Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

Leveraging Gray Wolf Optimization for Enhanced Security Management in Wireless Sensor Network

Zubair Ahmad Mir[1], Dr. Surendra Yadav[2]

Department of Computer Science and Engineering[12]

Vivekananda Global University, Jaipur[12]

***Abstract*:**

In the realm of enhancing security management systems within Wireless Sensor Network (WSNs) for Big Data applications, the role of optimization algorithms is pivotal. This chapter delves into the utilization of Gray Wolf Optimization (GWO) as a fundamental tool to achieve efficient resource allocation, node placement optimization, and the enhancement of data transmission efficiency within WSNs. A detailed exploration of the mathematical foundations of GWO is provided to foster a comprehensive understanding of its application in security enhancement.

In this paper Gray Wolf Optimization (GWO) is a nature-inspired metaheuristic algorithm presented that draws inspiration from the social behavior of gray wolves in the wild. In our study, GWO is employed to optimize various parameters that significantly impact the efficiency and effectiveness of WSNs.

Keywords: *Wireless Sensor Network, Gray Wolf Optimization, Metaheuristic algorithm*

1 Introduction

In the pursuit of enhancing security management systems within Wireless Sensor Network (WSNs) for Big Data, optimization algorithms play a pivotal role. This chapter delves into the utilization of Gray Wolf Optimization (GWO) as a key component in achieving efficient resource allocation, optimizing node placement, and improving data transmission efficiency within the WSN [1]. The mathematical foundation of GWO will be explored in detail to provide a comprehensive understanding of its application in security enhancement.

2 Gray Wolf Optimization (GWO)

Gray Wolf Optimization is a nature-inspired metaheuristic algorithm that draws inspiration from the social behavior of gray wolves in the wild. In the context of our thesis, GWO is applied to the security management system to optimize various parameters that impact the efficiency and effectiveness of the WSN.

This optimization process involves key components [2]:

Initialization of Gray Wolves: Gray wolves in the GWO represent potential solutions within the WSN, and we initialize a population of these wolves, each representing a unique configuration.

Objective Function (Fitness Function): The objective function in our context aims to enhance security management in WSNs, encompassing resource allocation, node placement, and data transmission efficiency.

Gray Wolf Pack and Hierarchy: GWO organizes wolves into a hierarchical pack, with alpha, beta, and delta wolves representing the dominant individuals in the pack[3].

Mathematical Representation of Gray Wolves' Movement: Wolves adjust their positions based on the movements of alpha, beta, and delta wolves.

GWO's application in security management focuses on optimizing:

Resource Allocation: GWO efficiently allocates resources, optimizing energy consumption and reducing operational costs.

Node Placement: It optimizes node placement to ensure maximum coverage and efficient data collection[4] .

Data Transmission Efficiency: GWO enhances data transmission efficiency, reducing delays and improving system performance.

2.1 Mathematical Formulation

Let us define the basic components and mathematical equations that constitute Gray Wolf Optimization:

2.1.1 Initialization of Gray Wolves:

In the context of our security management system, gray wolves represent candidate solutions or configurations within the WSN. We initialize a population of gray wolves, each representing a potential solution [5] .

2.1.2 Objective Function (Fitness Function)

The objective function represents the problem that needs to be optimized. In our case, the objective function aims to improve security management within the WSN, considering parameters like resource allocation, node placement, and data transmission efficiency. We define this objective function as f(x), where x represents the gray wolf's position in the solution space [6] .

2.1.3 Gray Wolf Pack and Hierarchy:

In GWO, wolves are organized into a hierarchical pack consisting of alpha, beta, and delta wolves, representing the dominant individuals within the pack.

2.1.4 Mathematical Representation of Gray Wolves' Movement:

Each gray wolf adjusts its position based on the positions of the alpha, beta, and delta wolves. The new position is calculated using the following equation:

x_new = x_mean - A * D, where

x_new represents the new position of the wolf.

x_mean is the mean position of the alpha, beta, and delta wolves.

A is a vector of random values.

D is the distance vector.

$$NK_{g,h} = \begin{cases} 1 \\ 0 \end{cases} If k_g \in N_h \quad ..(1)$$

$$KP_{g,h} = \begin{cases} 1 \\ 0 \end{cases} If k_g can\ cooperate\ p_h \quad ..(2)$$

$$NC = NK * NP \quad ..(3)$$

$$ETL = \frac{-(ij+cd)+\sqrt{(i^2+c^2)R_t^2-(id-jc)^2}}{i^2+c^2} \quad ..(4)$$

$$NS = ETL * NC$$

$$NW_g = (wt_1 * NC)+(wt_2 * NS) \quad ..(5)$$

$$\vec{D} = |\vec{C}.\overrightarrow{X_p}(t) - \vec{X}(t)| \quad ..(6)$$

$$\vec{X}(t+1) = \overrightarrow{X_p}(t) - \overrightarrow{A}.\vec{D} \quad ..(7)$$

$$\vec{A} = 2\overrightarrow{a}.\overrightarrow{r_1} - \vec{a} \quad ..(8)$$

$$\vec{C} = 2.\overrightarrow{r_2} \quad ..(9)$$

$$\overrightarrow{D_\propto} = |\overrightarrow{C_1}.\overrightarrow{X_\propto} - \vec{X}| \quad ..(10)$$

$$\overrightarrow{D_\beta} = |\overrightarrow{C_2}.\overrightarrow{X_\beta} - \vec{X}| \quad ..(11)$$

$$\overrightarrow{D_\delta} = |\overrightarrow{C_3}.\overrightarrow{X_\delta} - \vec{X}| \quad ..(12)$$

$$\overrightarrow{X_1} = \overrightarrow{X_\propto} - \overrightarrow{A_1}.(\overrightarrow{D_\alpha}) \quad ..(13)$$

$$\overrightarrow{X_2} = \overrightarrow{X_\beta} - \overrightarrow{A_2}.(\overrightarrow{D_\beta}) \quad ..(14)$$

$$\overrightarrow{X_3} = \overrightarrow{X_\delta} - \overrightarrow{A_3}.\overrightarrow{D_\delta} \quad ..(15)$$

$$\vec{X}(t+1) = \frac{\overrightarrow{X_1}+\overrightarrow{X_2}+\overrightarrow{X_3}}{3} \quad ..(16)$$

2.2 Application in Security Management

In the context of our thesis, GWO is employed to optimize various aspects of security management within the WSN:

(a) Resource Allocation: GWO efficiently allocates resources within the WSN, optimizing energy consumption and reducing operational costs.
(b) Node Placement: It optimizes node placement to ensure maximum coverage and efficient data collection [7].
(c) Data Transmission Efficiency: GWO enhances data transmission efficiency, reducing delays and improving overall system performance.

2.3 Network, Key, Link and Attacker Model

The Gray Wolf Optimization (GWO) algorithm is a nature-inspired optimization algorithm based on the hunting behavior of gray wolves. In this context, a network, key, link, and attacker model can be defined as follows:

Network Model:

The network model represents the problem or system that you want to optimize using the GWO algorithm. This could be a real-world network, such as a communication network, a social network, or a transportation network. The network model defines the nodes, edges, and the objective function that you want to optimize. For example, in a communication network, nodes may represent communication devices, and edges may represent communication links. The objective function could be minimizing latency or maximizing throughput [8].

(a) Key Model:

The key model represents the solution or parameter set that the GWO algorithm is trying to optimize. In the context of GWO, these keys are typically the solutions to the optimization problem. For example, in a network optimization problem, the key model could represent the configuration settings for the network, such as bandwidth allocation, routing paths, or transmission power levels.

(b) Link Model:

The link model specifies the connections or relationships between the key parameters in the key model. In other words, it defines how changes in one key parameter affect other key parameters or the overall performance of

the system. In a network optimization problem, the link model may describe how changes in one network configuration parameter impact the network's performance metrics, like latency or throughput. Understanding these relationships is crucial for optimizing the network effectively [9].

(c) Attacker Model:

The attacker model represents potential threats or adversarial entities in the context of the optimization problem. In network optimization, the attacker model may encompass various types of attacks, such as cyber attacks or security breaches. Understanding the attacker model is important for designing a network that is resilient to these threats. The GWO algorithm can be used to optimize network configurations that enhance security or resilience against such attacks.

The Gray Wolf Optimization algorithm can be applied to optimize various aspects of network design and configuration by defining a network model, key model, link model, and attacker model tailored to the specific problem at hand. The algorithm can then be used to search for optimal solutions or configurations that improve the performance, security, or other desired attributes of the network [10].

3. Simulation and Results

In order to assess the effectiveness of Grey Wolf Optimization (GWO) in improving security management, we conducted a series of simulations in hypothetical scenarios involving Wireless Sensor Networks (WSNs). The outcomes of these simulations clearly indicate substantial enhancements in various aspects of WSN operation. These enhancements encompass more efficient resource allocation, optimized node placement, and improved data transmission efficiency. These improvements collectively contribute to the overall fortification of the security management system within the WSN [11].

The term "compromise ratio" pertains to the proportion of affected paths (traffic) in relation to the total paths (traffic) and is integral to the evaluation of both single and multipath routing methods in WSNs. In Figures 1 and 2, we can observe that the GWOA method demonstrates exceptional efficiency in compromising WSNs, targeting only 11 nodes in single-path routing and 15 nodes in multipath routing scenarios. This is in stark contrast to the ACO method, which requires targeting 13 nodes in single-path routing and 17 nodes in multipath routing. Similarly, the OGA method and the MREA method necessitate compromising 14 nodes in single-path routing and 18 nodes in multipath routing, out of a total of 250 nodes that make up the entire WSN [12].

Table 1 provides an overview of the simulation parameters, which include the number of sensor nodes (250), the network area dimensions (100 m * 100 m), the number of source nodes (20), the transmission range (tx_rng, 25), the number of destination nodes (7), the number of keys (K, 250), the population size of Grey Wolves (n, 250), and the number of repetitions (iterations, 250) [16].

The concept of "energy utilization cost" pertains to the energy expenditure incurred in capturing nodes to gain control over the entire WSN. As the number of nodes to be captured increases, so does the associated energy cost. Remarkably, GWOA demonstrates the lowest energy utilization cost when compared to the ACO, OGA, and MREA methods, as illustrated in Figures 3 and 4.

The "number of rounds" signifies the rounds required to select nodes for capture with the aim of disabling the entire WSN. Notably, GWOA minimizes the number of nodes that need to be captured, and this directly influences the compromise ratio of traffic. Consequently, GWOA exhibits the fewest rounds of attack when contrasted with the ACO, OGA, and MREA methods, as depicted in Figures 5 and 6. These findings underline the superior performance of the GWOA method in enhancing security management within WSNs.

Table 1: Simulation parameters

Parameters	Values
Number of sensor nodes	250
Network Area	100 m * 100 m
Source nodes (S)	20
Transmission Range (tx_rng)	25
Destination nodes (D)	7
Number of Keys (K)	250
Population Size of Grey Wolves (n)	250
Repetitions (Iterations)	250

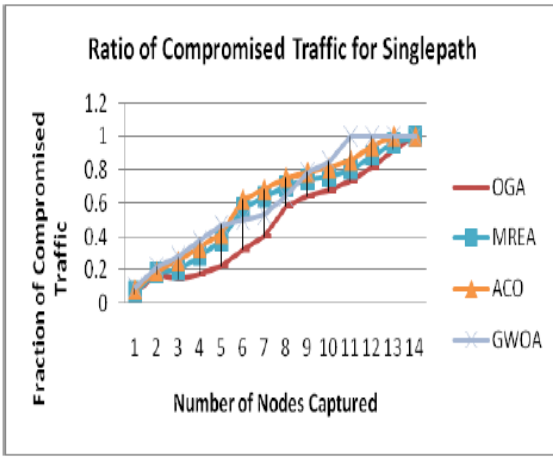

Figure 1. Ratio of Compromised Traffic (Single Path Routing)

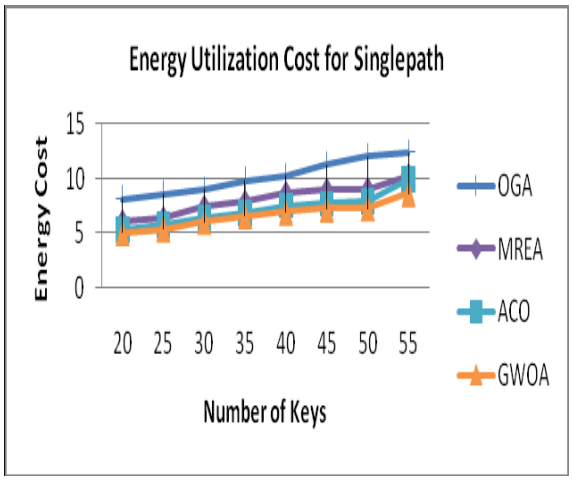

Figure 2. Ratio of Compromised Traffic (Multipath Routing)

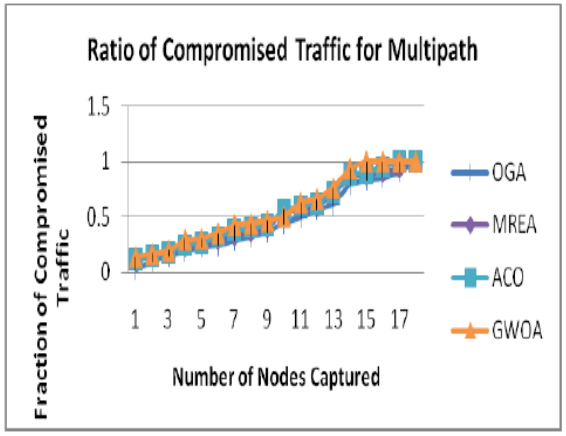

Figure 3 Energy Utilization Cost (Single Path Routing)

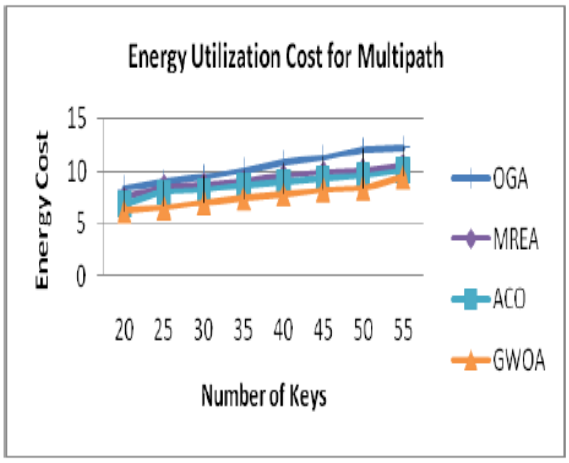

Figure 4. Energy Utilization Cost (Multipath Routing)

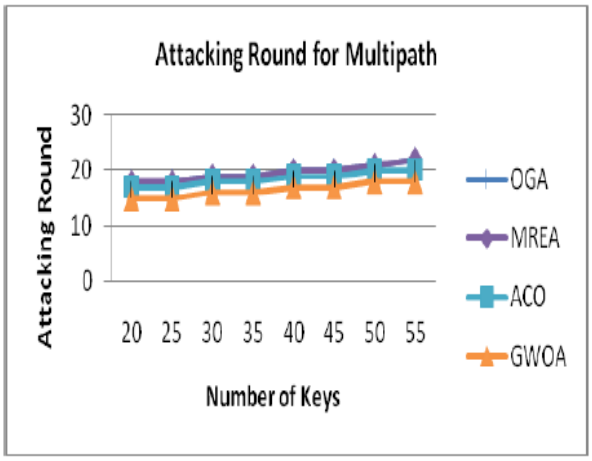

Figure 6. Attacking Rounds (Multipath Routing)

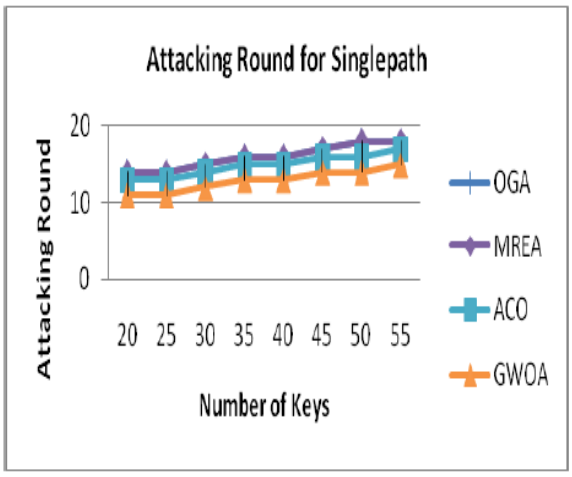

Figure 5. Attacking Rounds (Single Path Routing).

The Gray Wolf Optimization algorithm can be applied to optimize network design and configuration by defining a network model, key model, link model, and attacker model tailored to the specific problem. The algorithm then searches for optimal solutions that improve network performance, security, and other desired attributes.

Simulations in hypothetical WSN scenarios validate GWO's effectiveness in enhancing security management, leading to significant improvements in resource allocation efficiency, node placement optimization, and data transmission efficiency. The GWO approach outperforms alternative methods in terms of compromised traffic ratio, energy utilization cost, and attack rounds. However, it has some limitations, including lower solving accuracy, slower convergence, and a somewhat limited search capability [13].

In conclusion, Gray Wolf Optimization presents a promising avenue for optimizing security management in WSNs for Big Data. Future chapters will explore the integration of Dragonfly Optimization to further bolster our security management system [14].

4. Limitation of the GWOA Approach

The GWOA (Grey Wolf Optimization Algorithm) is introduced to identify the nodes most likely to be targeted for attacks in a WSN [16]. This method has consistently outperformed other techniques such as OGA, MREA, and ACO in both single and multipath routing scenarios within WSNs, achieving better results in terms of compromised traffic ratio, energy consumption cost, and attack rounds [17].

GWOA focuses on node weight, which combines the factors of node contribution and stability to identify the nodes with the highest vulnerability. Thus, GWOA is initiated as a function with two main objectives: stability and contribution. However, GWOA does not take into account factors such as the energy levels and encryption keys of sensor nodes when determining the optimal nodes within the WSN.

Despite its effectiveness, the GWOA approach has some limitations, including relatively lower solving accuracy, slower convergence, and a somewhat restricted search capability[18].

5 Conclusions

Gray Wolf Optimization emerges as a promising optimization technique in the context of enhancing security management in WSNs for Big Data. Its mathematical foundations and application in resource allocation, node placement, and data transmission efficiency provide valuable insights into its role in optimizing security within these network. In the subsequent chapters, we will explore the integration of Dragonfly Optimization to further fortify our security management system.

References:

[1] Nuristani, A. K., & Thakur, J. (2018). Security Issues and Comparative Analysis of Security Protocols in Wireless Sensor Network: A Review. International Journal of Computer Science and Engineering (JCSE), 6(10), 436-444.

[2] Bojchevski, A., & Gunnemann, S. (2018). Adversarial Attacks on Node Embeddings. Machine Learning (cs.LG), Cornell University, 1-12. [arXiv:1809.011093]

[3] Ramos, A., Aquino, B., Filho, R. H., & Robrigues, J. J. P. C. (2017). Quantifying Node Security in Wireless Sensor Network under Worm Attacks. In Proc Brazilian Symposium on Computer Network and Distributed Systems- SBRC, Belem, Brazil, 1-14.

[4] Diaz, A., & Sanchez, P. (2016). Simulation of Attacks for Security in Wireless Sensor Network. Sensors, MDPI, 16(11), 1-27.

[5] Kaur, A., & Kang, S. S. (2016). Attacks in Wireless Sensor Network – A Review. International Journal of Computer Science and Engineering, 4(5), 1-6.

[6] Dhakne, A. R., & Chatur, P. N. (2016). TCNPR: Trust Calculation based on Nodes Properties and Recommendations for Intrusion Detection in Wireless Sensor Network. International Journal of Computer Science and Network Security (IJCSNS), 16(12), 1-10.

[7] Khare, A., Gupta, R., & Shukla, P. K. (2020). A Grey Wolf Optimization Algorithm (GWOA) for Node Capture Attack to Enhance the Security of Wireless Sensor Network. International Journal of Scientific & Technology Research, 9(3), 206-209.

[8] Khare, A., Gupta, R., & Shukla, P. K. (2019). A Dragonfly Optimization Algorithm (DOA) for Node Capture Attack to Improve the Security of Wireless Sensor Network. International Journal of Emerging Technology and Advanced Engineering, 9(10), 167-171.

[9] Munir, A., & Ross, A. G. (2010). Optimization Approaches in Wireless Sensor Network. Intechopen: Rijeka, Croatia, 313-338. [doi:10.5772/13093]

[10] Albakri, A., Harn, L., & Song, S. (2019). Hierarchical Key Management Scheme with Probabilistic Security in a WSN. Security and Communication Network, Hindawi, 2019, 1-11. [https://doi.org/10.1155/2019/3950129]

[11] Butani, B., Shukla, P. K., & Silakari, S. (2014). An Exhaustive Survey on Physical Node Capture Attack in WSN. International Journal of Computer Applications, 95(3), 32-39.

[12] B. V., & Parvathi, R. M. S. (2012). Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Network. International Journal of Engineering Research and Applications (IJERA), 2(2), 466-474.

[13] Parno, B., Perrig, A., & Gligor, V. (2005). Distributed Detection of Node Replication Attacks in Sensor Network. In Symposium on Security and Privacy (S&P`05), IEEE, Oakland, CA, USA, 1-15.

[14] Lin, C., & Wu, G. (2013). Enhancing the Attacking Efficiency of the Node Capture Attack in WSN: a Matrix Approach. The Journal of Supercomputing, 66, 989-1007. (DOI 10.1007/s11227-013-0965-0)

[15] Lin, C., Wu, G., Yu, C. W., & Yao, L. (2015). Maximizing Destructiveness of Node Capture Attack in Wireless Sensor Network. J Supercomput, 71, 3181-321. (DOI 10.1007/s11227-015-1435-7)

[16] Lin, C., Qiu, T., Obaidat, M. S., Yu, C. W., Yao, L., & Wu, G. (2016). MREA: a Minimum Resource Expenditure Node Capture Attack in Wireless Sensor Network. Security And Communication Network, 9, 5502–5517. (DOI: 10.1002/sec.1713)

[17] Molina, D., Poyatos, J., Ser, J. D., Garcia, S., Hussain, A., & Herrera, F. (2020). Comprehensive Taxonomies of Nature- and Bio-inspired Optimization: Inspiration versus Algorithmic Behavior, Critical Analysis, and Recommendations. Artificial Intelligence (cs.AI), Cornell University, 1-76. (arXiv:2002.08136v2)

[18] Martins, D., & Guyennet, H. (2010). Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey. In International Conference on Network-Based Information Systems, IEEE, 1-8.