JOURNAL OF BASIC SCIENCE AND ENGINEERING

DESIGN A NETWORK INTRUSION DETECTION MODEL BY USING AD-HOC ON-DEMAND MULTIPATH DISTANCE VECTOR (AODMV) AND CLUSTER BASED ROUTING PROTOCOL

Mrs.V.Deepa[1] and Dr.N.Radha[2]

[1] Ph.D Scholar,Department of Computer Science, PSGR Krishnammal College for Women

deepa.rskumar@gmail.com

[2] Department of Data Analytics, PSGR Krishnammal College for Women

Abstract

THE INTRUSION DETECTION SYSTEM (IDS) IS ESSENTIAL FOR NETWORK SECURITY, BUT ITS COMPLEX ENVIRONMENT CAN RESULT IN HIGH FALSE DETECTION RATES DUE TO THE LARGE NUMBER OF NORMAL SAMPLES. TO TACKLE THIS ISSUE, A CLUSTER BASED ROUTING PROTOCOL, INTEGRATED TO ENHANCED GENERATIVE ADVERSARIAL NETWORK WITH BIDIRECTIONAL LONG SHORT-TERM MEMORY AND CROSS-CORRELATED CONVOLUTIONAL NEURAL NETWORK (CBRP-EGAN-BILSTM-CCNN) HAS BEEN DEVELOPED IN MANET. FIRST CLUSTER BASED MANET ENVIRONMENT WAS CREATED BY USING AD-HOC ON-DEMAND MULTIPATH DISTANCE VECTOR (AODMV) ROUTING PROTOCOL. VARIOUS ROUTING ATTACKS ARE SIMULATED AND NETWORK PARAMETERS ARE LEARNED FROM EACH AND EVERY NODE AND TRANSFERRED TO CLUSTER HEADS (CHS). CHS SHARE THEIR LOCAL AND GLOBAL INFORMATION AMONG THEM USING CLUSTER BASED ROUTING PROTOCOL (CBRP).THE DATASET HAS BEEN OBTAINED BY COLLECTING THE NETWORK PARAMETERS RESPECTIVE TO ATTACKS SIMULATION. THIS DATASET IS USED TO TRAIN THE EGAN-BILSTM-CCNN MODEL AND IT HAS BEEN DEPLOYED WITHIN EACH CH FOR INTRUSION DETECTION, ACHIEVING A BALANCE BETWEEN SECURITY AND PERFORMANCE IN MANETS AND TO BE MORE EFFICIENT IN FINDING THE EXTERNAL ATTACKS. IN THIS PAPER IT HAS ALSO BEEN PROVED THAT USING AD-HOC ON-DEMAND MULTIPATH DISTANCE VECTOR (AODMV) ROUTING PROTOCOL WILL PROVIDE MORE ACCURACY IN VARIOUS NETWORK PARAMETERS THAN AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) PROTOCOL.

Keywords

Attacks, AOMDV protocol, Routing protocol, IDs, Malicious nodes.

1. INTRODUCTION

A Mobile Ad hoc NETWORK (MANET) follows dynamic topology .It is defined as group of nodes arranged together and they are connected and communicate with other nodes via a shared

wireless channel without the assistance of a centralized authority or pre-built infrastructure [3]. MANET nodes can move throughout the network often, unpredictably, and randomly [7]. This node relocation has a trivial effect on the status of trust among nodes as well as the complexity of routing. This mobility leads to the uncertain architecture of the network and host connectivity. The constantly shifting network architecture requires the participating nodes to efficiently manage the network environment. The knowledge and dedication of the nodes to one another is the main emphasis of a communication. Every node switches between being the router and the host in turn. When a node initiates a discussion, it becomes the host. When nodes create and preserve paths to other nodes, they perform the role of routers [1].Because nodes are movable, the topology of the network is always changing. So due to high mobility of nodes MANET environment is highly vulnerable to threats. Now a days researchers recommending lot of studies centring on MANET security. Few researchers have proposed various routing protocols, methodologies to improve the security of MANET. Some of the researchers proposed Machine learning algorithms to build security model to prevent MANET threats.

1.1 MANET Routing Protocols

Due to the absence of centralized control, routing is very challenging in ad-hoc network technology. Routing protocol is responsible for establishing a path between the nodes. Routing protocols is categorized in to two types. They are Proactive and Reactive protocols.

Proactive protocols:

Another name for these protocols is table-driven routing. Every mobile node keeps an independent routing table with the details of all possible routes to other mobile nodes. Due to the unstable environment of the mobile ad-hoc network topology, the direction-finding information is restructured in the routing database based on the changes carried out by the network topology. Its drawback is that large networks find it difficult to use since the routing table's entries grow excessively large due to the requirement to retain route information to every potential node.

Reactive Protocols:

Routing overhead is reduced using reactive protocols, because in a reactive protocol, the routes will be discovered only if it is desired by the source node to initiate communication. When a dispatcher node wants to transmit some data packets to recipient node then path will be established by this protocol to implement the communication.. The route is kept up to date as long as the current link remains intact. Compared to pro-active routing methods, reactive routing protocols offer a lower routing overhead. The drawback is that a route discovery could require sending out a abundance of inquiry data over the whole network.[5] Dynamic Source Routing Protocol (DSR), Ad-hoc On-demand Distance Vector (AODV), and Ad-hoc On-demand Multipath Distance Vector

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

(AOMDV) are the three different forms of reactive protocols. This research paper discuss on AOMDV protocol evaluation along with CBRP.

Ad-hoc On-demand Multi path Distance Vector (AOMDV)

AOMDV is the extension of AODV protocol. Both belong to reactive protocols category. AOMDV and AODV differ mostly in how many routes are found in each route discovery [5].Every recipient node's routing item has a numerous subsequent stages and the associated hop counts on it. This sequence number is the same for every subsequent hop [4]. Established on the knowledge of a distance vector, AOMDV employs a hop-by-hop routing strategy. As the RREQ spreads throughout the intermediate and destination nodes of the AOMDV, it forms several reverse paths. In AOMDV, many discontinuous and loop-free pathways are found. Such pathways are found using a flood-based route discovery algorithm. By using the routing data that is already included in the AODV protocol, AOMDV's overhead is kept to a minimum. [6] Compared to AODV, the routing table entry structure for AOMDV is different. The advertised hop count feature is a new addition to the AOMDV route database. A pathway database comprising the next hop, finalized hop, hopping count, and termination time out can be utilized to retain additional information about each alternate path. When determining if two pathways are disjoint, last hop information is helpful. [7]

Cluster Based Routing Protocol

Dynamic source routing is the backbone for the CBRP source routing technology. The objective of the CBRP is dividing the network nodes in to different clusters .Cluster head will be elected for each cluster. Most of the researchers concentrated their focus on improving the efficiency of CBRP. As it is known that MANET environment follows unstable topology structure, the routing is also unhinged .As the impact of this uncertainty, if there is not enough energy, the cluster head may move away from the cluster or perish. If the network size increases the CH requires more energy consumption to communicate longer distance. To address this issue this paper introduce Enhanced Weighted Cluster Algorithm(EWCA) to improve the efficiency of CBRP.

2. OVERVIEW OF IDS

An intrusion detection system (IDS) is software or termed as set of instruction which efficiently monitors network behaviour spot out any up normal circumstances arises in the network. Many organisations are still using traditional methods like Firewall but these are not able to detect the new threats. An intrusion detection system is a powerful tool for witnessing network activities and to detect any micelles activity found. It allows the network to transfer the data and it completely substantiates any manifestation of unfamiliar activities. If any intrusion pointed out the IDS model will check the network activity with predefined patterns by comparing.

IDS can be divided in to 5 types.

- Host-based IDS- Monitor single host activity

- Network Based IDS-Monitor network traffic
- Protocol Based IDS-Control and interprets the protocol
- Application Based IDS- Controls and Interprets on applications
- Hybrid IDS-Combination of two or more approaches

An intrusion detection system acts as an adaptable safeguard technology for system security after traditional technologies fail. This research work is focusing on designing NIDS.

NDIS installed in a predetermined network node so they can monitor network traffic coming from all connected devices. The entire subnet's passing traffic is witnessed, and the traffic is associated to the list of known attacks by matching [11]. The administrator can receive an alert once an attack is detected or strange activity is noticed.

In MANET for detecting threats researchers have designed IDS model by adopting any of following types.

Standalone IDS

IDS software is installed on each MANET node. Due to the lack of cooperation between the network's nodes the local and global information cannot be shared by the nodes .This type of IDS model capable for working on single networks and not appropriate for complex or multilayer environment.

Hierarchical IDS

The system is divided into bunches, and in each Cluster Head (CH) IDS can be installed. Maintaining information about their cluster members and keeping an eye out for incursions is the major responsible for each Cluster Head (CH). The cluster head functions as an IDS agent both locally and globally. But this types fails to address the integrated attacks.

Distributed and cooperative IDS

Detection agent is allotted for every node in the network and it is responsible for identifying and compiling inter cluster, intra cluster responses [9]. In the event of global detection and extensive search circumstances, the agent collaborates with other nodes [9]. When an incursion is detected, a local or global agent will raise an alert. When there is uncertainty in the gathered evidence, nearby IDS agents work together to detect global intrusion. Additionally, this approach works best with flat network architectures and is inapplicable to multi-layer architectures.

3. PROPOSED MODEL

In the prevailing research work [3] of MANET IDS, Ad-hoc On-demand Distance Vector (AODV) protocol was used. It is an on request algorithm, because it will create a route between dispatcher and recipient based on the desire of the sender node. These routes details will be maintained as long as it is required by the dispatcher node. It will not discover multiple routes between the

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

dispatcher and recipient. It is challenging for the Cluster Head (CH) to detect the malicious nodes and gather the local information and Global information of cluster nodes.

If the network size is too large then the communication among the various Cluster Heads is difficult to share their local and global information of their clusters. It is difficult to find the external attacks also. Due to this Cluster Head energy will be drained and become slow in analysing. As a result network performance will be affected. These two problems have been addressed in this research work.

4. EXPERIMENTAL ANALYSIS

The MANET environment was created with 1000 nodes with the help of Ns2 simulator. The nodes are organized as clusters and for each cluster one node is elected as head termed as Cluster head. Ad-hoc On-Demand Multi path Distance Vector (AOMDV) protocol is used for path finding purpose. AOMDV has two major roles: Route discovery and route maintenance. AOMDV protocol will produce multiple route discoveries between source and destination node. Because of this protocol the Cluster Heads (CHs) can easily detect the compromised node among the multi routes. Thus cluster based MANET is designed and various routing attacks such as blackhole, greyhole, flooding, packet dropping and forging attacks are simulated.

4.1 Attacks Simulations methods

To observe the various network behaviour of the nodes the below mentioned circumstances are to be carried out and attacks are simulated.

1. **Black hole attack and Grey hole**: A MANET environment has been setup with AODMV attack and some compromised nodes are inserted in clusters and thus Black hole attack simulated and the network parameters have been measured based on the influence of black hole and grey hole attack. Then the system performance is compared.

2. **Packet-dropping attack**: Malevolent nodes are applied among the routing path between dispatcher and recipient and thus it lead to drop some packets of data before it reaches the corresponding receiver. The network's performance is compared and it is configured.

3. **Flooding attack**: In MANET many RREQ packets have been flooded over the MANET and thus create the flooding attacks and the network behaviour of the nodes are observed.

The network performance of each node that resultant to various attacks are transmitted to their Cluster Head (CH). Then Cluster Based Routing Protocol (CBRP) is applied to connect each Cluster Heads (CHs) in the MANET environment. This protocol will create a path between the Cluster Heads and helps the various Cluster Heads (CHs) to share their local and global information when different routing attacks are simulated. CBRP protocol can alert the Cluster Heads about the internal and external malicious nodes. The network parameters such as ratio of delivered packets, delay of communication, Dropped packets, Throughput [5] are obtained and

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

thus results in a training dataset. Then the EGAN-BiLSTM-CCNN [3] model within each Cluster Heads (CHs) is deployed using the obtained training dataset to detect and classify network intrusions.

4.2 AOMDV-CBRP Algorithm

In order to improve the efficiency of Cluster Based Routing Protocol, the efficient node has be selected as cluster head, for that this study introduce Enhanced Weighted Cluster Algorithm (EWCA).

The CH is elected based on node degree, distance from neighbour node, battery power, node mobility.

$$\text{Node weight } nW = x1+x2+x3+x4 \quad (1)$$

Where x1 represents degree of the node which implies number of neighbour's nodes, x2 denotes distance between those corresponding nodes to its neighbour, x3 represents power consumed by the node for transmission and x4 indicates measurement of mobility by taking the running average of all node speeds up to time T.

Calculating each nodes weight, the node with high transmission power and less mobility value will be elected as CH. Every CH will be assigned with ID and their members also be identified by their CH ID.

By implementing EWCA efficient node will be elected as CH and data can be transmitted in both inter cluster and intra cluster mode by exchanging information among the CHs. when delivering data from a source to a destination using CBRP, if a route error arises for any reason (for example, because the node after it moved or died and is no longer within the transmission range of the node forwarding the packets), the node that discovered the error will attempt to repair the route. If not, it sends a route error packet and instructs the source. To tackle this issue AOMDV protocol is used along CBRP. Whenever the communication initiated between source and destination node, AOMDV protocol will start discovering multipath between desired source and destination node.

Then Cluster based routing protocol will check whether the dispatcher and recipient node are in same cluster. If they are in similar cluster then CBRP will ask the corresponding Cluster Head to give the trust value of their cluster members. After receiving trust value, EGAN-BiLSTM-CCNN [3] IDS model will be applied to the Cluster Head to check for malicious node. If the dispatcher node and the recipient node are in diverse cluster then CBRP will ask the two corresponding Cluster Heads (CHs) to provide Trust value of their corresponding cluster members and after that it allows that two Cluster Heads (CHs) to share their routing information.

After exchanging the information, EGAN-BiLSTM-CCNN [3] IDS model will be applied to the Cluster Head to check for malicious node and if any malicious node found it will be removed and establish the safe communications.

Communication initiated

AODMV protocol discovery multiple routes

CBRP check location of source node and destination

If source and destination same cluster

CBRP check trust value from particular CH (Intracluster)

Getting Trust value, EGAN-BiLSTM –CCNN Ids model applied in CH to detect any malicious node.

Else if source and destination different cluster

CBRP check trust value from two corresponding CH (Intercluster)

Getting Trust value

5 PERFORMANCE COMPARISONS OF AODV AND AODMV PROTOCOLS

Packet Delivery Ratio

PDR represents the ratio of total number of packets received (Pr) at the recipient side to the total packets transmitted (Pt) from dispatcher.

$$PDR = (Pr / Pt) * 100 \qquad (2)$$

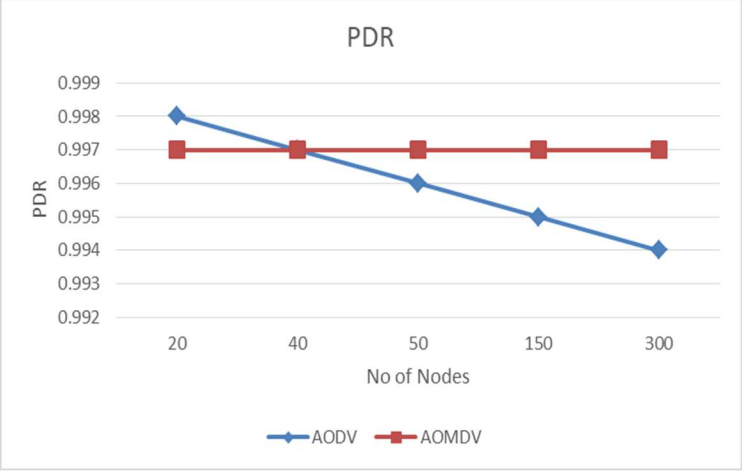


Figure 1. Ratio of delivered packet

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

From this graph it has been observed Packet Delivery Ratio is better in AOMDV when compared to AODV protocol. When the nodes quantity increases ratio of packet delivery starts decreases in AODV protocol, but in AMODV PDR remains stable.

End to End Delays

Duration taken by the packet to travel from dispatcher node to the recipient node in the network. The delay time is calculated from subtracting receiving time from sending time.

E2edelay = receiving time – sending time (3)

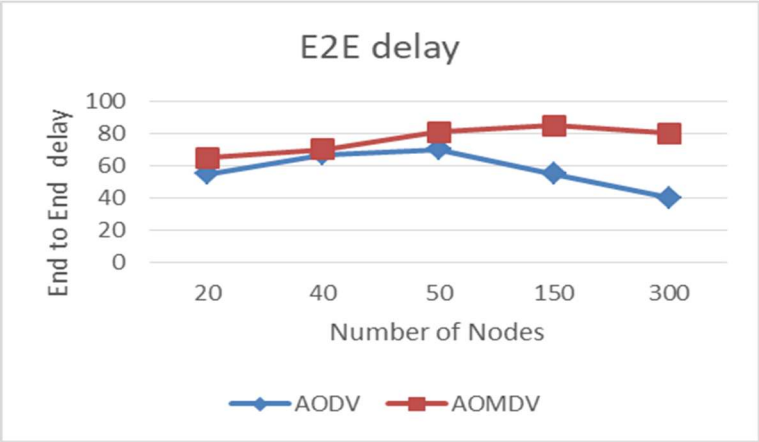


Figure 2. End to End Delays

This Graph visulaze when the number of nodes increases the AODV protocol takes more duration to transmit the data that termed as end to end delay whereas AOMDV protocol perform efficient for plenty of nodes.

Throughput

The aggregate data packets distributed to the endpoint throughout the entire time distributed by the total duration is the throughput. It can also mean the bits received in excess of the dissimilarity among the packets that were acknowledged initially and last.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

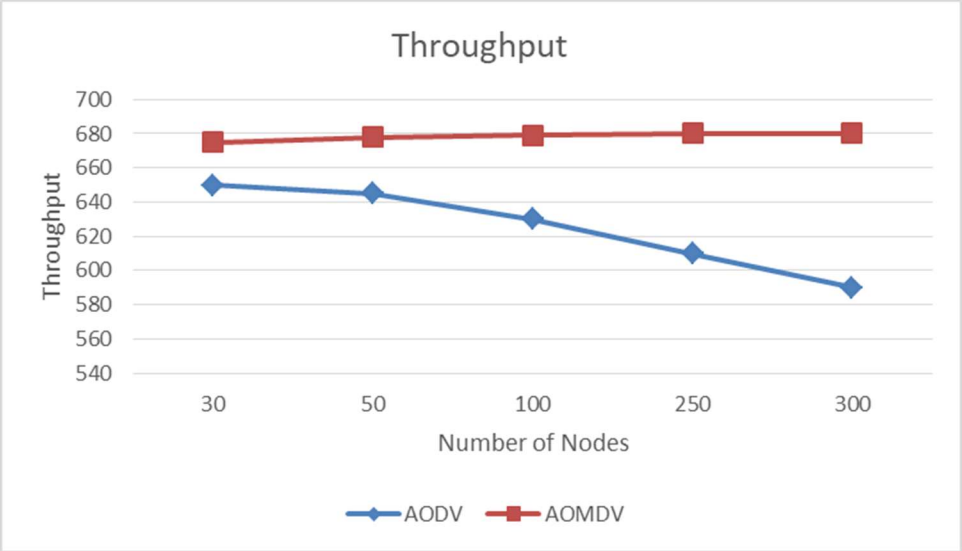
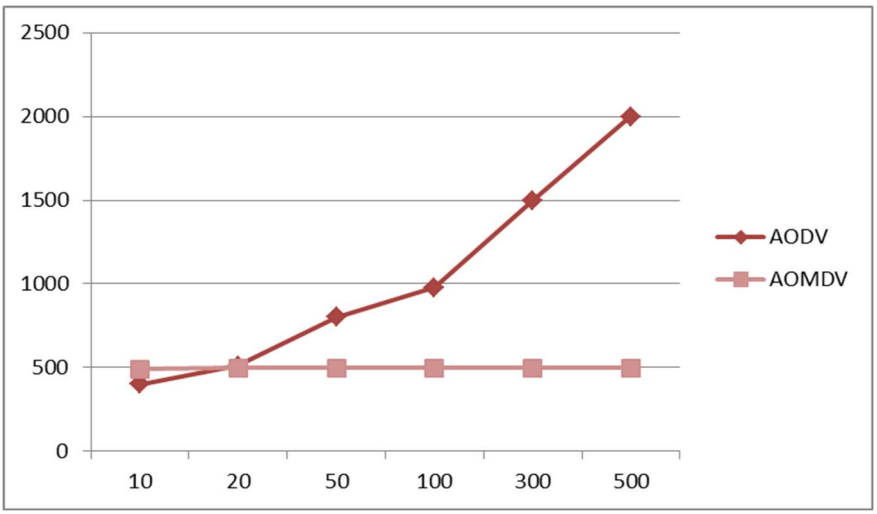


Figure 3. Throughput

Packet Dropped

These are some packets of data that are thrown down because of some sudden disturbance in the network. The graphs above show that there are more packets dropped in AODV than in AOMDV, concerning packet loss rates. This is so that the packet won't reach its destination if the link is lost hence this routing protocol AODV is a single path routing protocol. The packet will therefore be dropped. When an AOMDV link fails, the network will locate a different route, increasing the likelihood that a packet will be delivered.



Vol. 21, No. 1, (2024)
ISSN: 1005-0930

Figure 4 Packet Dropped

Cluster Head Energy

Every network nodes are built with finite energy and when the nodes are involved in any transaction they will use the energy, energy level will decrease. For cluster head they have to monitor their cluster nodes and also have to transfer the local and global information among different Cluster Heads (CHs). So the energy level of Cluster Head will decrease. So that Cluster based Routing Protocol (CBRP) along with both AODV, AOMDV protocol are implemented, performance of these protocols are compared and it has been demonstrated from the below graph that CH energy retains better in AODMV that AODV protocol.

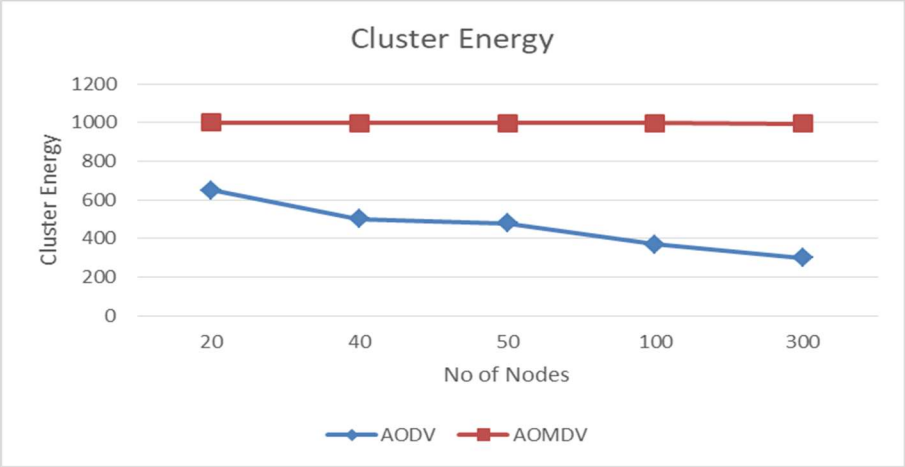


Figure 5. Cluster Head Energy

The comparison of protocol metrics like ratio of packet delivery, communication delay, dropped packets, throughput and energy level of CH between the performance evaluation of AODV and AOMDV ,it has been proved AOMDV protocol performs efficient than AODV protocol.

6 EXPERIMENTAL RESULTS

After applying AODMV protocol and Cluster Based Routing Protocol between the cluster heads when the various routing attacks such as black hole, grey hole, packet dropping, flooding attacks it is convenient for the Cluster Heads(CHs) to predict both the internal and external attacks in the MANET. Thus the network parameters obtained after simulations of attacks are accurate for

training the CBRP-EGAN-BiLSTM-CCNN IDS model. The comparison results of TL-EGAN-BiLSTM-CCNN model and the proposed model CBRP-TL-EGAN-BiLSTM-CCNN in terms of accuracy, precision, recall, F-score are demonstrated as a graph below.

6.1 PERFORMANCE EVALUATIONS

Accuracy: It is premeditated as the proportion of correctly recognized instances to the entire dataset. A higher accuracy indicates a better classification model.

$$Accuracy = \frac{True\ Positive\ (TP) + True\ Negative\ (TN)}{TP + TN + False\ Positive\ (FP) + False\ Negative\ (FN)} \quad (3)$$

TP represents number of samples classified as attack samples. TN represents amount of samples correctly categorized as normal data, FP represents amount of normal samples correctly categorized as an attack data, and FN is the quantity of attack samples erroneously categorized as normal data.

Precision: It is calculated by

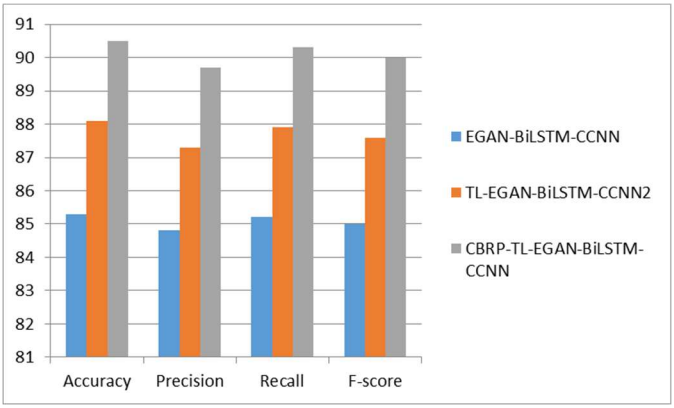
$$Precision = \frac{TP}{TP+FP} \quad (4)$$

Recall: It is calculated by

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

F-score: It is calculated by

$$F - score = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (6)$$



This graph represents the performance comparison of various IDS model and the proposed model CBRP-EGAN-BiLSTM-CCNN provides efficient rate of accuracy, precision, recall and F Score value.

Figure 6. Performance evaluation of Datasets with different IDS model

CONCLUSION

The objective of the recommended effort is to resolve the security issue with mobile ad hoc networks. Furthermost of the researchers are concentrating on building Intrusion Detection Model using machine learning techniques .Recently many researchers have been proved that designing a Network Intrusion detection model by implementing deep learning algorithms provide high accuracy rate in detection attacks. This research contributes a novel Network Intrusion Detection System model CBRP-EGAN-BiLSTM for MANET environment. Ns2 Simulator is used to provide the proposed concept's implementation. Both AODV and AOMDV protocols are used and also it has been proved that AOMDV protocol perform efficient than AODV protocol by accessing the system's performance in terms ratio of delivered packets, delay of communication, Dropped packets, Throughput [5]. This research concluded that the AODMV perform efficient than AODV protocol and by implementing CBRP protocol on the Cluster Heads(CH)s will improve the communication of the Cluster Heads(CHs) . In future this work can be extended by considering other layer attacks in MANET by applying various detecting techniques.

REFERENCES

[1] P.Visalakshi,S.Prabakaran "Detection and prevention of spoofing attacks in mobile adhoc networks using hybrid optimization algorithm." Journal of Intelligent & Fuzzy Systems, (2020).

[2] R Makani, BVR Reddy." Designing of Fuzzy Logic-Based Intrusion Detection System(FIDS) for Detection of Blackhole Attack in AODV for MANETs.", Cyber Security and Digital Forensics, – Springe-(2022).

[3] Venkatraman, D., & Narayanan, R. "Integrated framework for intrusion detection through adversarial sampling and enhanced deep correlated hierarchical network". Revue d'Intelligence Artificielle, 36(4), pp.597-605 (2022).

[4] R.Balakrishna, U.Rajeswar Rao, N Geethanjali, " Performance issues on AODV and AOMDV for MANETS", International Journal of Computer Science and Information Technologies,Vol,1(2),2010.

[5] Aditya Bakshi, A.K.Sharma, Atul Mishra ,"Significance of Mobile AD-HOC Networks (MANETS)," International Journal of Innovative Technology and Exploring Engineering (IJITEE),Volume-2,Issue-4,March

[6] Neelam Khemariya, Ajay Khuntetha, "Efficient algorithm for detection of Black hole attack in AODV based MANETs",International Journal of Computer Applications (0975-8887)Volume 66-No.18, March 2013.

[7] Baskar.M, Gnansekaran.,(2017), "Developing Efficient Intrusion Tracking System using Region Based Traffic Impact Measure Towards the Denial of Service Attack Mitigation", Journal of Computational and Theoretical Nanoscience, Volume No.14, Issue No.7, pp: 3576-3582, ISSN: 1546-1955 (Print): EISSN: 1546-1963 (Online) , July 2017.

[8] Kshmeera N. Khachar and Mrs. Jayna B. Shah," Detection and Prevention of Black hole Attack in Mobile Ad-hoc Networks: A Survey‖", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,P-ISSN: 2278-8727, Vol. 26, Issue 2, Ver. XI (May-April 2014), PP. 108-112.

[9] Martin K Parmar, Harikrishna B Jethva, "Survey on Mobile ADHOC Network and Security Attacks on Network Layer", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[10] Meghna Chabra and B.B. Gupta, "AN Efficient Scheme to Prevent DDos Flooding Attacks in Mobile Ad-hocNetwork (MANET)", Research Journal of Applied Sciences, Engineering and Technology 7 (10): 2033- 2039, 2014, ISSN: 2240-7459; e-ISSN: 2040-7467, PP. 2033-2039, © Maxwell Scientific Organization, 2014.

[11] Asma Tuteja, Rajneesh Gujral, Sunil Thalia, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2‖"2010 International Conference on Advances in Computer Engineering, 978-0-7695-4058-0/10 2010 IEEE.

[12] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamurlidhar, "A Mechanism for Detection of Grayhole Attack in Mobile Ad-hoc Networks", ICICS 2007, 1-4244-0983-7/07/$25.00©2007 IEEE.

[13] H. Alavizadeh and J. Jang-Jaccard, "Deep Q-learning based reinforcement learning approach for network intrusion detection," Computers, vol. 11, no. 3, pp. 1–19, 2022.

[14] S. Singh, D. Prasad, S. Rani, A. Singh, F. S. Alharithi et al., "Wireless body area routing protocols impact analysis on entity mobility models with static sink node," Applied Sciences, vol. 12, no. 11, pp. 5655, 2022.

[15] D. M. Khan, T. Aslam, N. Akhtar, S. Qadri and N. A. Khan, "Black hole attack prevention in mobile ad-hoc network (Manet) using ant colony optimization technique," Information Technology Control, vol. 49, no. 3, pp. 308–319, 2020.Lee, S.hyun. & Kim Mi Na, (2008) "This is my paper", ABC *Transactions on ECE*, Vol. 10, No. 5, pp120-122.