International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 02, Issue 03, May – June (2024)

RESEARCH ARTICLE

SELECTIVE FORWARDING ATTACKS DETECTION IN WIRELESS SENSOR NETWORKS USING BLUE MONKEY OPTIMIZED GHOST NETWORK

Jeyaraman Sathiamoorthy [1, *], M. Usha [2] and P. Senthilraja [3]

[1] Professor, Department of Computer science and Design, RMK Engineering College (Autonomous), RSM Nagar, Kavarapettai, Gummidipoondi Taulk, Thiruvallur District-601206, India.
[2] Professor and Assistant director, Department of Master of Computer Application, MEASI Institute of Information Technology, Royapettah, Chennai 600014, India.
[3] Assistant Professor, Department of Computer Science Engineering (Artificial Intelligence & Machine Learning), B.V. Raju Institute of Technology, Narsapur, Tuljaraopet, Telangana 502313, India.

Corresponding e-mail: jsathyam74@gmail.com

Abstract – Wireless Sensor Networks (WSNs) are increasingly the technology of choice due to their wide applicability in both military and civilian domains. The selective forwarding attack, one of the main attacks in WSNs, is the hardest denial-of-service attack to detect. The hostile nodes that initiate the selective forwarding attack will discard some or all of the data packets they receive. Numerous detection techniques for optional forwarding have been developed attacks are inaccurate or contain sophisticated algorithms, which is especially true when the attacker also uses other attacks like distributed denial of service, wormholes, and black holes to move through the network. To address these disadvantages, this research proposes a novel selective forwarding attack detection method based blue monkey-optimized ghost net (SAD-Ghost) method. To identify network threats, Blue Monkey optimization based on the hazard model is built in this case. A proposed technique to improve detection accuracy and minimize computation. The primary goal of the research is to develop a Selective Forwarding Attack Detection utilizing a blue Monkey optimized Ghost net to improve network lifetime. Initially, Blue Monkey optimization is used for optimal cluster head selection based on node degree and density. Moreover, cluster data are pre-processed using Tokenization, Normalization, and Reduction. The proposed method is utilized to detect intrusion in WSN and classify Normal, DDOS, Grey hole, and Blink litter. The experimental analysis demonstrates that the proposed method achieves a packet delivery rate of 97.6%, 95.3% and 90.50% and reduces energy consumption by 19.6%, 12.5% and 17.4% compared to existing clustering-based routing methods. Consequently, the proposed technique surpasses current methods in terms of network lifetime, energy efficiency, and packet delivery performance.

***Keywords** – Wireless Sensor Networks, Intrusion Detection, Blue monkey, Selective forwarding attack detection.*

1. INTRODUCTION

Wireless sensor networks (WSN) are regarded as one of the most important research subjects [1]. WSN has multiple uses in industries such as telecommunications, the military, healthcare, research, and agriculture. They are using networks to identify natural calamities like earthquakes, flooding, and volcanoes [2]. Many security risks have been introduced throughout the implementation and deployment phases of WSNs due to their broad use [3]. WSN face unique challenges such as limited storage, computing power, and battery life, making them vulnerable to attacks [4].

Altogether, people depend on networking networks to deliver fresh suggestions, solutions to their problems, and assistance in fulfilling their fundamental needs [5]. The most recent and frequently utilized technology Sensors that enable users to get data remotely and use it for a specific purpose are examples of advancements [6]. The Internet of Things (IoT) is a growing field of technology that uses sensors [7]. Researchers are increasingly interested in WSNs, as evidenced by a rise in research papers [8]. While WSN has benefits, it can also be vulnerable to DoS attacks due to security flaws.

Several security risks that could lead to data breaches are possible for users to encounter when utilizing WSN apps. Researchers have been working on new security methods to prevent DoS assaults from being successful [9]. Numerous technical developments have aided in the creation of creative strategies for sneaking in and thwarting such attacks. However, deep learning has developed the best defenses against these kinds of security threats and denial-of-service attacks. DoS attacks overwhelm a service, preventing it from offering services to other users [10]. A DoS attack overwhelms your site or infrastructure with traffic from several sources, typically barring access for some time.

One of the services that protects websites from DoS attacks is Cloudflare. It could be difficult to defend against DoS assaults. There is nearly no way to stop the flow of that torrent of illegal content because it is coming at you from everywhere on the Internet and around the world. It faced many security challenges due to limited resources, insufficient infrastructure, and a high volume of WSN usage. DoS attacks frequently target the World Wide Web (WWW), and stopping them is no easy task. To overcome these challenges Selective forwarding Attack Detection utilizing blue monkey optimized Ghost net (SAD-Ghost) has been proposed. These are the primary benefits of the suggested methodology:

- The primary goal of the research is to develop a Selective Forwarding Attack Detection utilizing a blue Monkey optimized Ghost net to improve network lifetime.
- Initially, Blue Monkey optimization is used for optimal cluster head selection based on node degree and density. Moreover, cluster data are preprocessed using Tokenization, Normalization and Reduction.
- The proposed method utilizes Ghost net to detect intrusion in WSN and classify normal, DDos Grey hole, Blink litter.
- As a result, the proposed techniques outperform existing methods based on network lifetime, alive nodes, and residual energy.

The following examples illustrate the remaining section of this study. Section 2 explains the literature review. In Section 3, the proposed SAD-GHOST is displayed together with an explanation and the associated algorithm. Section 4 offers the performance results and their analysis. Section 5 includes conclusions and suggestions for future work.

2. LITERATURE SURVEY

In 2020, Premkumar and Sundararajan et al. [11] Offered a deep learning-based defense mechanism (DLDM) to detect and isolate DoS attacks during the data forwarding phase (DFP). DoS attacks like flooding, homing, jamming, and weariness may now be identified with greater accuracy owing to a revolutionary approach that has been documented in studies. The system in the simulation shows extremely high levels of detection, throughput, packet delivery ratio, and accuracy. It also minimizes the number of erroneous alerts and wasted energy.

In 2020, Asad et al. [12] offered a novel feed-forward back-propagation-based deep neural network detection method for accurately identifying several of the proposed neural network architecture that can precisely identify and exploit the key high-level characteristics of packet forays in application layer DDoS attacks on a cutting-edge dataset that includes many DDoS attacks. Therefore, to overcome these obstacles or risks, they are trying to use artificial intelligence technology to identify them.

In 2022 Salmi and Oughdir et.al [13] suggested using CNN-LSTM to identify and categorize DoS intrusion attempts as floods, TDMA, blackholes, normal, or gray holes. The research used "A state-of-the-art dataset for a computer-generated WSN-DS. The dataset includes a built-in model" that accurately classified the provided attacks with 99% accuracy, showing promising results in attack detection.

In 2022, Salmi and Salim et.al. [14] proposed a method for noticing DOS attacks in WSN using a CNN-LSTM model. In this type of attack, the endpoints flood a specific target with traffic, preventing genuine users from accessing its services. The CNN-LSTM model developed was evaluated over 25 epochs and achieved accuracy, precision, and recall scores of 0.943, 0.958, and 0.921, respectively.

In 2021, Wazir Ali and Ahmad et al. [15] proposed the use of machine learning to sense flooding, and gray holes, to ensure the security of WSN, they must prevent black hole-distributed DoS attacks. The accuracy and speediness metrics were taken into consideration when conducting our review of the WSN-DS dataset. The J48 method boasts an impressive average processing time of just 0.54 seconds per sample, making it the fastest option available.

In 2020, Kim et al. [16] suggested a CNN-based approach for detecting DoS attacks using the datasets. Many layers were investigated in terms of their ability to do multiclass classification as well as binary classification. Following that, the suggested models were compared to an RNN model, and they outperformed the RNN model in both binary and multiclass classification. Over 97% accuracy was attained by the approach on both classification types.

To provide a stable network and reduce energy consumption in WSN, several related studies have been conducted. To encompass the lifespan of the network by reducing energy usage and reducing transmission delay, this research created the SAD-GHOST approach.

3. PROPOSED METHODOLOGY

This research proposes a novel Selective forwarding Attack Detection utilizing the blue monkey optimized Ghost net (SAD-Ghost) method has been proposed. Initially, Blue Monkey optimization is used for optimal cluster head selection based on node degree and density. Moreover, cluster data are pre-processed using Tokenization, Normalization, and Reduction. The proposed method is utilized to detect intrusion in WSN and classify Normal, DDOS, Grey hole, and Blink litter. Figure 1 shows the suggested method's general block diagram.

3.1 Blue Monkey Optimization using Cluster Head Selection

The blue monkey optimization strategy is utilized to suggest cluster head selection.

3.1.1 The inspiration for the blue monkeys

To add to security, Cercopithecus mitis works along with Cercopithecus ascanius. Males abandon the Cercopithecus mitis social system once they reach adulthood; hence, it is predominantly a female-dominated system. Cercopithecus mitis males rarely engage with the young. Young male Cercopithecus mitis should leave as soon as possible because it is a local species, which will increase their chances of surviving. They challenge the head of another family's family. If they succeed, they will control the family's leadership, which will give the young men the opportunity to socialize and get food and a place to live. The species, Cercopithecus mitis, is nomadic. Due to the accessibility of fruits and basic features, such as grander fruit patches, blue monkeys tend to waste time in forests.

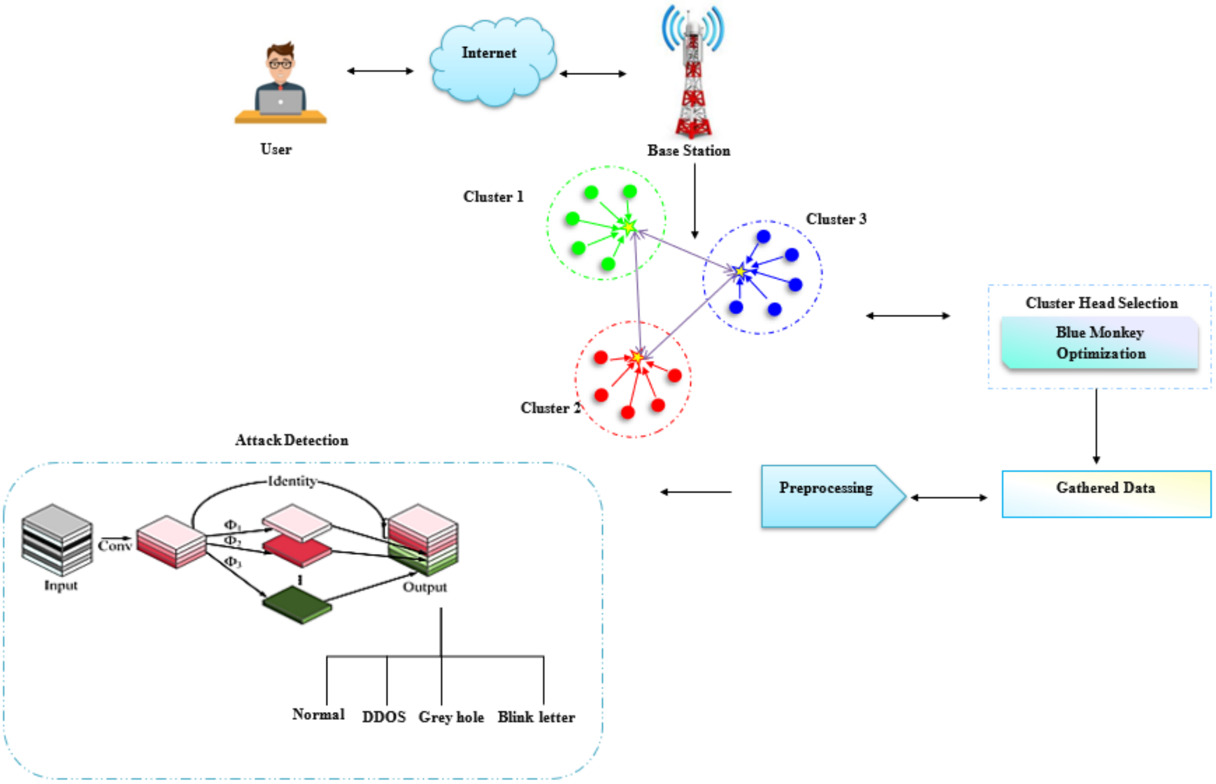

Figure 1. Proposed SAD-GHOST block diagram

Different from other species of monkeys are blue ones. They typically remain with their natal groupings since these social systems are dominated by women. However, after they reach adulthood, males leave their groupings. In the majority of blue monkey groups, there is just one male and many females and young children. This makes inbreeding more difficult. When the males reach adulthood, they leave the group and join another one, although it may take some time for them to find a new group, so they can appear to be lone males. When it comes to social interactions, blue monkeys lack robust instincts. There isn't much time for socializing; it usually happens while people are playing and taking care of one another.

The infants interact with their mothers as well as the other adults in the group. Because of this, these infants are rarely spotted with their male counterparts. Baby handlers handle all operations. The young females carry and protect the newborns as they take care of them. Babies are taught to react to all monkeys through this exercise. This computer program mimics the movements of the blue monkey. The monkey's area unit requires each cluster to move across the search space to mimic these kinds of interactions. Regarding the previous point, in a social setting, the stronger monkey and the one that begins scavenging for food across long distances are not included in the conventional field of view.

Additionally, male Cercopithecus mitis are territorial animals; thus, to get an advantage over the dominant male of a different family, they should leave the nest as soon as possible. The relationship between the males and the younger individuals of the species is currently minimal to nonexistent. If a man defeats another man, he takes over as the head of the family and can provide food, housing, and socializing for young men. Blue monkeys' new position in the group is determined by their previous position. Here is the conceptual framework of BMO equations:

Initialize the population: Generate an initial population of solutions randomly.

$$X_i = (X_{i1}, X_{i2}, \dots \dots \dots X_{id}) \; , \qquad \text{i =\{1,2,....N\}} \qquad (1)$$

where N is the population size and d is the dimension of the problem.

Evaluate the Fitness: Calculate the fitness value of each solution based on the objective function.

$$f(X_i), \qquad \text{i=1,2,.....N} \qquad (2)$$

Update positions: Update the positions of the monkeys based on their foraging behavior.

- **Exploration:** Monkeys explore the search space to find better solutions.

$$X_i^{(t+1)} = X_i^{(t)} + \alpha.rand.(X_j^{(t)} - X_k^{(t)}) \qquad (3)$$

where X_j and X_k are randomly selected monkeys, α is a constant, and a rand is a random number between 0 and 1.

- **Exploitation:** Monkeys exploit the known good solutions to refine their positions.

$$X_i^{(t+1)} = X_i^{(t)} + \beta.rand.(X_{best}^{(t)} - X_i^{(t)}) \qquad (4)$$

where $X_{best}^{(t)}$ is the best solution found so far and β is a constant.

Boundary check: Ensure that the new positions are within the predefined boundaries of the search space.

$$X_i^{(t+1)} = \max\left(min\left(X_i^{(t+1)}, X_{max}\right), X_{min}\right) \qquad (5)$$

Where X_{max} and X_{min} are the upper and lower boundaries of the search space

Algorithm 1: Blue Monkey Optimization
Initialize the blue monkey and children population BI (I=1...n).
Initialize power rate R and Weight w.
Distribute the fitness of children and all blue monkeys in each group
Calculate the fitness of children and all blue monkeys in each group.
For each group, select the worst value and the best value of fitness and store it in the current best. While children select the best fitness
T=1.
While (T≤ $maximum$ number of iterations)
Swapping the worst fitness in each group by the fitness in the children group.
Update the Rate and x position of all blue monkeys in each group by Equations 1 and 2.
Update Rate and x position of children by Equations 3 and 4.
Update the fitness of all blue monkeys and children.
Update Current Best:
New Best is better than current Best then current Best=New Best.
T=T+1.
End While
Return the optimal blue monkey.

3.2 Pre-Processing of Data

Network traffic processing produces observations represented by feature vectors. These can be classified in to four types they are Normal, DDOS, Grey hole, and blink litter used as input for data mining or machine learning algorithms. As these algorithms can learn from past data, they can automatically classify future observations.

3.2.1 Normalization

To select typical network traffic for testing and training, it is necessary. These datasets must be identified along with information regarding the normalcy or abnormality of the link. It can be difficult and time-consuming to label network traffic.

3.2.2 Tokenization

Its goal is to provide new features that are more discriminative than the original feature set. Machine learning algorithms may greatly benefit from this. Features can be created by hand or with the use of data mining techniques, including frequent-episode mining, association mining, and sequence analysis.

3.2.3 Reduction

It is frequently used to reduce the dataset's dimensionality by removing any superfluous or pointless characteristics. Known as feature selection, this optimization technique is frequently employed to mitigate "the curse of dimensionality. Consider feature extraction as an effective method for reducing data, achieved by transforming the original feature set into a more concise set of new features. PCA, a well-regarded linear technique, is widely used for efficient data reduction.

3.3 Intrusion detection via ghost network

Ghost network is used for the advantage of feature map redundancy and achieves better accuracy and latency than other lightweight networks by striking a balance between accuracy and real-time. ARM-based embedded systems enable exceptional algorithmic performance.

The Ghost Net harnesses the power of the Ghost module, incorporating cost-effective operations and standard convolution techniques. Through this approach, it efficiently merges the M layers of the original feature maps using a single convolution. The process involves two key sections: one that generates the necessary feature concentrations (m) through 1x1 ordinary convolution for identity, and another that utilizes depth-separable convolution blocks to stack and linearly transform the original feature maps (m) into compelling 'Ghost' feature maps layer by layer. These Ghost feature maps are then seamlessly combined with the m feature maps following the identity to create innovative new feature maps.

$$n = m \times s. \qquad (6)$$

Considering that a fundamental mapping has been included in the Ghost module and

$$m\cdot(s-1) = ns\cdot(s-1) \qquad (7)$$

Every linear transformation operation should have d × d as its kernel. Theoretically, the Ghost module can accelerate regular convolution by the following ratio:

$$RS = \frac{n\cdot w\prime\cdot h\prime\cdot c\cdot k\cdot k}{\frac{n}{s}\cdot w\prime\cdot h\prime\cdot c\cdot k\cdot k+(s-1)\cdot\frac{n}{s}\cdot w\prime\cdot h\prime\cdot c\cdot d\cdot d} = \frac{c\cdot k\cdot k}{\frac{1}{s}.c\cdot k\cdot k+(s-1)\cdot 1s\cdot d\cdot d} \approx \frac{c.s}{c+s-1} \approx s \qquad (8)$$

The width and height of the yield picture, represented as w' and h', are determined by the number of input channels, denoted as c, received by the convolution kernel. It has improved GhostNet in a few ways since the system in this study is meant to identify a fire in remote-sensing images. More specifically, it enhances the Ghost module with dynamic convolution to improve its ability to adjust to the compound and ever-changing morphology of flames.

The decision to utilize dynamic convolution to enhance GhostNet's Ghost module was influenced by existing literature. Dynamic convolution involves weighting four convolution kernels of the same dimension based on input characteristics.

$$out(x)=\alpha((\partial 1k1+\partial 2k2+\partial 3k3+\partial 4k4)\times x) \quad (9)$$

If each convolution kernel is represented by ki, the convolution operation is denoted by x, the activation function is α, and "the parameter for weighting that depends on the input sample." is αi. Equation 7 shows that αi is the result of focusing on the four essential calculations inside the dashed box.

$$\partial I\ (x)=Sigmoid\ (GAP(x)\ R) \quad (10)$$

where R is the matrix representing the relationship between the number of convolutional kernels and the input dimensions. The firmness of the feature layers to acquire global spatial information is represented by the GAP, and the weights of the four convolution kernels that were formed are represented by the sigmoid function. By integrating the data from several convolutional kernels, dynamic convolution broadens and deepens the network, enhancing the algorithm's ability to extract features. As deep learning progresses, there are an increasing number of various network architectures; nevertheless, as data sizes increased, researchers started focusing on sparse memory, and computational power was leveraged to create compact network models.

3.3.1 Ghost Bottleneck

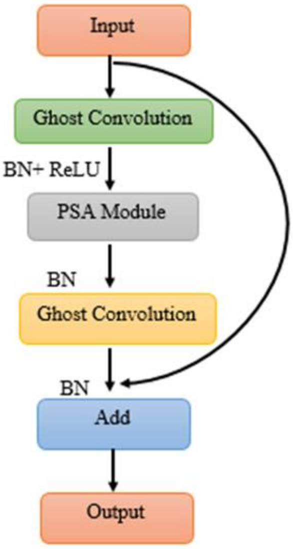

Figure 2. Ghost Bottleneck

Depicts the layout of a bottleneck with two-step sizes. A bottleneck is made by stacking two Ghost modules on top of one another, connecting a residual structure, and then further deepening the network structure. ResNet and the Bottleneck vary in that the Bottleneck adds the same residual structure to the output and adds a deep separable convolution operation with the middle. The goal is to successfully avoid the issues of performance deterioration and gradient vanishing. A batch normalizing procedure is carried out after each layer, and the ReLU function is engaged following the first bottleneck structure. With this structure, the problems of performance degradation and gradient vanishing are successfully avoided. After the first bottleneck structure, each layer is subjected to a batch normalization process before the ReLU function is activated. This topology aims to deepen the network structure while reducing the size of the feature layer.

4. RESULT AND DISCUSSION

To evaluate the performance of the proposed SAD-GHOST approach, we run extensive simulations in this section. Comparisons between the proposed protocol and RSA, RPL, and DOS are made. To compare the suggested technique with past attempts, the simulation time has been set to 1500 seconds.

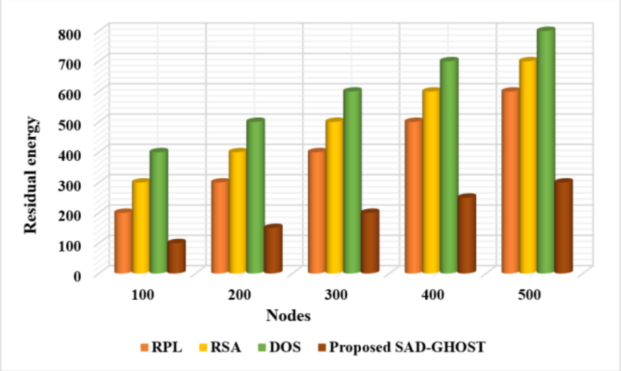

Figure 3. Residual energy vs. number of sensor nodes

Figure 3 illustrates that residual energy diminishes as the number of nodes decreases. Additionally, the proposed SAD-GHOST technique outperforms other routing methods, surpassing previous strategies in terms of average residual energy by 22.15%, 19.45%, and 10.34%.

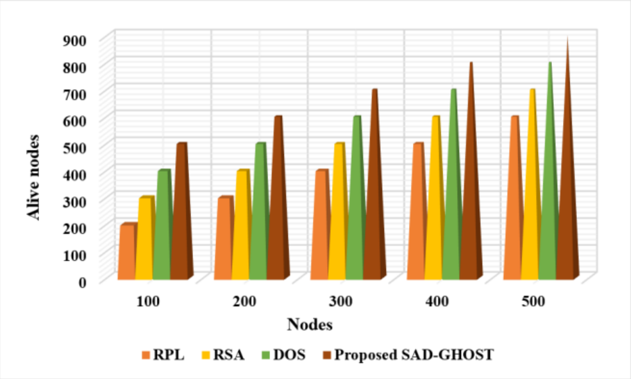

Figure 4. Alive nodes vs. number of sensor nodes

The proposed SAD-GHOST approach generates more alive nodes than the earlier DSO, RSA, and RPL methods, as demonstrated in Figure 4. The SAD-GHOST strategy is found to be superior when compared to older techniques, the proportion of active network nodes.

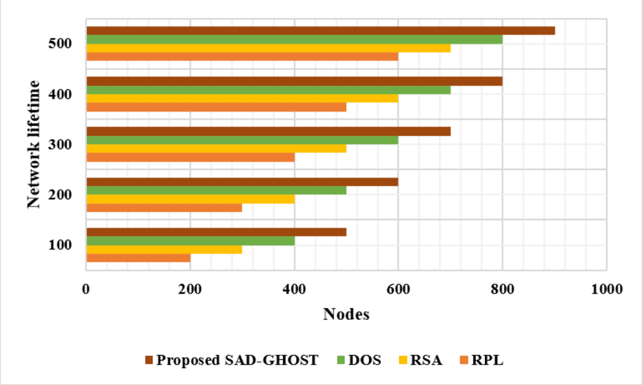

Figure 5. Network lifetime vs. number of Sensor nodes

Figure 5 shows the lifespan of the network for different node counts. The analysis demonstrates that even with a large number of nodes, the suggested SAD-GHOST model lengthens the network's lifespan. The comparable network lifespan determined by the existing methods (RPL, RSA, and DOS) is planned at 22.34%, 20.13%, 17.23%, and 19.04%, respectively.

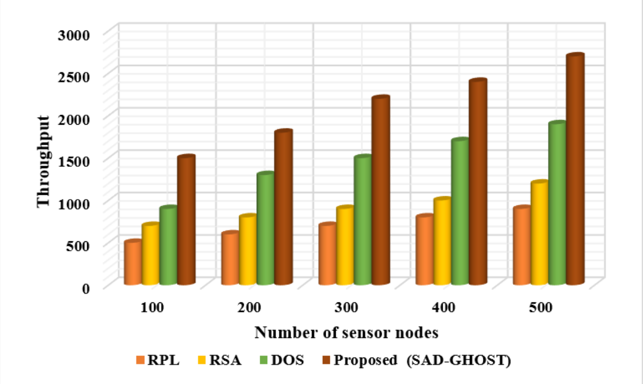

Figure 6. Throughput Vs Number of Sensor nodes

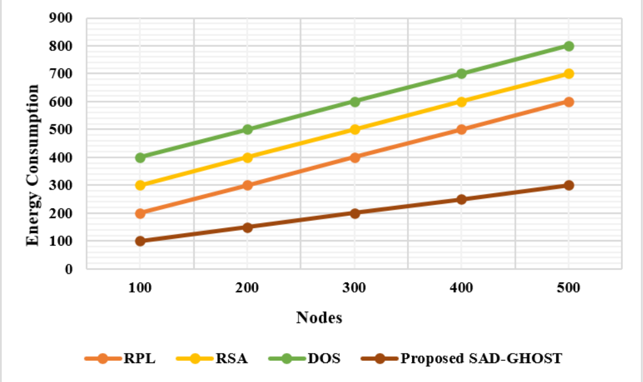

Figure 7. Energy Consumption Vs Number of Sensor Nodes

Figure 6 presents a throughput comparison between the SAD-GHOST strategy and previous methods. The results demonstrate that the proposed method performs exceptionally well in terms of throughput for all sensor nodes. One of the most crucial factors in the development of QoS is throughput. Thus, network scalability is guaranteed. Attaining optimal network performance is not solely dependent on network lifespan. Consequently, QoS factors are crucial for enhancing network efficiency and bolstering the dependability of routing algorithms. Any network's routing protocol's scalability is directly correlated with its throughput. Here, the proposed method's scalability reaches a limit when the number of nodes rises above 1000.

Figure 7 provides a detailed comparison of the SAD-GHOST technique to existing methods (RPL, RSA, and DOS), in terms of energy consumption vs nodes. The figure illustrated the RPL protocol's incapability to outperform other strategies with a maximum amount of energy usage. Additionally, compared to the RSA method, DOS obtained a somewhat reduced energy use. The proposed SAD-GHOST methodology, however, surpassed existing strategies with a lower energy consumption, while the present approach achieved a slightly higher energy consumption.

5. CONCLUSION

In this research proposed a novel selective forwarding attack detection method based blue monkey-optimized ghost net (SAD-Ghost) method. To identify network threats, Blue Monkey optimization based on the hazard model is built in this case. A proposed technique to improve detection accuracy and minimize computation. The primary goal of the research is to develop a Selective Forwarding Attack Detection utilizing a blue Monkey optimized Ghost net to improve network lifetime. Initially, Blue Monkey optimization is used for optimal cluster head selection based on node degree and density. Moreover, cluster data are pre-processed using Tokenization, Normalization, and Reduction. The proposed method is utilized to detect intrusion in WSN and classify Normal, DDOS, Grey hole, and Blink litter. The experimental analysis demonstrates that the proposed method achieves a packet delivery rate of 97.6%, 95.3% and 90.50% and reduces energy consumption by 19.6%, 12.5% and 17.4% compared to existing clustering-based routing methods. Consequently, the proposed technique surpasses current methods in terms of network lifetime, energy efficiency, and packet delivery performance. As a result, the proposed techniques outperform existing methods based on network lifetime, alive nodes, and residual energy.

CONFLICTS OF INTEREST

This paper has no conflict of interest for publishing.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] M. Faris, M.N. Mahmud, M.F.M. Salleh, and A. Alnoor, “Wireless sensor network security: A recent review based on state-of-the-art works”, *International Journal of Engineering Business Management*, vol. 15, pp.18479790231157220, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] M. Krichen, M.S. Abdalzaher, M. Elwekeil, and M.M. Fouda, Managing natural disasters: An analysis of technological advancements, opportunities, and challenges. *Internet of Things and Cyber-Physical Systems.* 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] R. Yarinezhad, and S.N. Hashemi, A sensor deployment approach for target coverage problem in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp.5941-5956, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] T. Jabeen, I. Jabeen, H. Ashraf, N.Z. Jhanjhi, A. Yassine, and M.S. Hossain, An intelligent healthcare system using IoT in wireless sensor network. *Sensors*, vol. 23, no. 11, pp.5055, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] P.A.D.S.N. Wijesekara, and S. Gunawardena, A Review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges. *Network*, vol. 3, no. 3, pp.343-421, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] B. Kapoor, B. Nagpal, and M. Alharbi, Secured healthcare monitoring for remote patient using energy-efficient IoT sensors. *Computers and Electrical Engineering*, vol. 106, pp.108585, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] A. Morchid, R. El Alami, A.A. Raezah, and Y. Sabbar, Applications of internet of things (IoT) and sensors technology to increase food security and agricultural Sustainability: Benefits and challenges. *Ain Shams Engineering Journal*, pp.102509, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] F. Zijie, M.A. Al-Shareeda, M.A. Saare, S. Manickam, and S. Karuppayah, "Wireless sensor networks in the internet of things: review techniques, challenges, and future directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, pp.1190-1200, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] A. Suhag, and A. Daniel, Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense. *Journal of Cyber Security Technology*, vol. 7, no. 1, pp.21-51, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ö. Aslan, S.S. Aktuğ, M. Ozkan-Okay, A.A. Yilmaz, and E. Akin, A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, vol. 12, no. 6, pp.1333, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] M. Premkumar, and T. Sundararajan, "Dldm: Deep learning-based defense mechanism for denial-of-service attacks in wireless sensor networks", *Microprocess Microsyst.* Vol. 79, pp. 103278, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] M. Asad, M. Asim, T. Javed, M.O. Beg, H. Mujtaba, and S. Abbas, "Deepdetect: detection of distributed denial of service attacks using deep learning", *Comput J.* vol. 63, no. 7, pp. 983–94. 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] S. Salmi, and L.Oughdir, "Cnn-lstm based approach for dos attacks detection in wireless sensor networks". *Int J Adv Comput Sci Appl. vol*. 13, no. 4, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] R, Wazirali, and R. Ahmad, "Machine learning approaches to detect dos and their effect on wsns lifetime", *CMC-Comput Mat Contin.* Vol. 70, no. 3, pp. 4921–46, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] J. Kim, H. Kim, M. Shim, and E. Choi, "Cnn-based network intrusion detection against denial-of-service attacks", *Electronics.* [CrossRef] [Google Scholar] [Publisher Link]

[16] L. Alsulaiman, and S. Al-Ahmadi, "Performance evaluation of machine learning techniques for DOS detection in wireless sensor network", arXiv preprint arXiv:2104.01963. 2021. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Jeyaraman Sathiamoorthy is currently working as a Professor RMK ENGINEERING COLLEGE, Kavarapettai in Chennai. He has completed M. Tech (CIT) and Ph. D from Manonmaniam Sundaranar University, Tirunelveli. He has 20 years of teaching experience and she has published papers in Network Security in National and International journals and has presented in International Conferences and Seminars. His current area of interest is Programming Languages, Algorithms and ad-hoc networks especially MANET, VANET, FANET and Underwater Communication.

M. Usha is currently working as a Professor cum Assistant Director in MEASI Institute of Information Teahnology, Chennai. She has completed M.C.A. and M. Phil in Computer Science from Bharathidasan University, Trichy. She has also done her M. Tech (CIT) and Ph. D from Manonmaniam Sundaranar University, Tirunelveli. She has 20 years of teaching experience and she has published papers in Network Security in National and International journals and has presented in International Conferences and Seminars. Her current area of interest is Operating Systems, Algorithms and ad-hoc networks especially MANET, VANET, FANET and Underwater Communication.

P. Senthilraja is currently working as an Assistant Professor at BV Raju Institute of technology, Narsapur in Telengana. He has completed M.Tech(CIT) from Manonmaniam Sundaranar University, Tirunelveli. He has 12 years of teaching experience and he has published papers in Network Security in National and International journals. His current area of interest is Machine learning, network security, ad-hoc networks especially MANET and VANET.

Arrived: 20.04.2024

Accepted: 08.06.2024