International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 05 | May 2021 www.irjet.net p-ISSN: 2395-0072

A COLLABORATIVE SECURITY FRAMEWORK FOR VANET USING OPTIMIZED ARTIFICIAL NEURAL NETWORK

[1]Mrs.R.Anjana devi, [2]V.Seethalakshmi, [3]S.S. Sreenidhi, [4]S.Sridevi, [5]B.Srilekha

[1]Assistant professor,[2,3,4,5]UG Scholars, Department of Electronics and Communication Engineering Adhiyamaan college of Engineering, Hosur, Krishnagiri, Tamilnadu, India.

[1]anjanadevi.ece@adhiyamaan.in, [2]lakshmiseetha2501@gmail.com, [3]1999sreenidhi@gmail.com, [4]ussridevi2000@gmail.com, [5]srilekhabalakrishnana@gmail.com

---

Abstract--*This project proposes Artificial Bee Colony assisted Neural Network optimization for reducing the attacker problems. VANET is a continuous self construct, infrastructure-less network in which mobile devices connected are wireless. It is collection of devices with wireless communication. In proactive technique to the WSN routing has to keep all the information regarding routing continuously. The full network should be acknowledged to all nodes. Every single knows the path which is having pre-defined path. The Location based key management system increases the security of the data transmission and reduce the attacker problems. Deep neural network based system can identify the attacker problems with its hidden layer, Artificial Bee Colony algorithm is used for optimization technique. This project is implemented with Network Simulator software.*

Key words—Artificial Bee Colony, Deep neural network, Vanet, Network simulator software.

1. INTRODUCTION

It is the vision of the Internet of Things (IoT) that in the near future many smart devices will be interconnected with each other and exchange information to support humans in their daily lives. While it is very fascinating to see how far the integration of this vision progressed during the past two decades, there are still some problems to solve. These days, many smart devices of different manufacturers exist, but the interconnection and management of these devices is still a long lasting task. There is no standardisation of devices to interconnect with each other has been created and, therefore, the implementation of IoT is often limited to the interconnection of devices of the same manufacturer. Consequently, we are currently still living in the use of Intranets of Things and not so far in the use of Internet of Things. To accelerate the integration of IoT, interfaces that promote the easy management and machine to machine communication of smart devices are needed. Software Defined Networking (SDN) is a promising technique to evaluate the management of IoT networks. When the size of conventional networks developed and the quantity of network devices of different manufactures increases the size of manageability, SDN was very success full in simplify the configuration of networks with devices of various manufacturers and reducing the need of human interaction.

Wireless Sensor Networks (WSNs) are a major component of the IoT. In WSNs many sensor nodes are used to gather the physical parameters in an area of interest. WSNs have been a subject of wide interest in the past two decades and therefore, they are well deliberate. But the development of IoT during the past few years, has added traction to WSN research. Instead of only sensing and collecting physical properties in an area of interest the sensor nodes become smarter and can now be seen as smart devices. The environment and output of these smart sensors might depend on other smart devices and therefore, communication between those devices probably can be done successfully.

SDN-Wise is one of these available and already implemented SDN frameworks. SDN-Wise is a Software Defined Networking solution for Wireless Sensor Networks. The aim of SDN-Wise is to evaluate the management of the network, the establishment of conventional applications, and the experimentation of new networking solutions (SDN-Wise).

A real world testbed that supports SDN-based applications and enables rapid prototyping, would speed up the integration of new applications and could help SDN to establish in WSNs. When SDN is more used in WSNs, the interconnection between WSNs simplifies and the adaptation of IoT could make a leap forwards.

1.1 OBJECTIVE

- To mitigate the Black Hole and Grey Hole attacker problems with ABC Assisted Neural network algorithm.
- To achieve highly secured data transmission from source node to destination node using Location based key management system.
- To reduce the packet drop and increase the data delivery ratio with high throughout.

2. LITERATURE SURVEY

[1]Xiaofei Wang [2020] et al proposes a Conventional traffic survey based on deep packet inspection (DPI) approach at switches cannot hold the elaborate knowledge of network applications going into internal changes, and the statistics-based reports of switches lack identification of the traffic. In addition to, DPI is generally expensive and has limited performance. Therefore, network-wise exact flow-awareness by packet sampling is highly desirable for fine-grained quality of service warranty, internal network management, traffic engineering, security examination, and so on. In this paper, we suggest a Spatial-Temporal Collaborative Sampling (STCS) framework in the flow-aware software-defined networks (SDN).[2]Yushu Zhang [2020] et al proposes a Cloud capability is taken to be extended to the border of the Internet for improving the security of data transmission. In this article, a secure transmission framework for CS data by integrating CS-based cipher and edge computing the vision of security, the double-layer encryption mechanism and double-layer authentication mechanism are rooted in it by developing some privacy-preserving operations, including CS-based encryption, CS-based hash, information splitting, strong encryption, and feature extraction. Most significantly, the proposed framework is very useful for resource-limited IoT applications.[3]Ahmed A [2020] et al proposes an attackers to use Remote Access Trojans (RATs) to balance and control a computer, which makes the RAT detection as an active research field. This paper introduces a Neural network-based framework for detecting understandable hosts and networks that are affected by the RAT-Bots. The proposed framework consists of two agents that are developed to achieve reliable previous detection of the RAT-bots. The first agent, the host agent, carries the response for observing the system behaviour of the processing host and elevating an alarm for any abnormality. The second agent, the network agent, detects the network traffic to extract any malicious patterns. The integrated technique improves both the detection ratio and accuracy. RAT-Bots detection framework. The action of the introduced framework is calculated by using real-world benchmark datasets.

3. PROPOSED SYSTEM

Vehicle-ad-hoc network (VANET) is a self-tuning network that does not have a responsible router; since there is no centralized node, and each node acts as a router. Each node has a limited range for data transmission in the network, and the data transmission occurs from one node to another node. The routing in VANET consider the entire nodes in the network as simple unless there is no difference in the data and router path is found. VANET determines applications in different fields like disaster management, vehicle computing, and more. For data transmission, path creation mechanisms such as proactive reactive, and hybrid routing protocol is declared. In a dynamic routing protocol, the routing data of nodes are collected in a table and is changed whenever the route is modified. In a reactive routing protocol, as the node suggests, the path is established whenever the source node wants to send information to the destination node that is, it works on-demand. The last protocol is formed by combining the merits of the above-defined routing protocol that is named as a hybrid routing protocol in VANET. Due to the free or the mobile nature of nodes, the network is vulnerable to different attacks such as the gray hole, black hole attack, and selective packet drop attack. Black hole and the gray hole attack are also known as packet drop attacks and output in packet drop during the communication process.

ADVANTAGES:

- Less packet drop.
- High delivery ratio.
- Highly secured data transmission.
- Less time consumption and energy consumption.

4. SYSTEM FUNCTION

ARCHITECTURE DESIGN

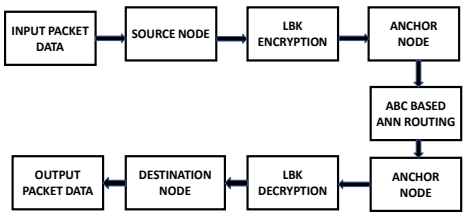

Fig 1: Architecture design for proposed system

5. ALGORITHMS

Artificial Bee Colony Algorithm

- ABC Artificial Bee Colony algorithm is introduced to achieve isolation, high performance, enhanced anomaly detection.
- To apply ABC, the considered optimization problem is first converted to the problem of detecting the best parameter vector which reduces an objective function. In this proposed method optimization technique is used.

Location based Security Key

- In WSNs, location information is important for the generation of shared keys and is highly applicable. Thus, location based key management is a core part of the research into WSN key management.

Artificial Neural Network clustering

- A novel fitness function has been developed for the ABC algorithm according to which the nodes are

segregated. Based on the segregated node list, the Artificial Neural Network structure is trained, which helps to deliver data with a small delay.

6. RESULTS

In this project, the proper routing is exhibited by combining artificial bee colony optimization (ABC) algorithm with artificial neural network (ANN). Here the routing path for the data transmission is obtained.

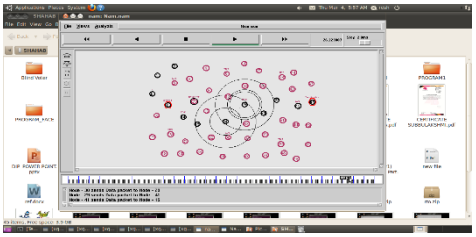

Fig 2: Neighbour node discovery

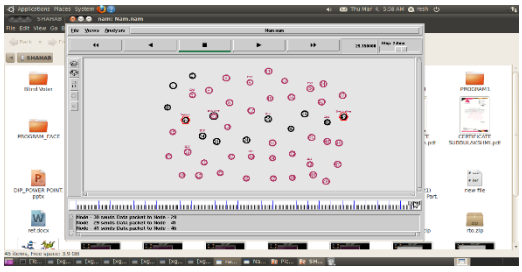

Fig 3: Final route path creation

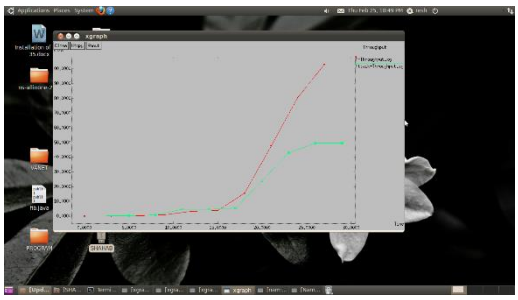

Fig.4: Throughput

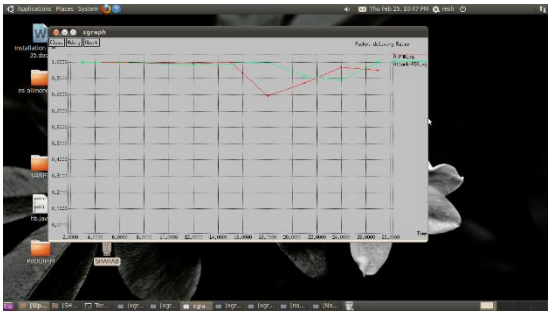

Fig 5: Packet delivery ratio

Fig 6: Packet drop

7. CONCLUSION

The performance of VANET has been affected by many attacker nodes, which becomes a great concern for the research. The identification of multiple threats in the network is a necessary job to enhance the lifetime of the network. Therefore, to improve the implementation of the network in the existence of malicious nodes, specifically BHA & GHA nodes, a security mechanism using ABC as a swarm-based approach and ANN as a machine learning technique has been used. ABC utilized the intelligent act of honeybees, which has been used to segregates the nodes depend on their properties, such as into two lists termed healthy and infected nodes lists. Furthermore, the attacker nodes list is subdivided into BHA nodes and the GHA nodes list. Using these properties, ANN trains the network. The performance has been analyzed based on PDR, throughput, and delay. The improvement against PDR, throughput, and delay compared to existing work such as 0.63 % 13.02 %, and 18.39 % has been attained compared to existing work.

REFERENCES

[1] XiaofeiWang,XiuhuaLi,Sangheon Pack,Zhu Han,Victor C. M. Leung,2020," STCS: Spatial-Temporal Collaborative Sampling in Flow-Aware Software Defined Networks", IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 999 – 1013.

[2] Yushu Zhang;Ping Wang, Liming Fang, Xing He,HaoHan,Bing Chen,2020," Secure Transmission of Compressed Sampling Data Using Edge Clouds",IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6641 – 6651.

[3] Ahmed A. Awad,Samir G. Sayed,Sameh A. Salem,2019,"Collaborative Framework for Early Detection of RAT-Bots Attacks",IEEE Access, vol.7, pp. 71780 – 71790.

[4] Chen Liu,Patrick Cronin,Chengmo Yang,2020,"Securing Cyber-Physical Systems from Hardware Trojan Collusion", IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 3, pp. 655 – 667.

[5] Weisong Wen,Xiwei Bai,Guohao Zhang,Shengdong Chen,Feng Yuan,Li-Ta Hsu,2020,"Multi-Agent Collaborative GNSS/Camera/INS Integration Aided by

Inter-Ranging for Vehicular Navigation in Urban Areas",IEEE Access, vol.8, pp. 124323 – 124338

[6] Liang Tan,Yue Pan,Jing Wu,Jianguo Zhou,Hao Jiang,Yuchuan Deng,2020,"A New Framework for DDoS Attack Detection and Defense in SDN Environment", IEEE Access, vol.8, pp. 161908 – 161919.

[7] Gilad Rosenthal,Ofir Erets Kdosha,Kobi Cohen,Alon Freund,Avishay Bartik,Aviv RonARBA,2020," Anomaly and Reputation Based Approach for Detecting Infected IoT Devices", IEEE Access, vol.8, pp. 145751 – 145767.

[8] Hong Liu,Pengfei Zhang,Geguang Pu,Tao Yang,SabitaMaharjan,YanZhang,2020,"Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing", IEEE Transactions on Vehicular Technology, vol. 69, no.4, pp. 4221 – 4232.

[9] Zhangjie Fu,Yuanhang Mao,Daojing He,Jingnan Yu,Guowu Xie,2019," Secure Multi-UAV Collaborative Work Allocation", IEEE Access, vol.7, pp. 35579 – 35587.

[10] Jing Chen,Kun He,Lan Deng,Quan Yuan,Ruiying Du,Yang Xiang,Jie Wu,2020,"EliMFS: Achieving Efficient, Leakage-Resilient, and Multi-Keyword Fuzzy Search on Encrypted Cloud Data",IEEE Transactions on Services Computing, vol. 13, no.6, pp. 1072 – 1085.

BIOGRAPHY:

Mrs. R. Anjana Devi,
Assistant Professor,
Engineering Department,
Adhiyamaan College of Engineering,
Anna University.