 02
Pages: 60-67
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.2.001

3: If $P_{i,j}^{k} = P_{i,j}^{k+1}$
4: Then, if $V_{i,j}^{k} \leq V_{i,j}^{k+1}$
5: Drop $V_{i,j}^{k}, P_{i,j}^{k}$
6: Else if then
7: Drop $V_{i,j}^{k+1}, P_{i,j}^{k+1}$
8. end if
9: end if
10: end if
11:Return L'

The following section outlines the main findings and experimental evaluation of our proposed work.

5. Results and Discussion

Based on the experimental analysis of the proposed method and comparison with other similar strategies, it is found that the proposed attack strategy has better performance when compared with the other strategies. It was found that the average return values of the proposed methodology is 1.52 times greater than spoofing, 1.73 times greater than jamming and 1.2 times greater than GMixed. In Fig.2, it is clear that the return attack values using the proposed methodology is 51% greater than spoofing, 56% greater than jamming and 11% times greater than GMixed. Fig.3 shows a comparative study of the other attack strategies and also represents the return values of attack when the frequency spectrums decreases.

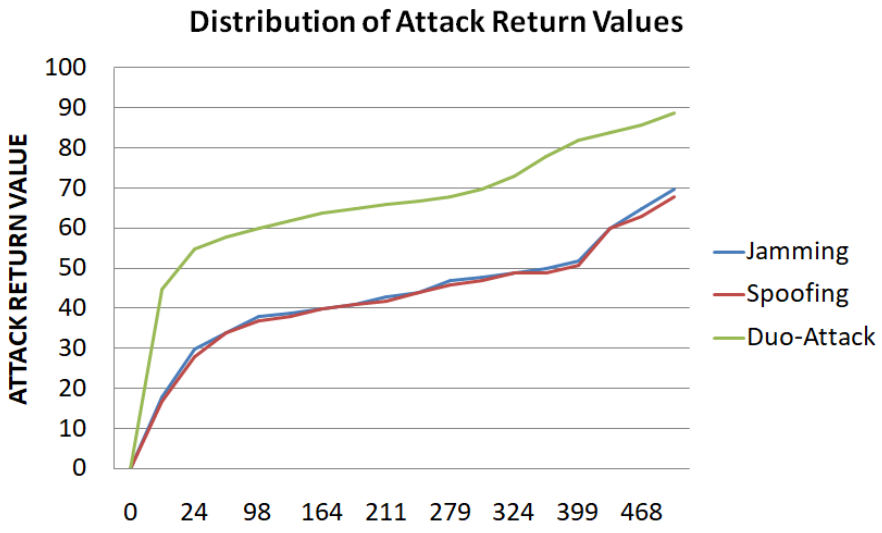
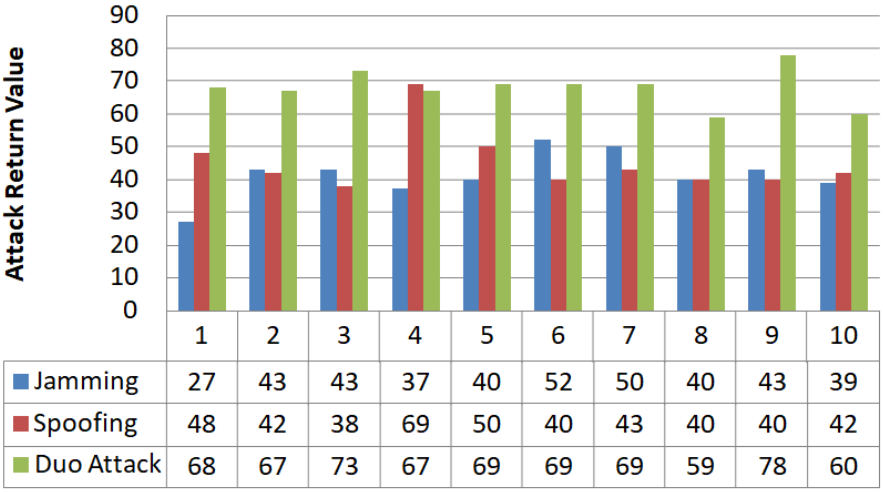


Fig.2. Distribution of return attacks

ISSN: 2582-3051

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 02
Pages: 60-67
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.2.001



	1	2	3	4	5	6	7	8	9	10
Jamming	27	43	43	37	40	52	50	40	43	39
Spoofing	48	42	38	69	50	40	43	40	40	42
Duo Attack	68	67	73	67	69	69	69	59	78	60

Fig. 3. Attack return values for Duo Attack Vs Jamming and Spoofing

6. Conclusion

In this paper we propose the use of spoofing and jamming attack strategies. In the WSGN, a distributed power system approach is used through dynamic programming. Two important algorithms are also proposed which will support the attacking strategy. The results of the experiment are analysed, evaluated and assessed leading to the conclusion that it offers better performance when compared with the other approaches that are in use today. Though there are many innovative technological advancement in transmitting data over WSGN, the proposed work proves to have better performance when compared with the commonly used Spoofing and Jamming.

References

[1] B. Fateh, M. Govindarasu, and V. Ajjarapu. Wireless network design for transmission line monitoring in smart grid. IEEE Transactions on Smart Grid, 4(2):1076–1086, 2013.

[2] J. Huang, H. Wang, Y. Qian, and C. Wang. Priority-based traffic scheduling and utility optimization for cognitive radio communication infrastructure-based smart grid. IEEE Trans. on SG, 4(1):78–86, 2013.

[3] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li. Time synchronization attack in smart grid: Impact and analysis. IEEE Transactions on Smart Grid, 4(1):87–98, 2013.

[4] Q. Peng, P. Cosman, and L. Milstein. Tradeoff between spoofing and jamming a cognitive radio. In Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, pages 25– 29, Pacific Grove, California, 2009. IEEE.

[5] K. Gai, L. Qiu, M. Chen, H. Zhao, and M. Qiu. SA-EAST: securityaware efficient data transmission for ITS in mobile heterogeneous cloud computing. ACM Transactions on Embedded Computing Systems, 16(2):60, 2017.

ISSN: 2582-3051

Journal of Electrical Engineering and Automation (EEA) (2020)
Vol.02/ No. 02
Pages: 60-67
https://www.irojournals.com/iroeea
DOI: https://doi.org/10.36548/jeea.2020.2.001

[6] Y. Fan, Z. Zhang, M. Trinkle, A. Dimitrovski, J. Song, and H. Li. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids. IEEE Trans. on SG, 6(6):2659–2668, 2015.

[7] Y. Wang, T. Gamage, and C. Hauser. Security implications of transport layer protocols in power grid synchrophasor data communication. IEEE Transactions on Smart Grid, 7(2):807–816, 2016.

[8] K. Gai, M. Qiu, H. Zhao, and J. Xiong. Privacy-aware adaptive data encryption strategy of big data in cloud computing. In 3rd Int'l Conf. on Cyber Sec. and Cloud Computing, pages 273–278. IEEE, 2016.

[9] L. Xiao, J. Liu, Q. Li, N. Mandayam, and V. Poor. User-centric view of jamming games in cognitive radio networks. IEEE Transactions on Information Forensics and Security, 10(12):2578–2590, 2015.

[10] J. Ma, Y. Liu, L. Song, and Z. Han. Multiact dynamic game strategy for jamming attack in electricity market. IEEE Transactions on Smart Grid, 6(5):2273–2282, 2015.

[11] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. Yang. Role-dependent privacy preservation for secure V2G networks in the smart grid. IEEE Trans. on Information Forensics and Security, 9(2):208–220, 2014.

[12] N. Zhang, N. Lu, N. Cheng, J. Mark, and X. Shen. Cooperative spectrum access towards secure information transfer for CRNs. IEEE J. on Selected Areas in Comm., 31(11):2453–2464, 2013.

[13] M. Pei, A. Swindlehurst, D. Ma, and J. Wei. Adaptive limited feedback for MISO wiretap channels with cooperative jamming. IEEE Transactions on Signal Processing, 62(4):993–1004, 2014.

Biography

Dr. S. Smys received his M.E and Ph.D degrees all in Wireless Communication and Networking from Anna University and Karunya University, India. His main area of research activity is localization and routing architecture in wireless networks. He serves as Associate Editor of Computers and Electrical Engineering (C&EE) Journal, Elsevier and Guest Editor of MONET Journal, Springer. He is served as a reviewer for IET, Springer, Inderscience and Elsevier journals. He has published many research articles in refereed journals and IEEE conferences. He has been the General chair, Session Chair, TPC Chair and Panelist in several conferences. He is member of IEEE and senior member of IACSIT wireless research group. He has been serving as Organizing Chair and Program Chair of several International conferences, and in the Program Committees of several International conferences. Currently he is working as a professor in the Department of Computer Science at RVS Technical Campus, Coimbatore, India.

Dr. Haoxiang Wang, works as professor in the Department of Electrical and Computer Engineering, in Cornell University, in Ithaca, USA. His research area includes Power electronics, instrumentation, electrical machines and drives, smart grids, power sources, renewable energy, intelligent systems, automation, control theory, circuits and systems, power systems, EHV, electric machines.

ISSN: 2582-3051