Cognitive Threats Detection Model using Nature Inspired Chimpanzee Optimization for IoT Networks (CCM-COM)

Vanitha V*[1], Bestley Joe S[1], Rahul Krishnan[1], Augustine Fletcher A.S[1], Anju M[1], Akila V[1]

[1] [1] Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India

vanithav@srmist.edu.in

Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India

vanithav@srmist.edu.in

Abstract. Emerging development of networking technology ensured fats and flexible communication. Wireless sensor network is applied in almost everywhere for efficient usage of network and data transfer. On the other side of the network, the flexibility leads to the hacking mechanism and unauthorized accessibility. The proposed approach is focused on designing an efficient and new approach for reducing the cyber threats in WSN 5G networks. The proposed model considers the deployment of wireless sensor network using shorting algorithm, the nodes are allowed to get communicated in the random space. The occurrence of malicious nodes are detected through cognitive control mechanism using Chimpanzee optimization model (CCM-COM) is proposed. The optimized network get self-repaired and reconnected to achieve high energy efficiency. The proposed system achieved with 64.17 seconds of propagation delay achieved from the repose of the COM model. Attacks such as Fake job alert, Fake app, android defender are classified here.

Keywords: IoT security, Network security, Wireless sensor network, Cyber security, Cognitive computing

1 Introduction

Numerous IoT devices are connecting the demand on home security, business networks, industrial communication, healthcare analysis, remote monitoring, and many others. It improves the environmental monitoring fore view. Various devices are getting connected within the single platform that enables the system to get accessible without authentication tool [1,2]. Critical infrastructures are developed and developing throughout the world which leads to many digital attacks where it increases the demand of cybersecurity from cyber-attacks which also paves to IoT based solutions [3]. Security to be increased due to the increase in use of IoT applications and development of intrusion detection system could be used for such threats [4]. Malware injections are increasing in the present architecture. The device connectivity is flexible using various embedded devices.

A. S. Edward et al. (eds.),*Proceedings of the International Conference on Advanced Research in Electronics and Communication Systems (ICARECS 2025)*, Atlantis Highlights in Engineering 38,
https://doi.org/10.2991/978-94-6463-754-0_55

the problem of IoT platform is that less expertized device managers that allows the unauthorized access generates security issues on existing premise [5]. The commonly faces problems in IoT networks are weak network authentication, insecurity in network service providers, insecure home and other ecosystem connectivity, insufficient privacy protection, lack of device management control, insecure default systems etc. IoT systems are working with continuous communicating devices rely on the internet protocols. Android oriented are malwares are increasing because of the increase in mobile device connectivity with IoT networks. Android malwares coming over the IoT cloud inject the false data into the mobiles and make the system to filter phishing attacks[6]. Fig 1. Presents

Fig. 1. System architecture of IoT systems

the system architecture of proposed IoT threats detection framework. Malicious activity-enabled APK programs are installed on the system without the user's knowledge once the confirmation email is sent. Official notification-based phishing attacks can be carried out by transmitting a complete record of information to the user system, such as appointment order confirmation letters, which can be altered by hackers[7]. By responding to the email that was sent, the user is able to provide crucial information like a contact number, the location of their address, and information about their salary by viewing the manipulated document that appears to be the original. People are able to lose money and more valuable information as a result of these official notifications that are based on phishing attacks [8]. Mobility-based phishing attacks can be carried out by sending a fake SMS as an advertisement that includes video links and messages through a variety of mobile services. The fraudulent SMS then asks recipients to update their contact information and change their password and PIN number by sending an OTP to the registered mobile number. This kind of attack is very dangerous because phishing can be handled by a user with prior information, but a user

without that information gives them all the credential data, takes control of the user account, and causes dangerous problems [9]. Over large distributed systems sensor networks data's are collected for monitoring irrespective of the field trials and evaluation of the planner practice [10].

- The proposed system is a planned strategy for developing a novel and effective approach to reducing cyber threats in WSN 5G networks.
- The shorting algorithm is used in the proposed model to set up a wireless sensor network, and the nodes are allowed to communicate in a random space.
- A cognitive control mechanism based on the Chimpanzee Optimization Model (CCM-COM) is proposed for detecting malicious nodes.
- To achieve high energy efficiency, the optimized network is self-repaired and reconnected.

The section provides background research on the work. System design descriptions with a tool selection strategy are presented in Section, and the design methodology to be used is presented in Section methodology. The results of the Section then discuss the algorithm stages and outcomes and conclude with suggestions for future improvements.

2 Background Study

S. Mahmoudzadeh et al. (2019) the author presented a differential evolution (DE) algorithm enabled dynamic underwater wireless sensor network (WSN). Depends on the deployment model promising solutions are created. Fast computational performance, efficient turbulence in uncertain vast environment of underwater. The major pitfall present in the system that constraints produced during the complex environment need to be solved. A. Celik et al.(2018) the author presented a system where localization in multi-hop underwater optical wireless sensor network is created. Different network parameters are measured. Network localization is accurately validated. Network localization is optimized that acts as the advantage. Accuracy of the system need to be improved. N. Saeed et al. (2019) the author presented an energy harvesting system in which optical wireless sensor network is created. Network localization is created using active Receiver signal strength details. By utilizing the kernel matrix the reduces the error estimation. Shortest path of each block is reduced. The system improves complex network issues. Z. Xi et al.(2019) the author presented a underwater wireless sensor network based on multiple access protocol(MAC). The system removes the reserved framework and work on the centralized network to achieve multi-channel collision avoidance network. Data loss during the communication, location problem need to be focused. I. Jawhar et al.(2018) the author presented an underwater autonomous vehicle monitoring using linear sensor network(LSN). Energy saving is focused by reducing the interferences. Packet delivery ratio is analyzed using the presented system. Y. Zhou et al. (2020) the author presented a cross layer network in wireless sensor network. The primary objective focused

here is to maximize the transmission rate. The algorithm get enhanced within few design perspectives configured to demonstrate the existing design procedure. Network reconfiguration is feasible with the system.

3 System Design

The major challenges in the wireless sensor network is the data loss rate and disconnection of the network due to malicious activity. The insertion of hacking mechanism in the network enable the system to get impacted by the wrong direction and thus the network loss is happening. The proposed model considers these constraints and formulate the optimized mechanism. The system need to be improved with the help of optimization process. Using MATLAB signal processing toolbox, the wireless sensor network is created and simulated.

4 Methodology

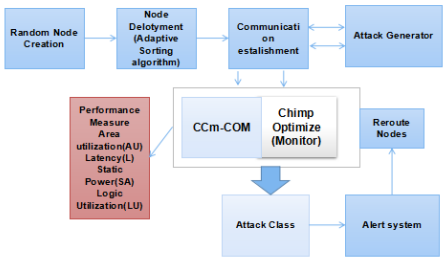

Fig. 2. System architecture

Fig 2. Shows the system architecture of the proposed attack detection framework in IoT networks using Chimpanzee optimization enabled cognitive control mechanism. The planned strategy for developing a novel and efficient strategy for reducing cyber threats in WSN 5G networks includes the proposed system. A wireless sensor network is set up in the proposed model using the shorting algorithm, and the nodes are allowed to communicate in a random space. For the purpose of identifying malicious nodes, a cognitive control mechanism (CCM-COM) based on the Chimpanzee optimization model is proposed. The optimized network is self-repaired and reconnected to achieve high energy efficiency.

4.1 Implementation summary

Wireless sensor network design where the module randomly places nodes in open areas to divide up the energy and distance expenses. Locating the cluster head in

an unfamiliar environment will be the next challenge. The process of connecting the nodes in a random manner is called communication establishment. After the nodes have been aligned and created, the next step is to connect them to the network. The established nodes connect with the nodes that are the shortest distance away from the cluster and try to find a blockage in the path. The Mac protocol is used in the dynamic off-loading module to evaluate the roots. The system also looked at a dynamic backhaul support model that should minimise data loss and dynamic offloading data that would be overlooked throughout the route based on energy efficiency, both of which successfully stop data loss. Chimp optimization is used in the proposed model to reorganize the suspected malicious network in the wireless channel. The role that WSN plays in any application has the greatest impact on the quick transfer of data. The network used chimp optimization to create adaptive routing, and the energy is also monitored after each iteration. The search for a malicious node is carried out when the network's energy is severely degraded. In case of malicious node is discovered then CCM enabled Chimp optimization is used to change the current path. In order to establish a network regarding suspicious activity, an alert system is provided. The role that WSN plays in any application has the greatest impact on the quick transfer of data. The network used chimp optimization to create adaptive routing, and the energy is also monitored after each iteration. The search for a malicious node is carried out when the network's energy is severely degraded. if a malicious node is discovered then. Chimp optimization is used to change the current path. In order to establish a network regarding suspicious activity, an alert system is provided. This study enable us to learn in-depth knowledge on wireless sensor networks. This study provides learning opportunity in MATLAB software and Communication Tool box. Let xi be the input random nodes and its positions, yi is the replacement of the node locations after the first iterations. These nodes are deployed by the algorithm steps below. The rest of the work is tested with various levels of analysis and found the attack patterns coming over the IoT network. The CCM-COM model adopts the dynamic changes occurring over the network and provides response in short span of time.

5 Results and Discussion

5.1 Network Creation

Fig 3. Show sthe basic node creation system using random sorting of node values. These node values are adaptively configuable. Based on the random distance and cost these values get varries. Fig 4. Illustrated the deployment of node using adaptive sorting technique. Based on the shortest distance between the nodes the connectivity is established. Fig 5. Shows the Sensitivity hyperplane that divides the performance of the node without CCM-COM model based optimization process. Fig 6. Shows the best score evaluated from the proposed CCM-COM model. As the number of iterations increases, the score of the proposed model get increased. The presented graph is shown with various levels of iterations and changes.

Algorithm 1 CCM-COM Algorithm

Input: Node positions x_i, distances d, Number of nodes N
Output: Optimized routing with attack detection

Step 1: Adaptive sorting of nodes based on distances
AdaptiveSort(x_i, distances(N))
Initialize(x_i, d) at $N = 0$
for $i = 1$ to N **do**
    $Priority\_dis \leftarrow \min\{x_i\}$ in all N
    $Current\_pos \leftarrow$ extract$\{\min(d(N))\}$
    Node_update(i, N)
end for
if attack detected ($attack == 1$) **then**
    Call_COM(N, i)
    Reroute($Priority\_dis$)
    Repeat communication
end if

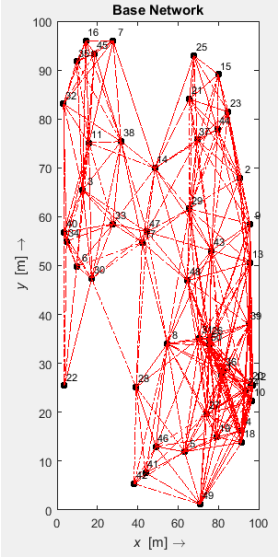

Fig. 3. Network creation

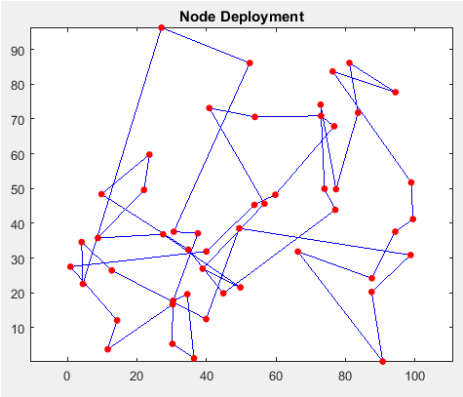

Fig. 4. Node deployment

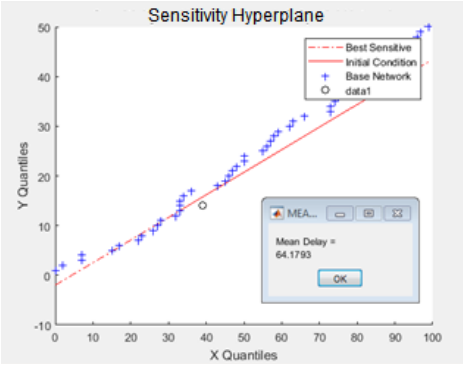

Fig. 5. Sensitivity hyperplane

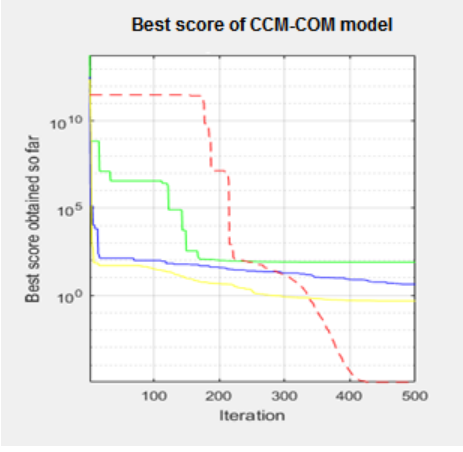

Fig. 6. Performance of CCM-COM model

6 Conclusion

New developments in the internet of things are bringing an abundance of adaptable applications that reduce human suffering in several ways. Ease of setup and integration with integrity-creating devices is the fundamental component of the Internet of Things. The proposed method has developed a threat detection system and provides security to the crucial problem. The model takes consideration of cognitive control mechanisms that safely regulate the flow of communication between nodes while an attack is happening. The existing nodes are mapped into the malicious nodes at random. Therefore, it makes sense to use the relative response and frequent changes in node values to identify malicious activity based on the differences in node behaviour. The nodes are rerouted here using the chimpanzee optimisation. Immediate steps are made to safeguard the data in order to prevent the issue of generating nodes with regular nodes.

References

1. Okafor, N. U., & Delaney, D. T. (2021). Missing data imputation on IoT sensor networks: Implications for on-site sensor calibration. *IEEE Sensors Journal*, **21**(20), 22833-22845.
2. AlSalem, T., Almaiah, M., & Lutfi, A. (2023). Cybersecurity Risk Analysis in the IoT: A Systematic review. *Electronics*, **12**(18), 3958, 1-12.
3. Das, R., & Gündüz, M. (2020). Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security Science*, **8**(4), 122–133.
4. Zrelli, A., Nakkach, C., & Ezzedine, T. (2022). Cyber-Security for IoT Applications based on ANN Algorithm. In *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, Shenzhen, China, pp. 1-5.
5. Stergiopoulos, G., Gritzalis, D., Vasilellis, E., & Anagnostopoulou, A. (2021). Dropping malware through sound injection: A comparative analysis on Android operating systems. *Computers & Security*, **105**, 102228.
6. Imtiaz, S. I., ur Rehman, S., Javed, A. R., Jalil, Z., Liu, X., & Alnumay, W. S. (2021). DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network. *Future Generation Computer Systems*, **115**, 844-856.
7. Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, **76**, 139-154.
8. Butt, U. A., Amin, R., Aldabbas, H., Mohan, S., Alouffi, B., & Ahmadian, A. (2022). Cloud-based email phishing attack using machine and deep learning algorithm. *Complex & Intelligent Systems*, 1-28.
9. Haider, S. K., Nauman, A., Jamshed, M. A., Jiang, A., Batool, S., & Kim, S. W. (2022). Internet of drones: Routing algorithms, techniques and challenges. *Mathematics*, **10**(9), 1488.
10. Singh, D., & Rawat, B. S. (2022, October). Cluster based Routing Protocol Design using Neural Networks for Wireless Sensor Networks. In *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, pp. 1-7. IEEE.