SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I11P103

Volume 10 Issue 11, 31-38, November 2023

Original Article

Slime Mould-Based Collaborative Deep Boltzmann Machine for Intrusion Detection Model in Mobile Ad Hoc Network

G. Parameshwar[1,4], N.V. Koteswara Rao[2], L. Nirmala Devi[3]

[1,3]*Department of Electronics and Communications Engineering, University College of Engineering, Osmania University, Hyderabad, India.*
[2]*Department of Electronics and Communications Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, India.*
[4]*Department of Electronics and Communications Engineering, Vidya Jyothi Institute of Technology, Hyderabad, India.*

[1]*Corresponding Author : paramesh.gujjula@gmail.com*

Received: 07 September 2023 Revised: 10 October 2023 Accepted: 08 November 2023 Published: 30 November 2023

Abstract *- Mobile Ad Hoc Network (MANET) is a dynamic wireless network developed by using wireless nodes without using any infrastructures. The significant features of MANET are low-cost infrastructure, self-organization, mobility and rapid deployment, which offer the opportunity to deploy it in various applications such as disaster relief, environmental monitoring and military communications. Based on the previous studies, improved Quality of Service (QoS) metrics with security problems during data communication are challenging with the increased wireless technology. By addressing these issues, here proposed a novel secured intrusion detection model in MANET. The cluster formation is effectuated with the Modified K-Harmonics Mean Clustering (MKHMC), and the cluster heads are selected with the proposed Chaotic Multi-verse Krill Herd Optimization (CMKHO) algorithm, which helps to provide energy efficiency, reduction in delay, and increased throughput. Meanwhile, this proposed blockchain-secured Slime Mould-based Collaborative Deep Boltzmann Machine (SM-CDBM) includes three stages, (i) learning the unimodal DBM models to identify the intrusion, (ii) learning the shared layer parameters utilizing a Collaborative Restricted Boltzmann Machine (CRBM), and (iii) fine-tuning the CDBM using the Slime Mould Optimization (SMO) algorithm. Simulations are effectuated in the NS2 tool and accomplish improved malicious node detection, end-to-end delay, energy efficiency, and overhead compared to other state-of-the-art approaches.*

Keywords *- MANET, Modified K-Harmonics Mean Clustering, Chaotic Multi-verse Krill Herd Optimization, Collaborative DBM, Slime Mould Optimization algorithm.*

1. Introduction

Mobile Ad-Hoc Networks (MANETs) [1] can be developed in a conscience method with none from before the supply chain and operations supervision, unlike standard cellular connections like Wi-Fi connectivity and data networks. These connections are less expensive and are suitable for scenarios like earthquakes, catastrophes, flash points, relief efforts, etc., because they don't depend on any from before the infrastructure.

Sensor networks, automotive wireless communications, robot communications, autonomous aerial vehicles [2], underwater networks, Internet of Things (IoT) [3], and other non-emergency applications are examples. As a result of the nodes' potential for continuous motion, the network architecture is dynamic and highly unstable. Especially compared to comparable bulk counterparts, communication networks have a shorter lifespan. Several abilities and frequency restrictions apply to the bandwidth links. Both unidirectional and bidirectional links are possible. These networks have lower efficiency since interference, withering, vibration, and orthogonal frequency division multiplexing [4]. The benefit of using a Mobile Ad Hoc Network is an internet connection without a wireless router. As a result, maintaining an ad hoc network may be less expensive than maintaining a standard network.

Shams et al. [5] have described a Support Vector Machine- Intrusion Detection System (SVM-IDS) to examine internet usage to find and eliminate rogue connections to boost performance. It is highly effective in identifying network attacks and eradicating faulty activities from the system. Hence, it poses a severe risk to impose operators and broadband connections. Islabudeen et al. [6] have presented a Smart Approach for Intrusion Detection and Prevention System (SA-IDPS) to use computational techniques to reduce

Mobile Ad Hoc Network assaults. To prevent invasion, a hash chain is used for the packet analyzer to identify the intrusion. The prevention rate is increased and reduces the false rate. Thus, it isn't effortless to implement in big real-world datasets. Krishnanet al. [7] highlighted a Modified Zone-Based Intrusion Detection System (MZBIDS) to protect from various threats, a more effective discharge mechanism must be constructed. The internal boundary executive and the remaining route's residents would find similar signatures. The technique is significant because it provides the boundary framework and offers a method to identify faulty nodes. It raises the delivery ratio and false alarms. Moreover, the performance should be extended for other communication systems.

Bala et al. [11] have implemented System Network Information-based Moderation and Mitigate (SNI-MM) routing models. This node uses its acquired parameters to build the network design for each time limit to accomplish detection capabilities. It raises the level of quality management. Hence, in a significant distribution situation, the framework can be improved with numerous users. The points below define the considerable contribution of this analysis.

- The Modified K-Harmonics Mean Clustering (MKHMC) model is used for cluster formation in MANET.
- The Chaotic Multi-verse Krill Herd Optimization (CMKHO) algorithm selects the best cluster heads, demonstrating energy efficiency, reduction in delay, and increased throughput.
- The intrusion detection in MANET is completed using blockchain with a secured Slime Mould-based Collaborative Deep Boltzmann Machine (SM-CDBM).
- During intrusion detection, the Slime Mould Optimization (SMO) algorithm fine-tunes the collaborative DBM.

The rest of the paper is outlined: The literature survey and the problem definitions are reviewed in section 2. Section 3 depicts the proposed model, and the experimental results are shown in section 4. At last, section 5 concludes the paper.

2. Literature Survey

Shams et al. [8] have described a Support Vector Machine- Intrusion Detection System (SVM-IDS) to examine internet usage to find and eliminate rogue connections to boost performance. The attack detection is identified with a rapid detection rate to demonstrate a computer model to increase extra structural elements by identifying and eliminating faulty nodes from the infrastructure. It is highly effective in identifying network attacks and eradicating erroneous activities from the system. Hence, it poses a severe risk to impose operators and broadband connections.

Islabudeen et al. [9] have presented a Smart Approach for Intrusion Detection and Prevention System (SA-IDPS) to use computational techniques to reduce Mobile Ad Hoc Network assaults. The four units are considered for classification, feature extraction, packet analyzer, and data pre-processing. To prevent invasion, a hash chain is used for the packet analyzer to identify the intrusion. The prevention rate is increased and reduces the false rate. Thus, it isn't straightforward to implement in big real-world datasets.

Abbas et al. [10] evaluated a detection system for masquerading attacks requiring temperature monitoring or a permanent relay node. It creates multiple identities and adopts them, leading to an irregular situation, namely, the simultaneous availability of individuality further than just the intermediate node. The connection examines both the prediction performance and the separation amongst nodes in the existence of variation. It shows good decision precision. Therefore, it operates in fixed points, which is inappropriate for ad hoc networks.

Bala et al. [11] have implemented a novel system network information-dependant paradigm of moderation to anticipate and mitigate routing assaults. The individual node can acquire more about the station's nodes, their counterparts' positions, energy characteristics, and relocation frequency through packet forwarding protocols associated with development. This node uses its acquired parameters to build the network design for each time limit to accomplish detection capabilities. It raises the level of quality management. Hence, in a significant distribution situation, the framework can be improved with numerous users.

Krishnan et al. [12] highlighted a Modified Zone-Based Intrusion Detection System (MZBIDS) to protect from various threats, a more effective discharge mechanism must be constructed. The internal boundary executive and the remaining route's residents would find similar signatures. It also prevents the precise location of domain residents from being known. The technique is significant because it provides the boundary framework and offers a method to identify faulty nodes. It raises the delivery ratio and false alarms. Moreover, the performance should be extended for other communication systems.

Thiagarajanet al. [13] suggested the Ad hoc On-demand Multipath Distance Vector (AOMDV) has developed techniques. The intermediate node is crucial in both locating and retaining the routes. Uni-path and multi-path are the two categories of routing. The multipath routing system can increase the ad-hoc network's reliability to assess the routing protocol's performance. It enhances intrusion detection and mobile ad-hoc networks. Thus, there are legal restrictions on both large-scale energy storage capabilities.

Pu et al. [14] describe a jamming-resilient multipath routing protocol called JarmRout because deliberate interference, jamming, and partial and regional malfunctions do not affect overall network performance. The packets are received from the transmission power to determine the connection capabilities among a station and its adjacent nodes.

The physical range scheme determines the maximum space routing transmissions connecting nodes at the source and destination. The performance increases the latency and ratio. Thus, it intends to create a limited testbed using secure propellers.

2.1. Problem Definition

The significant issues of security-based MANET are enclosed in this section. The source trust rate is calculated with the number of route requests generated to mitigate the attacks or intrusion. The trust value for the source MANET node is evaluated with,

$$S\text{-}T = (RR_{EQ}\ Count)^{-1} \quad (1)$$

The source node of the network is indicated with S, and T denotes the trust, and the trust value can be evaluated with the packets requested for the routing, i.e., RR_{EQ} by the nodes. However, the effectiveness of using trust value and its computation is low since each immediate node forwards the packet for the route selection.

Routing selected based on the trust value increases the retransmission concerning the breakage of links. Various researchers have used several techniques. The major issues for MANET-based communication based on state-of-art works are highlighted below,

- Optimized Cluster head selection is not effective.
- Trust management for the optimal route selection is not precise.
- Need optimized deep learning approach for intrusion detection and security compared to machine learning models.

3. Proposed Methodology

The task of intrusion detection among various cluster nodes is detected and reduced energy consumption and accuracy with an improved intrusion detection ratio. This paper combined three models such as cluster formation, selection of cluster head, and intrusion detection.

3.1. Formation of Clusters

Generally, the simple unsupervised learning algorithm is K-harmonic Means Clustering (KMC), and it is widely applied to resolve clustering issues. Use the centroid's optimal global position to improve the KMC [9]. This paper proposed a Modified K-harmonic Means Clustering (MKMC) model to form clusters in MANET. The *m* instances into *k*-clusters are divided using *k*-means clustering.

The subsets are attained from the partitioning of cluster instances, such as (y_1,…..Y_m). Set the *k*-centroids position, and the number of clusters is initialized. Assign the number of instances D_j to cluster $J^{th}(J:1....k)$ and $D(D_1……D_k)$ is the vector of *k*-means in the j^{th} cluster. A variance of the entire intra-cluster as the *k*-means clustering is from the minimization of squared error means. For *k*-means clustering, equation (2) displays the squared error function.

$$F(k) = \sum_{j=1}^{J} \sum_{i=1}^{m_j} \left(y_j - D_j \right)^2 \quad (2)$$

The error Function F(k) is among various *k*-means solutions. The new clusters are formed using the MKMC model for one or more centroids.

3.2. CH Selection Using the CMKHO Algorithm

After the cluster formation, the following necessary process is developing a CMKHO algorithm for the cluster head selection from different nodes, mitigating the dimensionality issues. This proposed approach selects the optimal CH from the number of nodes in the formulated clusters. This method is based on the Krill Herd's common characteristics and determines the Krill Herd's uncertainties. The locations of the Krill positions [10] can be impacted by the three terms: the motion of the Krill, foraging features, and random diffusion.

3.2.1. Krill Motion

The induced movement represents each individual in the herd and its maintenance, like the nodes in the formulated cluster. The numerical formulation is denoted as,

$$A_j(T+1) = A_{\max}\delta_j + \kappa_m A_j(T) \quad (3)$$

The maximum node packet sending speed and inertial weights concerning the base station are indicated as A_{max} and δ_j^{local}, respectively. The best solution from the nodes is calculated as the equation given below,

$$\delta_j^{target} = M^{best} k_{j,best} H_{j,best} \quad (4)$$

δ_j^{target} is the efficacy of the targeted node, and its coefficient is M^{best}.

$$M^{best} = 2\left[\frac{S+1}{Max_{iteration}} \right] \quad (5)$$

The interval of a random variable is from 0 to 1.

3.2.2. Foraging Characteristics

The foraging behaviour of Krill is formulated as,

$$FR_j(T+1) = FS_f \alpha_j + \kappa_f FR_j(T) \quad (6)$$

The weight of inertia and speed at the foraging stage are K_f and FS_f corresponding. The best food attractions are A_j^{best} and $\alpha_j=\alpha_j^{food} + A_j^{best}$.

3.2.3. Wormhole Tunnels

The global optimum includes two phases. The trade-off between exploration and exploitation is ascertained, and wormhole tunnels step of random diffusion step of CKH optimization.

Chaotic Multi-verse Krill Herd Optimization (CMKHO) is the developed method. Wormholes enhance the inflation rate, and they contain a considerable probability for each universe to offer local changes, which are explained as follows;

$$H_j^k = \begin{cases} H_k + DRT \times \left((CU_k - CL_k) \times rnd + CL_k \right) & rnd < 0.5 \\ H_k - DRT \times \left((CU_k - CL_k) \times rnd + CL_k \right) & rnd \geq 0.5 \end{cases} \quad (7)$$

Where, DRT is the constant coefficient and selects the node features based on k^{th} parameter is H_k. The upper and lower bounds are CU_k and CL_k in which the random number is rnd.

3.2.4. Chaotic Map

The proposed approach utilizes three types of chaotic maps to improve the chaotic Krill optimization: sinusoidal, cosine, and sine. In the exploitation stage, the rapid convergence-based global optimum is made. The chaotic maps and the random values are estimated with the following equation,

$$Best_C = 2\left(C(T) + \frac{1}{Max_t} \right) \quad (8)$$

The iteration at which the optimal best solution can be obtained is denoted as Max_t, and the best CH can be selected $Best_c$ from the formulated cluster. For the selection CH, the pseudocode used is illustrated in Algorithm 1.

The choice of CH helps provide better routing and speed of transmission packets from nodes to the base station. Hence, according to the proposed approach, the CH is selected based on the node's energy, distance and capability of the particular node.

Algorithm 1: CMKHO Pseudocode
Initialize the parameters of CMKHO, iteration (max) based on the nodes in the cluster
Chaotic map selection based on the random approach
Upgrade the δ_j^{local} (inertia weight)
Estimate the fitness value
While $m<M_{max}$
else
Not the maximum iteration
Do
Initiate the population from best to worst
For $j=1;N_p$
do
The movement of Krill is updated using equation (3)
Foraging behaviour is updated with equation (6)
The multi-verse-based wormhole tunnel model is updated with equation (7)
The chaotic map model is updated with equation (8)
end for
Store the new node location
m=m+1
end while
Acquire the optimal CH from the cluster.

3.3. Blockchain-Based Secured Trust Management-Based Routing

In the proposed approach, the blockchain establishes security and provides trust management in the MANET. Blockchains [11] are usually arranged sequentially in a chain structure of blocks with a distributed database that hoards the transaction details. Nowadays, blockchains are used not only for financial transactions but also for secured communication between other applications like MANET.

Blockchain enables trust without adopting third-party applications, and thus, the reason the work utilizes it for secured routing. When it is arduous to establish trust between the nodes, blockchain features provide better solutions with the multihop routing of MANETS. When the routing is secured from malicious attacks, it gives a better solution for preventing intrusion attacks. For intrusion detection, the proposed Slime Mould-based Collaborative Deep Boltzmann Machine (SM-CDBM) is elaborated on in the following section.

3.4. SM-CDBM for Intrusion Detection

The DBM is the major technique to detect intrusion. For CDBM, three stages of the training model are introduced. For intrusion detection, two unimodal DBM are trained [12]. The collaborative distribution learning task into three sub-tasks is divided, and the small number of iterations in the slime mould optimization algorithm fine-tunes the CDBM. During shared layer pre-training, freeze a lower layer with conventional methods.

The proposed algorithm is based on the Physarum polycephalum known as slime mould, and the species' life cycle. For the proposed CDBM's fine-tuning, the researcher utilized this SM [13] algorithm. Fine-tuning is effectuated to attain our proposed method's required intrusion detection accuracy. Fine-tuning might increase the iterations and epochs and adjust the learnable parameters and weights. Quickly converge the higher layers into local optima via slime mould. Referred as two models Intrusion_{DBM} and $\text{Non-Intrusion}_{DBM}$ it trains unimodal DBM. By giving input to DBM, the posterior is obtained with mean field interference after the pre-training. The logistic regression classifier was used to identify the unimodal intrusion identification $Q(H^2_{FK}=1/F)$.

Based on the CDBM shared layer, the blockchain-secured Slime Mould model pre-trains the parameters. The following equation expression describes the SM-CDBM model.

$$R(X,Y/\theta)=\sum_{H} R(X,Y,H) \tag{9}$$

$$R(X,Y/\theta)=\frac{1}{h}\sum_{H} \exp -e(X,Y,H) \tag{10}$$

From this,

$$Y=\left[Q\left(H^2_{FK}/F\right)\right]_{K=1,\ldots,R_2^F} \tag{11}$$

$$X=\left[Q\left(H^2_{SK}/S\right)\right]_{K=1,\ldots,R_2^S} \tag{12}$$

Belongs to Intrusion_{DBM} and $\text{Non-Intrusion}_{DBM}$, obtains the approximate posterior distribution marginal. The SM-CDBM parametric set is represented via $\theta=\{M_S, M_F\}$. When bias to CBDM top layers, the small random value initializes M_S and M_F. The log-likelihood is maximized to solve the optimization issue in MANET.

$$\theta=\arg\{\max_{\theta} \ln\ \delta\left(\theta/X,Y\right)\} \tag{13}$$

The slime mould optimization obtains the parameters based on the optimal values. The below equation delineates the true posterior distribution.

$$Q(H^3/x,y;\lambda)=\prod_{n=1}^{R_3}(H_n^3/X,Y) \tag{14}$$

From this, θ the current model parameter and the parameter of the mean field is δ. The lower bound is determined to enhance the variation, and slime mould optimizes the objective function in CDBM. Intrusion detection of MANET using SM-CDBM is illustrated in Figure 1. The SM-CDBM is initialized with the Unimodal DBM, and the collaborative RBM parameters are used. For MANET intrusion identification, collaborative space adopts the parameters in which the slime mould tunes the CDBM after this initialization. Apply it towards intrusion detection next to SM-CDBM training. At the hidden layer of CDBM, the intrusion present or not in MANET is identified.

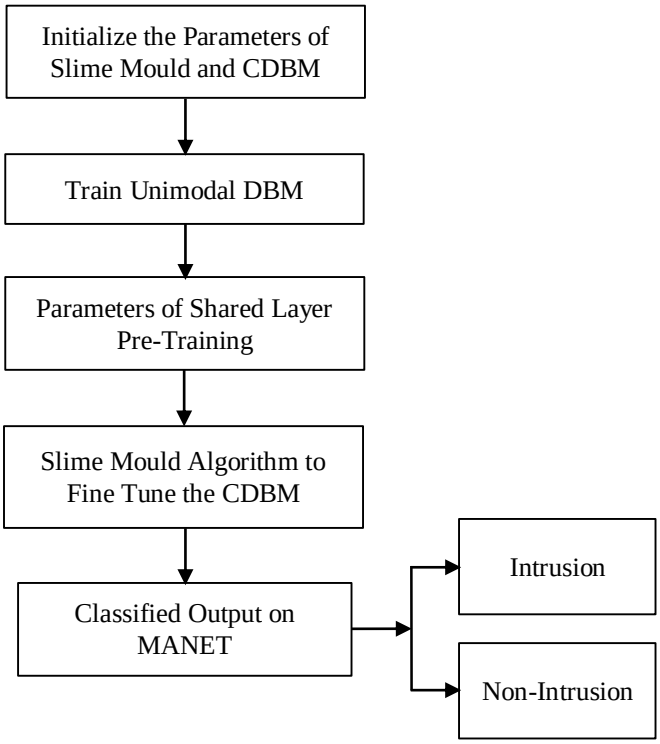


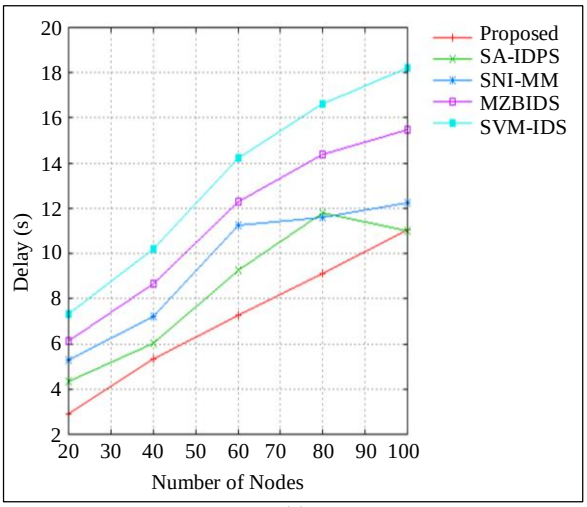
Fig. 1 Intrusion detection of MANET using SM-CDBM

4. Result Analysis

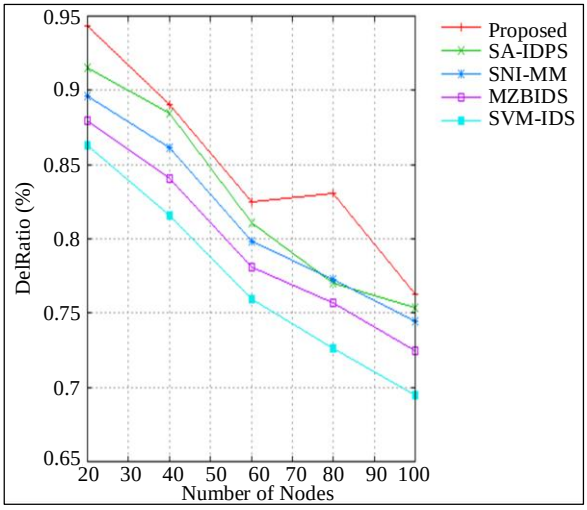
The experimental investigations and comparative studies are discussed in this section. NS-2 tool effectively implements the work. The results are plotted by varying the number of nodes and the number of attackers. The description of parameters is tabulated in Table 1. The comparative analysis based on the number of nodes' performances is delineated in Figure 2, in which the performances among delay, packet delivery ratio, drops, energy consumption, and throughput are plotted in Figure 2(a) to (e).

Table 1. Parametric description

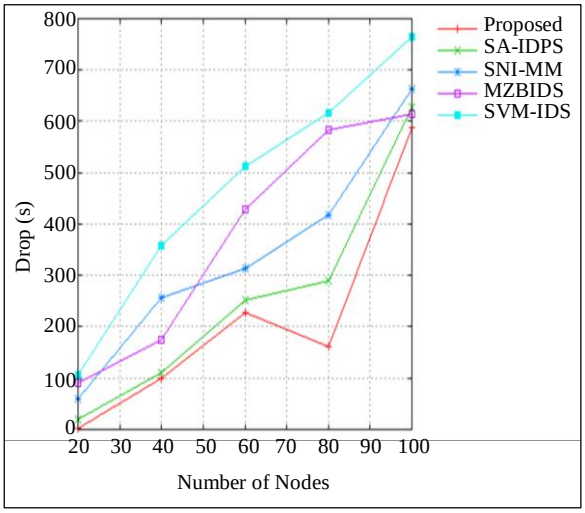
Variables	Ranges
Population Size	50
Number of Nodes	100
Simulation Tool	NS-2
Area of Simulation	500 * 500
Size of the Packet (Bytes)	500
Number of Iteration	100



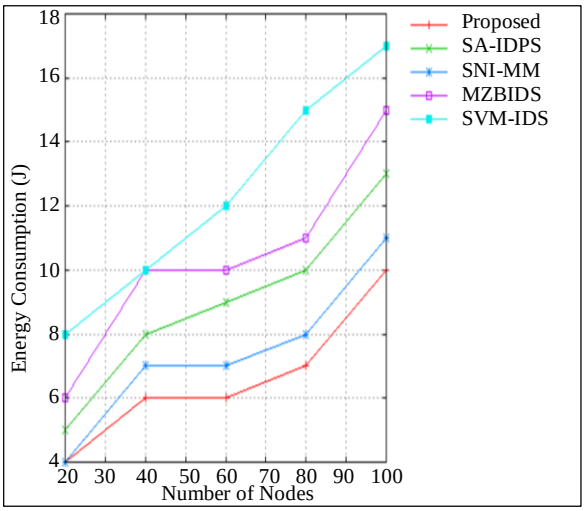
(a)



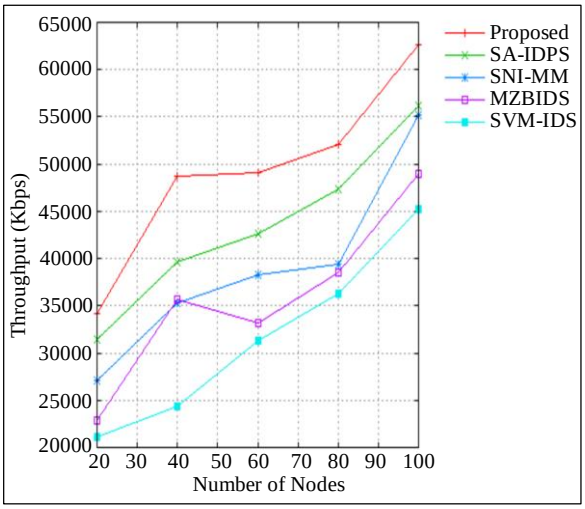
(b)



(c)



(d)

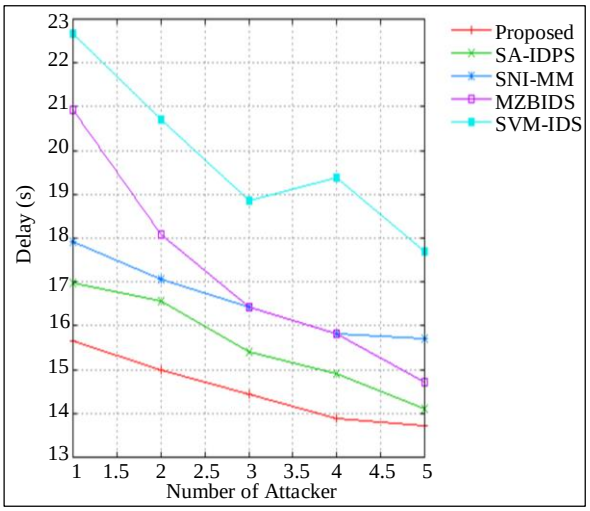


(e)

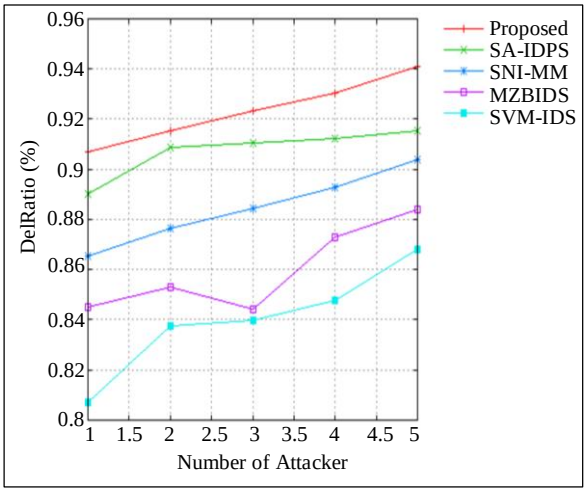
Fig. 2 Comparative analysis based on the number of nodes, (a) Delay, (b) Packet delivery ratio, (c) Drops, (d) Energy consumption, and (e) Throughput.

The number of nodes differs from 20 to 100 nodes. Depending upon the node performances, the proposed techniques demonstrated below 2s delay, more than 94% packet delivery ratio, below 0.1s drop, below 4J of energy consumption results and approximate 34000 Kbps of throughput rates. However, the proposed framework achieves minimum delay, drop, and energy consumption with higher throughput and packet deliver ratio than previous methods like SA-IDPS, SNI-MM, MZBIDS and SVM-IDS.

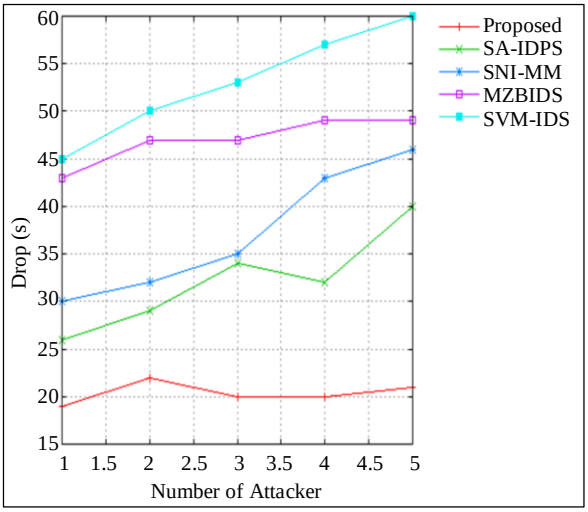
The results of the comparative analysis based on the number of attacker performances are shown in Figure 3, which shows the performances for the delay, packet delivery ratio, drops, energy consumption, and throughput are described in Figure 3(a) to (e). There is a variation between 20 and 100 nodes.



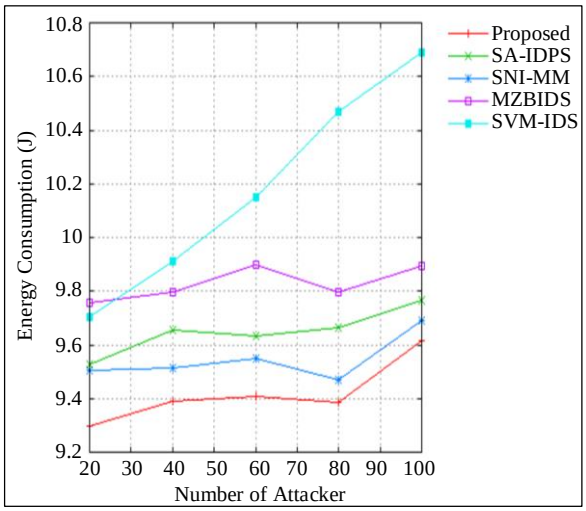
(a)



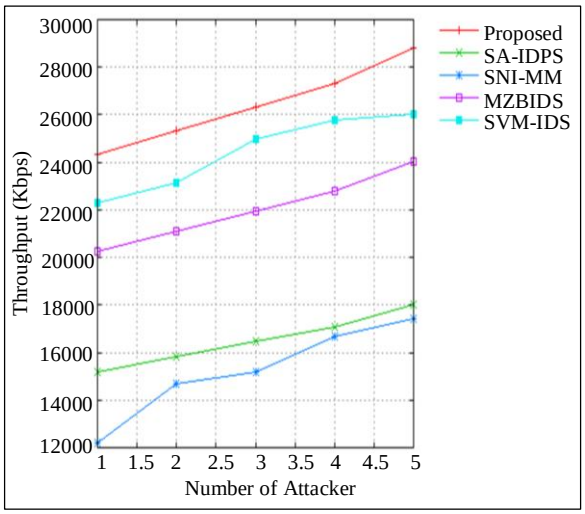
(b)



(c)



(d)



(e)

Fig. 3 Comparative analysis based on the number of attackers, (a) Delay, (b) Packet delivery ratio,(c) Drops, (d) Energy consumption, and (e) Throughput.

The proposed techniques showed below 16 s delay, more than 0.91% packet delivery ratio, below 19 s drop, near to 9.3J of energy consumption results, and approximately 24500 kbps of throughput rates depending on the node performances.

However, compared to earlier approaches like SA-IDPS, SNI-MM, MZBIDS, and SVM-IDS, the proposed framework achieves minimal delay, drop, and energy consumption with higher throughput and packet delivery ratio.

5. Conclusion

This paper presented a novel blockchain-secured Slime Mould-based Collaborative Deep Boltzmann Machine (SM-CDBM) for MANET intrusion detection. Network simulator-2 tool performs the experimental implementation.

To compare the state-of-art approaches, the proposed results demonstrated increased throughput, reduction in delay and energy efficiency with good results in communication overhead, energy efficiency, end-to-end delay and enhanced malicious node detection. The number of nodes differs from 20 to 100 nodes. However, compared to earlier approaches like SA-IDPS, SNI-MM, MZBIDS, and SVM-IDS, the proposed framework achieves minimal delay, drop, and energy consumption with higher throughput and packet delivery ratio regarding the number of nodes and attackers.

References

[1] Osamah Ibrahim Khalaf et al., "Efficient Dual-Cooperative Bait Detection Scheme for Collaborative Attackers on Mobile Ad-Hoc Networks," *IEEE Access*, vol. 8, pp. 227962-227969, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Vinicius Mariano Gonçalves, Ryan McLaughlin, and Guilherme A.S. Pereira, "Precise Landing of Autonomous Aerial Vehicles Using Vector Fields," *IEEE Robotics and Automation Letters*, vol. 5, no. 3, pp. 4337-4344, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Kamran Shaukat et al., "A Review on Security Challenges in Internet of Things (IoT)," *26th International Conference on Automation and Computing (ICAC)*, United Kingdom, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Seichiroh Osaki, Takumi Ishihara, and Shinya Sugiura, "Eigenvalue-Decomposition-Precoded Ultra-Dense Non-Orthogonal Frequency-Division Multiplexing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 12, pp. 8165-8178, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Erfan A. Shams, and Ahmet Rizaner, "A Novel Support Vector Machine Based Intrusion Detection System for Mobile Ad-Hoc Networks," *Wireless Networks*, vol. 24, pp. 1821-1829, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] M. Islabudeen, and M.K. Kavitha Devi, "A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad-Hoc Networks against Security Attacks," *Wireless Personal Communications*, vol. 112, pp. 193-224, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Zichen Zhang, Shifei Ding, and Yuting Sun, "A Support Vector Regression Model Hybridized with Chaotic Krill Herd Algorithm and Empirical Mode Decomposition for Regression Task," *Neurocomputing*, vol. 410, pp. 185-201, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Caciano Machado, and Carla Merkle Westphall, "Blockchain Incentivized Data Forwarding in MANETs: Strategies and Challenges," *Ad Hoc Networks*, vol. 110, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mohammad Rafiqul Alam et al., "A Joint Deep Boltzmann Machine (jDBM) Model for Person Identification Using Mobile Phone Data," *IEEE Transactions on Multimedia*, vol. 19, no. 2, pp. 317-326, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[10] Shimin Li et al., "Slime Mould Algorithm: A New Method for Stochastic Optimization," *Future Generation Computer Systems*, vol. 111, pp. 300-323, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] K. Bala, S. Jothi, and A. Chandrasekar, "An Enhanced Intrusion Detection System for Mobile Ad-Hoc Network Based on Traffic Analysis," *Cluster Computing*, vol. 22, pp. 15205-15212, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] R. Santhana Krishnan et al., "Modified Zone-Based Intrusion Detection System for Security Enhancement in Mobile Ad Hoc Networks," *Wireless Networks*, vol. 26, pp. 1275-1289, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] R. Thiagarajan, M. Rajesh Babu, and M. Moorthi, "Quality of Service Based Ad Hoc On-Demand Multipath Distance Vector Routing Protocol in Mobile Ad Hoc Network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 4957-4965, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Cong Pu, "Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks," *IEEE Access*, vol. 6, pp. 68472-68486, 2018. [CrossRef] [Google Scholar] [Publisher Link]