IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPROVED INTRUSION DETECTION SYSTEM USING FUZZY LOGIC FOR DETECTING ANAMOLY ANDMISUSE TYPE OF ATTACKS.

R.SUGUMAR[1], M.SARASWATHI[2]
1STUDENT 2 ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
PRIST DEEMED TO BE UNIVERSITY THANJAVUR, TAMILNADU, INDIA

Abstract The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc Network (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackersTo adjust to such trend strongly believe that it is vital to address its potential security issues. In this paper propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances. Use improved Kuok fuzzy data mining algorithm, which in turn a modified version of APRIORI algorithm, for implementing fuzzy rules, which allows us to construct if-then rules that reflect common ways of describing security attacks.

Keywords: *Cloud Computing, Traffic Prediction, Intelligent Transportation Systems (ITS), Machine Learning, Deep Learning, Big Data Analytics, Traffic Forecasting, Internet of Things (IoT), Real-Time Traffic Monitoring, Smart Cities, Traffic Congestion Management, Cloud-Based Traffic Systems, Artificial Intelligence (AI), GPS Data Analytics, Predictive Analytics.*

I. INTRODUCTION

MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly.

MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications

like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations. Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact those most routing protocols in MANETs.

Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants. Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the mobile ad hoc networks.

Intrusion Detection Systems (IDSs) are used with other preventive security mechanisms like access control and authentication, as a secondary line of defense to protect information systems. There are many reasons to ensure that IDS as a part of the defense system. First, traditional systems and applications were developed without security in mind. In other cases, systems/applications were developed to work in varied environments and are vulnerable when deployed. ID complements protective mechanisms to improve system security. Even if the preventive security mechanisms protect information systems successfully, it is desirable to know what intrusions occurred or are happening, to understand security threats and risks and so be better prepared for future attacks (Anand, & Patel, 2012).

Since Denning's seminal work in 1981 (Denning, 1987), many IDS prototypes were created. Sobirey has a partial list of 59 of them. IDS are an emerging computer security area due to issues in ensuring that information systems are of security flaws. Indeed, Landwehr et al. (1994) taxonomy of security flaws reveals that computer systems have security vulnerabilities despite their purpose, manufacturer or origin. It is also technically difficult and economically costly to ensure that computer systems/networks are not vulnerable to attacks.

II . LITERATURE REVIEW

In this paper [1] Broad casting is an effective mechanism for route discovery, but the routing overhead associated with the broadcasting can be large, especially in high dynamic networks. The protocol analytically and experimentally, and showed that the rebroadcast is very costly and consumes too much network resource. Optimizing the broadcasting in route discovery is an effective solution to improve the routing performance. Network density is high or the traffic load is heavy, the improvement of the gossip-based approach is limited, proposed a probabilistic broadcasting scheme based on coverage area and neighbor confirmation. Coverage area to set the rebroadcast probability, and uses the neighbor confirmation to guarantee reachability.

In this paper [2] A dynamic probabilistic broadcasting approach with coverage area and neighbor confirmation, the coverage area concept to adjust the rebroadcast probability of a node. One of the earliest broadcast mechanisms is flooding, where every node in the network retransmits a message to its neighbors upon receiving it for the first time. Although flooding is extremely simple and easy to implement, it can be very costly and can lead to serious problem, named as broadcast storm problem, which is characterized by redundant packet retransmissions, network bandwidth contention and collision. Neighbor knowledge scheme maintains neighbor

node information to decide whether it or the neighboring nodes have to rebroadcast or not.

In this paper [3] Routing overhead associated with the dissemination of routing control packets such as RREQ packets can be quite huge, especially when the network density is high and the network topology frequently changes. Issue of reducing the routing overhead associated with the route discovery and maintenance processes in on-demand routing protocols has attracted increasing attention. Location Aided Routing (LAR) algorithm as an approach to mitigate the route discovery overhead by utilizing location aided information for mobile nodes, location information can be obtained using the global positioning system (GPS) receivers.

In this paper [4] Routing overhead associated with the dissemination of routing control packets such as RREQ packets can be quite huge, especially when the network density is high and the network topology frequently changes. Issue of reducing the routing overhead associated with the route discovery and maintenance processes in on-demand routing protocols has attracted increasing attention. Location Aided Routing (LAR) algorithm as an approach to mitigate the route discovery overhead by utilizing location aided information for mobile nodes, location information can be obtained using the global positioning system (GPS) receivers. The localization of prior routing histories to localize the RREQ flood to a limited region of the network, Routing On-demand Acyclic Multi-path (ROAM) protocol mitigates the number of retransmissions of RREQ floods by using directed acyclic sub-graphs based upon the distance between the source and destination nodes.

In this paper [4] Gossiping to ad hoc unicast routing, it's usage of gossiping is very different from the work, try to ensure that messages are eventually delivered, even if there is no connected path between the source and the destination at any given point in time. Exists a path using communication links at some point in time, messages can be delivered through a random pair-wise exchanges among mobile hosts. Using gossiping mechanism to improve multicast reliability in ad hoc networks, they do not use gossiping to reduce the number of messages sent. Flooding is a basic element in many of the ad hoc routing protocols, as mentioned and comparing gossiping to flooding.

In this paper [5] Novomodo and related proposals are improvements over CRLs and OCSP, infrastructural requirements of these approaches can vary dramatically, depending on how users use their keys. First, since third party queries can come from anywhere and concern any client, every certificate server in the system must be able to ascertain the certificate status of every client in the system. One way to achieve implicit certification in the encryption context is identity based encryption (IBE). An IBE scheme uses a trusted third party called a Private Key Generator (PKG).The main algorithms in IBE are as follows Private key generation: For a given string ID, PKG uses (s, Paramus, ID) to compute the corresponding private key dID. Encryption: Sender uses (params, ID, M) to compute C, cipher text for M .However, there are two negative consequences: 1) private key escrow is inherent in this system – i.e., a PKG can easily decrypt its clients' messages; and 2) the PKG must send client private keys over secure channels, making private key distribution difficult. Decryption: Client uses (Paramus, dID , C) to recover M .

III. METHODOLOGY

The methodology of this comprehensive review on cloud-based traffic prediction systems involves a systematic analysis of existing research studies, technologies, and prediction models used in intelligent transportation systems. Initially, relevant research articles, conference papers, journals, and technical reports related to cloud computing, traffic forecasting, machine learning, and big data analytics are collected from reliable academic databases. The selected studies are then categorized based on their objectives, cloud architectures, data sources, prediction techniques, and performance evaluation methods. Various traffic data sources, including GPS devices, IoT sensors, traffic cameras, and mobile applications, are examined to understand their role in traffic prediction. Furthermore, different machine learning and deep learning algorithms such as Linear Regression, Support Vector Machines, Random Forest, Artificial Neural Networks, Long Short-Term Memory (LSTM), and hybrid models are reviewed and compared. The methodology also analyzes the advantages, limitations, scalability, and computational efficiency of cloud-based frameworks. Finally, the findings from the reviewed studies are synthesized to identify research gaps, current challenges, and future directions for developing efficient, secure, and intelligent cloud-based traffic prediction systems.

ALGORITHM

FUZZY LOGIC

Fuzzy logic is a form of many-valued logic derived from fuzzy set theory, introduced by Lotfi A. Zadeh in 1965, that deals with reasoning that is approximate rather than fixed and exact. Unlike classical binary logic, which considers only two states—true or false—fuzzy logic allows variables to have a degree of truth ranging between 0 and 1. This makes it particularly effective in handling uncertainty, imprecision, and vagueness in real-world systems where crisp boundaries are hard to define. In the context of computer science and artificial intelligence, fuzzy logic has been widely applied in areas such as control systems, decision-making, pattern recognition, and intrusion detection, where it helps model complex systems and interpret ambiguous data more effectively.

The fuzzy logic algorithm is a rule-based approach that handles uncertainty and imprecision in complex systems by mimicking human reasoning. It begins with the selection of relevant input variables, such as CPU usage, network traffic, or login attempts in the case of intrusion detection. These crisp input values are then converted into fuzzy values through a process called fuzzification, which uses predefined membership functions to represent linguistic terms like "low," "medium," or "high." Once inputs are fuzzified, a set of expert-defined IF-THEN rules is applied in the inference engine to evaluate the relationship between input conditions and output decisions.

ARCHITECTURE DIAGRAM

The architecture diagram of the cloud-based traffic prediction system consists of several interconnected layers that work together to collect, process, and predict traffic conditions. The first layer is the Data Collection Layer, which gathers traffic information from GPS devices, IoT sensors, traffic cameras, mobile applications, and road-side units. The collected data are transmitted through the Communication Layer using wireless networks and the Internet to the cloud platform. In the Cloud Storage Layer, large amounts of structured and unstructured traffic data are stored using distributed databases and cloud servers. The Data Preprocessing Layer then performs data cleaning, filtering, normalization, and feature extraction to improve data quality. The processed data are analyzed in the Traffic Analysis and Prediction Layer, where machine learning and deep learning algorithms are applied to forecast future traffic conditions, congestion levels, and travel times. Finally, the prediction results are delivered to the Application Layer, which provides real-time traffic information, route recommendations, and decision support services to drivers, traffic authorities, and smart city management systems. This architecture enables scalable, reliable, and real-time traffic prediction through the integration of cloud computing and intelligent transportation technologies.

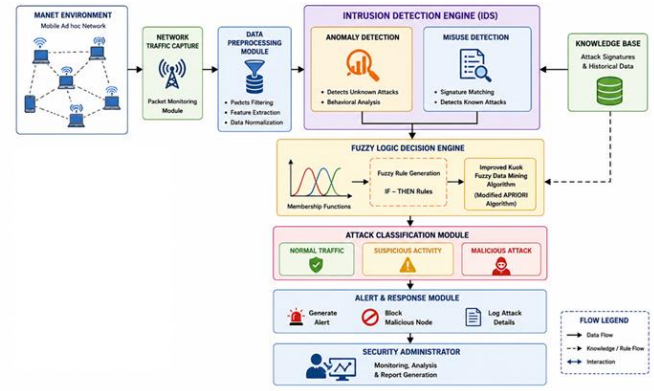


Fig. 1. Architecture Diagram

IV. EXPERIMENTAL RESULTS

The experimental results demonstrate the effectiveness of cloud-based traffic prediction systems in processing and analyzing large-scale traffic data in real time. Various machine learning and deep learning models were evaluated using traffic datasets collected from GPS devices, IoT sensors, traffic cameras, and mobile applications. The performance of the prediction models was measured using evaluation metrics such as accuracy, Mean Absolute Error (MAE), and Root Mean Square Error (RMSE). The results indicate that cloud-based frameworks significantly improve data processing speed, storage efficiency, and prediction accuracy compared to traditional traffic management systems. Deep learning models, particularly Long Short-Term Memory (LSTM) and hybrid approaches, achieved superior performance in forecasting traffic congestion and travel times.

IMPLEMENTATION

Server

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.

Client

A client is a piece of computer hardware or software that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network. Client–server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. This module how a city map is divided into several zones and how some of the intersections are chosen to be the boundary intersections that are located on the outline of a zone. Only the authorized person can enter by giving valid information. If the user provides the invalid information then permission denied navigating to other pages.

Router details

Router transmission can be illustrated using two-hop transmission. When two-hop transmission is used, two time slots are consumed. In the first slot, messages are transmitted from the source to the relay, and the messages will be forwarded to the destination in the second slot. The outage capacity of this two-hop transmission can be derived considering the outage of each hop transmission.

Attacker models

Normal Attack :Network attack is usually defined as an intrusion on your network infrastructure that will first analyse your environment and collect information in order to exploit the existing open ports or vulnerabilities - this may include as well unauthorized access to your resources, Active Attack : An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. Types of active attacks: In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized .Passive Attack : A passive attack on a cryptosystem is one in which the cryptanalyst cannot interact with any of the parties involved, attempting to break the system solely based upon observed data. This can also include known plaintext attacks where both the plaintext and its corresponding cipher text .

ACK implementation:

ACK is basically an end – to – end acknowledgment scheme .It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehavior is detected.The basic flow is if Node A sends an packet p1 to destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A) , if ACK from the destination get delayed then it S-ACK process will be initialized.

Secure Acknowledgment (S-ACK):

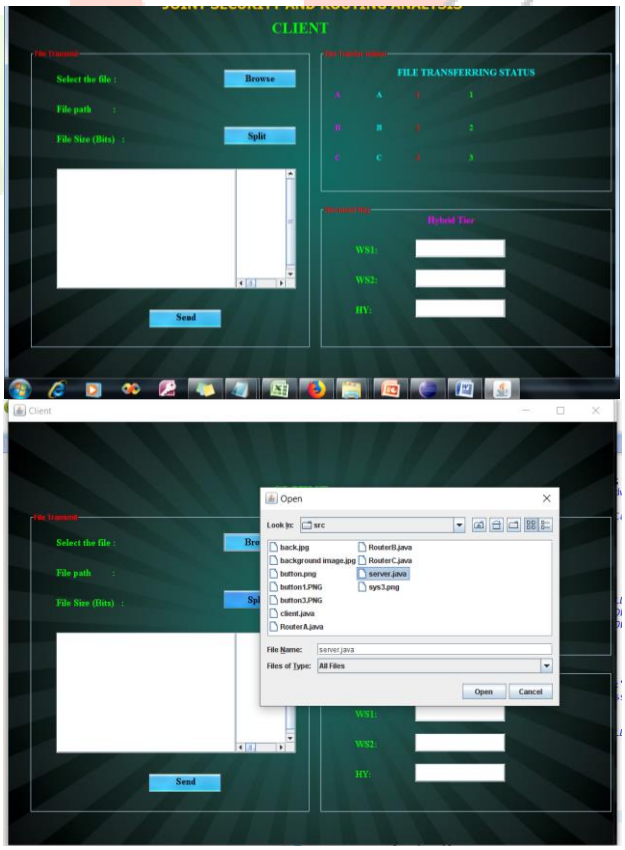
In the S-ACK principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

Misbehavior Report Authentication (MRA):

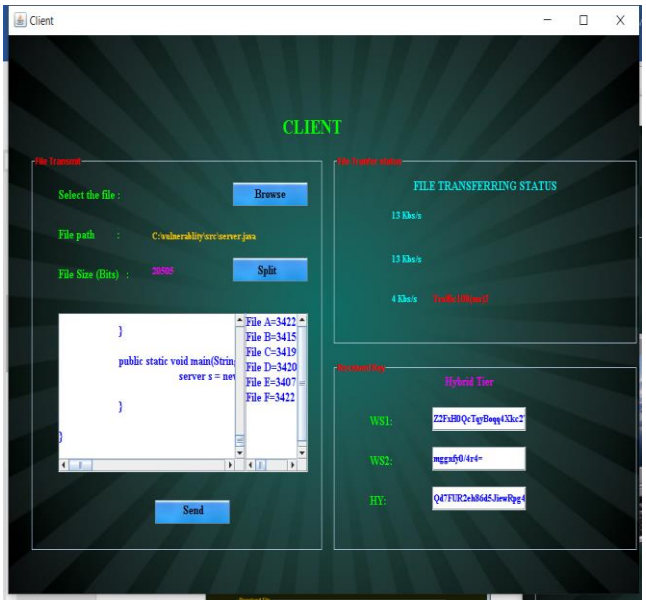
The MRA scheme is designed to resolve the weakness of watchdog with respect to the false misbehavior report. In this source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

Result & Analysis

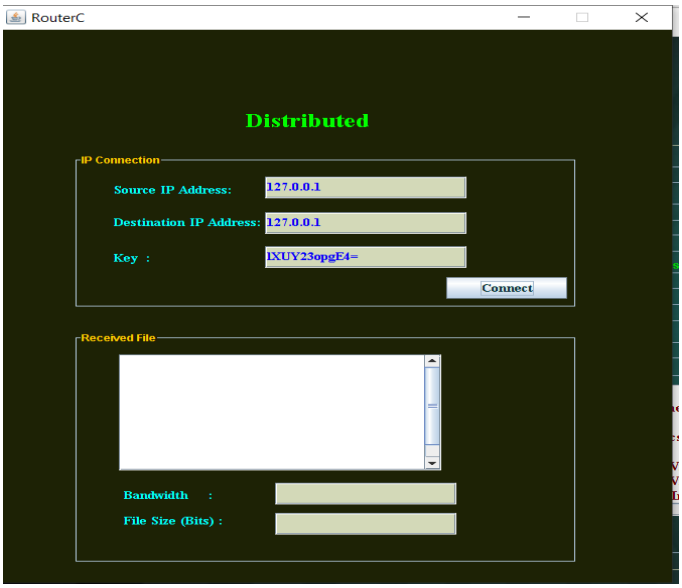
CLEINT



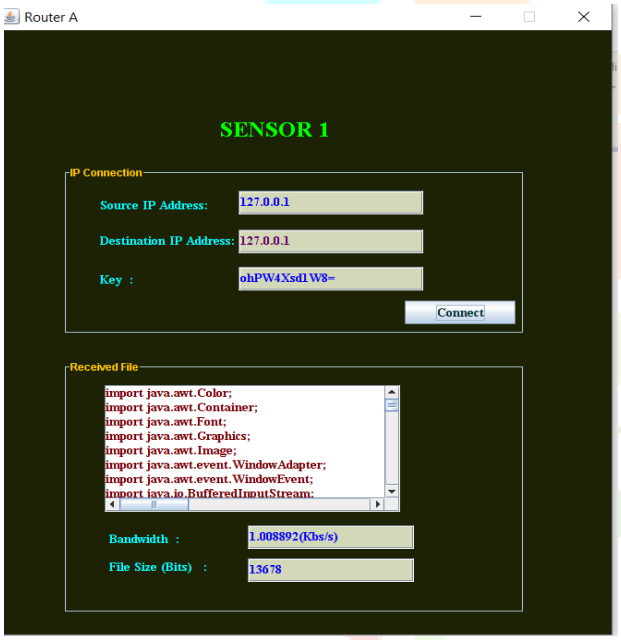
Client File Sended



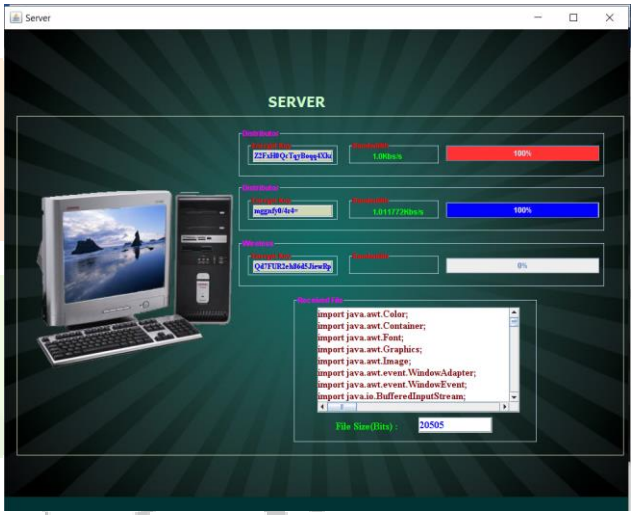
Distributed



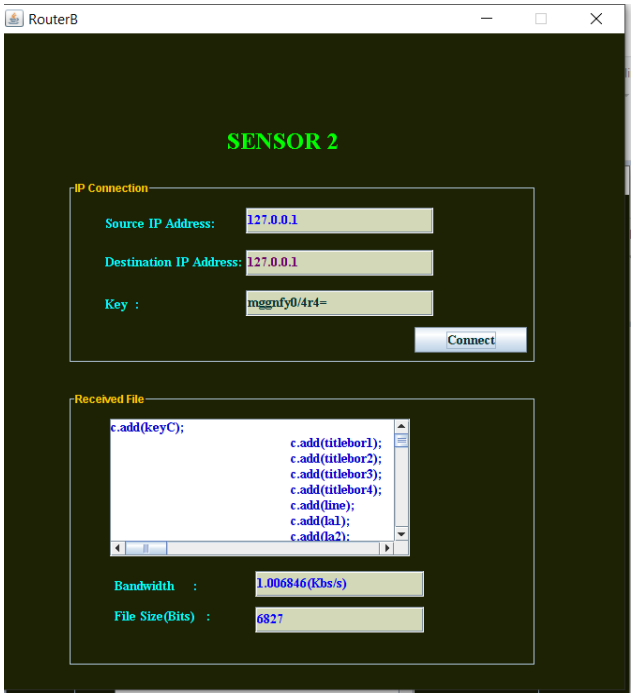
Sensor 1



Server



Sensor 2



V. PERFORMANCE ANALYSIS

The performance analysis of the cloud-based traffic prediction system focuses on evaluating its efficiency, accuracy, scalability, and computational capability in handling large volumes of traffic data. The system performance is assessed using various metrics such as prediction accuracy, precision, recall, Mean Absolute Error (MAE), Root Mean Square Error (RMSE), response time, and processing throughput. Experimental observations indicate that cloud-based architectures significantly reduce data processing time and improve resource utilization compared to traditional traffic management systems. Machine learning and deep learning algorithms, especially hybrid models and Long Short-Term Memory (LSTM) networks, provide higher prediction accuracy for traffic flow and congestion forecasting. The cloud environment also offers dynamic resource

allocation and scalable storage, enabling the system to process real-time data from multiple sources such as GPS devices, IoT sensors, and traffic cameras. Furthermore, the analysis shows that integrating cloud computing with artificial intelligence enhances the reliability and responsiveness of traffic prediction services. Although challenges related to network latency, data privacy, and security still exist, the overall performance results demonstrate that cloud-based traffic prediction systems are highly effective and suitable for intelligent transportation systems and smart city applications.Performance Analysis

VI. CONCLUSION

This research presented a novel Intrusion Detection System (IDS) for Mobile Ad Hoc Networks (MANETs) using a Mobile Sensor Network integrated with fuzzy logic to detect both anomaly-based and misuse-based attacks. The proposed system was evaluated against existing techniques such as Watchdog under various network conditions, including receiver collisions, limited transmission power, and false misbehavior reports. Simulation results demonstrated that the proposed approach achieves higher detection accuracy, lower false alarm rates, and improved reliability while maintaining efficient network performance. To further strengthen the security of the system, digital signature techniques were incorporated to protect acknowledgment packets from forged acknowledgment attacks, thereby enhancing the authenticity and integrity of communication. The integration of fuzzy logic enabled the IDS to effectively handle uncertain and dynamic network behaviors, resulting in more accurate intrusion detection and classification.

REFERENCES

[1].Trust-aware FuzzyClus-Fuzzy NB: intrusion detection scheme based on fuzzy clustering and Bayesian rule Neenavath Veeraiah1,2 • B. Tirumala Krishna3

[2].EE-LB-AOMDV: An efficient energy constraints-based load-balanced multipath routing protocol for MANET M. Naseem, G. Ahamad, S. Sharma, and E. Abbasi Int. J. Commun. Syst., vol. 34, no. 16, 2021, Art. no. e4946, doi: 10.1002/dac.4946.

[3].Energy Efficient Routing For Manet Using Optimized Hierarchical Routing Algorithm (EeOhra) S. Vinod Kumar, Dr. V. Anuratha INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 02, FEBRUARY 2020 ISSN 2277-8616

[4].Efficient Performance Analysis of Energy Aware on Demand Routing Protocol in Mobile Ad-Hoc Network Rajendra Prasad P Shiva Shanka IEEE © 2020 The Authors. Engineering Reports published by John Wiley & Sons, Ltd

[5].Multipath Routing Protocol Using Genetic Algorithm in Mobile Ad Hoc Network ANTRA BHARDWAJ AND HOSAM EL-OCLA , (Senior Member, IEEE) Access 2020

[6] I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: Research challenges," Ad Hoc Netw., vol. 2, no. 4,pp. 351–367, Oct. 2004.

[7] A. Purohit, P. Zhang, B. Sadler, and S. Carpin, "Deployment of swarms of micro-aerial vehicles: From theory to practice," in Proc. IEEE Int. Conf. Robotics Autom., 2014, pp. 5408–5413.

[8] J. Scherer, S. Yahyanejad, and S. Hayat, "An autonomous multi-UAV system for search and rescue," in Proc. 1st Workshop Micro Aerial Vehicle Netw. Syst. Appl. Civilian Use, 2015, pp. 33–38.

[9] D. Floreano and R. J. Wood, "Science, technology and the future of small autonomous drones," Nature, vol. 521, no. 7553, pp. 460–466, May 2015.

[10] M. Asapdour, B. Van den Bergh, D. Giustiniano, K. A. Hummel, S. Pollin, and B. Plattner, "Micro aerial vehicle networks: an experimental analysis of challenges and opportunities," IEEE Commun. Magazine, vol. 52, no. 7, pp. 141–149, Jul. 2014.

[11] J. Xie, Y. Wan, J. H. Kim, S. Fu, and K. Namuduri, "A survey and analysis of mobility models for airborne networks," IEEE Commun. Surveys Tut., vol. 16, no. 3, pp. 1221–1238, Dec. 2013.

[12] I. Bekmezci, O. Sahingoz, and ¸S . Temel, "Flying Ad-Hoc networks (FANETs):Asurvey," AdHocNetw., vol. 11, no. 3, pp. 1254–1270, 2013.

[13] G. G. Finn, "Routing and addressing problems in large metropolitan- scale internetworks," USC Information Sciences Institute (ISI),CA, USA, Tech. Rep. ISU/RR-87-180, 1987.

[14] P. Bose and P. Morin, "Online routing in triangulations," in Proc.Int. Symp. Algorithms Computation, 1999, pp. 113–122.

[15] C. Liu and J. Wu, "Efficient geometric routing in three dimensional Ad hoc networks," in Proc. IEEE INFOCOM, 2009,pp. 2751–2755.