AN EFFICIENT SECURE ROUTING FRAMEWORK FOR MESH NETWORK TOPOLOGY

Lingala Thirupathi

Research Scholar, Department of Computer Science and Engineering, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh – 530045, India
E-mail: thiru1274@gmail.com

P.V. Nageswara Rao

Professor, Department of Computer Science and Engineering, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh – 530045, India

Abstract

To improve the performance of the wireless network, different types of topologies were introduced like start, ring, bus, mesh and dynamic topology. However, providing the security is the very difficult because of the unique environment. But, affording the security is most required task to avoid less data transmission and high data loss. Hence, a novel Chimp based Associativity routing (CbAR) was proposed for predicting and neglecting the malicious events in the mesh network. The dataset that has utilized for the performance testing process is CICIDS database. Besides, the robustness of the proposed model is validated by launching the Denial of Service (DoS) attack in the mesh topology. Moreover, the planned model is tested in the python environment. Finally, the communication and attack prediction parameters like tthroughput, accuracy, delay, transmission time, packet drop and data transfer rate have been validated and compared with other existing models. In that, the presented model has gained high accuracy, throughput and data transfer rate. Also, it has minimized delay and data flow rate.

***Keywords*: Chimp optimization; Mesh topology; Attack detection; Wireless networks; Network security.**

1. Introduction

The group wireless nodes are called as wireless networks. Moreover, the wireless nodes have included tablets, computers and other electronic [Hua and Shunwuritu (2021)]. Hence, the data transmission between these wireless networks is processed based on the different types of topology characteristics [Dhar Dwivedi *et al.* (2021)]. The nodes that are arranged in the networks topology is connected in the basis of logically or physically [Thulasiraman *et al.* (2022)]. Some of the connected nodes are routers, switches, and feature routers, which are mainly represented by the graph [Yan *et al.* (2022)]. The network arrangement is combined by the nodes, and the lines are connected by the receiver as well as the sender of the topology network [Khamer *et al.* (2021)]. Some topologies are ring topology, mesh topology, bus topology, and so on [Taştan and Dalkiliç (2021)]. The network sensor is increases the complexities among the remote area [He *et al.* (2021)]; where the wireless development of scale is large by enabling the low-power communication of wireless network [Grigg *et al.* (2021); Collados-Lara *et al.* (2021)]. The network of mesh topology prevents the complexity in maintaining the network [Hortelano *et al.* (2021)]. However, the network has estimated the number which is required for the development field which is repeatedly prohibit the cost [Shin *et al.* (2021)]. The topology network of mesh is optimized basically fixes the isometric range of transmission over the elements of network [Chung *et al.* (2022)]. By linking the nodes one another the length of the path results the variability of significant the vegetation characteristics, terrain complex, and terrain [Oroza *et al.* (2021)]. Sequentially, the process structured the network heuristic in which the iteratively deploy and also adjust the elements of network, where the sensors connect nodes by aiming the base station with the help of uplink cellular and satellite [Basharat *et al.* (2022)].

The intensive labour processing the wireless network of mesh topology where the failure of node can be concern in the graph which is interconnected, result in the data loss among real time [Sharma (2021)]. Connectivity of node assumption is simplified and is improve the methodology. The architecture of mesh network topology [Talwar *et al.* (2021)] is described in Fig 1. In terms of, network sensor of wireless topology the terrain is complex. The network design has profit attention decades the last two potential disruption of communication from the cause of man-made or else natural [Laghari *et al.* (2021)]. By accessing the public needs the internal requirement is secured on account of networking devices of hardware arrangement [Hernández-Morales *et al.* (2022)]. In terms of, servers of the web will be access only by public for the purpose of placing orders. It calculates the method of

structured wireless optimization among the terrain of complex which cannot fix the length path [Khan *et al.* (2021)].

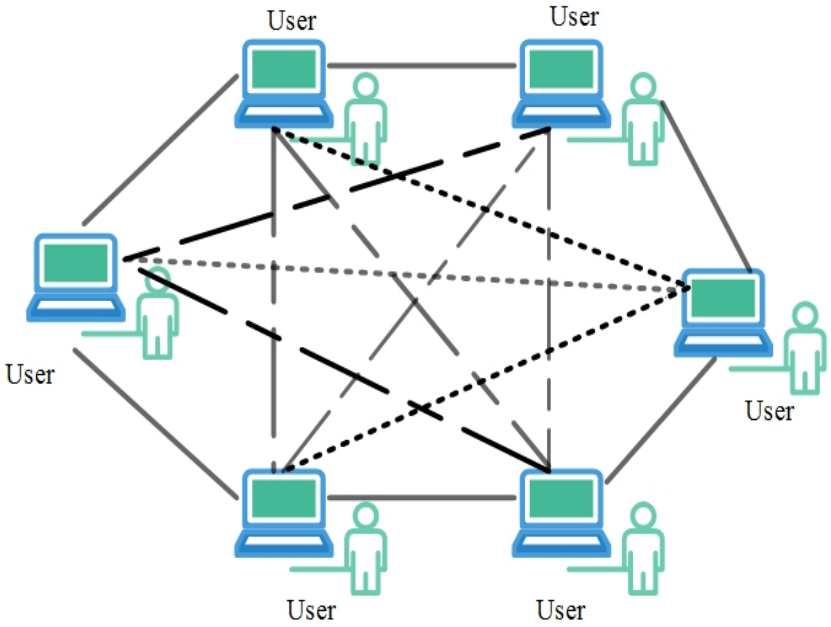

Fig. 1. Architecture of Mesh Network.

The function cost is minimum nodes linking by selecting the requirements of networks in order to connect the nodes and the highest number link the nodes of network [Shokouhifar (2021)]. The main objective is to design the network with low-cost of failure nodes for the construction of problem based on constructing the vertex of minimum network. To overcome the demerits from this method several techniques were proposed in past such as flying Ad hoc Networks [Cappello *et al.* (2022)], ADMM [Ma *et al.* (2021)] is used in this research work. However, the suitable solution is not found because of the attack harmfulness. So, the present work has decided to present the novel optimized security routing in mesh topology for enhancing the communication process.

The key contribution of this current study is detailed as follows,

- Initially, the mesh topology was designed with different users in the wireless environment.
- A novel CBAR has been introduced with the routing and security parameters, then the user system has been monitored.
- If there is any malicious activity then it is removed from the user environment.
- The communication parameters and malicious activities detection metrics were validated.
- Moreover, to check the robustness of the present model, the DoS attack has been launched then detection and neglecting process has become validated.
- Finally, the security improvement score has measured in terms of, Transmission time, Accuracy, delay, Throughput, packet drop and packet delivery rate.

The present research work is organized in the vision of; recent related works for this proposed model is presented in section 2. The problems of the existing models are exposed in 3rd section. Then the proposed solution for the defined problem is given in 4th section. The outcome of the proposed solution is presented in 5th section and section 6 concludes the research article.

2. Related Works

Some of the recent few literatures based on the multi-level framework protection are given below,

The service investment of the cyber security is based on the multi-level cyber security. Thus, Cappello *et al.* (2022) have proposed a method of Flying Ad hoc Networks which establishes the flow of optimal layers of network and also the optimal layers of security in terms of highest providers gain the revenue difference of service sales which is obtained by the cost as well as the resources is retained. However, the implementation of this technique is more complex.

The formation of network is trading the hybrid and also the community trading of multi-level. Thus, Ma *et al.* (2021) have proposed a method of ADMM that alternates the method of Multiplying. The network of multi-level trading hybrid framework is introduced by the construction with various modes of trading such as decentralized model of communication trading, network of two trading of hybrid, modern trading and trading based agent. The topologies have complex networks, losses of energy, and charge the regional and local levels respectively.

Here, securing the key management of multi-level protocol is based upon the dynamic structure of the M-tree. Therefore, Lin *et al.* (2021) have proposed a method of managing the security key based on a multi-level agreement. The 5G networking system will expose the information personally based on the wireless field network. The information communicated among the roadside equipment or the traffic sign can improve the road's safety. The security level of the system is low.

Bin-Yahya *et al.* (2022) have proposed obfuscation framework, which is based upon the network of energy-aware topology. It also attacks the highest cost, which is developed practically and efficiently. The mechanism of obfuscation introduces several false nodes that are undistinguished based upon the model of k-anonymity and the actual nodes. The proposed method is mainly based on a ranking of mutation route among different complex criteria like the reliability of nodes, linking the cost, consumption of energy, and overlapping the route. However, the rate of success is reduced, consumption of energy is low, and the lifetime of the network is high.

The secure parameters in the Internet of Things have secured the protocol in multilevel routing. So, Zhang *et al.* (2021) have proposed a method of EESMR which is based upon securing the multilevel routing with efficient energy. The cluster contains the solution of energy-conserving protocol based upon the routing of multi hop because of scalability; the communication is reduced over the network of IoT. The proposed system network's merits are throughput, adaptability, delivery of packet ratio, lifetime, and the energy of network balance.

3. System Model and Problem Statement

Securing the communication in the wireless network environment is the much needed task to preserve the privacy in the communication channel. But, affording the security range is a complex task because of the wireless environment and different tasks users. In addition, if the attack happened in the communication channel then it has degraded the communication performance and maximized the computation time. Hence, the network system has shown the high delay time and less packet transmission rate. The basic structure of the mesh topology along with the problem was illustrated in Fig. 2. The common demerit of the mesh topology was it was more costly when compared with the other topologies like bus and star. Moreover, if the rate of dataset was high then the topology would produce more delay time. Hence, including the security parameters in the mesh topology has recorded more resources, which have maximized the economic cost. In mesh topology less security only arises as well as due to many users being presented at a time, so the rate of packet transmission was low.

It has reduced the data transmission performance of the mesh topology. Considering these, the optimal solution has been predicted for tuning the security parameters in the mesh networks. Finally, the security robustness was validated against DoS attack.

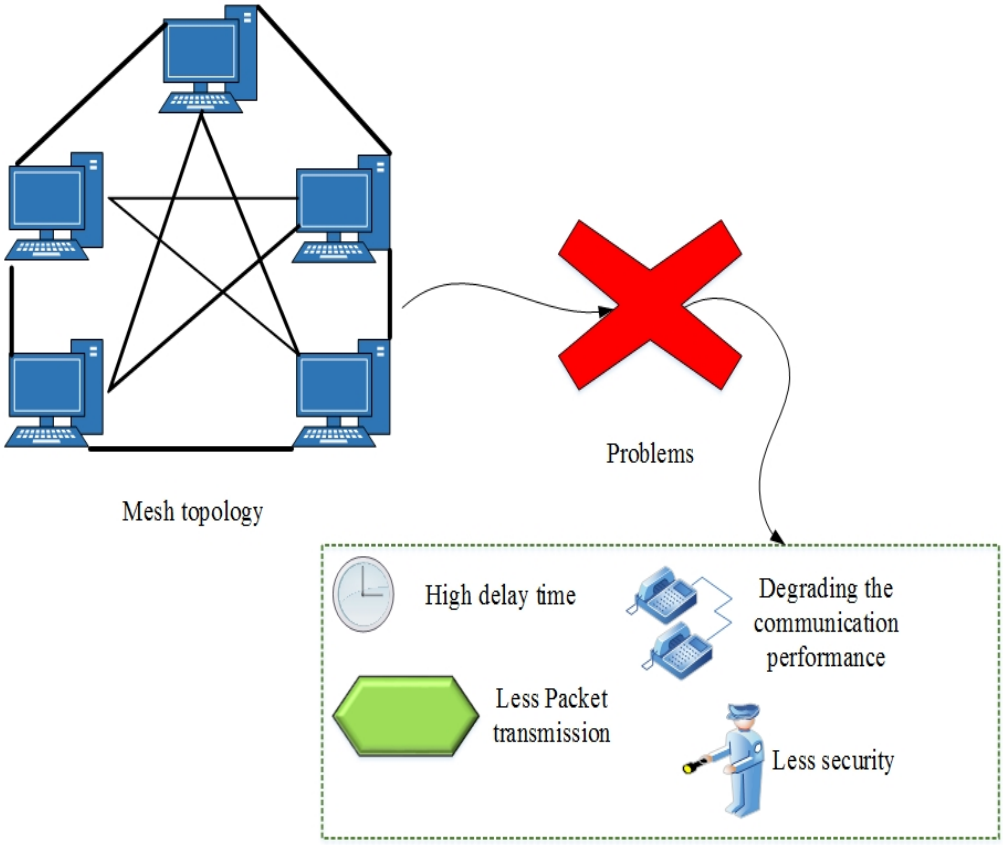

Fig. 2. System model with problem.

4. Proposed CbAR for Securing Mesh Network

A novel Chimp based Associativity Routing (CbAR) has been introduced as the security mechanism for the wireless network. The communication topology that was considered in this present study is mesh topology. In the primary phase, mesh topology has been designed with different users then a novel CbAR was developed as the secure routing protocol for improving the communication channel. The proposed architecture is described in Fig. 3. Finally, the robustness of the designed routing mechanism has been checked by launching the Denial of Service (DoS) attack in the communication channel. For maintaining the security as well as to enhance the security mechanism among the routing, the better model was developed through the chimp based scheme. After detecting the DoS attack, the stability rate of the communication path were improved to transmit the data efficiently, so the proposed model monitored each nodes and then maintained the stability of the path.

4.1. *Designing of mesh topology*

Initially mesh topology was designed with desired number of users. In this proposed model mesh topology was used to predict the attack and remove the attack in case the attack was present in the system. Moreover, adding as well as removing the nodes in mesh topology was easy so, here mesh topology was designed for predicting the attack. For finding the malicious nodes in the mesh topology and removing those nodes as well as providing the security proposed model was implemented. Moreover, the mesh topology was designed on the basis of eq. (1),

$$\lambda_m = m_1, m_2, m_3 \ldots\ldots\ldots\ldots m_n \tag{1}$$

Where, λ_m topology parameter in the model $m_1, m_2, m_3 \ldots\ldots\ldots\ldots m_n$ refers to the number of users in the mesh topology. Here, the mesh topology was designed with n number of users and each node was considered as user.

4.2. *Associative routing in Chimp optimization*

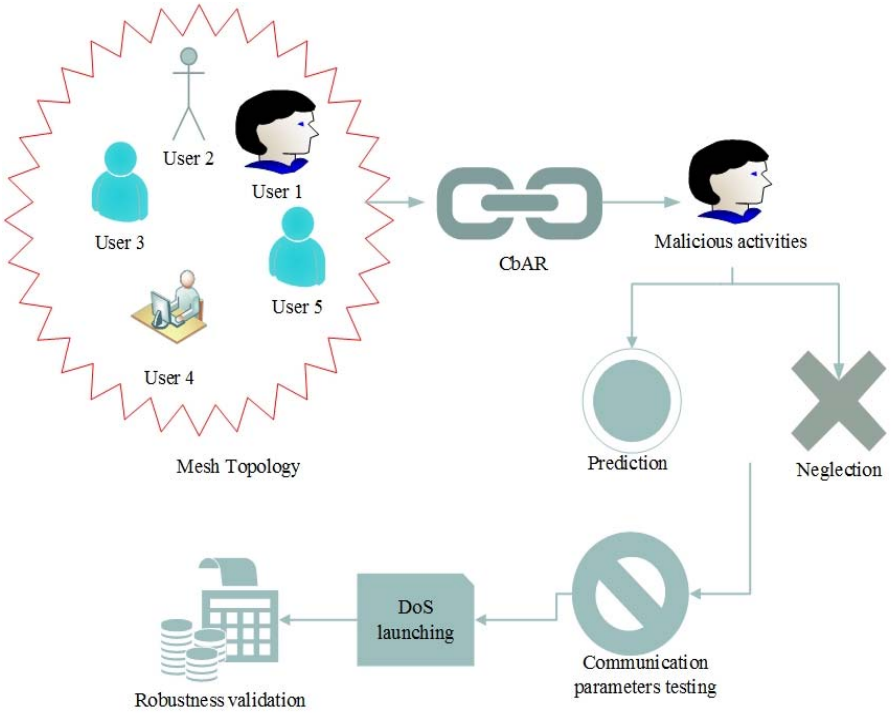

Fig. 3. Proposed architecture.

At the proposed model chimp optimization mechanism were used. Here, the parameters were calculated in accordance with the chimp fitness. Associative routing is the commonly used mobile routing protocol and these routing mechanism were mostly used in wireless mesh networks and wireless Adhoc networks for finding the path. In mesh network, each node was interconnected so for finding the path as well as finding the attack was the difficult task. Moreover eq. (2) was declared for associative routing in the chimp optimization model.

$$\alpha = 1 - \lambda_m \tag{2}$$

Here, α determines the routing parameter of the proposed model as well as λ_m refers to the amount of nodes present in the designed mesh topology. Subsequently, the proposed model uses the associative routing along with the mesh topology which easily finds the path and detects the attack if any of the attackers were present over the communication channel. Based on the chimp fitness the attack was detected over packet transmission. For comparison, initially fitness of each node was noticed after that those noticed fitness were compared with the chimp fitness. Consequently, optimized fitness was declared through the eq. (3),

$$O_p = cmp\left|\mu n_f\right| \geq \mu c_f \tag{3}$$

Where, O_p defines the optimization parameter, μn_f refers to the node fitness of the mesh network and μc_f corresponding to chimp fitness respectively.

4.3. *Finding and removing the malicious activities*

For finding the malicious activities in the mesh networks, initially designed mesh topology was connected with the proposed model. If any of the malicious nodes were presented among the mesh network, then the system identifies those nodes through the proposed model by activating the chimp fitness. Subsequently, the system monitors every node on transmitting the packets for detecting the malicious nodes. Hence, the Packet transmission and finding the malicious nodes were declared in the eq. (4),

$$P_t = P_1, P_{2.....} P_n \tag{4}$$

Here, P_t refers the packet transmitting parameter in the model $P_1, P_{2.....} P_n$ refers to the amount of packets transmitted over the communication channel. Moreover, attack detection was done on transmitting the packets. If any of the malicious nodes were presented then the attacker was sending the request to attack the system. Each node in the mesh topology was combined with the chimp fitness to determine the malicious node and the malicious nodes were determined based on the features of the data sets. Through the proposed model if any of the attackers were present, then the model close and stop down the process immediately. Attack detection was declared in eq. (5),

$$A^* D = P_t \{hp_n\} \tag{5}$$

Where, $A^* D$ denote the attack detecting parameter hp_n refers to the high consumption node; which was the attack detected node. After finding the attack, the attack was removed from the system. Consequently, the attack removing parameters were declared in the eq. (6),

$$R^* D = P_t - A^* D \tag{6}$$

At here, the parameter P_t total amount of packets transmitted over the communication channel $A^* D$ refers to the attack detected parameter. For removing the detected attack from the transmitted packet subtract the detected attack parameter from the total packet transmit. Malicious nodes were classified along with if condition was declared in eq. (7),

$$\delta = \begin{cases} if\,(hp_n = 0) \;\; ; \;\; non - malicious\,nodes \\ if\,(hp_n = 1) \;\; ; \;\; malicious\,nodes \end{cases} \tag{7}$$

Here, δ refers to the node classification parameter, hp_n refers to the high consumption node. For obtaining security here the malicious nodes were removed as shown in eq. (8),

$$r' = (\delta) - hp_n \tag{8}$$

For removing the malicious nodes the above eq. (8) was developed. High consumption node was considered as the malicious nodes; here the malicious nodes were removed from the detected nodes. r' is the parameter used for removing the malicious nodes, hp_n refers to the high consumption node δ refers to the attack detecting parameters. After removing the malicious nodes from the system, then the parameters were validated on the basis of throughput, accuracy, delay, packet drop, transmission time and packet delivery rate.

While applying the DoS attack to the model it finds the attack easily that has increased the performance of the proposed system. After launching the DoS attack, the robustness of the system was validated. The system causes some variations among the robustness in before and after launching the DoS attack. Outcomes were noted and compared with the existing models.

Algorithm 1: CbAR

Start
{
// Designing of mesh network with n number of nodes

$\lambda_m = m_1, m_2, m_3 \ldots\ldots\ldots\ldots m_n$

{

$designing \rightarrow \lambda_m$

// The mesh topology was developed with n number of users

}

Associative routing in chimp optimization
{

$\alpha = 1 - \lambda_m$

// α determines the routing parameter of the proposed model and λ_m refers to the amount of nodes present in the designed mesh topology

}
Chimp optimization ()
{

// initializing the optimization parameters and routing parameters

$\text{int } O_p, \left|\mu n_f\right|, \mu c_f ;$

// The node fitness were compared with the chimp fitness

}
Finding the malicious nodes()
{
// initializing the packet transmission attack detecting parameters

$\text{int } P_t, P_n, A^*D, P_t\{hp_n\}$

// Attack was detected while on transmitting the packets over the communication channel
}
Classification of malicious nodes ()
{

$if\,(hp_n = 1)$

{
non-malicious node
} else ***(malicious node)***
//the malicious nodes were removed from the system

$r' = (A^*D \times R^*D) - hp_n$

}
{
Validating the parameters()
}
Launching DoS attack ()
{
// for validating the robustness of the system DoS attack was launched
}
}
}
stop

The pseudo-code for chimp based algorithm was developed in algorithm 1 as well as the workflow diagram of the proposed model was illustrated in Fig. 4.

5. Result and Discussion

The implemented model was developed through the Python environment and running in windows 10 platform. Initially, the mesh topology was developed with desired number of nodes after creating the mesh topology fitness of each node in the mesh topology was measured and compared with the chimp fitness. Then with the help of proposed model the system were checked to know about the presence of malicious nodes. In case any of the malicious nodes were presented then the system quickly shut down and closed down the process. Moreover, the needed constraint to implement the proposed model was tabulated in Table 1.

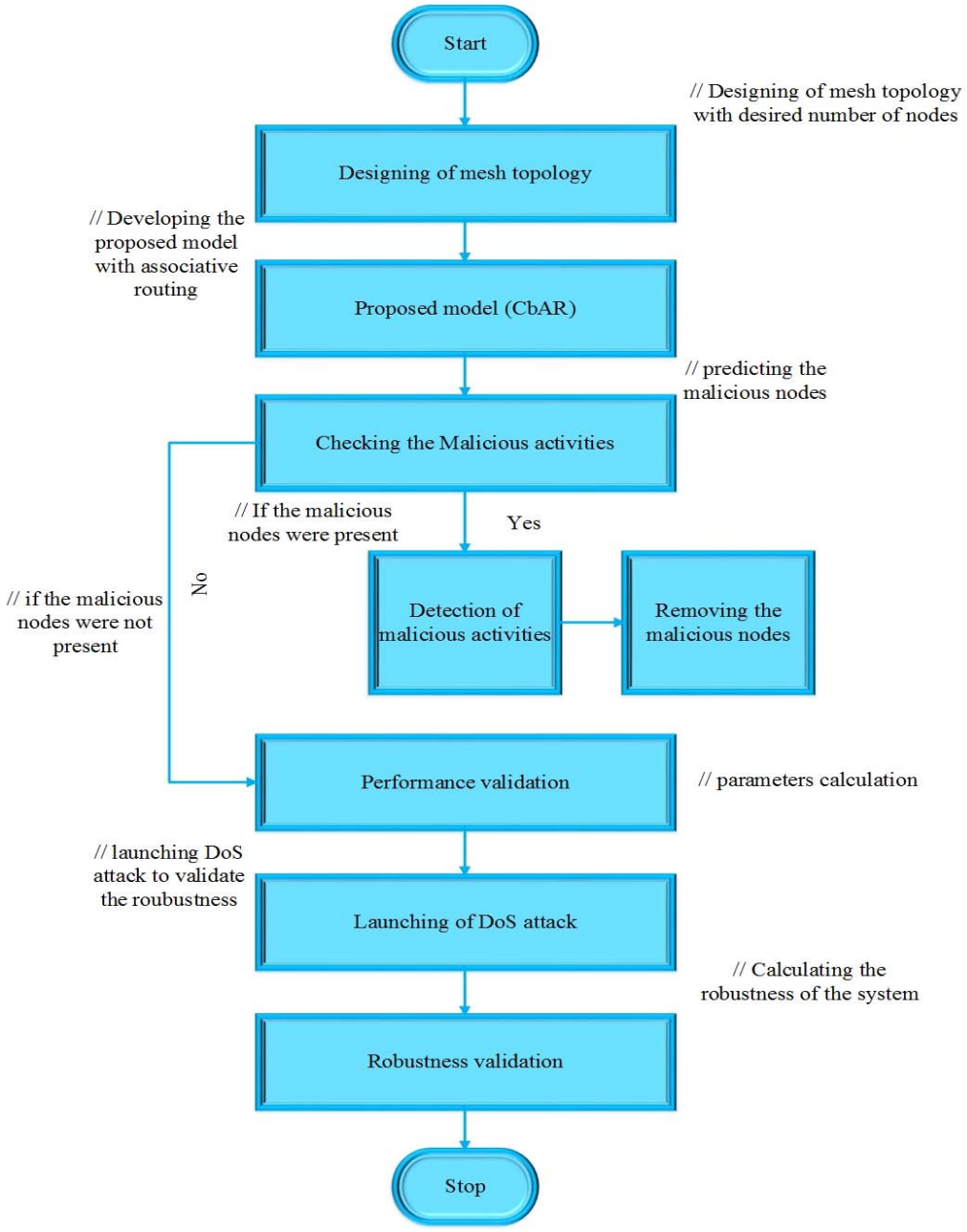

Fig. 4. Work flow of proposed model (CbAR).

Parameters specification	
Dataset	cicids
OS	Windows 10
Programming language	Python
Version	3.10

Table 1. Evaluation of parameters in the proposed model.

Subsequently, the implemented model was developed in the above mentioned python software 3.10 version. Moreover, the resultant data after attack launching as well as the robustness validation were evaluated along with the help of performance analysis. The comparison analysis of the implemented model was measured and compared with the other existing models to assure the performance of the proposed model.

5.1. *Case study*

In case study, the working method of the proposed model was explained detail. The main aim of developing the proposed model was to provide the system security among the attackers. However, to detect the attack easily, here associative routing was used along with the mesh topology. The proposed model was developed for finding the attackers and providing more security to the model. The proposed model was developed for providing more security during the packet transmission by detecting and neglecting the attacks in the designed mesh network. Basically, attackers were sending the request the connected users for acknowledging the request. In mesh topology adding and removing the nodes was easy. The advancement and flexibility has attracted this present research work for finding the security solution. Consequently, if any attacks were detected then the system would remove the nodes suddenly. After finding the routing rate in the mesh topology, and then the system validated the parameters with chimp fitness. The proposed model works to find the malicious activities in the mesh topology. After predicting the malicious user the system removes those unwanted node from the system. To check the working performance of the proposed system, DoS attack was launched. The performance of the model was noticed before and after applying the attack. Moreover, the rate of parameter also changed; higher rate of performance metrics were attained after applying the DoS attack and the performance validation was done for before and after applying the DoS attack. Fig. 5 illustrates the performance analysis of the proposed model after applying the DoS attack.

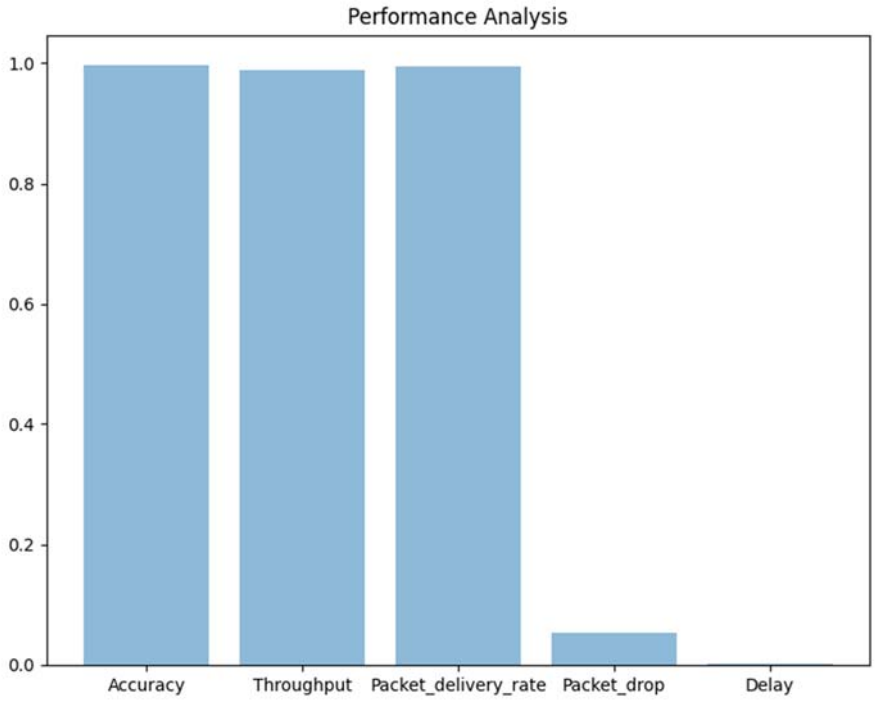

Fig. 5. Performance analysis of the proposed model (after launching the DoS attack).

Hence the parameter of the proposed model after launching the DoS attack was measured in terms of accuracy, throughput, packet delivery rate, packet drop as well as delay. The rate of accuracy obtained through the designed model was about 99.72%; throughput rate of the proposed model was at 98.87%; Packet delivery rate attained through the proposed model was about 99.43; due to higher rate of packet delivery more number of packets was transmitted over the particular time period. Packet drop is nothing but the loss of packet, in the proposed model the packet drop was about 0.0559 and the proposed model having the delay rate was 0.0027. However, the proposed model was attained the higher rate parameters; this will reduces the system, complexity and to reduce the computational time. High accuracy rate were achieved only when the system had exact prediction and detection capacity. After launching the DoS attack to the proposed model high rate of metrics were obtained. Consequently, before applying the DoS attack the performance as well as stability of the system was low.

The parameter validation of the proposed model was measured in before and after launching the DoS attack.

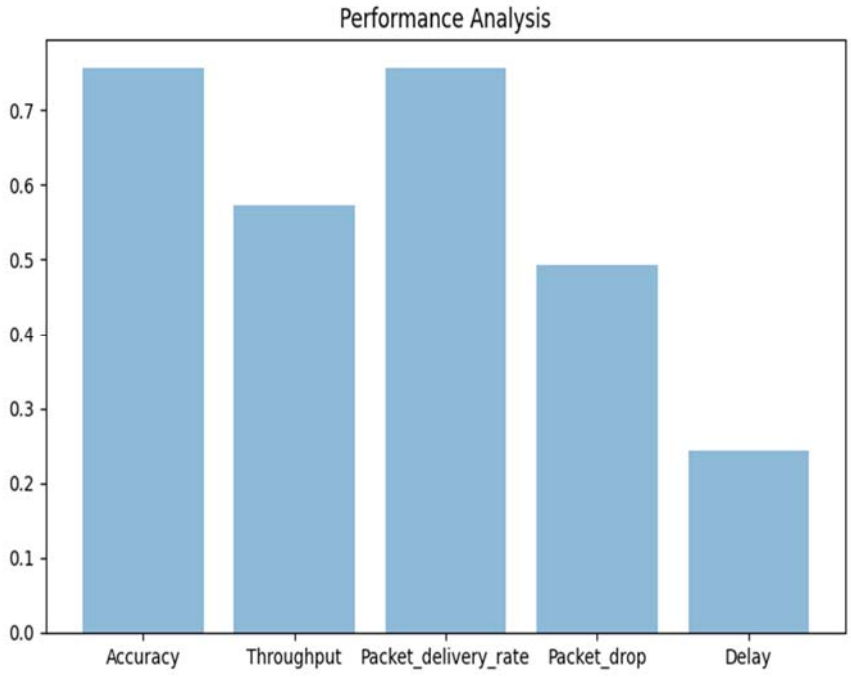

Fig. 6. Performance analysis of the proposed model (Before launching the DoS attack.

Fig. 6 shows the performance analysis of the proposed model before launching the proposed model. Moreover, before launching the DoS attack, the accuracy of the proposed model was about 75.58%; Throughput of the model was about 52.17; packet delivery rate of the proposed model before applying the DoS attack was about 7.58; Moreover, the packet drop and delay of the model was about 0.494 and 0.244. When compared with the performance of the proposed model before and after launching the DoS attack was varied. However, before launching the attack, the rate of parameters was low when compared with after launching the attack. After launching the attack the model finds the attacks easily if any of the attacks were detected in the system. So after launching the DoS attack, the performance of the parameters was high. High performance leads to low computation time, takes less time to execution and provides high stability to the system.

5.2. *Comparative Analysis*

To authenticate the implemented system, comparison analysis was done. At this section the result of the implemented model was compared along with the other existing models for proving that the proposed model having the high rate parameters. Some of the existing models used for comparing the proposed model was Robust and trusted scheme (RTS) [Haseeb *et al.* (2020)], Hybrid Mesh network (HMN) [Celebi (2022)], Transmission control Protocol (TCP) [Celebi (2022)], User Datagram Protocol (UDP) [Celebi (2022)], Wireless mesh Network (WMN) [Celebi (2022)], Spatial time division Multiple (STDM), Adhoc on demand Distance Vector (AODV) [Ghori *et al.* (2021)], optimized Adhoc on demand Distance Vector (OAODV) [Ghori *et al.* (2021)] and Mesh Analysis (MA) [Ghori *et al.* (2021)]. Moreover, at comparison the proposed model gives the better results than the existing models.

5.2.1 Throughput

Throughput defines the amount of information was processed by the system in the particular time period. Based on the time, amount of packet produced was evaluated in the proposed model. Moreover, throughput of the proposed model was declared through the eq. (9),

$$\rho = \frac{\omega p}{t} \tag{9}$$

Where, ρ refers to the throughput parameter of the proposed model, ωp defines the amount of information produced in the particular time period, t defines the time needed for the system to produce the number of packets. Throughput of the proposed model was compared with the other existing models such as Robust and trusted scheme (RTS), Hybrid Mesh network (HMN), Transmission control Protocol (TCP) and User Datagram Protocol (UDP). Among them, the proposed model attained 98.87% of throughput; it was high when compared with the existing models. Moreover, Fig. 7 explains the throughput comparison with other existing models.

5.2.2 Delay

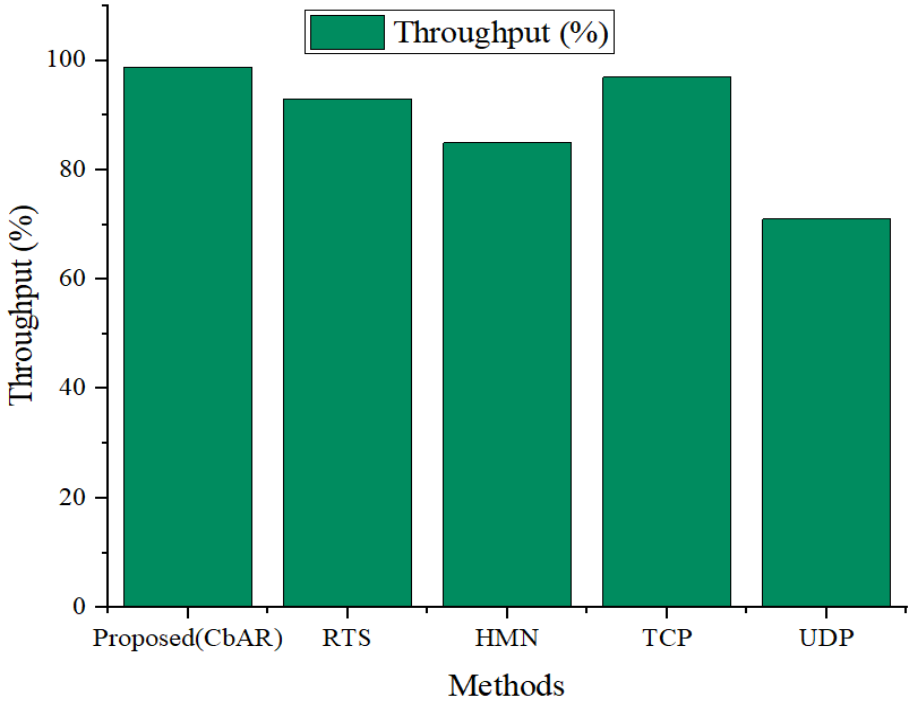

Fig. 7. Throughput comparison.

Basically delay happened in two ways such as transmission delay and propagation delay. Transmission delay refers the total amount of time needed to the router for pushing the packet. Moreover propagation delay is the amount of time taken to propagate the bit among one router to another. However, delay was evaluated in accordance with length as well as size of the packet, and delay of the proposed model was declared with eq. (10),

$$\sigma = \frac{l}{s} \tag{10}$$

Here, σ refers to the delay parameter of the model, l parameter defines the length of the packet and s defines the size of the packet.

Delay of the proposed model was compared with the other existing models like Hybrid Mesh network (HMN), Wireless mesh Network (WMN), Spatial time division Multiple (STDM), Adhoc on demand Distance Vector (AODV) and optimized Adhoc on demand Distance Vector (OAODV). Here, the delay rate of the proposed model was about 0.0027; it was very low when compared to the existing models. Moreover, the Fig. 8 shows the comparison of delay with the existing models.

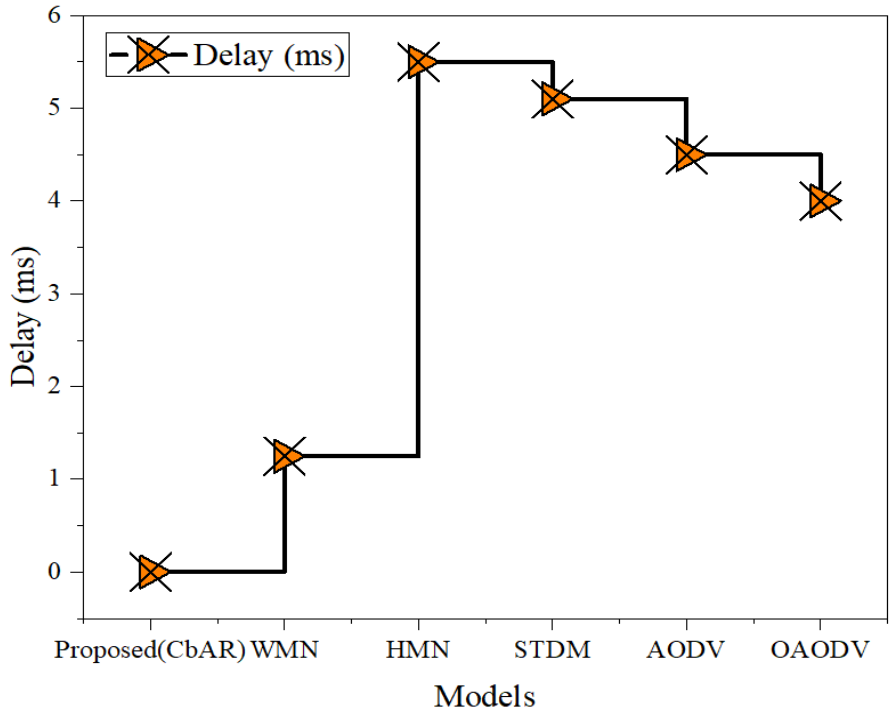

Fig. 8. Delay comparison.

5.2.3 Packet Delivery Rate

Packet delivery rate was defined as the amount of packets that reached the destination to the amount of packets sending from the source. Moreover, the packet delivery rate was measured through the eq. (11),

$$pdr = \frac{\alpha}{\alpha + \beta} \tag{11}$$

Where, pdr defines the packet delivery rate of the proposed model, α refers to the amount of packet that reached to the destination and the parameter β refers to the amount of packet send from the source to the destination.

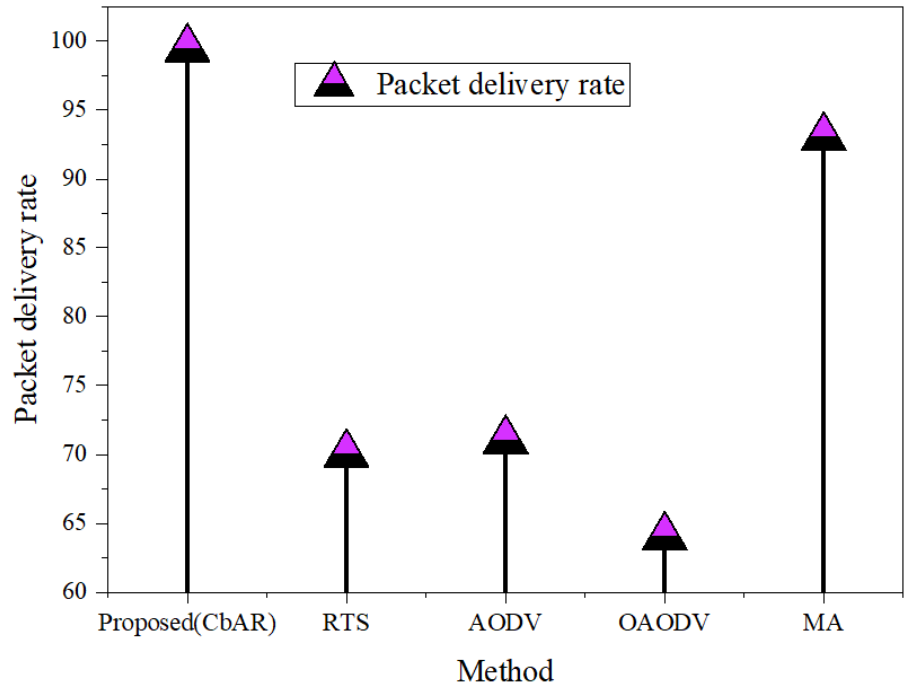

Fig. 9. Comparison of packet delivery rate.

Moreover, the packet delivery rate of the proposed model was compared with the Robust and Trusted scheme (RTS), Mesh Analysis (MA), Adhoc on demand Distance Vector (AODV) and optimized Adhoc on demand Distance Vector (OAODV). Among them the proposed model attains the 99.43% of packet delivery rate. High packet delivery rate provides low computational time as well as less reducing the complexities. Moreover, the comparison of packet delivery rate of the proposed model was compared with the other existing models were shown in the Fig. 9.

5.3. *Discussion*

In this section, the rate of parameter attained through the proposed model was discussed. Moreover the performance rate of the proposed model such as throughput of the proposed model was about 98.87%; Accuracy of the proposed model was about 99.72%; lower delay was developed through the proposed model about 0.002. Lower rate of time needed for transmitting the information about 1.476, packet drop of the proposed model was about 0.0559 as well as the delivery rate of the packet was high about 99.43%. The metrics and the performance rate of the metrics were tabulated in Table 2.

Performance validation	
Metrics	**Performance (%)**
Throughput	98.87
Accuracy	99.72
Delay	0.0027
Transmission time	1.476
Packet drop	0.0559
Packet delivery rate	99.43

Table 2. Performance validations.

Parameters were measured on the basis of after and before applying the DoS attack. However the proposed attaining the higher rate parameter after applying the Dos attack was illustrated in the Fig. 10.

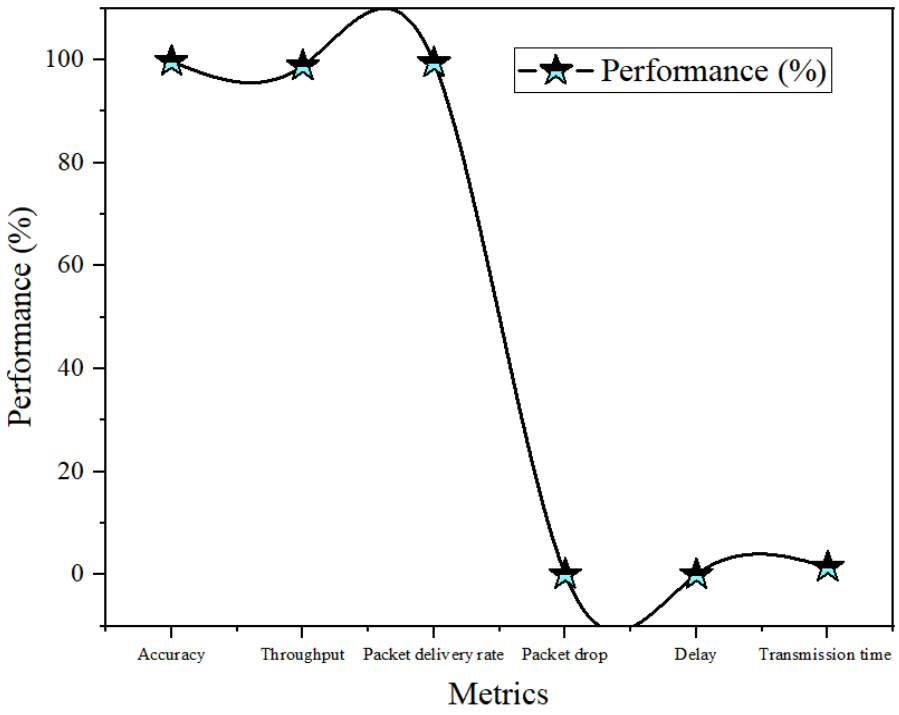

Fig. 10. Overall performance of the proposed model.

6. Conclusion

In this research, to provide the better security a novel CbAR has been presented. Moreover, the presented model is validated through the CICIDS databases. After training the CICIDS, the chimp fitness solution has activated for predicting the malicious action. If any malicious or abnormal behaviours are found then it is neglected from the network architecture. Finally, the presented model's performance was justified with DoS attack. Moreover, the proposed model attained the throughput rate was about 98.87%; when comparing with the existing models 1% of the throughput were developed in the proposed model. Delay of the proposed model was about 0.0027; when comparing with the existing models 2% of delay was improved in the designed model. Moreover, the Packet delivery rate of the proposed model was about 99.43; compared to the other models 2% of the delivery rate were improved in the proposed model. However, the accuracy was the proposed model was about 99.72%, lower rate of packet drop were attained through the proposed model was about 0.055. Moreover, the proposed model needs 1.476 b/s times for transmitting the packets. Consequently, the proposed model reaches high performance rate when compared with the existing models as well as the CbAR model was better for detecting and preventing the attack.

Acknowledgments

None

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Basharat, M.; Naeem, M.; Qadir, Z.; Anpalagan, A. (2022): Resource optimization in UAV-assisted wireless networks—A comprehensive survey. Transactions on Emerging Telecommunications Technologies, pp. e4464.
[2] Bin-Yahya, M.; Shen, X. (2022): Secure and energy-efficient network topology obfuscation for software-defined WSNs. IEEE Internet of Things Journal.
[3] Cappello, G. M.; Colajanni, G.; Daniele, P.; Sciacca, D. (2022): A constrained optimization model for the provision of services in a 5G network with multi-level cybersecurity investments. Soft Computing, pp. 1-18.
[4] Celebi, H. (2022): A Dual-Radio Hybrid Mesh Topology for Multi-Hop Industrial IoT Networks in Harsh Environments. Balkan Journal of Electrical and Computer Engineering, **10**(2), pp. 125-131.
[5] Chung, D. J.; Madison, G. P.; Aponte, A. M.; Singh, K.; Li, Y.; Pirooznia, M.; Bleck, C. K. E.; Darmani, N. A.; Balaban, R. S. (2022): Metabolic design in a mammalian model of extreme metabolism, the North American least shrew (Cryptotisparva). The Journal of physiology, **600**(3), pp. 547-567.
[6] Collados-Lara, A. J.; Pardo-Igúzquiza, E.; Pulido-Velazquez, D. (2021): Assessing the impact of climate change–and its uncertainty–on snow cover areas by using cellular automata models and stochastic weather generators. Science of the Total Environment, **788**, pp. 147776.
[7] Dhar Dwivedi, A.; Singh, R.; Kaushik, K.; Mukkamala, R. R.; Alnumay, W. S. (2021): Blockchain and artificial intelligence for 5G-enabled internet of things: challenges, opportunities, and solutions. Transactions on Emerging Telecommunications Technologies, pp. e4329.
[8] Ghori, M. R.; Wan, T. C.; Sodhy, G. C.; Rizwan, A. (2021): Optimization of the AODV-Based Packet Forwarding Mechanism for BLE Mesh Networks. Electronics, **10**(18), pp. 2274.
[9] Grigg, S.; Pullin, R.; Pearson, M.; Jenman, D.; Cooper, R.; Parkins, A.; Featherston, C. N. (2021): Development of a low-power wireless acoustic emission sensor node for aerospace applications. Structural Control and Health Monitoring, **28**(4), pp. e2701.
[10] Haseeb, K.; Din, I. U.; Almogren, A.; Islam, N.; Altameem, A. (2020): RTS: A robust and trusted scheme for IoT-based mobile wireless mesh networks. IEEE Access, **8**, pp. 68379-68390.
[11] He, Q.; Sun, X.; Yan, Z.; Fu, K. (2021): DABNet: Deformable contextual and boundary-weighted network for cloud detection in remote sensing images. IEEE Transactions on Geoscience and Remote Sensing, **60**, pp. 1-16.
[12] Hernández-Morales, C. A.; Luna-Rivera, J. M.; Perez-Jimenez, R. (2022): Design and deployment of a practical IoT-based monitoring system for protected cultivations. Computer Communications, **186**, pp. 51-64.
[13] Hortelano, D.; Olivares, T.; Ruiz, M. C. (2021): Reducing the energy consumption of the friendship mechanism in Bluetooth mesh. Computer Networks, **195**, pp. 108172.
[14] Hua, J.; Shunwuritu, N. (2021): Research on term extraction technology in computer field based on wireless network technology," Microprocessors and Microsystems, **80**, pp. 103336.
[15] Khamer, L.; Labraoui, N.; Gueroui, A. M.; Ari, A. A. A. (2021): Enhancing video dissemination over urban VANETs using line of sight and QoE awareness mechanisms. Annals of Telecommunications, **76**(9), pp. 759-775.
[16] Khan, I. U.; Shah, S. B. H.; Wang, L.; Aziz, M. A.; Stephan, T.; Kumar, N. (2021): Routing protocols & unmanned aerial vehicles autonomous localization in flying networks. International Journal of Communication Systems, pp. e4885.
[17] Laghari, A. A.; Wu, K.; Laghari, R. A.; Ali, M.; Khan, A. A. (2021): A review and state of art of Internet of Things (IoT). Archives of Computational Methods in Engineering, pp. 1-19.
[18] Lin, H. Y.; Hsieh, M. Y.; Li, K. C. (2021): A Multi-level Security Key Management Protocol Based on Dynamic M-tree Structures for Internet of Vehicles. 2021 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), IEEE.
[19] Ma, L.; Wang, L.; Liu, Z. (2021): Multi-level trading community formation and hybrid trading network construction in local energy market. Applied Energy, **285**, pp. 116399.

[20] Oroza, C. A.; Giraldo, J. A.; Parvania, M.; Watteyne, T. (2021): Wireless-Sensor Network Topology Optimization in Complex Terrain: A Bayesian Approach. IEEE Internet of Things Journal, **8**(24), pp. 17429-17435.
[21] Sharma, D. D. (2021): A low latency approach to delivering alternate protocols with coherency and memory semantics using PCI Express® 6.0 PHY at 64.0 GT/s. 2021 IEEE Symposium on High-Performance Interconnects (HOTI), IEEE.
[22] Shin, J.; Chang, Y. K.; Heung, B.; Nguyen-Quang, T.; Price, G. W.; Al-Mallahi, A. (2021): A deep learning approach for RGB image-based powdery mildew disease detection on strawberry leaves. Computers and electronics in agriculture, **183**, pp. 106042.
[23] Shokouhifar, M. (2021): FH-ACO: Fuzzy heuristic-based ant colony optimization for joint virtual network function placement and routing. Applied Soft Computing, **107**, pp. 107401.
[24] Talwar, S.; Himayat, N.; Nikopour, H.; Xue, F.; Wu, G.; Ilderem, V. (2021): 6g: Connectivity in the era of distributed intelligence. IEEE Communications Magazine, **59**(11), pp. 45-50.
[25] Taştan, S. İ.; Dalkiliç, G. (2021): Smart Home System Using Internet of Things Devices and Mesh Topology. 2021 6th International Conference on Computer Science and Engineering (UBMK), IEEE.
[26] Thulasiraman, K.; Lin, T.; Javed, M.; Xue, G.; Zhou, Z. (2022): Circuits/cutsets duality and theoretical foundation of a structural approach to survivable logical topology mapping in IP-over-WDM optical networks. Optical Switching and Networking, **44**, pp. 100653.
[27] Yan, B.; Liu, Q.; Shen, J. L.; Liang, D. (2022): Flowlet-level multipath routing based on graph neural network in OpenFlow-based SDN. Future Generation Computer Systems, **134**, pp. 140-153.
[28] Zhang, Y.; Ren, Q.; Song, K.; Liu, Y.; Zhang, T.; Qian, Y. (2021): An Energy Efficient Multi-Level Secure Routing Protocol in IoT Networks. IEEE Internet of Things Journal.

Authors Profile

Lingala Thirupathi has received his B.Tech in Computer Science and Information Technology from Jyothishmathi Institute of Technology & Science, Karimnagar, Affiliated to JNTUH, Telangana in 2005 and M.Tech in Software Engineering from Sreenidhi Institute of Science & Technology, Ghatkesar, Affiliated to JNTUH, Telangana in 2007, he is pursuing Ph.D in Computer Science & Engineering from GITAM (Deemed to be University), Vishakhapatnam, AP. He is having 14+ years of experience in Teaching and Industry; he worked as a Consultant for HTC. He is qualified in Telangana State Eligibility Test and awarded GOLD MEDAL in M.Tech academics. He has achieved All India Rank-611 in GATE and he has done many certifications from Oracle (Oracle PL/SQL Certified Associate), CISCO, Microsoft, Coursera, Alison and Udemy. He is a Palo Alto Networks Authorized Cybersecurity Academy Instructor and Cisco Instructor. He has published 20+ articles in national and international journals and published Patents in India and Australia. He has published text book on “Machine Learning Architecture a Recent Paradigm” (ISBN: 9781956102819) and “Computer Networks and Simulation” (ISBN: 9789355743206, 9355743203). His area of research includes Computer Networks, Network Security, Internet of things, Machine learning & Artificial intelligence.

P.V. Nageswara Rao, Professor, Department: Computer Science & Engineering, GITAM School of Technology, GITAM (Deemed to be University), Visakhapatnam. He has published more articles in national and international journals. His area of research includes Computer Networks & Soft Computing.