Proceedings of the Second International Conference on Edge Computing and Applications (ICECAA 2023)
IEEE Xplore Part Number: CFP23BV8-ART; ISBN: 979-8-3503-4757-9

# Crow Search Optimization to Identify Adversary Nodes in Wireless Networks

Gnanajeyaraman Rajaram
*Department of Applied Machine Learning, Saveetha School of Engineering, Saveetha Institute of Medical And Technical Sciences,*
Chennai, Tamil Nadu, India
gnanajeyaramanrajaram114@gmail.com

T. Stephen Thangaraj
*Department of Computer Science and Engineering,*
*Paavai Engineering College,*
Namakkal, Tamil Nadu, India
dr.stephen1979@gmail.com

A. Packialatha
*Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advanced Studies,*
Chennai, Tamil Nadu, India
packialatha.se@velsuniv.ac.in

R. Deepa
*Department of Computer Science and Engineering,*
*Vels Institute of Science, Technology & Advanced Studies,*
Chennai, Tamil Nadu, India
deepar.se@velsuniv.ac.in

2023 2nd International Conference on Edge Computing and Applications (ICECAA) | 979-8-3503-4757-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICECAA58104.2023.10212309

***Abstract*—Adversary node detection systems have become a vital component due to the malware attacks. These systems are very important for network security due to internet's widespread development and increased accessibility to global data systems. This paper presents a Crow Search Optimization Algorithm (CSOA) to detect the adversary node in a wireless network. The Rivest, Shamir, Adleman (RSA) algorithm transmits secure data at first. It uses the public key to encrypt the data and the private key to decrypt the data and the adversary nodes can't access or modify the real data. One of the significant problems is when an unknown attack occurs on the network due to the high volume of data while the detection's accuracy and false alarm rate decline. The proposed system aims to improve accuracy by identifying the adversary nodes using CSOA algorithm. From the results, it is observed that the CSOA mechanism reduces the loss ratio and improves throughput of the network.**

***Keywords*— *Crow search optimization algorithm, Adversary node detection, Secure data transmission, Wireless sensor network***

## I. INTRODUCTION

Wireless networks are essentially a collection of nodes dispersed over a wide region, allowing the needed data to be gathered [1]. However, nodes are also susceptible to attacks from malicious software, hackers, adversaries, defective hardware, natural phenomena, etc. Therefore, it is essential to defend a node from assault since if it does, the node's information could be inaccurate, resulting in inaccurate data analysis and unneeded results [2]. Because wireless networks are transient and lack infrastructure, network anomalies are frequently prevalent. These abnormalities may have several causes, including faulty network hardware, network congestion, adversary, and active attacks. An acute anomaly known as intrusion threatens the network's availability and service integrity.

Because of ongoing hardware advancements, personal Digital Assistants, mobile phones, and converged devices like PDA phones continue to gain considerable computing, storage, and communication capabilities. The communicating devices in the majority of these cases may or may have yet to develop reliable relationships with one another. These ecosystems are open and dynamic, making identification and authentication complex tasks. Devices can readily spoof IP addresses and adopt "fake" identities. Utilizing communication protocols that use cryptography, mobile devices can increase security. However, since authentication services might not be accessible, it can be challenging to determine the identities of trustworthy devices. A machine can be taken or cooperated and then attempt to undermine the network it is a part of, even in the presence of pre-distributed security credentials.

The following are the difficulties with the design of wireless networks [3]. **Adverse situation:** Surrounding-related parameters can cause the node to stop functioning if deployed arbitrarily into a space. An attacker can exploit this circumstance and control it. **No observation:** SNs are placed in areas where it is impossible to conduct continuous observation, making it simple for an adversary to physically tamper with them before attacking a greater scale. **Restricted Resources**: The nodes need energy, memory, and other resources for data communication and collection in order to function. Since a node only has a limited amount of these resources, using them all up could cause the nodes to stop working, which could cause system delay, garbled messages, packet drops, etc. **Consistency**: In wireless networks, node data may be distorted owing to channel errors, which may cause struggles. The data may also be distorted at highly busy nodes, making attacks simple to launch. The overload results increase delay, which causes synchronization issues and lag in the system, including nodes, due to higher congestion.

An identifying malicious node detection based on correlation detection (IMCD) for recognizing adversary nodes established on correlation theory and serves to protect against fault data injection attacks [4]. First, irregularities within groups of sensor data that are of a similar kind are identified via the use of temporal correlation. Second, malicious nodes are discovered using geographical correlation as the basis for the analysis. Third, the malicious

nodes that have been detected are checked for validity using event correlation. The findings of the experiments demonstrate that this approach provides lesser ratio of false-positive and false-negative than those of the classic fuzzy reputation model and weighted-trust-based mechanisms. The adversary node detection process among nodes in the wireless network is shown in Figure 1. From this figure, the node m act as an adversary. This mechanism uses the CSO algorithm to separate the m adversary node efficiently. Further, the RSA algorithm provides data security in the wireless network.

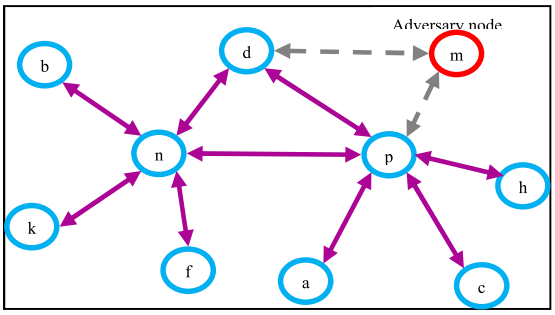


Fig. 1. Adversary node detection in wireless network

## II. Literature Review

ANFIS, which stands for Adaptive Neuro-Fuzzy Inference System, will be used to locate the intrusion nodes[5]. Optimizing the parameters of the ANFIS model, which is trained on a network traffic dataset, is accomplished with the help of the CSO method. This model is used to differentiate between normal and adversarial nodes. The threshold-based intrusion detection is used to identify and defend against a wide range of threats, including floods, wormholes, and black hole assaults, among others [6]. This mechanism uses two different threshold values, both of which are subject to dynamic adjustment dependent on the circumstances of the network. The first threshold value is used to determine whether or not an attack is really taking place, while the second threshold value is utilized to determine whether or not to begin the process of mitigating the attack.

Support vector machines (SVM)-are primarily based on intrusion detection systems (IDS) [7]. The suggested IDS comprises three primary elements: feature selection, feature scaling, and an SVM classifier. The feature scaling mechanism takes the features that were picked using the feature selection method and normalizes them to a typical range. The feature selection method selects the most relevant characteristics to the problem by using mutual information. In order to decide whether traffic is reliable otherwise unreliable, the SVM classifier must first be trained with the help of the chosen and scaled characteristics.

A decentralized malicious node detection approach established on the Received Signal Strength [8]. These techniques separate the malicious nodes and block these nodes operation in the network. This technique also detects the malicious node position. MANETs make use of methodologies such as context-free grammar (CFG), often known as the Fibonacci-Pascal triangle (FPT) [9]. The CFG uses this mechanism and FPT mechanisms in this scenario. In order to isolate the mobile node, the CFG is used, and the FPT is utilized to mask the mobile nodes' true information. A confidential message is sent to the destination in order to prevent mobile observers from intercepting the data flow. The findings of the simulation show that using a dynamic estimate of the Quality of Service (QoS). However, this mechanism not provides secure information from sender to receiver. Genetic Algorithm-based SVM and the Genetic Algorithm-based Decision Tree have been presented to identify malicious nodes [10]. Following identifying the malicious node, the Dijkstra algorithm is applied to the network to locate the most effective routing route. The QoS is conscious of asynchronous duty-cycled in the light of constructing the routing, wherein waiting for the delay and discarding malicious packets are crucial to the network's overall performance [11].

The QoS is conscious of asynchronous duty-cycled technique is used for minimizing the congestion [12]. This mechanism uses sleep delay and queue length as its two primary inputs. Metrics aware of QoS standards may be used to create a routing protocol that is aware of QoS standards. This can improve QoS performance. It is proposed that a solution can be found for an adaptive distributed system that can detect malicious nodes in an IPv6-based network [13]. Distributed algorithms and a group-based mechanism to decision-making form the foundation of the proposed intrusion detection system. It presents a novel idea of estimating the probability of malicious behavior in sensor nodes, an important innovation. The suggested procedure is built and put through its paces by using a wide variety of situations while operating in one of three distinct network scenario. Lastly, the completed study demonstrated that the suggested method is energy efficient and can identify malicious nodes.

Trust is an attack-resistant malicious node detection mechanism that has been proposed in order to increase the level of network security [14]. In this mechanism, malicious nodes are identified based on the behaviors observed by the nodes themselves, as well as recommendations shared by other nodes. Malicious intent on the part of a node might force it to behave in a way that dramatically degrades its performance. This is because the majority of currently available routing protocols are designed to discover the most efficient route.

An incentive mechanism should be included in the decision-making process for MANET routing so that inappropriate conduct may be addressed through protocols based on the trust vector concept for routing [15]. By observing the flow of communication between neighboring nodes, each node would assess the trustworthiness of its neighbors according to its own internal criteria. At the same time, the dynamics of trust are considered while speaking about robustness. This strategy enhances efficiency by using the Dynamic Source Routing protocol. Ant Based Routing Algorithm for balanced the load and optimize the routing path is discussed in [16].

## III. Proposed Methodology

The foundation of the Crow search method is the idea of attacker node detection in wireless networks. Utilizing crows' innate capacity to look for and spot potential environmental risks is the primary premise behind this strategy. This mechanism uses the CSOA algorithm to isolate adversary nodes in a network. As following is how the Crow search algorithm operates: Crows are first introduced into the network as a group. Each crow has a distinctive ID and a

GPS receiver. After then, the crows start searching the network for adversary nodes. A crow notes the ID, location, and other pertinent details of any adversary nodes it finds.

Based on the manager's analysis of the packet loss ratio, delay, available bandwidth, and energy information, the CSO algorithm then identifies which nodes are most likely to be adversaries. Following that, these nodes are segregated and eliminated from the network.

**CSO algorithm procedure:**

The CSO mimics how crows hide food. Crows are smart birds that can recognize concentrates and alert their species to danger. One of the ways they show their cunning is by hiding food and remembering where it is [17].

1) Initializing a d-dimensional random swarm of crows.
2) Each crow is assessed using a fitness function, and its result is stored as an preliminary memory value. Every crow keeps a record of its hiding spot in its memory variable mi.
3) Crow chooses a arbitrary another crow, xj, as well as generates a random number to update its location.

Crow xi will follow xj to learn about mj if this value exceeds the threshold. Crow updates its location by choosing a different crow at random, say xj, and following it to find mj. Following that, fresh xj is determined as follows:

$$X_j = X_{j,1}, X_{j,2}, X_{j,3}, \ldots X_{j,d} \quad (1)$$

where $SS^{j,iter}$ denotes the likelihood that a crow will be aware, iter denotes the number of iterations, $r_j$ denotes random numbers and $SS^{j,iter}$ is the length of a crow's flight to indicate memory.

$$X^{iter+1} = X^{iter} + R_m + ss^{j,iter} * K^{j,iter} - X^{iter} \quad (2)$$

**CSO-based fitness function Computation:** This mechanism computes the fitness by applying parameters like node energy, packet loss ratio, and delay. This fitness function calculation is given below.

$$F = \alpha_1 * fn_1 + \alpha_2 * fn_2 + \alpha_3 * fn_3 + \alpha_4 * fn_4 \quad (3)$$

where $\alpha_1 - \alpha_4$ denotes the parameters of weight, $fn_1$ indicates the node energy, $fn_2$ represents the packet loss ratio, $fn_3$ indicates the node bandwidth, and $fn_4$ represents the delay. Figure 2 demonstrates the architecture of the CSOA system.

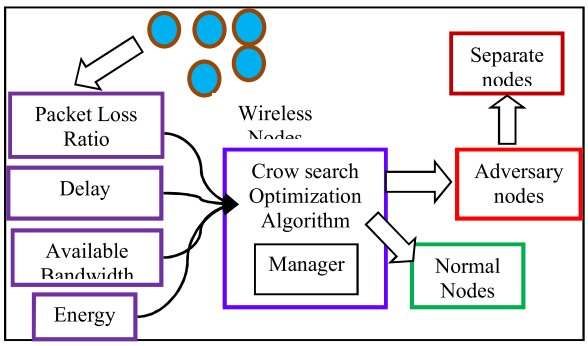


Fig. 2. Architecture of the CSOA mechanism

The adversary node has the highest energy compared to the average energy value. Also, the adversary node has the highest packet loss ratio than the neighbour nodes. In addition, the adversary node takes more time to transmit the data to one another. Furthermore, the adversary node has the highest available bandwidth but forwards the busy message during data transmission. As a result, the highest residual energy, highest packet loss ratio, highest available bandwidth, and highest delay node separate the adversary nodes in the wireless network.

After selecting the relay node from the nearby nodes, the route discovery is made using the DSR. To locate routes, this system uses DSR control messages such as route request (RREQ), route reply (RREP). Find the secure route by using the CSO fitness function generated based on the QoS criteria. All nodes are initially broadcasted with the RREQ by the sender. The chosen best relay node will then deliver the RREP message back to the sender node in the following step. The same process is carried out repeatedly till the receiver node is reached. The data packets are transferred over the network using the secure route when the sender receives the RREP message. Additionally, this route discovery phase maintains the route via the RERR.

**Data Security:**

After identifying adversary nodes from the route, provide data security by applying the RSA algorithm. RSA is a public key cryptography technique that utilizes public and private keys to encrypt and decrypt the data. The sender node encrypts the original data. This data is known as plain text, and the plain text is changed to the cipher text utilizing the public key; the sender forwards this cipher text via selected relay nodes to the receiver. Finally, the receiver node received this cipher text and then converted the original text via private key. The RSA algorithm is a better security algorithm. Hence, the receiver received without modified data in the wireless network.

## IV. Results And Discussion

In this part, the simulation results of IMCD and CSOA algorithms based on DSR are discussed. Network simulator-2 is the program that is used to carry out the simulations. The CSO using RSA methods may identify the attacker node quickly and securely transport data from the sender to the recipient. The CSOA modeling simulation's parameter settings. The performance of the CSOA technique is assessed using QoS characteristics such as adversary node detection ratio, false alarm ratio, throughput, and loss ratio.

Figure 3 demonstrates the packet loss ratio of CSOA and IMCD mechanisms based on adversary nodes. From the simulation results, the CSOA and IMCD mechanism loss ratio is also raised when the adversary nodes count increases. Compared to the IMCD and CSOA mechanisms, the CSOA mechanism minimizes the packet loss ratio.

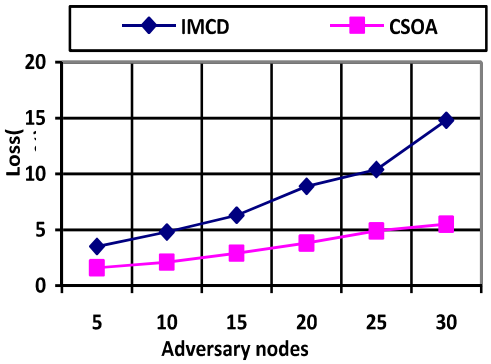


Fig. 3. Loss ratio of IMCD and CSOA Mechanisms based on adversary nodes based on adversary nodes

Figure 4 demonstrates the detection ratio of IMCD and CSOA mechanisms based on adversary nodes. The adversary node count rises from 5 to 30 nodes the detection ratio is minimized. Compared to the IMCD and CSOA mechanisms, the proposed CSOA mechanism is slightly minimized but increases the detection ratio compared to the conventional IMCD mechanism, because, the CSOA mechanism uses the CSO algorithm to separate the adversary nodes efficiently.

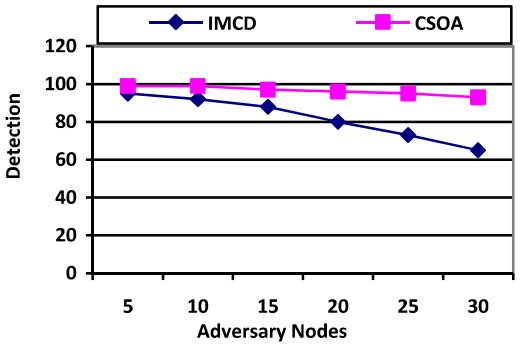


Fig. 4. Detection Ratio of IMCD and CSOA Mechanisms based on adversary nodes

Figure 5 demonstrates the false alarm ratio of IMCD and CSOA mechanisms established on adversary nodes. When increases the adversary node counts, the false alarm ratio also increases. From this figure, the CSOA mechanism using the CSO algorithm has a very lesser false alarm ratio. But, the IMCD mechanism has a higher level of false alarm ratio.

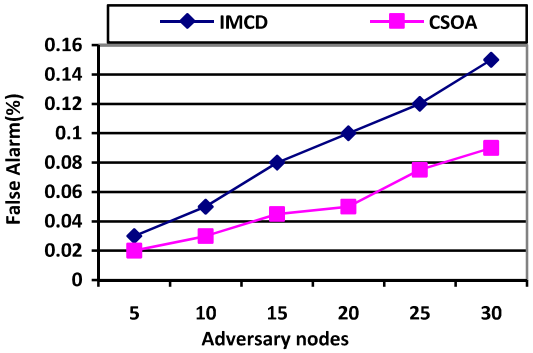


Fig. 5. False Alarm of IMCD and CSOA Mechanisms based on adversary nodes based on Adversary nodes

Figure 6 illustrates the throughput ratio of IMCD and CSOA mechanisms established on adversary nodes. From this figure, when increases the adversary nodes from 5 to 30 adversary nodes, the CSOA mechanism has a little minimizes the throughput. But, the IMCD mechanism highly minimizes the throughput ratio. The CSOA mechanism is almost 90%, but the IMCD mechanism reaches below 80%.

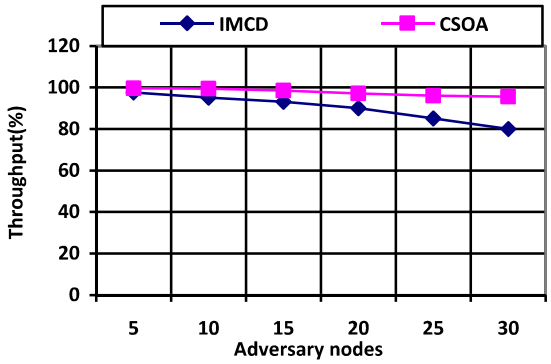


Fig. 6. Throughput ratio of IMCD and CSOA Mechanisms based on adversary nodes based on adversary nodes

## V. Conclusion

This research study introduced CSOA to detect adversary nodes. This mechanism aims to detect the adversary nods and secure data transmission from sender to receiver. This mechanism uses the CSO algorithm to compute the fitness function based on node energy, node delay, node loss, and available bandwidth. Hence, it detects the adversary node reach above 95%. In addition, the RSA algorithm is used to transmit the data confidentially. The RSA algorithm uses the public and private keys to forward the decrypted data. Hence, the adversary node is not able to access the real data. The experimental outcomes demonstrate the CSOA mechanism raised the detection ratio and reduced the false alarm ratio. Furthermore, the CSOA mechanism raised the throughput and minimizes the packet loss ratio. The research may include energy efficiency and bandwidth resource allocation concept in future.

## References

[1] S. Yuvarani, A. Gayathri, K. J. Velmurugan, V. Meenakshi, S. Sadhana and C. Srinivasan, "Quality of Service Factor based Unfailing Route Formation in Wireless Sensor Network," International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics, pp. 617-622, 2023.

[2] A.Unnikrishnan, and V. Das, "Cooperative Routing For Improving The Lifetime Of Wireless Ad-Hoc Networks," International Journal of Advances in Signal and Image Sciences, vol. 8, no. 1, pp. 17-24, 2020.

[3] C. Liang, and F.R. Yu, "Wireless network virtualization: A survey, some research issues, and challenges," IEEE Communications Surveys and Tutorials, vol. 17, no. 1, pp. 358-380, 2014.

[4] Y. Lai, L. Tong, J. Liu, Y. Wang, T. Tang, Z. Zhao, and H. Qin, "Identifying malicious nodes in wireless sensor networks based on correlation detection," Computers and Security, vol. 113, no. 2022, 2022.

[5] S. Manimurugan, A.Q. Majdi, M. Mohmmed, C. Narmatha, and R. Varatharajan, " Intrusion detection in networks using Crow search optimization algorithm with adaptive neuro-fuzzy inference system," Microprocessors and Microsystems, vol. 79, no. 2020, 2020.

[6] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, and T. Karygiannis, and Y. Yesha, "Threshold-based intrusion detection in ad hoc networks and secure AODV," Ad Hoc Networks, vol. 6, no. 4, pp. 578-599, 2008.

[7] E.A. Shams, and A. Rizaner, "A novel support vector machine-based intrusion detection system for mobile ad hoc networks," Wireless Networks, vol. 24, pp. 1821-1829, 2017.

[8] A. Gupta, and M. Kalra, "Intrusion detection and prevention system using cuckoo search algorithm with ANN in cloud computing," Sixth International Conference on Parallel, Distributed and Grid Computing, pp. 66-72, 2020.

[9] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, "RSS-based localization in the presence of malicious nodes in sensor networks," IEEE Transactions on Instrumentation and Measurement, vol .70, pp. 1-16, 2021.

[10] S. Durga Devi, and D. Rukmani Devi, "Malicious node and malicious observer node detection system in MANETs," Concurrency and Computation: Practice and Experience," vol. 33, no. 3, pp. 1-9, 2021.

[11] M.B.E. Sajid, S. Ullah, N. Javaid, I. Ullah, A.M. Qamar, and F. Zaman, "Exploiting machine learning to detect malicious nodes in intelligent sensor-based systems using blockchain," Wireless Communications and Mobile Computing, pp. 1-16, no. 2022, 2022.

[12] P. Shi, C. Gu, C. Ge, and Z. Jing, "QoS aware routing protocol through cross-layer mechanism in asynchronous duty-cycled WSNs," IEEE Access, vol. 7, pp. 57574-57591, 2019.

[13] R. Rathee, F. Ahmad, C.A. Kerrache, M.A. Azad, "A Trust framework to detect malicious nodes in cognitive radio networks," Electronics, vol. 8, no. 11, pp. 1-12, 2019.

[14] K. Grgic, D. Zagar, and V. Krizanovic Cik, "System for malicious node detection in IPv6-based wireless sensor networks," Journal of Sensors, vol. 2016, pp.1-20, 2016.

[15] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K.Y. Lam, "Trust-based malicious node detection in MANET," In 2009 International Conference on E-Business and Information System Security, IEEE, pp. 1-4, 2019.

[16] H. Azath, A. K. Velmurugan, K. Padmanaban, A. M. Senthil Kumar, and Murugan Subbiah , "Ant based routing algorithm for balanced the load and optimized the AMNET lifetime," AIP Conference Proceedings, vol. 2523, no. 1, pp.1-15, 2023.

[17] A. Khanna, P. Rani, P. Garg, P.K. Singh, and A. Khamparia, "An enhanced crow search inspired feature selection technique for intrusion detection based wireless network system," Wireless Personal Communications, vol. 127, no. 3, pp. 2021-2038, 2022.