Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1457–1472
DOI : 10.47974/JDMSC-1771

Securing wireless sensor network from node capture attack using an efficient optimization defense strategy model

Amara S A L G Gopala Gupta *
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram
A. P.
India

Syam Prasad Gudapati †
Department of Computer Science and Engineering
Sri Vasavi Institute of Engineering & Technology
Nandamuru
Krishna
A. P.
India

Praveen Tumuluru §
Department of Computer science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram
A. P.
India

Abstract

Wireless Sensor Networks (WSNs) are a promising evolving technology for recent real-world applications in collaborative settings. These applications ranging from household monitoring to crucial military applications transmit critical data and thus more challenging approaches are required for providing security. In WSNs, a node capture attack (NCA) is a more serious attack among various attacks which supports an impostor to perform different network (NW) operations, and thereby the security of the entire NW is compromised easily.

* *E-mail:* **amara_gupta@yahoo.com (Corresponding Author)**
† *E-mail:* **syamprasad.gudapati@gmail.com**
§ *E-mail:* **praveenluru@gmail.com**

For conquering the surpassing issues of sensitivity-related techniques and for enhancing the NCA's AE, we establish the NCA technique amalgamating several objectives like speed and location to lessen comprehensive intricacy. For securing the NW out of the NCA, this study proffers Improved Flower Pollination Optimization Defense Strategy Algorithm (IFPODSA) intending to compute the multiple objective functions for effectual chief administration procedure employing Hankel matrix formation. This proffered IFPODSA is correlated with two prevailing methodologies like Fruit Fly Optimization Algorithm (FFOA) and Finding Robust Assailant Optimization-Particle Swarm Optimization and Genetic Algorithm (FRAOPSOGA) concerning diverse criteria. Consequently, it has been observed that the proffered IFPODSA attains 458.7 kbps of throughput, 81.56% of PDR, 18.2% of energy consumption, and 64.36% of overhead.

Subject Classification: *68M25, 68M18.*

Keywords: *Security, Wireless sensor networks, Optimization, Key management, Capture attack.*

1. Introduction

Wireless Sensor Networks (WSNs) remain a conception, and the chief tool remains the sensor. Sensors' employment could efficiently sense the outward environment, and, later, with the assistance of a wireless network (NW) for data transference, it achieves user requirements [1]. The WSNs' protection should be given importance since this remains reinforced by great technological content and intricate framework, and when there remains an issue, the results will be inconceivable. WSNs' properties turn them susceptible to several attacks that acutely impact the secrecy, unity, and data presence [2]. Particularly, if the NW's routing remains attacked, the data gathered by the sensor node (SN) could not be transferred to the destination sink node (SkN) punctually and precisely.

Similar to the conventional computer communication NW, WSNs' security threat (ST) chiefly occurs out of diverse attacks [3]. ED attacks in WSNs could be evaded by employing symmetric key-related cryptographic (CG) approaches for managing access to communication amidst SNs [4].

An effectual and practical key task methodology for wide-range WSNs by employing a haphazard graph approach has been provided [5].

In spite of the absence of the ST paradigm over the past few years, exertions were performed to comprehend and alleviate NCA and cloning attacks [22]. Effectual methodologies for detecting cloned nodes within the NW have been defined in [8].

The defense schemes have been classified as:

- Watchdog (WD) strategy: It remains a significant procedure for the detection of misconduct nodes [9].
- Rating strategy: This strikes a resonant chord in the importance of creating selfish pay.
- Virtual currency: It presents a selfish node kind named nuggets. For insulating a node's nuggets out of illicit exploitation, a tamper resilient production unit saving entire pertinent IDs, nugget counter, and CG items remain mandatory.
- Route DOS avoidance: It occurs at the routing layer for evading DOS attacks with the collaboration of several nodes.

This study's inspiration remains as ensues: to the finest of our knowledge, there remain nil dispensed resolutions for the issue of identifying the NCAs within WSNs. Ensuing a novel alluring research thread, which concentrates upon exploiting motility for administering protection attributes for WSN and AHN, a novel capture identification architecture, which exploits node motility, has been proffered. This study's inputs include:

- Improved Flower Pollination Optimization Defence Strategy Algorithm (IFPODSA) has been modeled to compute the multi-objective function (MOF) for effectual key management (KM) procedure by employing Hankel matrix (HM) formation.
- NCA assessment has been carried out employing the Received Signal-based Trust Value Adversary paradigm in which SN functions according to the attacker's command disregarding the real procedure.

2. Literature Survey

Bhatt et. al. (2020) present a Fruit Fly Optimization AG (FFOA) NCA AG concentrating upon multiple intentions like serving maximal node and key and expense to some resources for detecting the optimum NW nodes (NWNs). FFOA's outcomes generate additional compromised traffic (CT), low attack rounds, and energy's low price when compared with Genetic AG (GA) and some NCAs' AGs [10].

Jamshidi et. al. (2020) propose a methodology that remains beneficial out of WD nodes (WDN), and the objective of this remains that each NWN detected with its ID should possess equivalent meeting modification by WDN. This has been noticed that the maximum RNs have been detected when the FI's probability remained below 0.005%. The disadvantage remains that this presented additional computative intricacy [24].

Khare et. al. (2022) put forth an NCA by capturing some nodes via an intruder for capturing the whole WSN by excerpting beneficial data such as keys, routing procedures, and data out of WSNs. This BHOA has been implemented upon a function of Vertex Participation [12].

Devi et. al. (2022) highlight acquiring the optimum pre-processed data that will be augmented with the employment of the Modified Particle Swarm Optimization (MPSO) approach. [13].

Shukla et. al. (2015) establish detecting strong assailant optimization-PSO and genetic NCA AG having multiple intentions by employing optimization function to give efficient resolution for NCA. It has been confirmed with the simulation's outcomes that Finding Robust Assailant Optimiozaton-Particle Swarm Optimization and Genetic AG (FRAOPSOGA) generated greater CT when correlated with the matrix AG, and, thus, the attack's efficacy with FRAOPSOGA has been high [14].

Guo et. al. (2021) suggest a power IoT data defense scheme centered upon enhanced identify-related dynamic clustering. Initially, the terminal gadget fixes the private key for resolving the terminal protection verification's key escrow issue in the IoT paradigm [15].

Anand et. al. (2022) recommends a methodology for identifying and evading black hole attacks by employing the hidden Markov paradigm, and this is employed for detecting MNs too [23].

Adnan et. al. (2021) examine disparate WSNs defense schemes out of outward attackers as well as inward nodes performing greedily or malignantly by employing the game theory (GT) technique [17].

Deng et. al. (2020) provide the architecture for optimum defense resource allotment for lessening the NW threat [18].

Bagali et. al. (2019) suggest the Efficient Channel Access (ECA) paradigm by employing the cross-layer (CL) model to alleviate reactive jammer [19].

Ahlawat et. al. (2021) explore the NCA's issue and proffer a protected hybrid key pre-distribution (HKP) strategy for WSNs. [20].

Anzani et. al. (2019) contemplate a hybrid key pre-dispensation technique centered upon symmetric combinatorial-related mode. These fuse the symmetric course's squares of action for creating novel key-rings

(KR) against creating a contradictory plot that has been received a handle on in cross-breed symmetric technique called merging hybrid symmetric (MHS) model. [21].

It has to be observed that the prevailing methodologies are proffered to enhance the energy efficiency (EE) in WSNs. A few of these are employed in CL techniques and a few of these are employed in optimization protocols (OPs). Likewise, in the prevailing Ops, the entire optimum layers possess an equivalent quantity of time (t) for their disparate manners. Additionally, the fundamental optimized defense scheme paradigm remains to encounter the less accuracy drawback of optimization, tardy convergence in the final phase, and effortless slipping into a local optimum. It uses heterogeneous NW data's huge quantity in resolving the user detection issue.

3. Proposed Methodology

This research is planned to focus on an optimization algorithm for the construction of a defense strategy for improving security in WSN. To improve security flower pollination-based optimization is adopted for construction. The IFPODSA functionality is based on the weighted factor. Once the weights are estimated NW updates each node parameter. With the update of node position and location, effective paths are identified with a reactive routing strategy. With the application of the proposed weighted Flower Pollination algorithm, it is expected that data were transmitted through the optimal path. This involved the identification of malicious paths and security was also improved. Figure 1 indicates the overall working procedure of the proposed model.

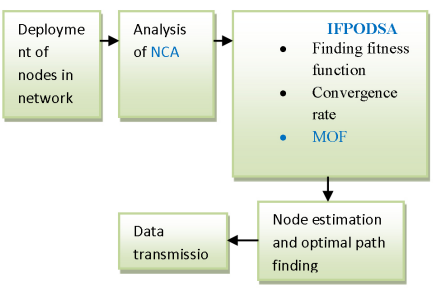

Figure 1

Overall working procedure of the proposed security model

3.1 *Network model*

The Base Station (BS) is deployed such that it is far from the sensing field. After deployment, BS and SNs are stationary. A gateway is also deployed in the same NW field at the center of the NW. After deployment, the gateway node is stationary and rechargeable. It is assumed that S sensors are randomly deployed in a field to monitor the environment as indicated in figure-2. The ith sensor is represented by si and the subsequent set of SNs S= s1 to sn. This proposed scheme comprises NW creation and data transmission phases. In the former, CH for every cluster as well as GN is selected and in the latter, data is transmitted.

A group of sensors form a cluster, and each sensor can choose to become a gateway with a certain probability. A cluster head (CH) can only have one gateway to connect to the sink. The CH selects the gateway from the nodes that are closer to the sink than the CH itself, and the nodes must be within one hop of distance from the CH. The gateway belong to the cluster or may not belong to the cluster. The CH sends a Gateway Selection Message (GSM) to the selected gateway, which allows knowing which node the gateway is connected to. It decides how much data to send to each CH based on its workload. If a CH has a heavier workload, the gateway will send it fewer sensor readings. This helps to stabilize the energy consumption among the CHs, reducing the frequency of CH retirement and, ultimately, cluster reformation.

$$E_{cl} = lE_{elec}(k-1) + l_{amp}E\sum_{k=0}^{n} d^2 \text{ to } CH \tag{1}$$

in which l and E_{elec} portray the length of the messages and transmit electronics accordingly. l_{amp} indicates transmit amplifier. The distance betwixt a cluster member (CM) and its CH will be portrayed by d to CH.

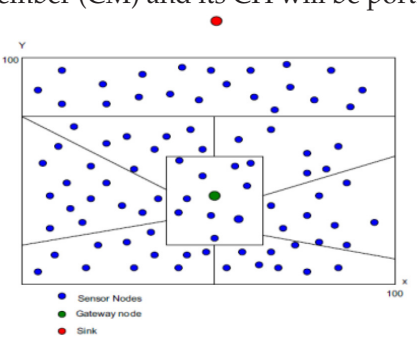

Figure 2

Node deployment in the NW

$E[\sum_{k=0}^{n} \text{distance}^2 \text{ to } CH]$ is the expected sum of the square distance of cluster members from their corresponding CH.

In the proposed model, if the distance between any two CHs is greater than d, then the cluster is divided into two separate areas. The CH is identified using the following expression:

$$E = \sum_{k=0}^{n} d^2 \text{ to } CH = 2\pi\theta CH \int_0^{\text{distance}/2} r^3 \, dr \tag{2}$$

Now all the sensors with a distance, not more than *distance*/2 from other CHs, are secure nodes in other CHs but not the nodes of the current CH.

3.2 *Analysis of NCA*

This section elaborates on two circumstances to further understand the threat model of an NCA in WSN.

3.3 *IFPODSA*

Initially, nodes are deployed in the NW using IFPAO. When a new node is added, the Coverage Ratio (CR) and Area Coverage (AC) are evaluated based on the estimated Reg(i) = Height(i) x Width(i). Generally, pollination from the same flower results in the growth of various plants. The protocols used in IFPAO are:

Here IFPAO is involved in three different operations. The objective function (OF) of IFPAO is given by

$$Objective\,Function(OF) = \max\,(CR, AC) \tag{3}$$

OF constraints are hence used for the below-mentioned Process

- Selection of SN
- Discovering the Route and selecting the best path
- Optimum transmission

The IFPA optimization process checks the sensors, sensing region, target, and covered directions for verification during deployment. The total AC is calculated by.

$$Total\,AC = \sum_{n=1}^{a} \sum_{m=1}^{a} x(n, m, c) \tag{4}$$

and then CR is calculated using

$$\text{Total } CR = \frac{\text{Total cover area}}{\text{Total network area}} \tag{5}$$

To begin with, SNs are deployed in optimal locations with accurate sensing perspectives based on the target object's CR, AC, and coverage. Once deployed, information about the SNs is added to the RankD lists. Each flower is represented as a vector by combining information about the CR, Area,I(cover), AC,I(node), times and energy. In FPA, it is decided whether the best fitness result is achieved through pollination. By motivating IFPAO and maintaining covered paths, targets, and optimal sensors, AC, CR, and energy are optimized. SN classification is determined by their locations in the NW plane (X, Y), the total number of sensors N in a specified region, radius R, number of directions K, and even targets at the initial stage. The best solution is obtained by comparing the CR, AC, maximum energy and target coverage with neighboring flowers. This process is repeated until the stopping criteria are met.

3.4 *Multi-Objective function*

The MOF's chief intention remains to identify the trade-off betwixt contradictory objectives and seeking solutions.

$$\text{minimise}\{f_1(x),\ldots f_n(x)\} \tag{6}$$

$$\delta_j(x) \le 0, \text{ for } j = 1,2,\ldots.J \tag{7}$$

$$\gamma_k(x) = 0, \text{for } K = 1,2,3\ldots K \tag{8}$$

$$lb_i \le x_i \le ub_i, \text{for } i = 1,2,\ldots n \tag{9}$$

in which $\delta_j(x)$ and $\gamma_k(x)$ represent limitation functions; lb_i and ub_i represent bottom and top bounds of associated variable x_i accordingly. N_i portraying the samples' quantity.

3.5 *Mathematical model of IFPODSA*

The key management is done by the improvement in data collection and security of WSN and the way in establishing the protected connection and refreshing the key using certain schemes.

- Generation of Matrix H from DSA

  It is significant for an empowered NW to show a larger prime number *p* that can recognize the area of finite space and select the OF. Consider the scale of WSN is given as *N*, the matrix *H* is named as a square matrix with ascending rate of skew diagonal form '*S*' that has the private message with area rate of $(\beta+1)*N$ and $(\beta+1)*(\beta+1)$, and, hence, the matrix is given as

$$H = \begin{matrix} S0 & S1 & S2 & \dots & \dots & S(N-1) \\ S1 & S2 & S3 & S4 & \dots & \vdots \\ S2 & S3 & S4 & \dots & \dots & \vdots \\ \vdots & S4 & S5 & S2 & S1 & S(N-4) \\ \vdots & \vdots & \vdots & S1 & S(N-4) & S(N-3) \\ S(N-1) & \dots & \dots & S(N-4) & S(N-3\_ & S(N-2) \end{matrix} \quad (10)$$

- Generation of matrix Z

  Z can be obtained by transforming the H matrix, the sequence $\{Hn\}\, n \geq 0$

$$Z = \sum_{k=0}^{n} H(k) \quad (11)$$

- Generation of Matrix $\boldsymbol{A}$

  Matrix A is the obtained by computing $H$and Zthat is given as $A = H.Z$

  Since the matrix $H$is symmetric, we can obtain that

$$A = H.Z = A = (H.Z)^T.Z = H^T.Z^T.Z = (H.Z)^T \quad (12)$$

- IFPO-oriented key allocation: In this model, before the message broadcasted using the unicast DFA algorithm reaches the Base station, a protected pair-wise key is generated through the first communication.

IFPODSA – Pseudocode

Step-1 Initialize a population of flowers at random positions as cluster centers

Step-2 Compute best solution 'B' from the initial population

Step-3 Coverage estimation

$$Reg(i) = Width(i) \times Height(i)$$

Area coverage

$$Total\ AC = \sum_{n=1}^{a} \sum_{m=1}^{a} x(n, m, c)$$

Coverage ratio

$$Total\ CR = \frac{Total\ cover\ area}{Total\ network\ area}$$

Step-4 Creation of Rank D lists

Step-5 Initialize the key management process Initialize the key management process with Generation of Matrix H,Z & A

Key allocation- pair-wise key transformation

Step-6 Data transmission

4. Performance Analysis

This proposed IFPODSA method is compared against the present method in terms of different performance metrics like EE, Packet Delivery ratio (PDR), EC, Throughput, control overhead, and end-to-end delay of the NW. To verify IFPODSA to be more efficient than the existing techniques such as FFOA and FRAOPSOGA the graphs are given here. The required Simulation area is 100m×100m, No. of SNs are 100, No. of gateways are 5, No. of CH is 25, No. of sinks are 6, Simulation time is 500s, Node placement is Random and channel type is wireless.

4.1 *Energy Efficiency*

It is defined as the continuous-time taken from t1 to t2 for measuring the energy consumed.

Table 1 presents the analysis of EE and figure 3 depicts the comparison of EE with the existing FFOA and FRAOPSOGA against the proposed IFPODSA method.

Table 1

Analysis of EE

Nodes	FFOA	FRAOP SOGA	IFPODSA
0	0	0	0
20	6	9	18
40	11	15	24
60	17	26	39
80	26	35	51
100	32	43	68

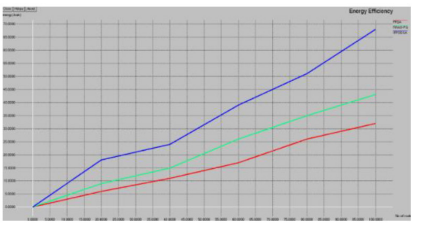

Figure 3

EE of the network

4.2 *Packet delivery ratio*

This gives the proportion of successfully transmitted packets from source to destination node.

$$PDR = \frac{\text{Number of packet received succesfully}}{\text{Total number of packets forwarded}}$$

Table 2 shows the analysis of Packet PDR and figure 4 compares the PDR of the existing FFOA, FRAOPSOGA, and proposed IFPODSA methods.

Table 2

Analysis of PDR

Nodes	FFOA	FRAOP-SOGA	IFPOD-SA
0	99.2451	99.2457	99.0824
20	86.2567	90.1475	98.0941
40	80.2457	85.1968	98.3547
60	76.1247	83.7548	97.516
80	70.2555	78.1468	97.3547
100	65.3547	74.1867	96.3457

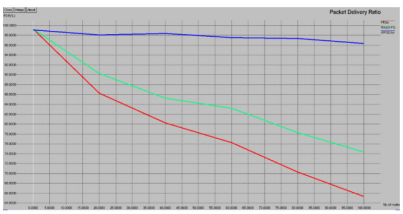

Figure 4

PDR of the network

4.3 *Energy Consumption*

This is the sum of the energy of every hop which is calculated by

$$Energy = \frac{1}{p}\sum_{n}^{p} E_n$$

Where p is the hops of multi-hop routing and En is the energy of n^{th} hop.

Table 3 presents the analysis of EC and figure 5 compares the EC of the existing FFOA, FRAOPSOGA, and proposed IFPODSA methods.

Table 3

Analysis of EC

Nodes	FFOA	FRAOP-SOGA	IFPOD-SA
0	0	0	0
20	15	12	6
40	22	19	11
60	39	29	18
80	53	41	24
100	68	57	32

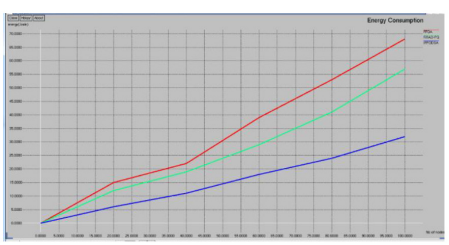

Figure 5

EC of the network

4.4 *Throughput*

It refers to the data flow rate of a communication channel.

$$\text{Throughput} = \sum \frac{(\text{number of successful packets}) * (\text{average packet size})}{\text{Total Time sent in delivering that amount of data}} (\text{bits} / \text{sec})$$

Table 4 represents the analysis of throughput and figure 6.

Table 4

THROUGHPUT of EC

Nodes	FFOA	FRAOP-SOGA	IFPOD-SA
0	420.234	500.234	685.177
20	387.247	420.178	644.178
40	265.174	380.9875	523.178
60	159.475	250.7814	423.1574
80	123.7458	150.264	286.347
100	87.170	100.3254	190.457

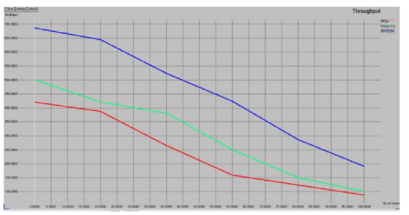

Figure 6

THROUGHPUT of the network

Compares the throughput of the existing FFOA, FRAOPSOGA, and proposed IFPODSA methods.

4.5 *Over Head*

This is equal to the total packets that are transferred from one node to other.

Table 5 presents the analysis of overhead Figure 7 compares the overhead of the existing FFOA, FRAOPSOGA, and proposed IFPODSA methods.

Table 5

Analysis of Over Head

Nodes	FFOA	FRAOP-SOGA	IFPOD-SA
0	0	0	0
20	7345	5178	4267
40	9234	6734	5975
60	10543	8356	7835
80	11675	9345	8234
100	13567	10345	9386

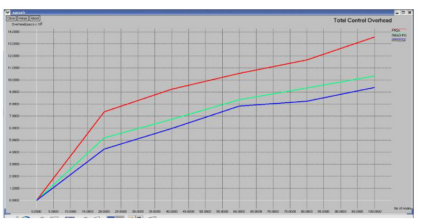

Figure 7

Control Over Head of the network

4.6 *End to End Delay*

Total hops (p) necessary for routing divided by the total nodes (tn) available in the NW is considered as the end-to-end delay and is estimated by

$$Delay = \frac{p}{tn}$$

Table 6 presents the analysis of end to end delay Figure 8 depicts the comparison of end-to-end delay of existing FFOA, FRAOPSOGA, and proposed IFPODSA.

Table 6

Analysis of End-End Delay

Nodes	FFOA	FRAOP-SOGA	IFPOD-SA
0	0	0	0
20	78.252	54.972	24.012
40	121.742	101.142	45.012
60	198.864	167.286	69.112
80	259.135	221.533	81.429
100	339.219	287.279	102.238

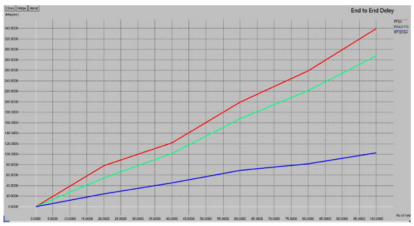

Figure 8

End-End Delay of the network

Table 7 presents the overall comparative analysis between the existing FFOA, FRAOPSOGA, and proposed IFPODSA methods.

Table 7

Overall Comparative Analysis

Parameters	FFOA [9]	FRAOPSOGA [14]	IFPODSA (Proposed)
EE	18.4	25.6	40
PDR	79.5	85.11	81.56
EC	39.4	31.6	18.2
Throughput (kbps)	240.507	300.46	458.74
Overhead	199.39	166.44	64.36

5. Conclusion

IFPODSA has been proposed to calculate the MOF for an efficient key management process using HM formation which will increase the security by finding a MOF for NCA in WSN. Simulation results suggest that IFPODSA is an efficient optimization that provides high accuracy in detecting trust content in the presence of MNs. Moreover, the performance of IFPODSA is compared with FFOA and FRAOPSOGA, which clearly shows that IFPODSA performs better by achieving 458.74 kbps of throughput, 81.56% of PDR, 18.2% of EC, 64.36% of overhead. Future work is to use coalitional GT for the detection process of possible attacks in the NW with the minimization of time.

References

[1] Huanan, Z., Suping, X., & Jiannan, W., Security and application of wireless sensor network. Procedia Computer Science, 183, 486-492 (2021).

[2] Zheng, G., Gong, B., & Zhang, Y., Dynamic network security mechanism based on trust management in wireless sensor networks. Wireless Communications and Mobile Computing (2021).

[3] Biswas, R. N., Mitra, S. K., & Naskar, M. K., Localization under node capture attacks using fuzzy based anchor mobility control. *Journal of Ambient Intelligence and Humanized Computing*, 1-30 (2022).

[4] Bathla, R., & Ahlawat, P., Adversarial Modeling in WSN and its Application in Key Distribution. In *Journal of Physics: Conference Series*, Vol. 2062, No. 1, p. 012001, (2021, November). IOP Publishing.

[5] Wang, J., Zhou, L., Tian, L., Yu, X., & Liu, C., Early Detection of Node Capture Attack in the Internet of Things. In 2021 IEEE 4th International Conference on Electronics and Communication Engineering (ICECE), pp. 132-135 (2021, December). IEEE.

[6] Yousefpoor, M. S., Yousefpoor, E., Barati, H., Barati, A., Movaghar, A., & Hosseinzadeh, M., Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. *Journal of Network and Computer Applications*, 190, 103118 (2021).

[7] Prashant Manuja & Rajveer Singh Shekhawat. Developing information security metrics and measures for risk assessment of an organization,

Journal of Discrete Mathematical Sciences and Cryptography, 25:4, 1195-1202 (2022), DOI: 10.1080/09720529.2022.2075092.

[8] Jane Nithya, K., & Shyamala, K., A Systematic Review on Various Attack Detection Methods for Wireless Sensor Networks. In International Conference on Innovative Computing and Communications, pp. 183-204, (2022). Springer, Singapore.

[9] Chen X Q, Makki K and Kang Yen, "Sensor network security: a survey" Communications Surveys & Tutorials, IEEE, Second quarter, 11(2): 52–73 (2019).

[10] Bhatt R, Maheshwary P, Shukla P, Shukla P, Shrivastava M and Changlani S, "Implementation of Fruit Fly Optimization Algorithm (FFOA) to escalate the attacking efficiency of node capture attack in Wireless Sensor Networks (WSN)", Computer Communications, vol.149, pp.134-145 (2020).

[11] Kritsanapong Somsuk & Chalida Sanemueang. Increasing security to public key cryptography for point-to-point communication, *Journal of Discrete Mathematical Sciences and Cryptography* (2021), DOI: 10.1080/09720529.2021.1930656.

[12] Khare, Ankur, Rajendra Gupta, and Piyush Kumar Shukla. "Improving the protection of wireless sensor network using a black hole optimization algorithm (BHOA) on best feasible node capture attack." IoT and Analytics for Sensor Networks. Springer, Singapore, 333-343 (2022).

[13] Devi, P. P., & Jaison, B., Optimal Scheme for the Detection and Classification of Clone Node Attack in WSN Using TAIGBRFCNIA. Wireless Personal Communications, 1-15 (2022).

[14] Shukla P. K, Goyal S, Wadhvani R, Rizvi M. A, Sharma P and Tantubay N, "Finding robust assailant using optimization functions (FiRAO-PG) in wireless sensor network", Mathematical Problems in Engineering (2015).

[15] Guo, D., Zhang, N., Wang, Y., Cui, Y., Jiang, B., She, R., ... & Ma, W., Research on Information Security Defense Based on Improved Identity-Based Dynamic Clustering Authentication Algorithm. In *Journal of Physics: Conference Series*, Vol. 1757, No. 1, p. 012136 (2021). IOP Publishing.

[16] Devanshi Ledwani, Himanshi Saini, Lalita Ledwani, Swami Nisha Bhagirath & Vaibhav Bhatnagar. Review on security

issues and solutions in cloud computing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:7, 2149-2158 (2022), DOI: 10.1080/09720529.2022.2133253.

[17] Adnan, M., Yang, T., Das, S. K., & Ahmad, T., Utility of Game Theory in Defensive Wireless Sensor Networks (WSNs). In International Conference on Innovative Computing and Communications, pp. 895-904, (2021). Springer, Singapore.

[18] Deng, Y. J., Li, Y. Q., Qin, Y. H., Dong, M. R., & Liu, B., Optimal defense resource allocation for attacks in wireless sensor networks based on risk assessment model. Chaos, Solitons & Fractals, 137, 109780 (2020).

[19] Bagali, S., & Sundaraguru, R., Efficient channel access model for detecting reactive jamming for underwater wireless sensor network. In 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), pp. 196-200 (2019, March). IEEE.

[20] Ahlawat, P., & Dave, M., An attack resistant key predistribution scheme for wireless sensor networks. *Journal of King Saud University-Computer and Information Sciences*, 33(3), 268-280 (2021).

[21] Anzani M., Javadi H.H.S., Modirir V. Key-management scheme for wireless sensor networks based on merging blocks of symmetric design. Wireless Networks, pp. 1–13 (2019).

[22] Hu, B., Tang, W., & Xie, Q., A Two-factor Security Authentication Scheme for Wireless Sensor Networks in IoT Environments. Neurocomputing (2022).

[23] Anand, S., & Muhammad Rafeeque, K., Enhancing the Security in Wireless Sensor Network Using Hidden Markov Model. In Soft Computing for Security Applications, pp. 409-423 (2022). Springer, Singapore.

[24] Jamshidi M, Poor S. S. A, Arghavani A, Esnaashari M, Shaltooki A. A and Meybodi M. R, "A simple, lightweight, and precise algorithm to defend against replica node attacks in mobile wireless networks using neighboring information", Ad Hoc Networks (2020).