wjert, 2022, Vol. 8, Issue 3, 166-174. Original Article ISSN 2454-695X

World Journal of Engineering Research and Technology

WJERT

www.wjert.org

SJIF Impact Factor: 5.924

INTERUSION DETECTION SYSTEM USING DATA MINING

***[1]Dr. Devinder Singh and [2]Anjali Pathania**

[1]GNDEC Ludhiana (Punjab) India.

[2]GGI Khanna (Punjab).

Article Received on 28/12/2021 **Article Revised on 18/01/2022** **Article Accepted on 08/02/2022**

***Corresponding Author**
Dr. Devinder Singh
GNDEC Ludhiana (Punjab) India.

ABSTRACT

In this paper we have presented a hybrid model for IDS using ANN and data mining approaches. it is important to deploy a hybrid network using ANN based and data mining-based IDS systems that can enable the system in making decisions on intrusion in a mobile environment. MANET is an infrastructure-less ad-hoc network. It is a collection of mobile nodes that are connected in an arbitrary and dynamic manner. ANN (Artificial Neural Network) is a type of Machine Learning scientific and statistical model that is used by computer systems in order to perform a task without involvement of explicit intrusion, rather than relying on interference and patterns instead. As there is node mobility that can impose different security issues, MANET's are found more susceptible in security provision. In order to resolve this security issue, some authentication and encryption techniques can be proposed for the first-line defense in order to mitigate the security risks. However, complete eradication of these types of risks is next to impossible. For the Second line defense, the necessity of an Intrusion Detection System (IDS) is essential in this case. IDS can be referred as a method tool or resource that can help to detect access and warn for any activity of unapproved or unauthorized network activity. The current research has been done to prevent the network from the intruders. The number of attackers has been increased in the network because of more usage of technology and wireless network. Data is not allowed by the attackers to transmit successfully from source node to destination node. These intruders want to steal data and let to the unsuccessful transmission. In this research we are deploying 48 to 66 nodes in a defined communication area of 1000*1000 height and width. While starting the transmission source node and destination node is defined. After that while using IDS and AODV protocol

route is created between destination and source node. If network decreases its performance will need to apply cuckoo search as an optimization algorithm. Cuckoo search algorithm extracts the properties and observe the energy been consumed by each node. Optimized properties provided as an input to the decision tree classifier with the help of this, system is being prepared according to their properties. If there will be a chance for existence of intruder in the network then it will be classified using decision tree algorithm.

KEYWORDS: Manet, Computational model, Neural network.

INRODUCTION

An artificial neural network is an information processing technique which is used for recognizing the relationships in the set of data that access the working of brain. ANN is also known as computational model which is based on biological neural networks. With the flow of information, the structure of ANN is affected. Is consists of an interconnection collection of networks. With the help of neural network, the changes which occurs is based on input and output. In brain billion of cells are there which is known to be a neuron, which help in processing the information in the form of electronic signals. Neuron helps in completing the brain process and consisting of knowledge of neurons and cells. A neural network is connected where the set is weighted with the associated with it to complete the thing and need the cells to fulfill it with the terms of neuron. ANN can be used for the complex ability of relationships for finding the pattern in data. With the help of neural tools data warehousing firms are gleaning the use of network.

The ANN based detection models fundamentally classify and learn the features of the nodes' observed behavior by the proper utilization of the detection algorithm. In this case, the appropriate and suitable features are taken into account as input. The module design of MANET system requires the best energy efficient features. Thus, in order to save the energy, the IDS models should consume very little energy in order to achieve the targeted performance from the MANET system. In this process each of the node responses in the process of intrusion identification as an IDS agent is involved in each of the nodes. In this regard, it can be considered that an IDS agent is able to collect and detect the local data for the identification of the attack in a network. With the need of element to use the nodes in the complete form whereas the used network is organize the system where to have the process form up to down for having the input with to create the output and the things the ANN based element the order to save the data from the position the tree used to formulate the given number which is use to

have the detection based model which is used to have the input the ANN and need to utilize to go among the data where to have the ANN is used for finding the working of brain cells.

Each device in MANET is connected between the power of remaining device in the same technology along with the used complete in the form of network and having the charge. They can act as both routers and hosts. The main challenge in building a MANET is the supply of each device to keep the information needed to properly route the traffic. More frequent tearing connections and re-association put an to have the same incomplete network where to have the need the charge due to company improvement As a MANET's are in use where to gain the problem with the help of network much important is content the domain the network where to have the sign the things to motivate the knowledge where to have the same implementation to increase the network for the data mining to join the different nodes where to have the need we will communicate with the nodes.[4]

Applications of MANET

Cell phones which is mostly in today's time and used with the advance technology when we don't need to suffer due to these technology used in the generation. Everything can be done on mobiles and need to be done with the complete facilities.The increased collision due to the emergence of buried terminals, intrusion detection, unidirection all inks; The repeated break of the path due to the transfer of nodes makes a high loss of network packet.Due to the collision caused by the emergence of buried terminals, intrusion detection, unidirectional link sand other factors; repeated interruption of the path due to the transmission of nodes will lead to a large loss of network packet data.Most of the systems are similar to a specific shared system, which usually relies upon several assumptions of personality, where every single PC communicates to one specific character. Intrusion generally happens as soon as an undependable PC is apprehended to claim various dissimilar characters. These issues typically arise when a reputation framework for example, a particular record sharing reputation on a particular system) is misled into a disproportionately large impact on a trust attacking PC.

Problem Formulation

The task performed by the network is tried to change in every research but it never led to the constant position for the summary. The intruder may get infected with wrong selected root, the root which will be selected should be well maintained so that the intruders will not affect. It is always seen that by using the wrong path or shortcut path the problem may occur so by

this there is more chances of problem instead of using wrong path the right path be taken. In the same area the discussions seem to be trustable part where it is used in the network. In containing each node which lead to be able to handle the data matter which contain the practical of maintain used network of having the good complete used the network which is containing the limit of the network The route been stimulated with the need to confirm the routing protocol. The key question for this is the basic in the research community. Due to lack of dynamic topology, there are many problems which occurs in the ad-hoc network where to use this addresses the limit the way to connect and the problem occur must be contained which is used in the network. When it is used near to complete the data and having the minimum cost of the complete research where to need be done to have done. The different topologies been used for the research and need to complete.

The nodes containing mobility is a creating problem in terms of management for the mobility, security and which lead to less minimum designing for the security and used in the network of the limited usage of trees which lead to many nodes. This tell the details regarding the research the review of routing protocols which are existing present in the protocols and used in the network of used of network which led to the problems. The ad hoc network which contains the malicious nodes. The researchers examines the detailed about the work regarding the work which is taken as network they decided to look at the matter the researchers has been pay attention towards the secured and safe based routing mechanism for transferring the data Some intrusion are same and some are different types are normal and some are smart intrusions. With the smart behavior of intruders, the term" SMART" is been attached. There are many types of intruders in the MANET such as black hole, Grey hole and intrusion. In the process of discovering the routing AODV (Ad hoc Demand Distance vector) is the more dangerous intrusion. AODV is a harmful protocol and on demanding routing protocol in proposed work, the active route is reacted quickly with the dynamic topologies. In the case of constant node AODV supports the multi cast packet transmission. A small intrusion is called as insider while the communication in the network is entering the position. The weakness of a reputation for a intrusion system depends on what are the identifiable identities, which use it gain great influence. The weakness of a reputation for a intrusion system depends on what the work, in which system receives inputs from objects that are uninspiring to bring them into a trust worthy and if the reputation system takes care of all the same individuals.

RESULTS AND DISCUSSIONS

By the segment of this chapter, the depicted outcome has been taken out with the help of MATLAB simulator using 48 to 66 nodes. When the axis is takes in the form of 48 square nodes and another node as 66 the mechanism which is form that is represented as AODV form where we use 1000 as a width for the calculation.In the proposed work the PDR (Packet Delivery ratio) is observed mainly in two cases: The packet delivery ration of the purposed research work is observed .In the presence of intrusion After removing intrusion from the network. When the average network is taken as a channel for the communication that is used for delivering the message by the throughput and containing the things which is recognized. Both the conditions are formed down in the table

No of Replication	With Intrusion	After Prevention
1	8.1022	8.2056
2	1.063	1.0976
3	2.4691	2.4967
4	3.2997	3.3226
5	4.1919	4.2113
6	5.1548	5.1703
7	6.0135	6.0276
8	7.0117	7.0239
9	0.0103	0.0218
10	0.0098	0.017
11	0.0089	0.01714
12	0.0786	0.0866
13	0.0741	0.0857
14	0.0069	0.0134
15	0.0629	0.0690
16	0.0054	0.0117
17	0.0564	0.0645
18	0.0058	0.0109
19	0.0053	0.0104
20	0.006	0.0099

The complete values for PDR is used to have the measure the network for having the intrusion design and when it is completed the network between is joined together the values which are observed is 0.082 and 0.097 respectively. Thus, while utilizing CS in hybridization there is the increment of 22.99% with ANN and DT. It represents the throughput value which are obtained for the proposed work. The average rate of network throughput with during the over a communication channel for a communication for using the message. The results measured for the work which has purposed within the table.

No of repetitions	With Invasion	After Precluding
3	23.0784	11.8765
5	8.5045	17.8735
8	254.0026	219.9267
6	267.6785	364.8803
3	39.3245	527.2567
9	35.5647	142.6784
1	14.3673	86.2618
4	92.8846	27.7736
8	12.6571	57.7891
2	72.3151	67.2683
11	92.186	7.0965
15	31.3643	36.2858
17	67.8816	62.8089
19	16.7736	61.6916
12	18.297	25.2137
13	1.496	6.4976
17	14.178	19.1156
18	1.4286	6.4138
19	1.4843	6.3489
20	1.3452	6.2539

When the network is used formed to complete the intrusion which it is determined and the network the values which are produced that are 33.47 and 35.39 respectively. Thus, there is an increment of 17.18%. The chart shows the increasing values by the compacting the impact on another value which is observed after the intrusion in the network. When the network is down the maintain form is used for changing the values then this formula is used for containing the network.

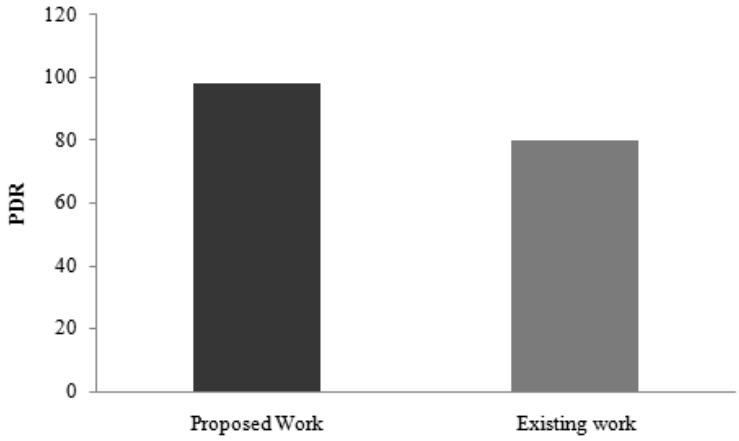
The proposed work represents the energy which is consumed in Milli joules. Consumption of energy is measured by the ratio of total energy which is consumed by the complete number of containing are formed in the deployed network. While using Cuckoo Search along with Artificial neural network & Decision tree with the proposed the used containing with system the energy consumption been consumed. After 3 the network from intrusion, the energy while transmitting the data from source to destination has decreased. The values which are determined are listed in table.

Number of Iterations	With Intrusion	After Prevention
1	1.7818	1.7754
2	2.4306	2.3645
3	0.8627	0.6875
4	1.5089	1.56
5	2.65	2.7539
6	2.5547	2.5128
7	1.6367	1.2456
8	0.5672	0.5682
9	1.6214	1.5146
10	2.6145	2.3898
11	2.3145	2.6754
12	1.2346	1.2767
13	0.0145	0.0657
14	1.3765	1.3145
15	2.3467	2.3890
16	1.1562	1.5678
17	0.0207	0.0215
18	2.4618	2.4250
19	1.4176	1.3674
20	3.1531	3.1356

The consumption of energy is average which is determined with the help of intrusion and after completing the network and removal of network which is designed from the intrusion is 1.30mJ and 1.66mJ. Therefore, the used consumption is counted as is determined by 3.45% by comparing both used elements are compared present of network in the consumption of energy in the presence of intrusion. By hybridizing with the need of element like ANN with DT is important due to the prevention of network. In the proposed network the structure of ANN is used with input layer, along with output layer and a single layer is hidden.

Comparison of proposed work with existing work

In purposed research, the research which is performed by **E. A. Shams, & A. Rizaner (2018)** is differentiated. In the existing research, Support Vector Machine (SVM) is used by the authors for the identification of intrusion in MANET.



In single intrusion node the PDR which is measured has been influenced which is around 97 %, whereas in the proposed research PDR is measured by the single invasion which is single present as 78%. Thus, there is an increment of 26.5 % in the PDR which is analyzed. MATLAB simulator is used for this research while using the algorithm cuckoo search and decision tree. With the help of neural network, the input and output are seemed to be observed, while connection the layers with the nodes the progress has been noticed that the performance is up to 75% which led to improvement.

CONCLUSION

MANET is made up of individual devices for communicating with each other with proper convenience. The concept of the network is no longer familiar for the users with a typical router for sending wireless signals. In the Ad hoc network the developer must consider network configuration which is used for network implementation. MANETs are most popular network which are extensively used for no consolidate security management. In the purposed work we have mitigated the intrusion in MANET by designing IDS using cuckoo search algorithm. Optimization algorithm is used for reducing the energy consumption rate, delay as well as bit error rate of the replicate work. AODV routing protocol was utilized for creating the route among objectives and inception. CS optimization algorithm is used for optimizing the route and for discovering the intrusion within the route. After this CS algorithm discovered the optical route for the packet data transmission by using its fitness function. The growth of the purposed mechanism will run on MATLAB with 50-100 nodes. After estimating the parameters, we concluded that the results obtained by CS optimization algorithm along with decision tree are better than the results of AODV protocol. It has been concluded that while applying CS algorithm the energy consumed by the mode up to 7.33% has been reduced. MANET is constructed with independent devices for communicating with

each other. The concept of this type of network cannot be used by the end users with wireless signals. MANETs are found more susceptible in security provision. In order to resolve this security issue, some authentication and encryption techniques can be proposed for the first-line defense in order to mitigate the security risks. However, complete eradication of these types of risks is next to impossible. For the second-line defense, the necessity of an Intrusion Detection System (IDS) is essential in this case. However, for creating better accuracy in the MANET tools, most of the researchers use a hybrid model of ANN and Data Mining.

REFERENCES

1. Jain et.al. In Information and communication technology, Springer, Singapore, 2018; 2(1): 39-47.
2. Chhabra, G.S. et.al. International Journal of Mobile Network Design and Innovation, 2018; 8(4): 225-234.
3. Abdel-Azim.et.al, 2018; 20(3): 585-592.
4. Alex Hind.et.al. International Journal of information and Education Technology, 2017; 3(1).
5. Arun Birder, International journal of Engineering Research and technology (IJERT), 2016; 2(7): 1757-1761.
6. Bow-Nan Cheng; Moore, S. n Military communications conference-(MILCOM,12), 2012; 1-6.
7. Gurpinder Singh.) International journal of computer science and information technology, 2014; 2(4).
8. Harjeet Kaur et.al International journal of computer science and information technology, (IJCSIT), 2017; 4(3): 498-500.
9. Tajinder deep Singh, Harpreet Kaur Arora, International Journal of Advanced Computer Science and Applications, 2015; 4(2).
10. Fabrice Le Fessantet.al Computer Communications, 2016; 35: 234-248.
11. D. Zexi and H. Feidan, "Cuckoo search algorithm for solving numerical integration," IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Shenyang, 2015; 1508-1512.
12. J. Peng, K. Li and G. W. Irwin, "A New Jacobian Matrix for Optimal Learning of Single-Layer Neural Networks," in IEEE Transactions on Neural Networks, 2008; 19(1): 119-129.