Hen maternal care inspired optimization framework for attack detection in wireless smart grid network

Narmadha Ganesamoorthy[1], B. Sakthivel[2], Deivasigamani Subbramania[3], K. Balasubadra[4]
[1]Department of Electrical and Electronics Engineering, Sethu Institute of Technology, Virudhunagar, India
[2]Department of Electronics and Communication Engineering, Pandian Saraswathi Yadav Engineering College, Sivagangai, India
[3]Faculty of Engineering, Technology and Built Environment, UCSI University, Kuala Lumpur, Malaysia
[4]Department of Information Technology, RMD Engineering College, Chennai, India

Article Info

Article history:

Received Jul 28, 2022
Revised Jun 8 2023
Accepted Jun 13, 2023

Keywords:

HMCO
Jamming attack
Network security
Optimization
Smart distribution grid
Smart grid

ABSTRACT

In the power grid, communication networks play an important role in exchanging smart grid-based information. In contrast to wired communication, wireless communication offers many benefits in terms of easy setup connections and low-cost high-speed links. Conversely, wireless communications are commonly more vulnerable to security threats than wired ones. All power equipment devices and appliances in the smart distribution grid (SDG) are communicated through wireless networks only. Most security research focuses on keeping the SDG network from different types of attacks. The denial-of-service (DoS) attack is consuming more energy in the network leads to a permanent breakdown of memory. This work proposes a new metaheuristic optimization inspired by maternal care of hen to their children called hen maternal care (HMCO) inspired optimization. The HMCO algorithm mimics the care shown by hen for their children in nature. The mother hen is always watchful and protects its chicks against predators. All chickens utilize different calls to designate flying predators like falcons and owls from ground seekers like foxes and coyotes, showing that they can both survey a danger and advise different chickens how to set themselves up. Our method shows greater performance among other standard algorithms.

Corresponding Author:

Narmadha Ganesamoorthy
Department of Electrical and Electronics Engineering, Sethu Institute of Technology
Virudhunagar, India
Email: gnarmadhame@gmail.com

1. INTRODUCTION

Wireless communication technology is used in smart grids for various applications like generation monitoring, fault detection and metering [1]. It is an essential part of the smart grid to interconnect customers with minimized cost. The problems in a wired network like installation cost etc, are effectively overcome by wireless communication. But it is vulnerable to security attacks due to its wireless transfer nature of data in a network like jamming attacks, selfish attacks, and block hole attacks [2], [3].

As shown in Figure 1 wireless medium in the smart grid interconnects power generating sources and customers. In the spectrum sensing stage attackers get chances to intrude a system by jamming or spoofing attacks [4]. In Figure 1 grey color circle denotes attack points when connecting data centres to power users and power generating units.

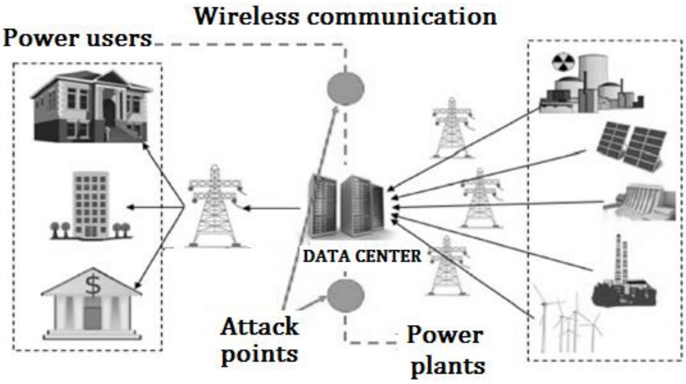

Figure 1. Structure of grid and attacking points

When compared to the other attacks, a jamming attack causes a major impact on a network. It blocks the data from the source to a destination point by generating higher strength signal to corrupt the original data. There are four types of jamming attacks: constant jamming, deceptive jamming, reactive jamming, random jamming [5], [6].

The conventional security algorithms of third-party authentication and cryptography techniques are not suitable for smart grid communication due to their low bandwidth limitations. By considering the network security in the sensing device group network (SDGN), a novel and innovative meta heusterics algorithm of hen's maternal care optimization (HMCO) is developed with the maternal behavior of hen from the predators. This algorithm is developed by studying the biological behavior of the hen which saves the chick with the high attacking potential against the predators. Similarly, on absorbing this behavior of hen, the wireless security of SDGN can be optimized against the jamming attacks to achieve high security in it [7], [8].

The rest of the paper is organized as follows. In section 2 explores related works of anti-jamming in wireless sensor network (WSN) and optimization in WSN. In section 3 explains the biological behavior of hen's maternal care. In section 4 depicts the proposed algorithm of HMCO and section 5 gives the simulation results and the paper is concluded with section 6.

2. LITERATURE REVIEW

Various works have been focusing on outlining the different jamming techniques for corrupting the network throughput and the relating countermeasures. For instance, Tanveer *et al.* [9] addressed four types of basic jamming attacks, containing the constant jammer, the random jammer, the deceptive jammer and the active jammer. Ahmed *et al.* [10] proposed a learning-based jamming attack detection by introducing the learning and attacking phase in attack detection with energy constraint. Mustafa *et al.* [11] authors presented a centralized Availability History Vectors based algorithm to select fault-independent routing paths, and a distributed routing protocol for the effective overcoming of jamming attack impact. D'Oro *et al*. [12] proposed a performance-aware online greedy algorithm and problem decomposition method to provide low-complexity cooperative power control and user scheduling problem under minimum quality-of-service requirements for jamming attack. Zhang *et al.* [13] proposed a jamming-resilient secure neighbor discovery scheme for mobile ad-hoc networks (MANETs) based on direct sequence spread spectrum and random spread-code pre-distribution. It enables neighboring nodes to securely recognize each other even in the presence of jamming nodes. Wang *et al.* [14], the two-player asymmetric zero-sum game based jamming attack prevention has been proposed. D'Oro *et al.* [15] proposed a game-theoretic model for the interactions of a jammer and a communication node that exploits a timing channel to increase resilience to jamming attacks.

Various evolutionary and swarm intelligence optimization algorithms have been proposed to solve real-world problems. Meta heuristic algorithms are inspired by the nature or behavior of animals in daily life. The examples of such methods are ant colony optimization (ACO) [16], [17], bat algorithm [18], and particle swarm optimization (PSO) [19], [20]. The hybrid optimization algorithms are proposed by combining genetic algorithms (GA) and PSO to solve the optimization problems [21], [22]. Hu *et al.* [23] gave three ACO algorithms namely the ant system (AS), ant colony system and enhanced AS along with their usage in the WSN routing process Chicken swarm optimization (CSO) is bio-inspired meta heuristic optimization algorithm proposed by Chen *et al.* [24]. The algorithm mimics the hierarchal order of a chicken swarm and the behaviors of its individual's chickens. Hafez *et al.* [25] proposed an l triangular mutation based on PSO with attack detection ADOV techniques for attack detection in a network. It is used as a PSO to maintain the average data packet drop ratio in particular for overall network. Tague *et al.* [26] applied an elephant herd optimization (EHO) algorithm for network intrusion detection. In order to increase the accuracy of attack detection, EHO based feature selection is used to delete irrelevant feature data. Punal *et al.* [27] used the chicken swarm optimization technique for feature selection in data mining applications. Chiang and Hu [28] used an artificial bee colony algorithm and or-opt algorithm to identify the best effort routing path in terms of attacker free and increased lifetime.

3. BIOLOGICAL BEHAVIOR OF HEN'S MATERNAL CARE

Being precocial classes, hatchlings are free to move and feed in independence shortly after hatching. The chicks are hatched by artificial incubation in large groups, without a mother hen and these kinds of characteristics are consumed for profitable egg and meat production. Though at the stage of this precocial, motherly contact ranges for 5-12 weeks indeed [29]. At this stage, the provision of protective care strongly and fruitfully impacts the social growth of chicks. An artificial nurturing of hatchlings may lead to hostile and long-living welfare concerns of the chicks.

3.1. Role of maternal care

Mother hens have an important part in directing their chick's behaviour and have an ability to safeguard their chick's reaction to stressors. A mother hen is a key to directing the chick's behaviour and allowing chicks to improve food partialities. With the rearing of a mother hen, the chicks are minimum fearful and show a superior level of behavioral synchronization than the chicks reared artificially.

3.2. Flow of hen's maternal care

- Imprinting
- Communication between mother and chick
- Teaching
- Behavioral synchronization
- Mediating the chicks fear and stress response

These are the steps in which hens cared for their chicks, to increase the knowledge and the safety of its chicks. On considering the safety of chicks, the mother hen follows some procedure for the prevention and alertness of chick. Some of the behaviors of hen towards its chicks are given below:

3.3. Pre-hatching communication

Even before the day of hatching of the egg, mother hen and the chick started to pass on information. If the chick gives out calls for help, the mother hen voices or moves near to the shell. Only after observing these moves of its mother, an unhatched or unborn chick become silent or else it starts to give out pleasure calls. After hatching, the bird may easily identify its mother hen due to these voices given before hatching.

3.4. Maternal attraction and alarm calls

The mother hen uses attraction or alarm calls to instill various vocalizations to the chick for its instructions [30]. In order to interconnect its chicks and help to maintain the family unit, it employs three various calls like roosting calls, maternal cluck calls and feeding calls, which are the primary ways of maternal vocalization [31]. The roosting calls are the calls that are classified by long humming sounds with rhythm, are used to charm the chicks to rest under their mother at night time. The maternal cluck calls are employed by the mother hen which attracts and maintains the family as a unit. It is slow and rhythmic in nature. The mother hen repeats these behaviors for the whole day to habituate the chicks, but this increases the anxiety of chicks. Due to its higher volume and frequency, the alarm calls are very much distinguished by the attraction calls [32]. Alarm calls are distinct for both aerial and ground predators, which helps the chick to prevent itself from some dangerous predators. Neither type of alarm calls has been shown to increase the memory formation in the chicks, unlike the attraction calls [33]-[36].

3.5. Maternal feeding behavior

The mother hen produces a shrill swift vocalization specifically along with pecking behavior, when it finds a food stuff. This peculiar pecking behavior of mother hen helps the little chicks by hastening them to feed on food, because the chicks tend to peck at eatable and non-eatable items by mistake. Any how by this behavior the chicks consequently learn by trial-and-error method. By creating the chick's pecking and attraction towards the hen, the maternal feeding makes easy of gaining adaptive seeking skills and also the knowledge of palatability to the chicks.

The maternal hen calls consisted of five specific vocalizations that are differed in terms of biological meaning and rhythmic quality: (a) a food call, (b) a follow-me call, (c) a roosting call, (d) a fear call, and (e) a predator call. Characteristics of the calls are summarized in Table 1.

Table 1. Characteristics of five maternal hen calls

	Characteristics of five maternal hen calls				
	Food call	Follow call	Roosting call	Predator call	Fear call
Attraction	Y	Y	Y	N	N
Alarm	N	N	N	Y	Y
Cyclic rhythm	Y	Y	N	Y	N
Food related	Y	N	N	N	N

4. PROPOSED HMCO ALGORITHM

In this paper, by using this HMCO optimization. It is easy to identify the different jamming attacks in SDG. The proposed method considers various metrics like packet delivery ratio (PDR) and received signal strength (RSSI) for the effective measurement and identification of jamming.

4.1. Hen care optimizer

There are many optimization techniques proposed so far, many of them are motivated by hunting and search behaviours. To the best of our knowledge, however, there is no technique in the literature that explains maternal care of hens to their baby chickens. This inspires our attempt to mathematically model the social behavior of mother hen for caring chickens, proposes a new algorithm inspired by a hen, and investigates its abilities in solving benchmark and real engineering problems.

Now, we can summarize the characteristics of hen's caring so as to develop the hen inspired algorithms. Now, we use the following rules:

- Hen's vocal volume intensity works as a function of distance from predators to chickens. The hen's volume intensity increases when the predator to chick distance decreases. Conversely, the volume intensity decreases when the predator to chick's distance increases.
- An observing factor (K) of hen is directly proportional to the distance between hen to chicks.
- The volume intensity is (I) affected by the landscape of the objective function. For optimization problems, and intensity can simply be proportional to the volume of an objective function.

The overall objective of hen's care is to find the best volume intensity level to maintain all the chickens in a particular boundary (by alarm call) and keep away the predators at a particular distance from chicks. Based on the above rules, the basic step for HMCO Algorithm 1 is summarized as the pseudo-code.

Algorithm 1. The basic step for HMCO algorithm is summarized as the pseudo-code

```
Objective function f(X) X = ($X_1$ … $X_n$) $^T$
Generate initial population of chicks $X_i$ where i = (1,2, …, n)
Volume (Alarm call) intensity $I_i$ at $X_i$ is determined by f($X_i$)
Define sound absorption coefficient γ
While (t < max generation)
For each chick
Update the predator and chick positions
Observing factor varies with the distance as exponential function
Update new volume intensity
End For
T = t + 1
end While
Return $I_i$
```

4.2. Observation factor

In the simplest form, volume intensity I (d) varies according to the distance between hen to chick and distance between predators to chick. For a given medium, absorption co-efficient ϒ, and volume intensity varies with distance (d). The combined effect of distance and absorption is approximated as gaussian form.

$$I(d) = I_0\, e^{-r}(d_1^2 + d_2^2) \quad (1)$$

or

$$I(d) = I_0\, e^{r\,(d_1^2 - d_2^2)} \quad (2)$$

observing factor K of mother hen is given as;

$$K(d) = K_0\, e^{\gamma(d_1^2 - d_2^2)}$$

where K_0 is observation factor at $d_2 = 0$
d_1 is the distance between hen to predator
d_2 is the distance between hen to chick

4.3. Movement of chicks

The distance between any chick and mother hen at X_i and X_m is a cartesian distance. $r_{ij} = \| X_i - X_m \|$. The movement of chick 'i' is to mother hen is determined by,

$$X_i = X_i + K_0 e^{-\gamma(d_1^2 - d_2^2)} + \alpha\,(r - 1/2) \tag{3}$$

where the second term due to observation factor at this term r is randomization. Where r is a random number with uniform distribution in [0,1].

5. SIMULATION RESULTS

Our proposed work detects jamming attack based on the parameters of packet delivery ratio and signal strength variation. Signal strength variation is denoted as (ΔS) and it is taken in dB. i.e., (ΔS) = *SS*observed-*Ss*network, where *SS*observed is signal strength variation in the presence of attack and *Ss*network is the signal strength without any jamming attack.

In the channel, the jamming pulse generates gaussian noise that can appear numerous times. In order to find the jamming attack N samples of channel's received energy s (t) are collected. Then, consecutive samples like s (k), s (k-1), s (k-N+1) taken to find jamming attack by using the (4),

$$T_{(k)} = \left(\frac{\sum_{j=k-N+}^{k} {}_{1}(s(j)^2}{N} \right) \tag{4}$$

In the (4), T(k) represents the average jamming pulse used to find out jamming attack by comparing with the threshold value δ. In order to avoid false detection, rate the threshold δ is calculated carefully. The factors collected by the detector in a given sample window of time for detecting the jamming attack and its types are as follows: (1) packet delivery ratio, (2) network allocation vector (NAV) of each packet transmission, (3) signal strength variation (ΔS), and (4) pulse width (PW) value (the time for which (ΔS) is greater than (T) threshold value).

By using MATLAB simulation, a network of 250*250m^2 is created with random deployment. The performance of the proposed method analyzed the parameters of end-to-end delay, packet delivery ratio, detection ratio and false-positive probability. The detection ratio of a method is defined as the ratio of the number of correctly recognized jammer nodes. The false-positive probability of the method defined the ratio of the misidentified nodes overall jammer nodes.

The performance of our proposed HMCO detection method is analyzed and compared with the conventional algorithms of ACO and PSO. We created the four types of jammers in the network: Constant jammer, deceptive jammer, random jammer and reactive jammer. The performance of delay, detection rate is analyzed and plotted for a varying jamming node or jamming ratio.

Form Figures 2 and 3 observed that as the jammers increase the throughput and the packet delivery ratio decreases while the delay increases. When compared to PSO and ACO optimization, the proposed method shows a higher delivery ratio and reduced end to end delay. Figures 4 and 5 shows the detection rate and the false positive probability for corresponding jammer insertion. The proposed method shows a higher detection rate and lowers false positive probability because of solving the objective function. It is practically verified that when compared to the other two algorithms, the HMCO optimization provides better results in terms of all parameters.

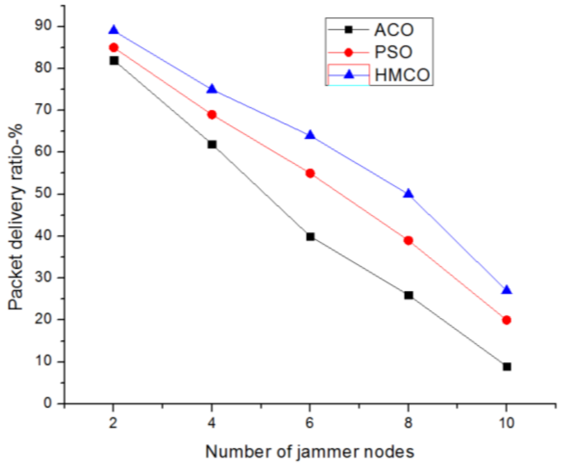

Figure 2. Number of jammer nodes versus packet delivery ratio

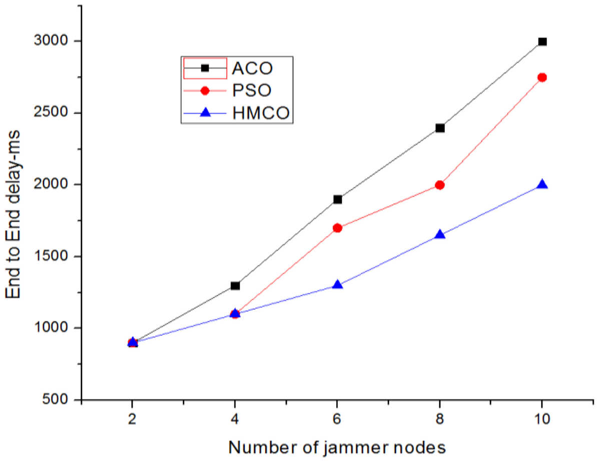

Figure 3. Number of jammer nodes versus delay

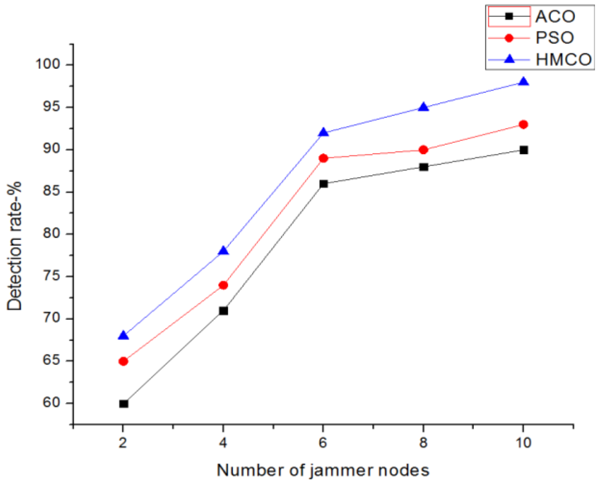

Figure 4. Number of jammer nodes versus detection rate

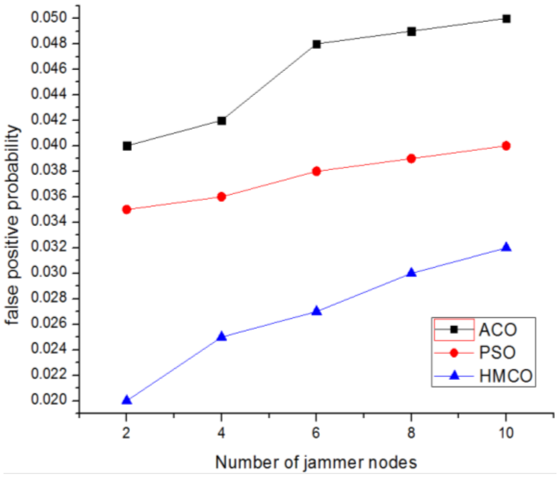

Figure 5. Number of jammer nodes versus false positive probability

6. CONCLUSION

In this work, a novel method to detect a jamming attack in a wireless smart grid network using hen maternal care optimization is presented. The HMCO algorithm mimics the care shown by hen for its children naturally. By using this HMCO optimization, it is effective to identify the jamming attacks in SDG. The performance of our proposed HMCO detection method is analyzed with the parameters of detection rate, false positive probability, delay and packet delivery ratio. Our method shows greater performance among other standard algorithms such as PSO and ACO.

REFERENCES

[1] X. Wang and P. Yi, “Security framework for wireless communications in smart distribution grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809–818, 2011, doi: 10.1109/TSG.2011.2167354.

[2] T. Liu *et al.*, “A dynamic secret-based encryption scheme for smart grid wireless communication,” *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1175–1182, May 2014, doi: 10.1109/TSG.2013.2264537.

[3] V. C. Manju and K. M. Sasi, “Detection of jamming style DoS attack in Wireless Sensor Network,” in *Proceedings of 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, PDGC 2012*, 2012, pp. 563–567, doi: 10.1109/PDGC.2012.6449882.

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” *Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 46–57, 2005, doi: 10.1145/1062689.1062697.

[5] Z. Yang, P. Cheng, and J. Chen, “Learning-Based Jamming Attack against Low-Duty-Cycle Networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 6, pp. 650–663, 2017, doi: 10.1109/TDSC.2015.2501288.

[6] J. Chen, A. J. Gallo, S. Yan, T. Parisini, and S. Y. R. Hui, “Cyber-Attack Detection and Countermeasure for Distributed Electric Springs for Smart Grid Applications,” *IEEE Access*, vol. 10, pp. 13182–13192, 2022, doi: 10.1109/ACCESS.2022.3145015.

[7] D. Mukherjee, B. Kumar Sethi, S. Chakraborty, R. Banerjee, P. Kumar Guchhait, and J. Bhunia, “Real-time Mitigation of Effects of False Data in Smart Grid: A Data Diode Approach,” *IEEE Region 10 Humanitarian Technology Conference, R10-HTC*, vol. 2021-September, 2021, doi: 10.1109/R10-HTC53172.2021.9641729.

[8] A. Althobaiti, A. Jindal, A. K. Marnerides, and U. Roedig, “Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods,” *IEEE Access*, vol. 9, pp. 159291–159312, 2021, doi: 10.1109/ACCESS.2021.3131220.

[9] M. Tanveer, A. U. Khan, N. Kumar, A. Naushad, and S. A. Chaudhry, “A Robust Access Control Protocol for the Smart Grid Systems,” *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6855–6865, May 2022, doi: 10.1109/JIOT.2021.3113469.

[10] S. Ahmed *et al.*, “Signcryption Based Authenticated and Key Exchange Protocol for EI-Based V2G Environment,” *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5290–5298, Nov. 2021, doi: 10.1109/TSG.2021.3102156.

[11] H. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, “Jamming-Resilient Multipath Routing,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 852–864, Nov. 2012, doi: 10.1109/TDSC.2012.69.

[12] S. D’Oro, E. Ekici, and S. Palazzo, “Optimal power allocation and scheduling under jamming attacks,” *IEEE/ACM Transactions on Networking*, vol. 25, no. 3, pp. 1310–1323, 2017, doi: 10.1109/TNET.2016.2622002.

[13] R. Zhang, J. Sun, Y. Zhang, and X. Huang, “Jamming-Resilient Secure Neighbor Discovery in Mobile Ad Hoc Networks,” *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5588–5601, 2015, doi: 10.1109/TWC.2015.2439688.

[14] Q. Wang, T. Nguyen, K. Pham, and H. Kwon, “Mitigating Jamming Attack: A Game Theoretic Perspective,” *IEEE Transactions on Vehicular Technology*, 2018.

[15] S. D’Oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, “Defeating jamming with the power of silence: A game-theoretic analysis,” *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2337–2352, 2015, doi: 10.1109/TWC.2014.2385709.

[16] R. Forsati, A. Moayedikia, R. Jensen, M. Shamsfard, and M. R. Meybodi, “Enriched ant colony optimization and its application in feature selection,” *Neurocomputing*, vol. 142, pp. 354–371, 2014, doi: 10.1016/j.neucom.2014.03.053.

[17] D. Rodrigues *et al.*, “A wrapper approach for feature selection based on Bat Algorithm and Optimum-Path Forest,” *Expert Systems with Applications*, vol. 41, no. 5, pp. 2250–2258, 2014, doi: 10.1016/j.eswa.2013.09.023.

[18] A. Unler, A. Murat, and R. B. Chinnam, “Mr2PSO: A maximum relevance minimum redundancy feature selection method based on swarm intelligence for support vector machine classification,” *Information Sciences*, vol. 181, no. 20, pp. 4625–4641, 2011, doi: 10.1016/j.ins.2010.05.037.

[19] H. H. Inbarani, A. T. Azar, and G. Jothi, “Supervised hybrid feature selection based on PSO and rough sets for medical diagnosis,” *Computer Methods and Programs in Biomedicine*, vol. 113, no. 1, pp. 175–185, 2014, doi: 10.1016/j.cmpb.2013.10.007.

[20] J. H. (John H. Holland and J. H, “Adaptation in natural and artificial systems : an introductory analysis with applications to biology, control, and artificial intelligence,” *University of Michigan Press*, p. 211, 1992, [Online]. Available: https://www.mendeley.com/research-papers/adaptation-natural-artificial-systems-76/.

[21] Ghamisi P. and Benediktsson J.A, “Feature selection based on hybridization of genetic algorithm and particle swarm optimization,” *IEEE Geoscience and Remote Sensing Letters*, vol. 12, no. 2, pp. 309–313, 2015.

[22] S. Kaur and T. Sharma, “Optimistic Attack Detection Using Triangular Mutation based Particle Swarm Optimization in Wireless Multimedia Sensor Networks,” *Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018*, pp. 762–767, 2018, doi: 10.1109/CESYS.2018.8723976.

[23] H. Xu *et al.*, “Application of elephant herd optimization algorithm based on levy flight strategy in intrusion detection,” Proceedings of the 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2018, pp. 16–20, 2018, doi: 10.1109/IDAACS-SWS.2018.8525848.

[24] R. C. Chen, W. L. Chang, C. F. Shieh, and C. C. Zou, “Using hybrid artificial bee colony algorithm to extend wireless sensor network lifetime,” Proceedings - 3rd International Conference on Innovations in Bio-Inspired Computing and Applications, IBICA 2012, pp. 156–161, 2012, doi: 10.1109/IBICA.2012.27.

[25] A. I. Hafez, H. M. Zawbaa, E. Emary, “An innovative approach for feature selection based on chicken swarm optimization,” 2015 7th International Conference of Soft Computing and Pattern Recognition (SoCPaR), 2015, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7492775/.

[26] P. Tague, M. Li, and R. Poovendran, “Mitigation of control channel jamming under node capture attacks,” *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp. 1221–1234, 2009, doi: 10.1109/TMC.2009.33.

[27] Ó. Puñal, C. Pereira, A. Aguiar, and J. Gross, “Experimental characterization and modeling of RF jamming attacks on VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 524–540, 2015, doi: 10.1109/TVT.2014.2325831.

[28] J. T. Chiang and Y. C. Hu, “Cross-layer jamming detection and mitigation in wireless broadcast networks,” *IEEE/ACM Transactions on Networking*, vol. 19, no. 1, pp. 286–298, 2011, doi: 10.1109/TNET.2010.2068576.

[29] Z. Lu, W. Wang, and C. Wang, “Modeling, Evaluation and Detection of Jamming.”

[30] B. E, D. M, and T. G., “Swarm intelligence: from natural to artificial systems,” 1999.

[31] M. Dorigo and K. Socha, “Ant colony optimization,” *Handbook of Approximation Algorithms and Metaheuristics*, pp. 26-1-26–14, 2007, doi: 10.1201/9781420010749.

[32] R. C. Eberhart and J. Kennedy, “Particle Swarm Optimization in Neural Networks,” *IEEE International Conference*, 1995.

[33] G. McBride, I. P. Parer, and F. Foenander, “The Social Organization and Behaviour of the Feral Domestic Fowl,” *Animal Behaviour Monographs*, vol. 2, pp. 125–181, 1969, doi: 10.1016/s0066-1856(69)80003-8.

[34] S. E. Field, N. S. Rickard, S. R. Toukhsati, and M. E. Gibbs, “Maternal hen calls modulate memory formation in the day-old chick: The role of noradrenaline,” *Neurobiology of Learning and Memory*, vol. 88, no. 3, pp. 321–330, 2007, doi: 10.1016/j.nlm.2007.04.001.

[35] R. M. Evans, “Stimulus intensity and acoustical communication in young domestic chicks.,” *Behaviour*, vol. 55, no. 1–2, pp. 73–80, 1975, doi: 10.1163/156853975X00416.

[36] N. E. Collias, “The Vocal Repertoire of the Red Junglefowl: A Spectrographic Classification and the Code of Communication,” *The Condor*, vol. 89, no. 3, p. 510, 1987, doi: 10.2307/1368641.

BIOGRAPHIES OF AUTHORS

Dr. Narmadha Ganesamoorthy has teaching experience of 15 years till date. She has done the research in VLSI for cryptographic applications especially for public key cryptography. But not focused on cryptographic algorithms, design-oriented approach is followed to bring the optimization in the cryptographic design without sacrificing the level of security. Now, she is working on the development of MOSFET structure for the detection of biomarkers and application of VLSI in Biomedical image processing application. As an academician, she has taught more than 10 Courses for the Under Graduate Engineering students. She has conducted the technical seminars and workshop in the presently working institution. She acts as a reviewer for a greater number of Web of Science indexed journals. He can be contacted at email: gnarmadhame@gmail.com.

Dr. B. Sakthivel received a B.E. degree in Electronics and Communication Engineering from the SACS MAVMMM Engineering, college, Madurai. He completed M.E. in Anna University. He completed Ph.D. in Anna University He is currently working as an Associate Professor in the Department of ECE at Pandian Saraswathi Yadav Engg college where he heads the VLSI Lab. He has a focus on VLSI architecture design, particularly as applied to data path circuits like adders and multipliers. He can be contacted at email: 786sakthivel@gmail.com.

Dr. Deivasigamani Subbramania received his B. Eng. in Electrical and Electronics Engineering, Thiagarajar College of Engineering, M. Eng. in Applied Electronics Engineering, Thanthai Periyar Government Institute of Technology from the University of Anna, India, Ph.D. in Engineering (Medical Signal Processing using Machine Learning Methods), Multimedia University, Malaysia. Currently working as an Assistant Professor at the Faculty of Engineering, Technology and Built Environment, UCSI University, Malaysia. He served in various academic positions such as Deputy Dean, HOD, and Programme Co-ordinator. He has to date, published over 35 scientific articles in international journals and conferences. His current research expertise and interest areas include Medical Signal Processing and OBE. He is a Senior Member of IEEE and a registered Chartered Engineer with the Engineering Council United Kingdom. He is a serving reviewer of various international journals. He can be contacted at email: deivasigamani@aimst.edu.my.

K. Balasubadra received her B.E. Degree in Electronics and Communication Engineering in 1988 from PSNA College of Engineering and Technology, Dindigul, Madurai Kamaraj University and M.E Degree in Applied Electronics from the Government College of Technology, Coimbatore, Bharathiar University in 1997. She received her Doctorate Degree in Information and Communication Engineering from Anna University, Chennai, in 2009. She can be contacted at email: ggpriya2019@gmail.com.