International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET229464

# An Efficient Routing Scheme for Manet Using 3des Approach in CNN Technique

**Bavani. B[1], Mrs. Shirlin[2], Dr. Ferlin Deva Shahila[3]**
[1]M.E(Applied Electronics) Dept of ECE, LITES, Thovalai, India
[2]Dept of ECE, LITES, Thovalai, India
[3]Head of Department, Dept of ECE, LITES, Thovalai, India

**Article Info**
Volume 9, Issue 4

Page Number : 410-438

**Publication Issue :**
July-August-2022

**Article History**
Accepted : 10 August 2022
Published: 27 August 2022

## ABSTRACT

A Mobile ad-hoc network (MANET) is an instance of intelligent transportation system.It provides Mobile-to-Mobile communication with the assistance of road side infrastructure for the purposes of in-mobile entertainment and safer road environment. MANET is characterized by highly mobile, predetermined topology and the requirement of reliable time bound message delivery over error prone shared wireless medium. The security solutions are constrained by these characteristics. By generating a secret group key that can be used to encrypt or authenticate the members of MANET. To address this need, a new secure 3DES algorithm and Convolutional Neural Network are proposed, which prevents several attacks. The enforceability and the privacy of the proposed scheme are demonstrated to study the secure-efficiency.The performance analysis of this technique is implemented in NS2 Software.

Keywords : Electrical Safety System, Power System Control

## I. INTRODUCTION

A Mobile ad hoc network is an autonomous collection of nodes do not rely on any pre- established infrastructure that forms dynamic communicative network. Nodes in these network make use of mobility and wireless communication to maintain connectivity. However, the limited propagation range of these wireless environment make a challenging issue to establish the routes. Subsequently, MANETS are multi-hop infrastructures less network that establishes the routes themselves “on the fly”. These networks are suitable for applications like battlefield, emergency search, rescue operations, vehicular ad-hoc communications and mining operations etc. In such applications, communication and collaboration of nodes among the group is necessary. Therefore, multicast communication is very much intended to the group communication which saves network resources and bandwidth. Moreover, Multicasting is a service for disseminating information to a group of hosts that sends the data from a source to multiple destinations in the network.

The unique properties of multicast communication is first, the node can join anytime and can leave anytime from multicast group dynamically. Second, the nodes have no constraints on the group regarding its location and members in the group. Third, a node may be a member of several groups. However, the nodes have send the packets to the members in the group, even it is not a member of a group.Over the last decade, researchers proposed several multicast routing protocols for MANETs for effective multimedia communication. More importantly these routing protocols can be categorized intotreebased and mesh-based routing protocols. However, other multicast routing protocols are also available, which is out of scope of this paper.

First, the tree based multicast routing protocols maintains a single path and establishes a shared multicast routing tree to transmits the packets from source to receivers in a multicast group. The main idea behind these protocols is to maintain memory for their children instead of all the nodes. Additionally, these protocols do not provide sufficient robustness due to the limited bandwidth efficiency. One of the tree based multicast routing protocol is MAODV. While, Mesh based multicast routing protocols establishes a mesh network and maintains multiple paths between sources to receivers. Due to the multiple paths, mesh based multicasting is more suitable for frequently changing topological environments and provide more robustness. PUMA and ODMRP are the routing protocols that falls under mesh based routing protocols. Moreover, in spite of the routing issue many mobile adhoc network applications requires various multicast routing protocols that need to operate correctly even in hostile environment. Because the MANETS are more vulnerable to different routing attacks wormhole, black hole, rushing attack, man in the middle attack, etc., due to its inherited characteristics of MANETs.

Networks are a group of system networks linking together. There are two main classifications, Peer to Peer and Client/Server. Networks can be characterized by their size and purpose. The size of the network is explained by geographical area that they occupy and the number of links that are part of the network. Some networks based on size are; LAN (Local Area Network), WAN (Wide Area Network), MAN (Metropolitan Area Network), PAN (Personal Area Network). Some Networks based on their purpose are; SAN (Storage Area Network), VPN (Virtual Private Network), MANET (Mobile Ad-Hoc Network). In this paper we discussed about the intrusion detection systems on MANETS. Mobile Ad-Hoc Network or MANET is an infrastructure-less IP based on network of mobile and wireless machine nodes. It is a type of ad- hoc network that can change locations and configure itself while moving.

In MANET each node act as a “router” to transmit the traffic to other specific node in the network. MANETs is very successive, attractive, and pervasive technology in wireless network. To maintain the mobility is an important task done by MANETs. MANETS is much more easier to be affected by different types of attack because it provides distributed architecture, volatile network topology, limited bandwidth of single hop and multi hope. In single hope, the entire node is in the defined coverage area, if there is intermediate node used for communication between two nodes is been called multi hop network. In MANETs there are two types of attack possible one is active attack and the other is Passive attack. MANETs is used in emergency requirements because it allows easy deployment, minimal configuration, and low cost. However, it has restricted the battery power and resources. The aim of networking is to facilitate the exchange of data such as audio, text or video between various points across the world. For the delivery of data, various types of switching techniques are used in networking. The various types of switching techniques are packet switching, message switching and circuit switching. In this paper, we are dealt with packet switching.

## II. LITERATURE REVIEW

A collection of tiny power, multifunctional and communications nods with observation and recording situations at distinct places, afterwards, convert this data to signals that can be processed, Such nodes are randomly implemented on a large or small scale, this becomes a significant field for study because these networks are used today in numerous consumer and industrial applications, for instance in healthcare, the industry, the transport system, government security and military systems, the environment and agriculture and underwater sensor systems. If the amount of sensors is big, this enables for greater monitoring with greater accuracy, but it can be very costly or even impossible to charge or replace batteries because of the challenging environment.

Active research work for MANETs is carrying on mainly in the fields of Medium Access Control (MAC), routing, resource management, power control, and security. Because of the importance of routing protocols in dynamic multi-hop networks, a lot of MANET routing protocols have been proposed in the last few years. Considering the special properties of MANET, when thinking about any routing protocol, generally the following properties are expected, though all of these might not be possible to incorporate in a single solution. A routing protocol for MANET should be distributed in manner in order to increase its reliability. A routing protocol must be designed considering unidirectional links because wireless medium may cause a wireless link to be opened in unidirectional only due to physical factors. The routing protocol should be power-efficient. The routing protocol should consider its security. A hybrid routing protocol should be much more reactive than proactive to avoid overhead. A routing protocol should be aware of Quality of Service (QoS). On the basis of the above requirements, several existing studies are carried out as follows.

Lei Deng et al [2021] proliferation of real-time applications over wireless communications, it becomes more and more important to support delay-constrained traffic in MANETs. In such applications, each packet has a given hard deadline: if it is not delivered before its deadline, its validity will expire and it will be removed from the system. This feature is fundamentally different from the traditional delay-unconstrained one. We for the first time investigate distributed scheduling schemes for a topology-transparent MANET to support delay- constrained traffic.

Carlo Kleber da Silva Rodrigues et al [2019] proposes a novel BitTorrent-like algorithm for video-on-demand streaming over mobile ad hoc networks: the BT-MANET algorithm. Its conceptual innovations mainly lie on (i) a flexible data-transmission scheme between direct neighbors and on (ii) a sliding window to prioritize data request, settling a compromise between data diversity and playing continuity. Through a number of simulations and assessing four different competitive metrics, we are able to validate our proposal and confirm its attractive performance for on-demand streaming.

Taj Rahman et al [2020] have extensively studied clustering schemes and divided the schemes into multiple types based on the Cluster Head (CH) selection criteria, which provides a good understanding of how each type of clustering algorithm differs from each other. The authors analyzed the performance of existing schemes based on the quality of service (QoS) metrics. Based on findings, the authors clarified some important tradeoffs between QoS metrics and also established some important factors influencing the efficiency of clustering schemes.

Ruo Jun Cai et al [2019] propose an evolutionary self-cooperative trust (ESCT) scheme that imitates human cognitive process and relies on trust-level information to prevent various routing disruption attacks. In this scheme, mobile nodes will exchange trust information and analyze received trust information based on their own cognitive judgment. Eventually, each node dynamically evolves its cognition to exclude malicious entities. The most attractive feature of ESCT is that they cannot compromise the system even if the internal attackers know how the security mechanism works.

Masood Ahmad et al [2019] Mobile ad hoc networks (MANETs) are self-organized networks without any fixed infrastructure. The topology changes are very frequent in MANETs due to nodes' mobility. The topology maintenance creates an extra overhead, as the mobility information of a single node is shared with all nodes in the network. To address the topology maintenance overhead problem in MANETs, the researchers proposed different cluster-based algorithms to reduce the size of a routing table. The clusters are formed to locally adjust the topology changes within the cluster. If a node wants to communicate with a node outside the cluster, it only communicates with its cluster head (CH). The CH communicates with other CHs to transmit data toward the destination. To efficiently utilize the clustering mechanism in MANETs, stable and balanced clusters are required. To form good quality and optimized clusters, some metrics, such as relative mobility (node speed and direction), node degree, residual energy, communication workload, and neighbor's behavior, are required.

TaoufikYeferny et al [2019] considering the great success of mobile devices in recent years, P2P applications have also been deployed over mobile networks such as mobile ad-hoc networks (MANETs). However, the mismatch between the P2P overlay and the MANET underlay topologies makes the resources lookup mechanism in mobile P2P applications very difficult. Therefore, this downside is the main hindrance to the deployment of such applications over MANETs. To overcome the mismatch issue, we propose in this paper RLSM-P2P a cross- layer resource lookup scheme for Mobile P2P applications. The main thrust of RLSM-P2P consists of building an efficient unstructured P2P overlay that closely matches the underlay physical network and swiftly adapts to its volatility and dynamicity by considering different MANET constraints.

BurhanUl Islam Khan et al [2021] examines a pragmatic scenario as a test case wherein the mobile nodes must exchange multimedia signals for supporting real-time streaming applications. There exist two essential security requirements viz. i) securing the data packet and ii) understanding the unpredictable behavior of the attacker. The current study considers sophistication on the part of attacker nodes. They are aware of each other's identity and thereby collude to conduct lethal attacks, which is rarely reflected in existing security modeling statistics. This research harnesses the potential modeling aspect of game theory to model the multiple- collusion attacker scenario. It contributes towards i) modeling strategies of regular/malicious nodes and ii) applying optimization principle using novel auxiliary information to formulate the optimal strategies.

Nousheen Akhtar et al [2019] present a bandwidth aware routing scheme (BARS) that can avoid congestion by monitoring residual bandwidth capacity in network paths and available space in queues to cache the information. The amount of available and consumed bandwidth along with residual cache must be worked out before transmitting messages. The BARS utilizes the feedback mechanism to intimate the traffic source for adjusting the data rate according to the availability of bandwidth and queue in the routing path. We have performed extensive simulations using NS 2.35 on Ubuntu where TCL is used for node configuration, deployment, mobility and message initiation, and C language is used for modifying the functionality of AODV.

Osamah Ibrahim Khalaf et al [2020] Security and correspondence happening between network central points will be an instance for principal issues in Mobile Ad-hoc Networks (MANETs). Due to some ideas created by the organization leading to avoid attacks but may end

in failure due to inappropriate way and thus attacks need recognized and cleared. The Dual- Cooperative Bait Detection Scheme (D-CBDS) is one of the ways that is in the stake for the discovery of MANET-dark/dim opening assailants. The current CBDS calculation consolidates the intensity of proactive and responsive security advancements to characterize lure mode assailants as proactive and receptive engineering. In CBDS, an adjacent source node is randomly selected as a bait target for searching. By reverse tracking as a reactive method, the attackers are identified. However, in some time, the chosen bait destination node may be an intruder that is not handled in the current CBDS approach.

Jae Seang Lee et al [2019] mobile ad-hoc network (MANET), unmanned vehicles are deployed for surveillance and reconnaissance. They send multimedia data to a center node in real time. In this letter, we propose a centralized TDMA slot and power scheduling schemes which maximize energy efficiency (EE) considering Quality-of-Service (QoS) for the tactical MANET. We formulate this problem as a non-concave ratio optimization, and propose the optimal slot allocation and power control algorithms based on the Dinkelbach method and the concave- convex procedure.

BabatundeOjetunde et al [2019] introduce a new mobile payment system utilizing infrastructureless mobile Adhoc networks to enable transactions that permit users to shop in disaster areas. Specifically, we introduce an endorsement-based mechanism to provide payment guarantees for a customer-to-merchant transaction and a multilevel endorsement (MLE) mechanism with a lightweight scheme based on Bloom filter and Merkle tree to reduce communication overheads. Our mobile payment system achieves secure transaction by adopting various schemes such as location-based mutual monitoring scheme and blind signature, while our newly introduced event chain mechanism prevents double spending attacks.

Fifi Farouk et al [2020] a Vehicular Ad-hoc Network (VANET) is a type of Mobile Ad- hoc Network (MANET) that is used to provide communications between nearby vehicles, and between vehicles and fixed infrastructure on the roadside. VANET is not only used for road safety and driving comfort but also for infotainment. Communication messages in VANET can be used to locate and track vehicles. Tracking can be beneficial for vehicle navigation using Location Based Services (LBS). However, it can lead to threats on location privacy of vehicle users; since it can profile them and track their physical location. Therefore, to successfully deploy LBS, user's privacy is one of major challenges that must be addressed. In this paper, we propose Privacy-Preserving Fully Homomorphic Encryption over Advanced Encryption Standard

(P 2 FHE-AES) scheme for LBS query.

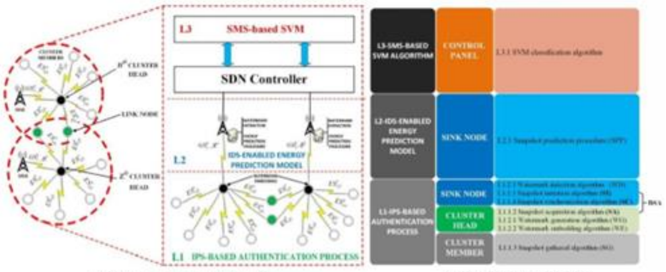
Jae Seang Lee et al [2020] on a future tactical-battle field network, combat radio nodes will be deployed for various operations, forming a mobile ad-hoc network (MANET). However, because of the nodes' mobility, a single group might be divided into several small groups with fewer nodes. Conversely, several small groups might be merged into one group. In such an environment, an unmanned aerial vehicle (UAV) will provide an effective way to improve network coverage and connectivity among the small groups. However, some issues should be considered for the optimal deployment of the UAV. One issue is to find the proper position of the UAV, which enhances the connectivity among the groups, because a tactical network places a high priority on network survivability rather than throughput maximization. We also need to exploit real topographic information to obtain more accurate connectivity information among nodes. Second, an efficient resource allocation scheme for reliable communications through the UAV should be taken into account. Since most of the links between the UAV and the ground nodes are line-of-sight (LoS), due to the good quality of these links, the traffic via the UAV will be heavy in spite of the limited data slot resources.

M. Sivaram et al [2019] the quality of service (QoS) is improved by enhancing the capability of the DBTMA for better network service in the MANETs. The proposed method uses an improved DBTMA called Retransmission Dual Busy Tone Multiple Access (RDBTMA) protocol. This is based on two elements namely: busy tones and Ready to Send/Clear to Send (RTS/CTS) dialogues. In addition to this fast retransmission, a strategy is used further to improve its effectiveness. The retransmission strategy is adopted using negative acknowledgment after the collision occurred by the hidden nodes. A hidden node, where the collision occurs at access point, listens to the NACK signal and uses the signal to determine the requirement fast retransmission scheme. The proposed method is simulated and compared against existing methods in terms of various network parameters.

Bin Yang et al [2019] investigates the non-asymptotic capacity in MANETs under a general packet routing scheme with multicast traffic, where each source has multiple destinations. Under the routing scheme, when the destinations move into the communication range of their source, a packet at source will be directly sent to destinations; otherwise, it can be replicated to multiple different relays, which help to forward it to destinations. To study the non-asymptotic capacity in the MANETs, we first develop the two Markov chain theoretical frameworks to characterize the fastest packet propagation process at source and the fastest packet reception process at destinations under the routing scheme. Based on these two theoretical frameworks, we then derive an analytical expression for the capacity.

## III. RELATED WORK

A plethora of research works have been performed to address high security and low- latency solutions for resource constrained WSNs. In this context, some of the existing IPS based authentication procedures have been developed using classical key management authentication mechanisms. For example, an IPS combining Internet Protocol (IP) trace-back with an enhanced adaptive acknowledgment (EAACK). Moreover, Location-Based Keys (LBKs), binding private keys of individual nodes to both their identifications and geographic locations. These approaches improved the security at the cost of increasing the latency of the network. To address the challenges associated with the low-latency requirements, some works used physical


CLUSTER MEMBERS
1st CLUSTER HEAD
LINK NODE
2nd CLUSTER HEAD
L3 SMS-based SVM
SDN Controller
L2
IDS-ENABLED ENERGY PREDICTION MODEL
L1 IPS-BASED AUTHENTICATION PROCESS
L3-SMS-BASED SVM ALGORITHM
CONTROL PANEL
L3.1 SVM classification algorithm
L2-IDS-ENABLED ENERGY PREDICTION MODEL
SINK NODE
L2.1 Snapshot prediction procedure (SPP)
L1-IPS-BASED AUTHENTICATION PROCESS
SINK NODE
CLUSTER HEAD
CLUSTER MEMBER
DSA

(a) SDN-based three layers' framework

(b) Security framework stack

Figure 3.1 A collaborative security framework for SDWSNs

Layer features. For instance, a two-factor user authentication mechanism was recommended, where the authors devised an authentication mechanism comprising of registration and authentication phases. Furthermore, the authors in, explored a biometric-based continuous authentication technique, without the the need for an authentication server. These approaches reduced the latency but at the cost of increasing the complexity of the authentication procedures.

Furthermore, some works also exploited physical layer features in IDS to achieve low- latency in WSNs. In this context, a novel intrusion detection scheme based on energy prediction for cluster-based WSNs was introduced in, wherein the authors used the energy states of wireless sensor nodes to predict malicious behaviors at a given time. Excessive false alarms are a common artifact of these approaches.

Consequently, machine learning procedures have been widely used to develop IDS-based solutions. For instance, the use of neural networks and watermarking techniques was suggested in. A SVM methodology was proposed in, while a hybrid machine learning approach for network anomaly detection was put forward in. A hybrid anomaly based IDS was recommended which employed SVM and multi-layer perceptron (MLP) to identify anomalies in the network. Further, the authors in presented an intrusion detection engine based on neural networks combined with a protection method-based on a watermarking technique. While these algorithms improve the accuracy of network anomaly detection models, they also introduce high computational cost which is inadequate for WSNs. Even though relevant works have been proposed in the literature to target security issues in SDWSNs, challenges such as high security, excessive false alarms, low-latency, and high computational cost still remain unaddressed.

## IV. CONTRIBUTIONS

To address these imperative challenges, in this paper, a bottom-up security framework is designed. The novelty of the proposed work lies in devising and evaluating a collaborative framework which amalgamates a recurrent lightweight authentication method in conjunction with intrusion detection and a real-time smart monitoring system; achieving lightweight authentication and enhanced anomaly detection mechanisms in SDWSNs.

Since a single-gateway (cluster head) architecture is not scalable and might cause an incremental overhead in large scale WSNs, the proposed work uses a cluster-based SDWSN architecture that provides a hierarchical organization to a flat sensor network topology, considerably reduces the latency of the network. This architecture consists of four kinds of dynamic nodes, namely, cluster members, cluster heads, link nodes, and sink nodes. Further, in this framework, a Distributed Snapshot Algorithm (DSA) is executed to capture network snapshots periodically so as to obtain the global energy state of the WSN; wherein the global energy state corresponds to a map of the energy state for each node at a given moment. Moreover, the DSA is also used to dynamically adapt the network topology within the cluster to reduce the energy consumed for communication; thus, extending the lifetime of the network while achieving an acceptable performance for data transmission.

The proposed framework hierarchically combines three security layers. At the bottom of this approach (Layer L1), an IPS-based authentication process is designed to provide a lightweight security scheme in the data plane. In the middle of the framework (Layer L2), an IDS-enabled energy prediction model within the edge is designed with the aim of supplying a cost-effective intrusion detection solution near the data plane. Finally, at the top of this framework (Layer L3), in the control plane, a SMS-based SVM algorithm is introduced to achieve isolation, high performance, enhanced anomaly detection, and efficient mitigation by segregating malicious nodes over the SDWSNs. Since the SMS-based SVM algorithm has global visibility of the sensor network, it can see the correlations between true positives, which lets it filter out the False positives. Thus, the main contributions of this work are summarized as follows:

1) A novel security scheme based on network snapshot readings, providing continuous authentication in large scale SDWSNs, is proposed.

2) A watermarking technique is exploited to guarantee the accuracy of concurrent authentications while performing data integrity checks for the entire SDWSN.

3) The authentication method is improved by introducing a link node, which creates a connection between all the cluster of sensors.

4) An edge computing empowered IDS is leveraged to efficiently handle the limited resources in SDWSNs.

5) A two label dataset is generated in the edge, with the aim to train an SVM classification algorithm that is subsequently used by the SMS; wherein the latter is deployed at the control plane and is designed to correlate the alerts from the low-delay IDSs distributed across the edge network.

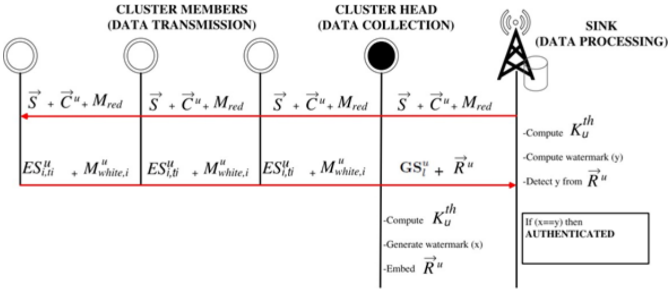


Figure 3.2 DSA-based authentication and a watermarking technique

Moreover, analysis of the computational complexity is provided and simulations showing the effectiveness of the proposed framework are executed by leveraging the AVISPA tool and MATLAB. The results demonstrate an accuracy of 84.75%. The remainder of this paper is organized as follows: Section II and Section III introduce the different layers of the proposed framework. In Section IV, security analysis and performance evaluation are conducted. Finally, the paper is concluded in Section V, where some future endeavors are also put forward.

## V. SYSTEM MODEL

Aiming to achieve high-security, address the limited resources constraints and take advantage of SDN architectures, our work proposes a collaborative security framework design, as depicted in Fig.3.1a. To summarize, the proposed security framework possesses a hierarchical structure and comprises of three layers. At the bottom of the framework stack, in the data plane, in L1, an IPS-based authentication process is performed. At the middle, at the edge, in L2, an IDS-enabled energy prediction model is executed, and finally, in the control plane, in L3, the SMS-based SVM algorithm is designed. In this context, in L1, a cluster-based WSN is created and DSA is employed, where the sink nodes initiate the snapshot acquisition process by sending a marker message to their cluster heads in order to form a global energy state of the network. Afterwards, the marker message is propagated to the cluster members. Each member sends its energy state back to its cluster head post receiving the message.

Once the cluster head collects the global energy state from its cluster members, it protects the data using a watermarking embedded method with the aid of a generated public key and other security parameters to ensure that the derived data will not be altered on the fly by possible malicious attackers. Consequently, the network snapshot and the watermarked data is forwarded to the sink node. Likewise, the sink sends a copy of the energy map to the control plane, which is located in the cloud. Moreover, in the edge, the sink node periodically receives the snapshot readings aiming to detect the embedded watermark for the sake of continuous authentication and for the subsequent energy consumption prediction procedure. Furthermore, the appropriate watermarked data is considered reliable, while the data without a correct watermark is marked as unreliable. Subsequently, in L2, an IDS-enabled energy prediction model is executed, where a Markov chain prediction procedure is used to detect nodes' misbehavior. Conclusively, to amalgamate this framework, in the control plane, in L3, an SMS-based SVM algorithm is designed where the dataset resulting from L2 is processed by employing a SVM classification algorithm. A summary of the security framework stack is presented in Fig.3.1b.

## VI. PROPOSED SCHEME

In the following subsections, the proposed L1, L2, and L3 layers along with their corresponding stack of algorithms are elaborated.

### L1:IPS-BASED AUTHENTICATION PROCESS

In SDWSN applications, the reliability and the integrity features of the cluster nodes should not be compromised. However, if the data transmission is not reliable, the integrity of the whole network is affected. To handle this security challenge, this work considers deploying an IPS-based authentication mechanism which is an amalgamation of the DSA and watermarking techniques. The designed mechanism aims to provide a two-way authentication handover between the cluster node, the cluster head, and the sink node.

In the following subsections, the sublayers, the DSA-based authentication procedure, and the watermarking-based authentication technique are detailed.

1) L1.1:DSA-Based Authentication Procedure: As illustrated in Fig. 3.2, this procedure starts when the sink node initiates snapshot acquisition by sending the first message to its cluster head; from there, the request message is propagated to every cluster member. After receiving this message, every cluster member sends its energy state back to its cluster head which is then used to generate the key fingerprint with other security parameters. It is worth mentioning that a link node could receive multiple request messages from multiple clusters' heads. Thus, each link node must send a reply back to all of them, in order to provide scalability for large-scale WSN and maximize the efficiency of the authentication procedure. Before data transmission, the energy state of the cluster heads is embedded into the global energy state gathered by them. The concurrent snapshot readings gathered in a given time by the uth cluster head are represented as follows.

GSu l = [E Su 1,t1 , E Su 2,t2 ..., E Su i,ti ], (3.1)

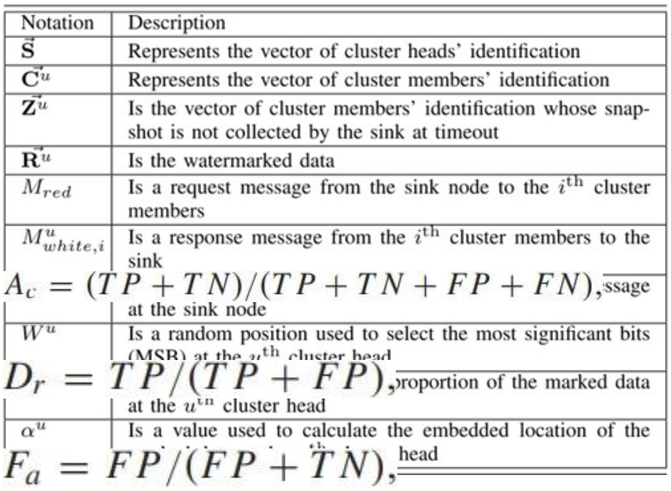
whereGSu l represents the snapshot readings collected in l cycles at ti time of arrival from the ith cluster member E Su i,ti to the uth cluster head. This time of arrival significantly reduces the possibility of impersonation of the GSu l vector by an intruder. This is due to the random behavior of wireless communications which makes the time of arrival unforeseeable. The cluster head then averages the GSu l vector to generate the kth u fingerprint using the following equation.

kth u = E[GSu l ], (3.2)

where E[.] is the mean operator. Afterwards, the kth u fingerprint is encrypted with the advanced encryption standard (AES) algorithm with a key length of 128 bits [28]. The generated kth u fingerprint contributes to making the public key unpredictable. Further, the aim of the DSA is to obtain a distributed network global state by recording the consistent energy state at a specific time [29]. In this sense, as shown in Fig. 1b, the DSA is divided in four algorithms hierarchically distributed as follows:

- The Snapshot-Initiation (SI) algorithm (L1.1.1), launched by the sink node;
- The Snapshot-Acquisition (SA) algorithm (L1.1.2), exploited by the cluster head;
- The Snapshot-Gathering (SG) algorithm (L1.1.3), executed by the cluster members;

TABLE 3.1 ALGORITHMS' NOTATIONS



| Notation | Description |
|---|---|
| $\vec{S}$ | Represents the vector of cluster heads' identification |
| $\vec{C^u}$ | Represents the vector of cluster members' identification |
| $\vec{Z^u}$ | Is the vector of cluster members' identification whose snapshot is not collected by the sink at timeout |
| $\vec{R^u}$ | Is the watermarked data |
| $M_{red}$ | Is a request message from the sink node to the $i^{th}$ cluster members |
| $M^u_{white,i}$ | Is a response message from the $i^{th}$ cluster members to the sink |
| [illegible] | [illegible] ssage at the sink node |
| $W^u$ | Is a random position used to select the most significant bits (MSB) at the $u^{th}$ cluster head |
| [illegible] | [illegible] proportion of the marked data at the $u^{th}$ cluster head |
| $\alpha^u$ | Is a value used to calculate the embedded location of the [illegible] head |

The Snapshot-Synchronization (SC) algorithm (L1.1.4), exploited by the sink and the cluster head nodes.

Next, we detail the four algorithms which use the notations presented in Table 3.1.

a) L1.1.1: Snapshot-initiation algorithm: Since DSA collects snapshots through messages, it is important to ensure message delivery. Thus, in order to solve this problem, we implement a two- way handshake between the cluster node and the sink node. Here, the authentication procedure relies on the SI algorithm, which assumes that the number of sensor nodes and their first snapshot is known by the sink in a setup stage. The sink ensures reliable E Su i,ti delivery by keeping a table indexed with nodes' identification. In this context, the sink node sends an initial Mred message to its cluster head. The SI algorithm execution ends only when the sink node acquires the network snapshot from all functioning nodes. In this manner, the sink node waits until timeout tw expires.

The evaluation of L3's classifier accuracy uses L2's output as ground truth, where trusted and malicious nodes are represented by a non-linear classification model. The obtained results demonstrate that there are 61 False Alarms (FA) as shown in Table V, where T P is the true positive (a malicious node detected as a malicious node), T N is the true negative (a trusted node identified as a trusted node), F P represents a false positive (a trusted node detected as a malicious node), and F N is a false negative (a malicious node recognized as a trusted node). The performance evaluation of the experiment is carried out by evaluating the accuracy Ac of the framework, the detection rate Dr, and the false alarm Fa rate by using the following equations.

$$A_c = (TP + TN)/(TP + TN + FP + FN), \tag{3.3}$$

$$D_r = TP/(TP + FP), \tag{3.4}$$

$$F_a = FP/(FP + TN), \tag{3.5}$$

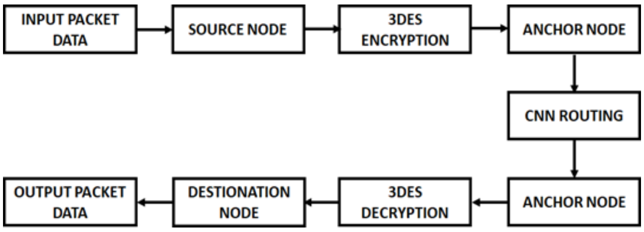
From the experimental results and the performance evaluation, Ac is found to be 84.75%, Dr is equal to 87.55%, which was increased in comparison with the second layer, whereas the false alarm rate is equivalent to 14.36%. To the best of our knowledge, the concept of a unified SDN-based security framework stack, integrating IPS, and a hierarchical collaborative anomaly detection system has never been attempted in any previous research works.

## VII. PROPOSED SYSTEM

### INTRODUCTION

In the recent years, one could assist to a spectacular growth in the use of wireless equipments. The number of mobile devices such as PDAs, mobile phones laptops, is also tremendously increasing. To ensure the connectivity between all these devices, ad hoc networks appear to be a promising solution. An ad hoc network is a collection of wireless mobile nodes, which communicate together without the assistance of any fixed nor central infrastructure. MANET an autonomous collection of mobile nodes forming a dynamic wireless network. The administration of such a network is decentralized, i.e. each node acts both as host and router and forwards packets for nodes that are not within transmission range of each other. A MANET provides a practical way to rapidly build a decentralized communication network in areas.

PROPOSED SYSTEM



3DES algorithm is introduced to achieve isolation, high performance and enhanced anomaly detection. To apply 3DES, the considered optimization problem is first converted to the problem of finding the best parameter vector which minimizes an objective function. In this proposed method optimization technique is used. A novel fitness function has been designed for the 3DES algorithm based on which the nodes are segregated. Based on the segregated node list, the CNN structure is trained, which helps to deliver data with a small delay. The list of affected nodes and the normal node is created by a 3DES algorithm based on which accurate route is selected by the CNN algorithm. This process helps to enhance the speed and hence reduce the delay. In MANETs, location information is important for the generation of shared keys and is highly applicable. Thus, DES based key management is a core part of the research into MANET key management. This key management system is used to improve the stability and security of the transmission.

### DES ((DATA ENCRYPTION STANDARD) ALGORITHM

DES algorithm was born in the mid-1970s. It is a block cipher algorithm, which isgrouped in 64-bit data encryption and decryption. And the data encryption and decryptionalgorithm are using the same structure, in which only the use of keys are in different order. The length of keys is 56-bit (the keys are usually expressed as 64-bit, but each eighth bit is used as parity check bit and can be ignored). And very little keys are considered as the weak keys, but they can be easily avoided.

DES is a symmetric-key algorithm based on a Feistel network. As a symmetric key cipher,it uses the same key for both the encryption and decryption processes. The Feistel network makesboth of these processes almost exactly the same, which results in an algorithm which is more efficient to implement.

DES has both a 64-bit block and key size, but in practice, the key only grants 56-bits of security. 3DES was developed as a more secure alternative because of DES's small key length. In3DES, the DES algorithm is run through three times with three keys, however it is only considered secure if three separate keys are used.

3DES runs the DES algorithm three times, with three 56-bit keys:

- Key one is used to encrypt the plaintext.
- Key two is used to decrypt the text that had been encrypted by key one.
- Key three is used to encrypt the text that was

- **decrypted by key two. 3DES keying options:**

Technically, 3DES can be implemented with three different key configurations. Despite this, the second and third option are insecure and should never be implemented.

Keying option one – This option uses three independent keys and is the most secure. Keying option two – In this configuration, the first and third keys are the same.

Keying option three – This uses three identical keys. When identical keys are used, the decryption process in the second stage cancels out the first encryption, leaving only the final encryption to alter the data. This makes the result the same as ordinary DES.

## DES ALGORITHM - ENCRYPTION PROCESS

DES algorithm encryption process can be divided into 5 steps to operate:

- 64-bit key produces 16 sub-keys through a Sub-key algorithm which are K1, K2...K16used respectively for the first, second...sixteenth iterative encryption.
- 64-bit plaintext was rearranged after the IP(Initial Permutation) and divided into left side L0 which is the left 32 bits and right side R0 constituted by the right 32bits.
- R0 is encrypted by the sub-key K1 through the encryption function. The result is a 32-bit data set f (R0, K1), the diagram shown in Figure 4.3 A 32-bit data set L0$\oplus$ f (R0, K1) is gotten after f (R0, K1) combines with L0 using mode 2. Then this set is used as the R1 in the second iteration and R0 is used as the L1 of the second iteration. Thus the first iteration encryption is completed.
- The second iteration encryption to the sixteenth iteration encryption keys were used to sub-keys K2 ... K16, and their processes are same to the encryption in the first iteration.
- At the end of the sixteenth iteration encryption it creates a 64-bit data set. Its left 32-bit is considered as R16 and the right 32-bit is L16. After the two sides merged, 64-bit encrypted messages will be got by the data rearranged through inverse initial permutation IP-1. By now all the encryption process is over.

- DES encryption process mathematical formula described as follows:$L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ $i = 1,\ 2,\ 3, \ldots, 16$

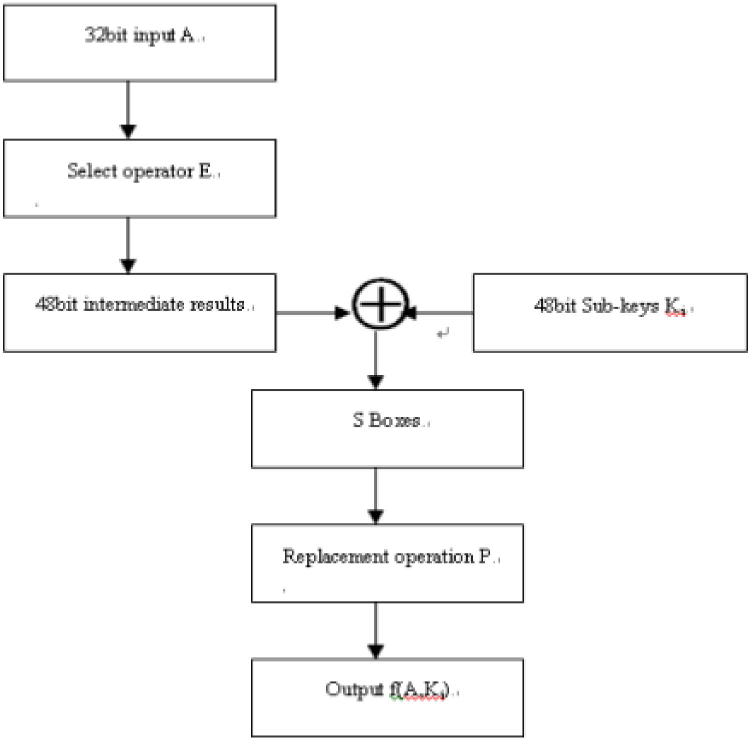


**Figure. 4.2** Encryption Function f

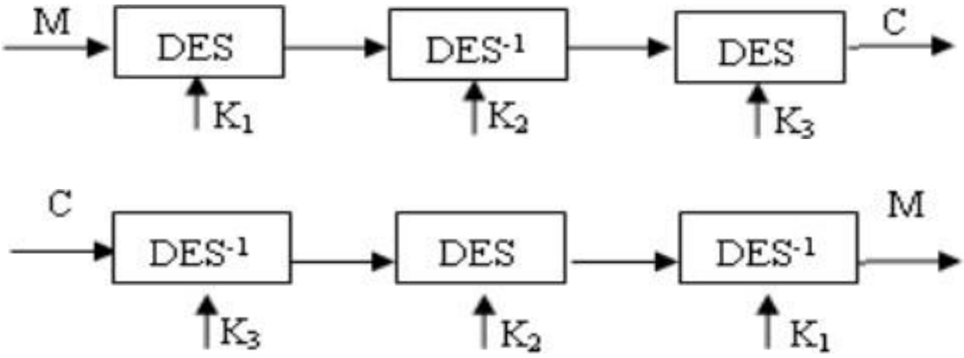


**Figure 4.3** 3DES Encryption/Decryption Process

Inversed DES encryption process and using the decryption sub-key Ki, the encrypted messages can be decrypted. 3DES is a more secure DES morphing. 3DES algorithm is the cumulative computing of the three times DES algorithm that is the process of Encryption - Decryption - re-encryption. In order to obtain higher security, three keys should be separate. In essence, this is equivalent to use a length of 168-bit keys for encryption. The structure of 3DES algorithm is shown in Figure 4.3.

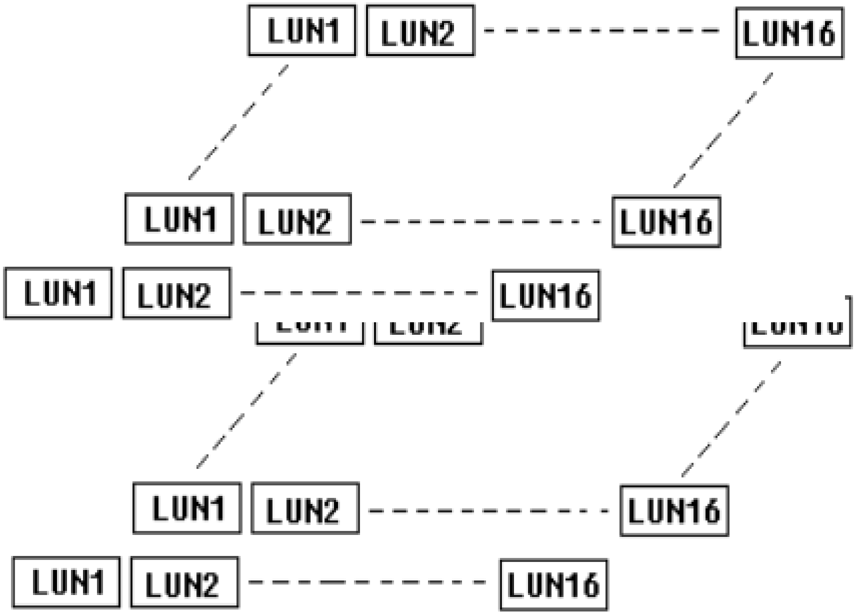
### 4.3.2 S-BOX DESIGN

S-box is a critical step in DES algorithm which is a complex nonlinear function and all other operations are linear. Through the non-linear transform of S-box, plaintext has been able to express well as the confusion to have strong security. It is a certain difficult to realize the S-box whose realization is the main factor of impacting the speed of overall encryption and decryption. Therefore, this work aims the original algorithm for improving S-box, uses a single S-box to replace the original eight, and the expanded 48-bit data is divided into eight blocks. These data is passing S-box through a MUX and then the generated results are composed into a 32-bit data which input permutation matrix P. This will significantly reduce the size of the circuit, at thesame time as a result of the reduced size of the entire circuit power consumption will reduce circuit will reduce so as to enhance the overall performance of the system.

### 4.3.3 LUN FUNCTION

A logical unit number (LUN) is a unique identifier for designating an individual or collection of physical or virtual storage devices that execute input/output (I/O) commands with a host computer, as defined by the Small System Computer Interface (SCSI) standard.

Each packet of the DES algorithm requires sixteen LUN operations. If using sequence circuit structure, one encrypted packet can be only generated after sixteen LUN operations. This method significantly reduces the efficiency of the encryption. Therefore, high-speed DES algorithm uses pipeline structure, as shown in figure 4.4



sixteen iterative design sixteen computing modules, respectively, called as LUN1, LUN2… LUN16. Data is computed pipeline operation in each module. When the first i input data is computed the first j operation, the firsti+1 input data is computed the first j-1 operation and the first i+2 input data is computed the first j-2 operation…in order to improve the computing efficiency of the system. 3DES algorithm is based on DES algorithm, so completing a 3DES encryption /decryption algorithm needs forty- eight LUN operations.

Figure 4.4 The Pipeline Structure of DES

Therefore, the encryption efficiency will be even lower if not using pipeline structure. Considering the efficiency, 3DES also uses pipeline structure in this article. The pipeline structure of 3DES is based on which in DES. In the DES algorithm, two signals flag and ready are set, which respectively represents the end and the beginning of the sixteenth operation. When the sixteenth operation begins in the first DES, the data is beginning to load in the second DES. When the sixteenth operation ends, the second DES begins operating. When the sixteenth operation ends in the second DES, the third DES begins operating. In this way, supposing completing a LUN operation needs n clocks, sixteen LUN operations need n+15 clocks(completing a DES), so completing a 3DES needs 3(n+15)-2 clocks.

The peripheral circuit to achieve 3DES algorithm includes four selectors, a key-module and a control-module. The four selectors choose the correct data path between the internal and external in DES algorithm (DES composes the convergence of 3DES) driven by the control- module. The key-module driven by the control-module selects one output among the 48 sub-keys produced from the three keys K1, K2, K3 to participate in iterative calculations. The control- module needs produce the right signal for driving the input clock, key and encryption/decryption operators, to control the entire system work correctly.

## CONVOLUTIONAL NEURAL NETWORK (CNN)

Convolution neural network (also known as Convolution Neural Network or CNN) is a type of feed-forward neural network used in tasks like image analysis, natural language processing, and other complex image classification problems. It is unique in that it can pick out and detect patterns from images and text and make sense of them. Before diving deeper into this topic, let's take a step back and understand the origin of the Convolutional Neural Network (CNN).

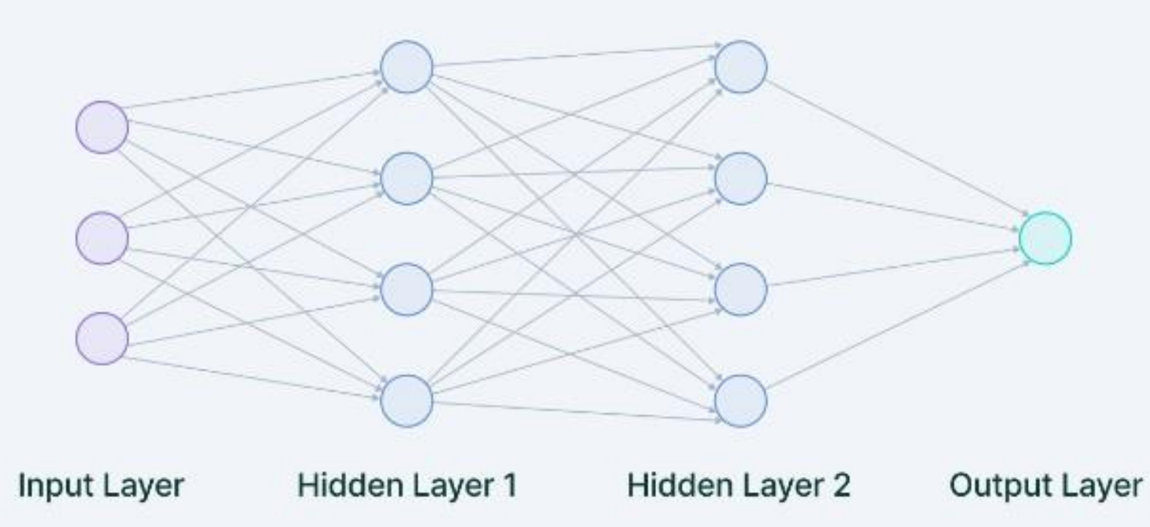


**Figure 4.5** convolutional neural networks look at one patch of an image

## ALGORITHM FOR CNN CLASSIFIER

1. 2-D convolutional layer with 96 filters of [11 11] size where stride is 4.
2. ReLU layer
3. MaxPooling layer
4. 2-D convolutional layer with 10 filters of [5 5]
5. ReLU Layer
6. MaxPooling layer
7. Fully connected layer with output size of 512
8. ReLU Layer
9. Dropout layer with dropout probability 0.1
10. Fully connected layer with output size of 2 to classify stroke as hemorrhagic orischemic

11. Apply softmax layer
12. Classify image dataset using classification layer

DES DECRYPTION

In DES, the decryption process is incredibly straightforward. The algorithm's Feistel structure allows it to easily be reversed. The process is run almost exactly the same to decrypt information. The only difference is that the sub keys are applied in reverse. This is an efficient setup, because it means that the same software and hardware can be used in both the encryption and decryption processes.

To decrypt the data, it first goes through an initial permutation, then the block is split and the right half goes through the F function. The difference is that in the first round of decryption, the 16th subkey is applied. Everything else proceeds as normal. Once the F function is complete, it is XORed with the left side of the block.

The blocks are switched over and the result goes through the same process for the second round, with the only exception that the 15th subkey is applied. This process continues up until the 16th round, when the 1st subkey is used. Just like in the encryption process, the blocks aren't swapped in the final stage, and then the data undergoes a final permutation. This finishes the decryption process, resulting in the original plaintext of the message.

Take the text that has been encrypted with key one, then send it through the "decryption" process
with key two:

1. Key schedule – the 16 sub keys are derived from key three
2. Initial permutation
3. The block is split into left and right halves
4. The right half is sent through the F function

 Expansion permutation
 XOR with the sub key for the round
 Substitution
 Permutation

5. XOR the result of the F function with the left side
6. Make the old right side the new left side, and the result the new right side
7. Repeat the above steps 14 times
8. The right half is sent through the F function

 Expansion permutation
 XOR with the sub key for the 16th round
 Substitution

 Permutation

9. XOR the result of the F function with the left side
10. Combine the left and right sides of the block together
11. Final permutation

The result is the 3DES decrypted form data.

SYSTEM TESTING

It is a critical software quality assurance method. It ensure that the designed system network work properly based on the requirement of the user.

5.1 TESTING TYPES:

The testing process is classified into four types. They are

- System Testing
- Unit Testing
- Integration Testing
- Functional Testing

5.1.1 SYSTEM TESTING:

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

5.1.2 UNIT TESTING:

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit test sensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

INTEGRATION TESTING:

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

5.1.4 FUNCTION TESTING:

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

ValidInput : identified classes of valid input must be accepted. InvalidInput : identified classes of invalid input must be rejected. Functions : identified functions must beexercised.

Output : identified classes of application outputs must be exercised. Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

## VIII. RESULTS AND DISCUSSION

### MODULE IMPLEMENTATION

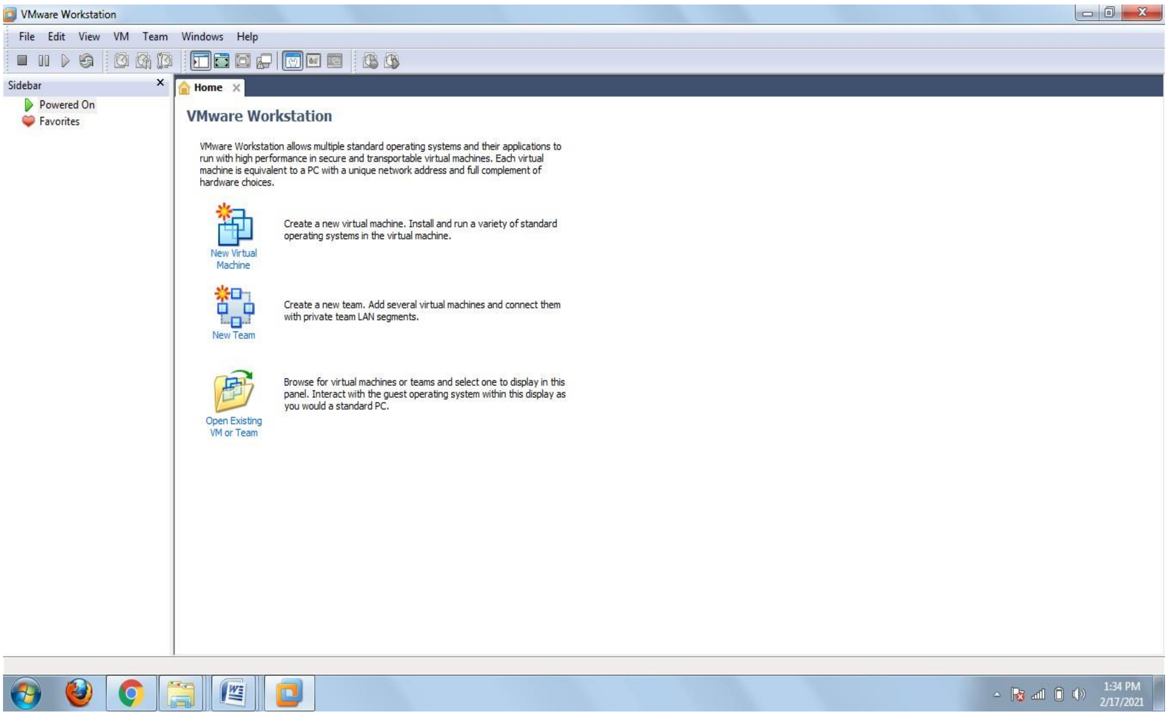
VMware Workstation Pro is a hosted hypervisor that runs on x64 versions of Windows and Linux operating system. It enables users to set up virtua machines (VMs) on a single physical machine and use them simultaneously along with the host machine. Each virtual machine can execute its own operating system, including versions of Microsoft Windows, Linux, BSD, and MS-DOS. VMware Workstation is developed and sold by VMware, a division of Dell Technologies. There is a free-of-charge version, VMware Workstation Player, for non- commercial use. An operating systems license is needed to use proprietary ones such as Windows. Ready-made Linux VMs set up for different purposes are available from several sources.

VMware Workstation supports bridging existing host network adapters and sharing physical disk drives and USB devices with a virtual machine. It can simulate disk drives; an ISO image file can be mounted as a virtual optical disc drive, and virtual hard disk drives are implemented as .vmdk files.

VMware Workstation Pro can save the state of a virtual machine (a "snapshot") at any instant. These snapshots can later be restored, effectively returning the virtual machine to the saved state, as it was and free from any post-snapshot damage to the VM.

VMware Workstation includes the ability to group multiple virtual machines in an inventory folder. The machines in such a folder can then be powered on and powered off as a single object, useful for testing complex client-server environments.

*VMware Home Screen:*



VMware Workstation

VMware Workstation allows multiple standard operating systems and their applications to run with high performance in secure and transportable virtual machines. Each virtual machine is equivalent to a PC with a unique network address and full complement of hardware choices.

Create a new virtual machine. Install and run a variety of standard operating systems in the virtual machine.

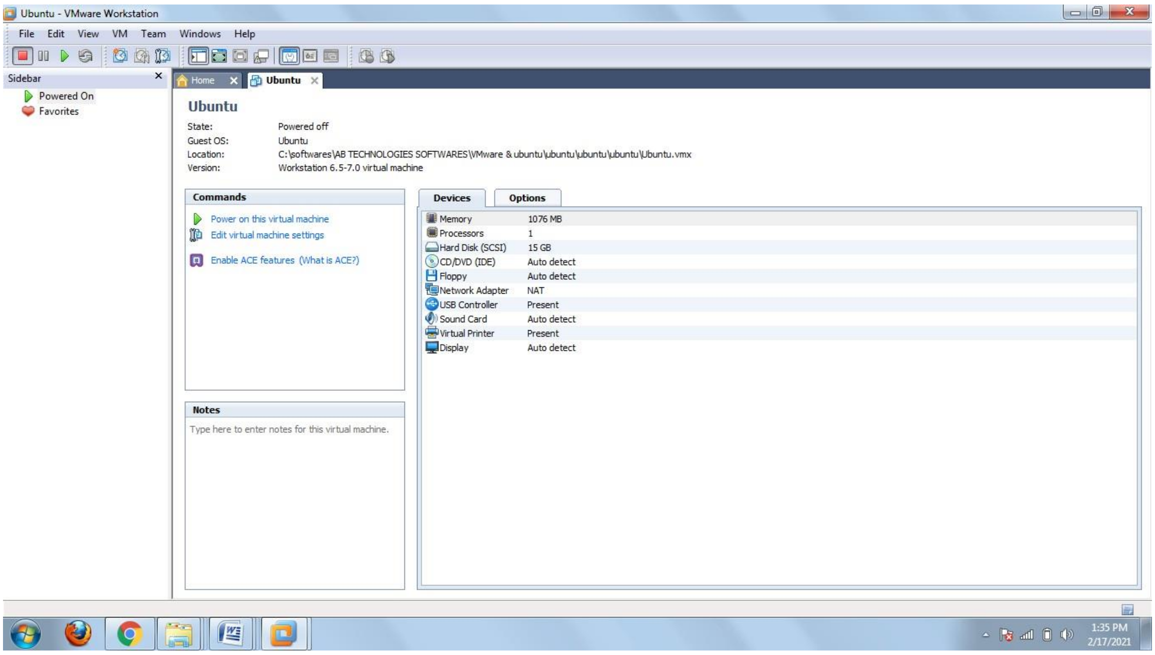
Create a new team. Add several virtual machines and connect them with private team LAN segments.

Browse for virtual machines or teams and select one to display in this panel. Interact with the guest operating system within this display as you would a standard PC.

**Figure 6.1 VMware Home Screen**

Ubuntu is built on Debian's architecture and infrastructure, and comprises Linux server, desktop and discontinued phone and tablet operating system versions. Ubuntu releases updated versions predictably every six months, and each release receives free support for nine months with security fixes, high-impact bug fixes and conservative, substantially beneficial low- risk bug fixes.The first release was in October 2004.

Current long-term support (LTS) releases are supported for five years, and are released every two years. Since the release of Ubuntu 6.06, every fourth release receives long-termsupport (LTS). Long-term support includes updates for new hardware, security patches and updates to the 'Ubuntu stack' (cloud computing infrastructure). The first LTS releases weresupported for three years on the desktop and five years on the server; since Ubuntu 12.04 LTS, desktop support for LTS releases was increased to five years as well. LTS releases get regular point releases with support for new hardware and integration of all the updates published in that series to date.


Ubuntu - VMware Workstation
File
Edit
View
VM
Team
Windows
Help
Sidebar
Powered On
Favorites
Home
Ubuntu
Commands
Power on this virtual machine
Edit virtual machine settings
Enable ACE features (What is ACE?)
Notes
Devices
Options
1:35 PM
2/17/2021

Ubuntu

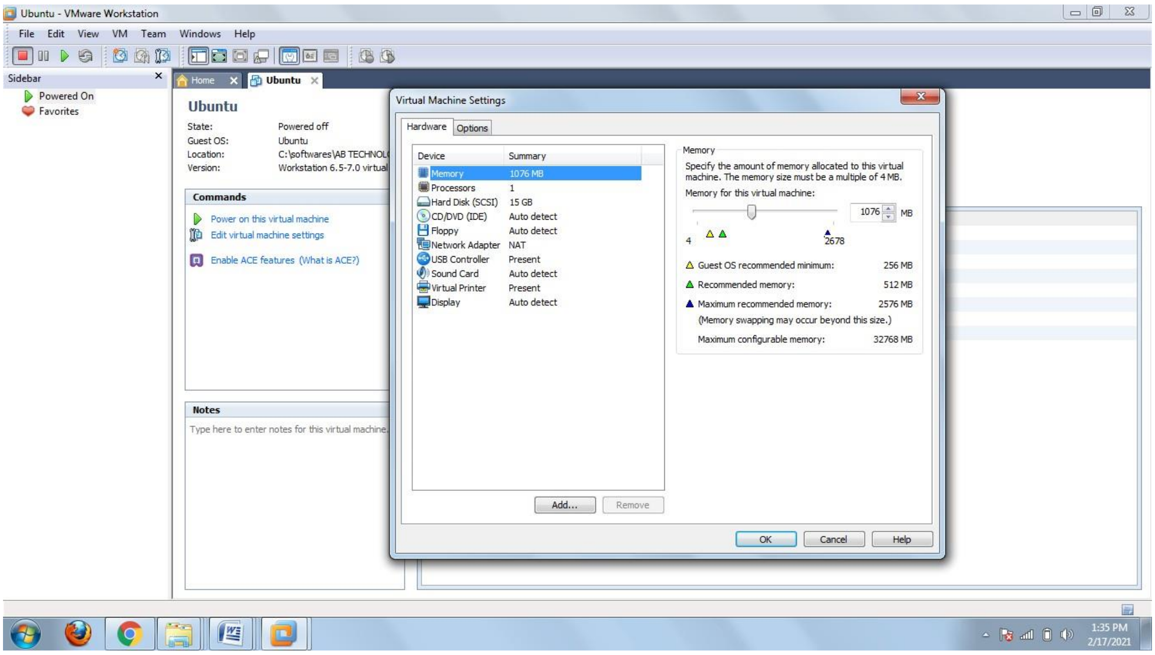
| | |
|---|---|
| State: | Powered off |
| Guest OS: | Ubuntu |
| Location: | C:\softwares\AB TECHNOLOGIES SOFTWARES\VMware & ubuntu\ubuntu\ubuntu\ubuntu\Ubuntu.vmx |
| Version: | Workstation 6.5-7.0 virtual machine |

Type here to enter notes for this virtual machine.

| | |
|---|---|
| Memory | 1076 MB |
| Processors | 1 |
| Hard Disk (SCSI) | 15 GB |
| CD/DVD (IDE) | Auto detect |
| Floppy | Auto detect |
| Network Adapter | NAT |
| USB Controller | Present |
| Sound Card | Auto detect |
| Virtual Printer | Present |
| Display | Auto detect |

*Figure 6.1(a) VMware Home Screen*

Ubuntu packages are based on packages from Debian's unstable branch, which are synchronised every six months. Both distributions use Debian's deb package format and package management tools (e.g. APT and Ubuntu Software). Debian and Ubuntu packages are not necessarily binary compatible with each other, however, so packages may need to be rebuilt fromsource to be used in Ubuntu. Many Ubuntu developers are also maintainers of key packages within Debian. Ubuntu cooperates with Debian by pushing changes back to Debian, although there has been criticism that this does not happen often enough. Ian Murdock, the founder of Debian, had expressed concern about Ubuntu packages potentially diverging too far from Debian to remain compatible. Before release, packages are imported from Debian unstable continuously and merged with Ubuntu-specific modifications. One month before release, imports are frozen, and packagers then work to ensure that the frozen features interoperate well together.


Ubuntu - VMware Workstation
File Edit View VM Team Windows Help
Sidebar
Powered On
Favorites
Home
Ubuntu
Commands
Power on this virtual machine
Edit virtual machine settings
Enable ACE features (What is ACE?)
Notes
Type here to enter notes for this virtual machine.
Virtual Machine Settings
Hardware
Options
Add...
Remove
OK
Cancel
Help
1:35 PM
2/17/2021

Ubuntu

State: Powered off
Guest OS: Ubuntu
Location: C:\softwares\AB TECHNOL
Version: Workstation 6.5-7.0 virtual

| Device | Summary |
|---|---|
| Memory | 1076 MB |
| Processors | 1 |
| Hard Disk (SCSI) | 15 GB |
| CD/DVD (IDE) | Auto detect |
| Floppy | Auto detect |
| Network Adapter | NAT |
| USB Controller | Present |
| Sound Card | Auto detect |
| Virtual Printer | Present |
| Display | Auto detect |

Memory

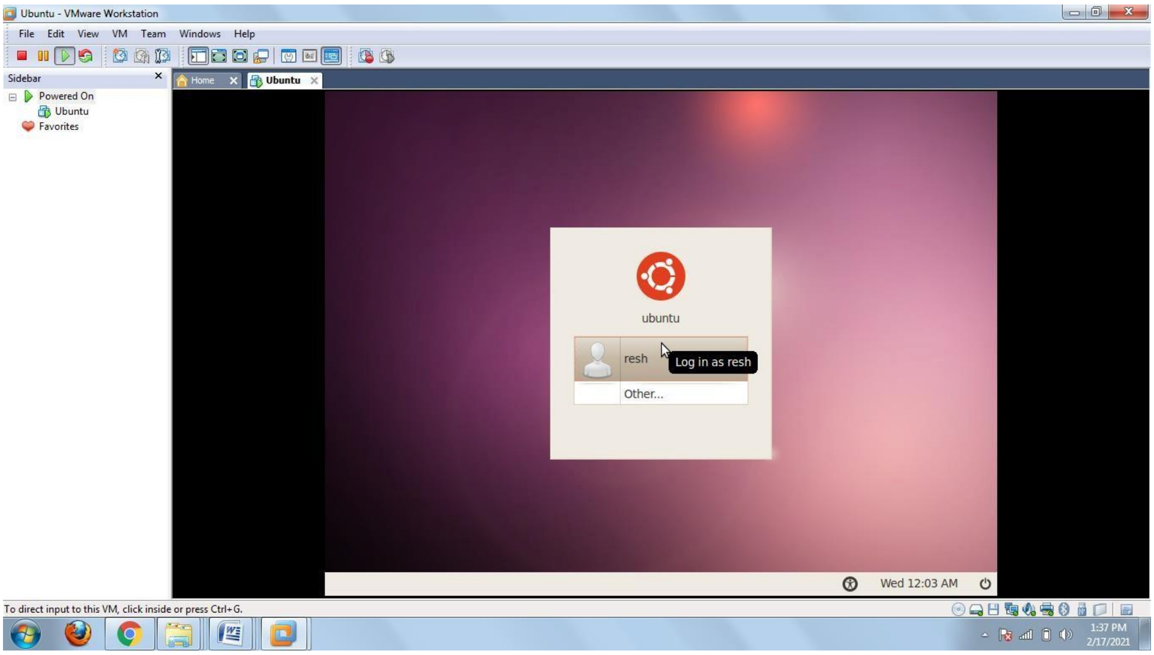
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 1076 MB

4 2678

| | |
|---|---|
| Guest OS recommended minimum: | 256 MB |
| Recommended memory: | 512 MB |
| Maximum recommended memory: | 2576 MB |
| (Memory swapping may occur beyond this size.) | |
| Maximum configurable memory: | 32768 MB |

## LOGIN PAGE:



To direct input to this VM, click inside or press Ctrl+G.

Figure 6.2 Login Page

## UBUNTU HOME SCREEN:

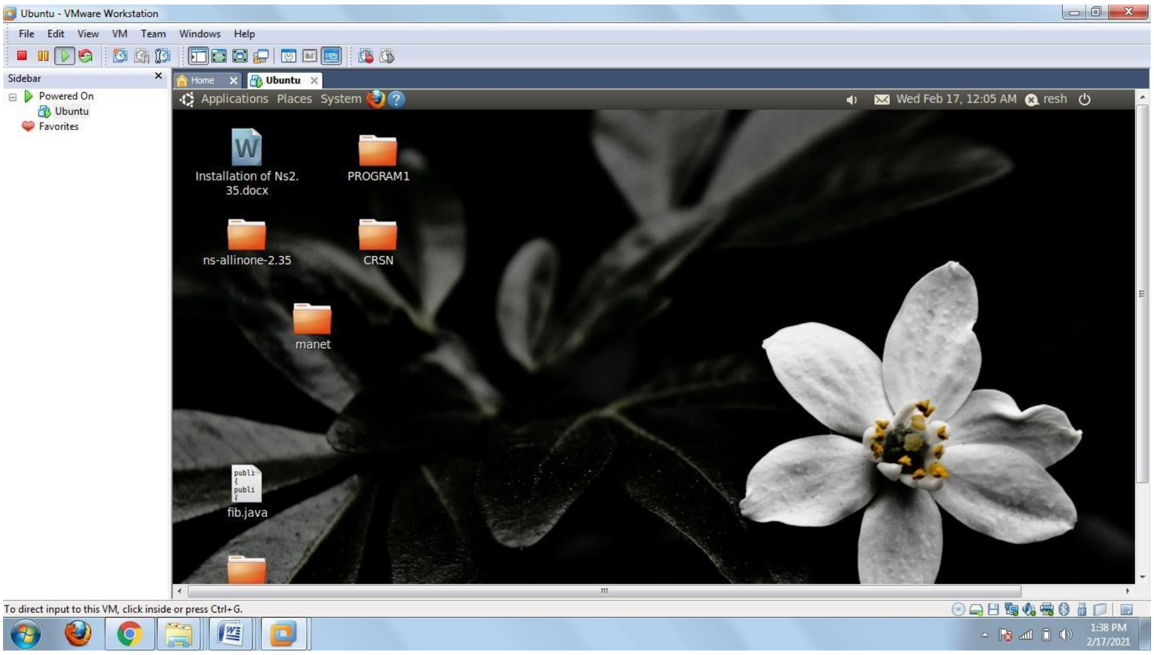
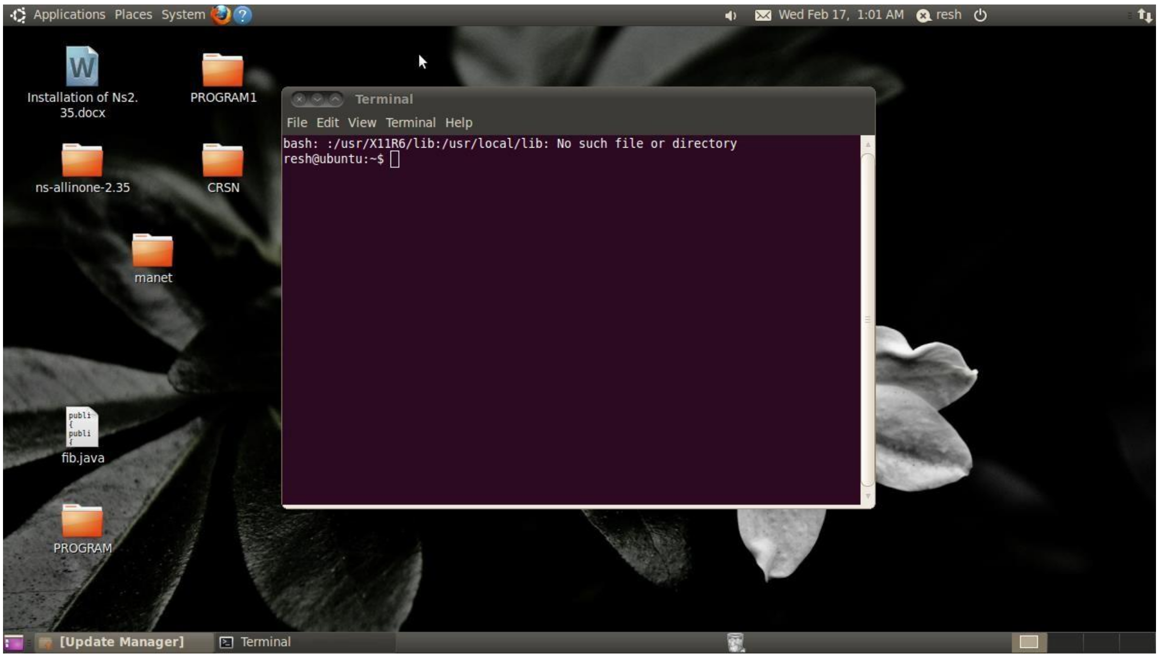

Ubuntu - VMware Workstation
File Edit View VM Team Windows Help
Sidebar
Powered On
Ubuntu
Favorites
Home
Ubuntu
Applications Places System
Wed Feb 17, 12:05 AM
resh
Installation of Ns2.35.docx
PROGRAM1
ns-allinone-2.35
CRSN
manet
fib.java
To direct input to this VM, click inside or press Ctrl+G.
1:38 PM
2/17/2021

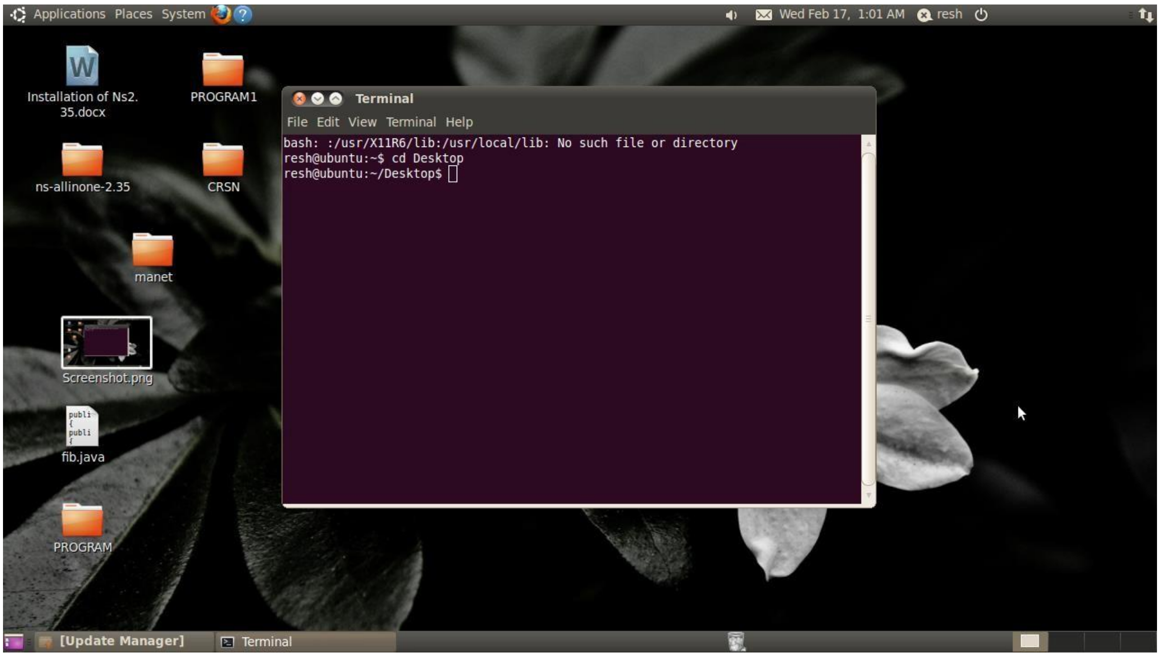
*Figure 6.3 Ubuntu Home Screen*

To access the pop-up menu, click on application → terminal. A command window will open.



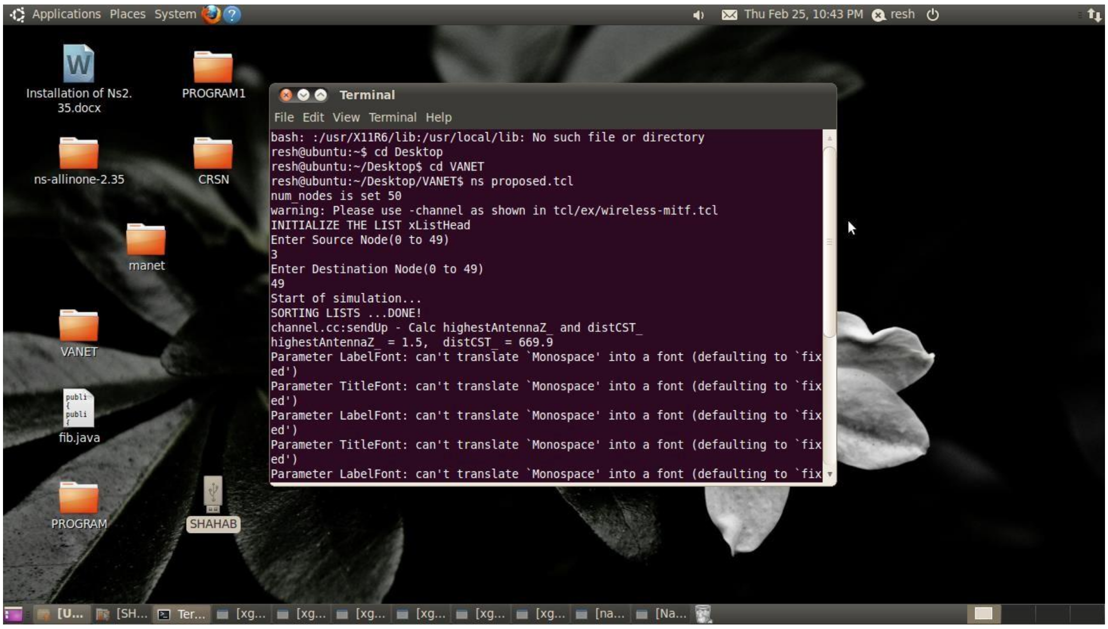
```
bash: :/usr/X11R6/lib:/usr/local/lib: No such file or directory
resh@ubuntu:~$ 
```

Type cd Desktop to direct the command window to desktop.



```
bash: :/usr/X11R6/lib:/usr/local/lib: No such file or directory
resh@ubuntu:~$ cd Desktop
resh@ubuntu:~/Desktop$ 
```

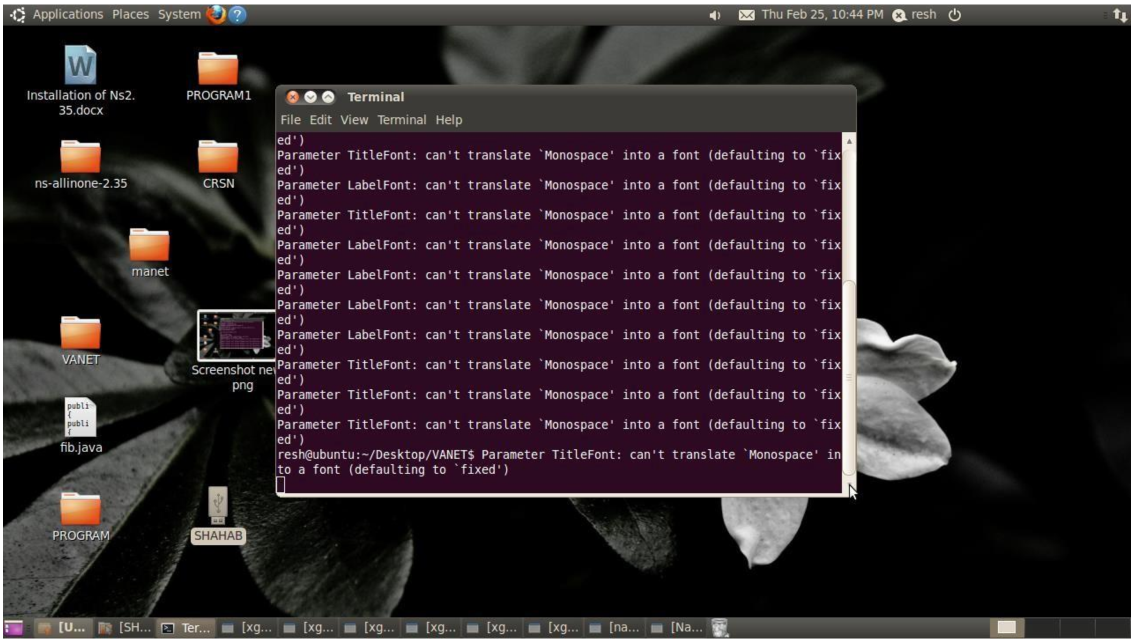
Type cd folder name where the program file is stored.



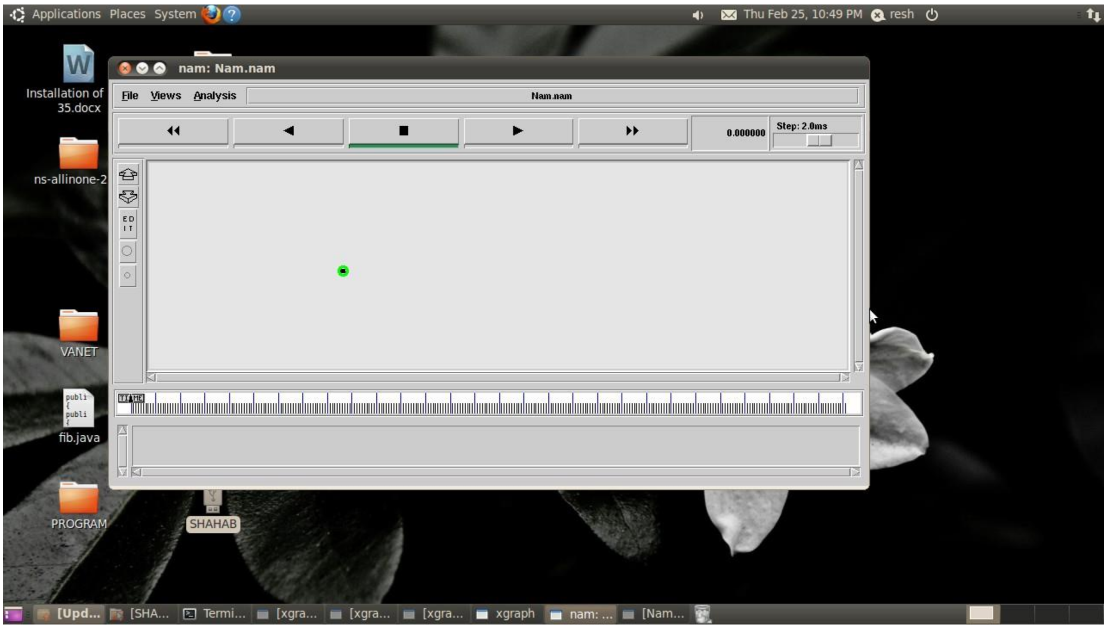
```
bash: :/usr/X11R6/lib:/usr/local/lib: No such file or directory
resh@ubuntu:~$ cd Desktop
resh@ubuntu:~/Desktop$ cd VANET
resh@ubuntu:~/Desktop/VANET$ ns proposed.tcl
num_nodes is set 50
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Enter Source Node(0 to 49)
3
Enter Destination Node(0 to 49)
49
Start of simulation...
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 669.9
Parameter LabelFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter TitleFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter LabelFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter TitleFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter LabelFont: can't translate `Monospace' into a font (defaulting to `fix
```

Type ns proposed.tcl and press enter. A command window as shown in above figure willappear. Initially the network assigns a total of 50 nodes.

The source node and destination node has to be decided by the user. The network selects numberof antennas for data transmission between source node and destination node.



```
ed')
Parameter TitleFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter LabelFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter TitleFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter LabelFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter LabelFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter LabelFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter LabelFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter TitleFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter TitleFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
Parameter TitleFont: can't translate `Monospace' into a font (defaulting to `fix
ed')
resh@ubuntu:~/Desktop/VANET$ Parameter TitleFont: can't translate `Monospace' in
to a font (defaulting to `fixed')
```



## NODE CREATION

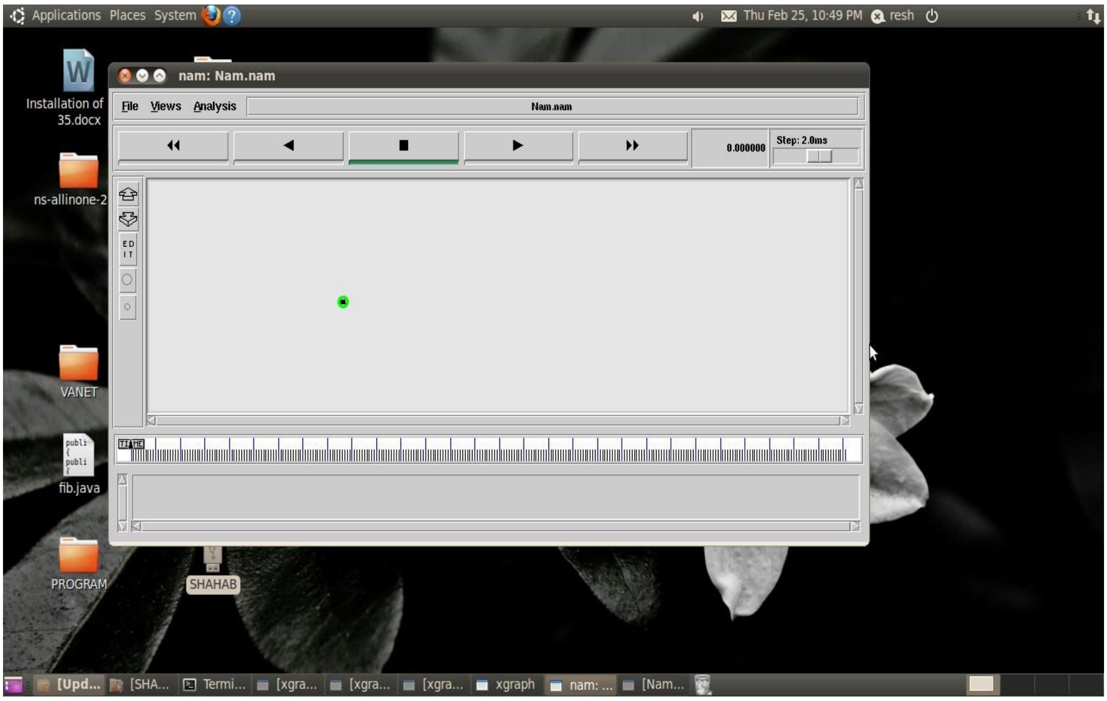
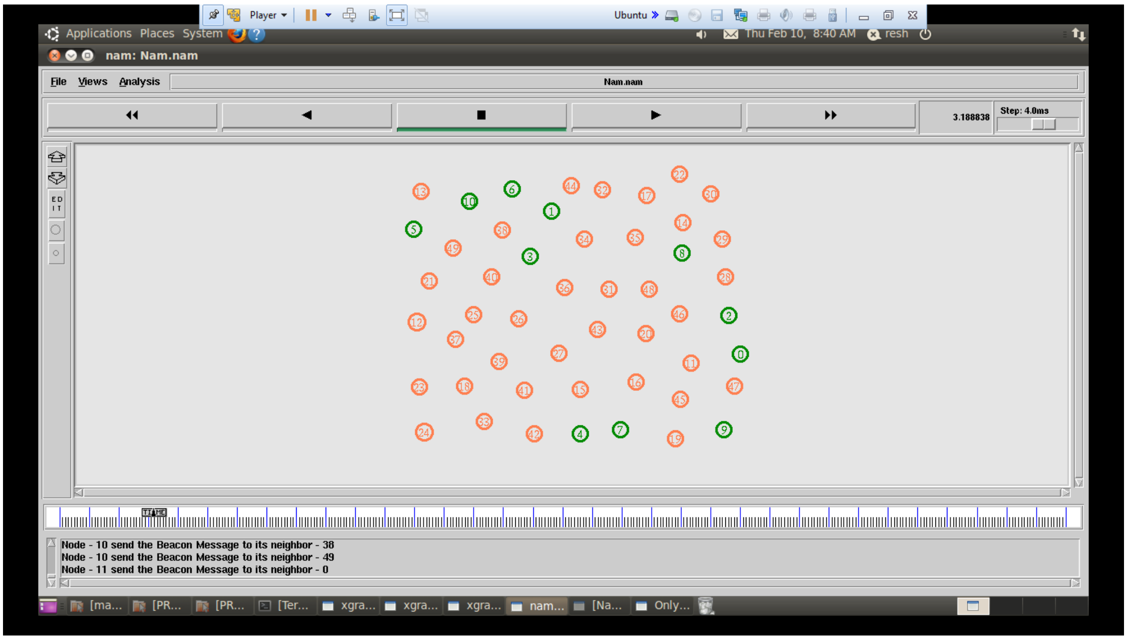


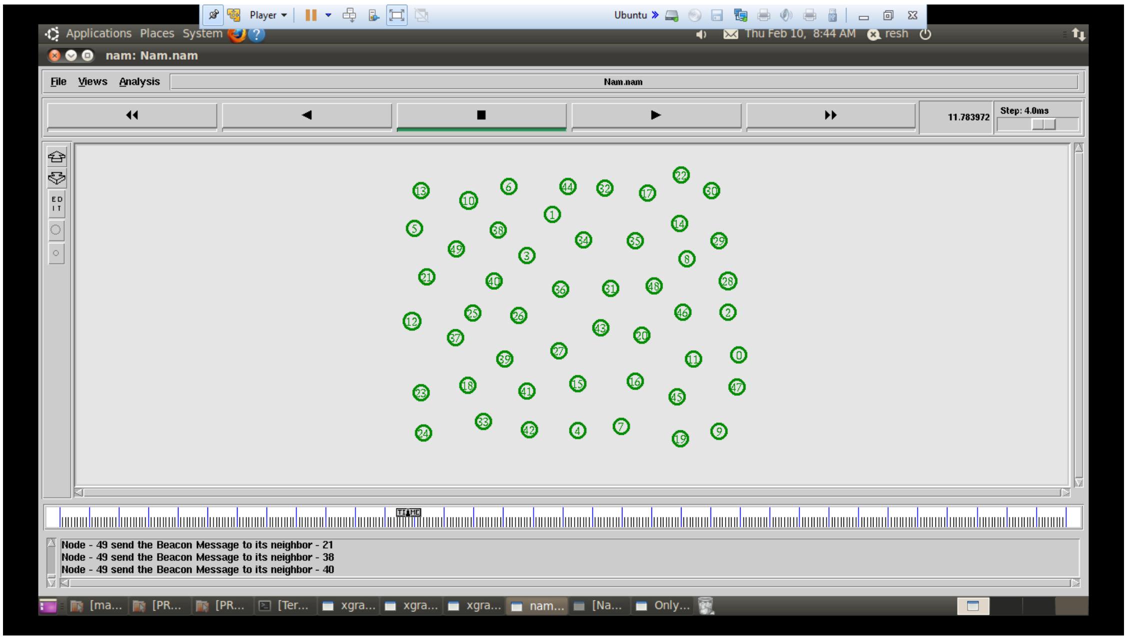
**Figure 6.4** NODE Creation

## NEIGHBOUR NODE DISCOVERY



```
Node - 10 send the Beacon Message to its neighbor - 38
Node - 10 send the Beacon Message to its neighbor - 49
Node - 11 send the Beacon Message to its neighbor - 0
```

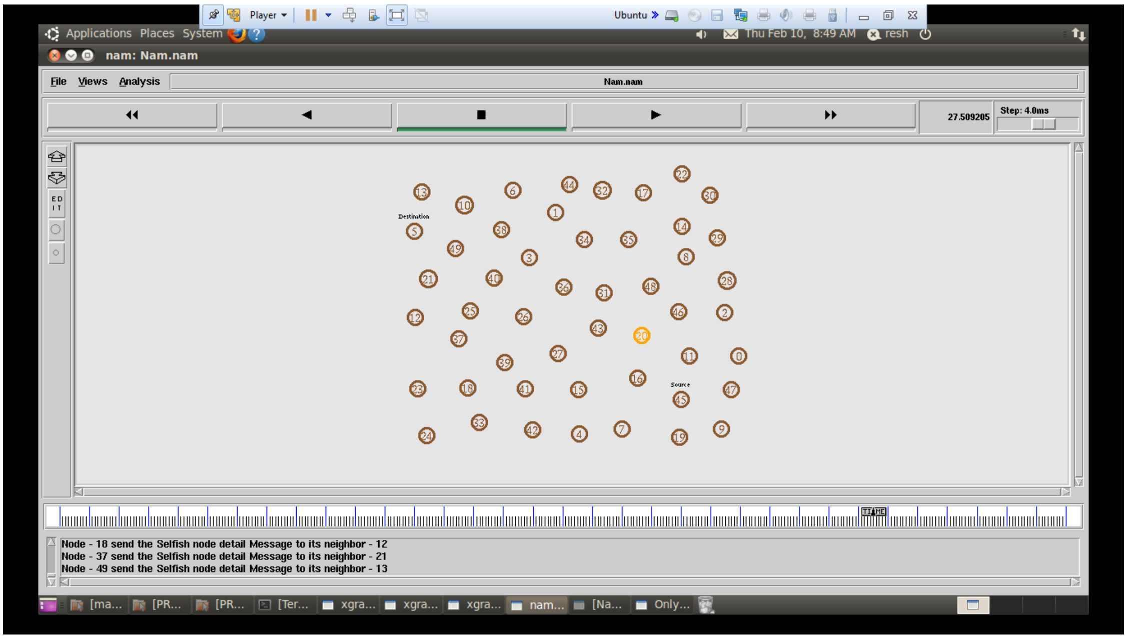
**Figure 6.4 (a)** Neighbor Node Discovery



```
Node - 49 send the Beacon Message to its neighbor - 21
Node - 49 send the Beacon Message to its neighbor - 38
Node - 49 send the Beacon Message to its neighbor - 40
```

**Figure 6.4 (b)** Neighbor Node Discovery

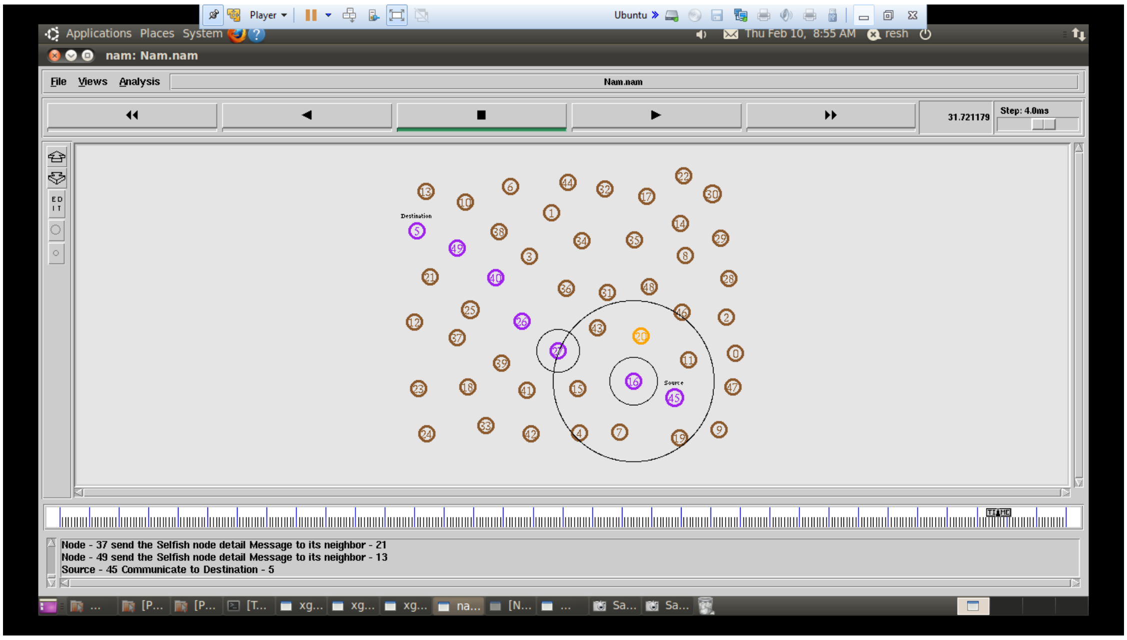
## ROUTING PATH CREATION



```
Node - 18 send the Selfish node detail Message to its neighbor - 12
Node - 37 send the Selfish node detail Message to its neighbor - 21
Node - 49 send the Selfish node detail Message to its neighbor - 13
```

**Figure 6.5** Routing Path Creation

## FINAL ROUTING PATH FOR THE DATA TRANSMISSION



```
Node - 37 send the Selfish node detail Message to its neighbor - 21
Node - 49 send the Selfish node detail Message to its neighbor - 13
Source - 45 Communicate to Destination - 5
```

***Figure 6.6 Final Routing Path For The Data Transmission***

The anchor node formation between source node and anchor node. In this project main objective is to minimize the energy consumption.

## THROUGHPUT

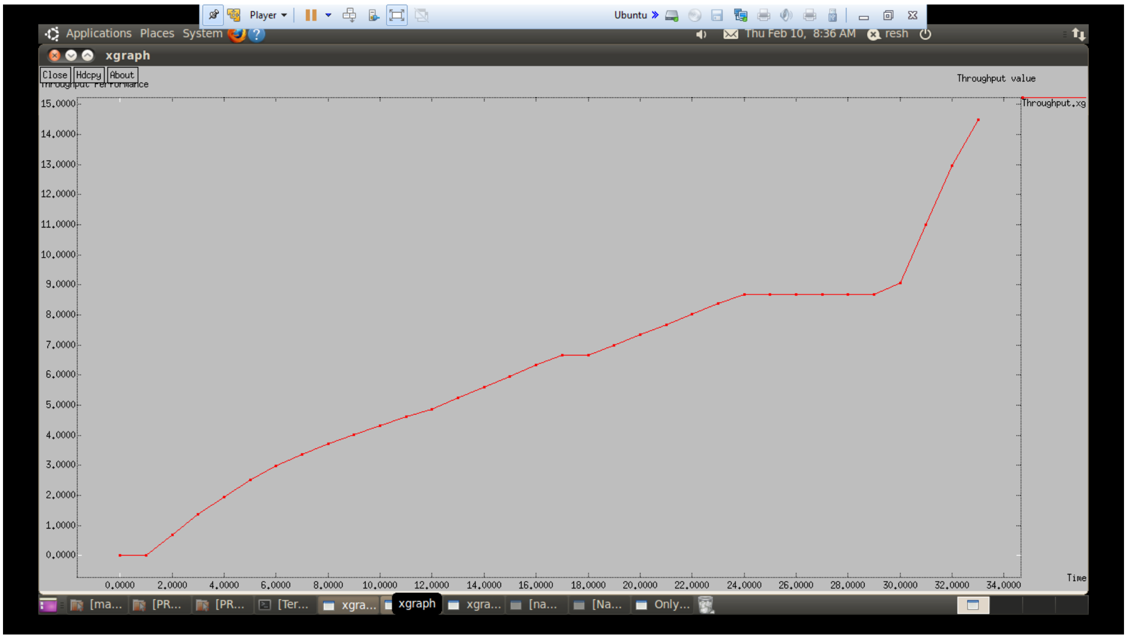


**Figure 6.7** Throughput

In data transmission, network throughput is the amount of data moved successfully on communication channel, the data that these messages contain may be delivered over physical or logical data.

## PACKET DELIVERY RATIO

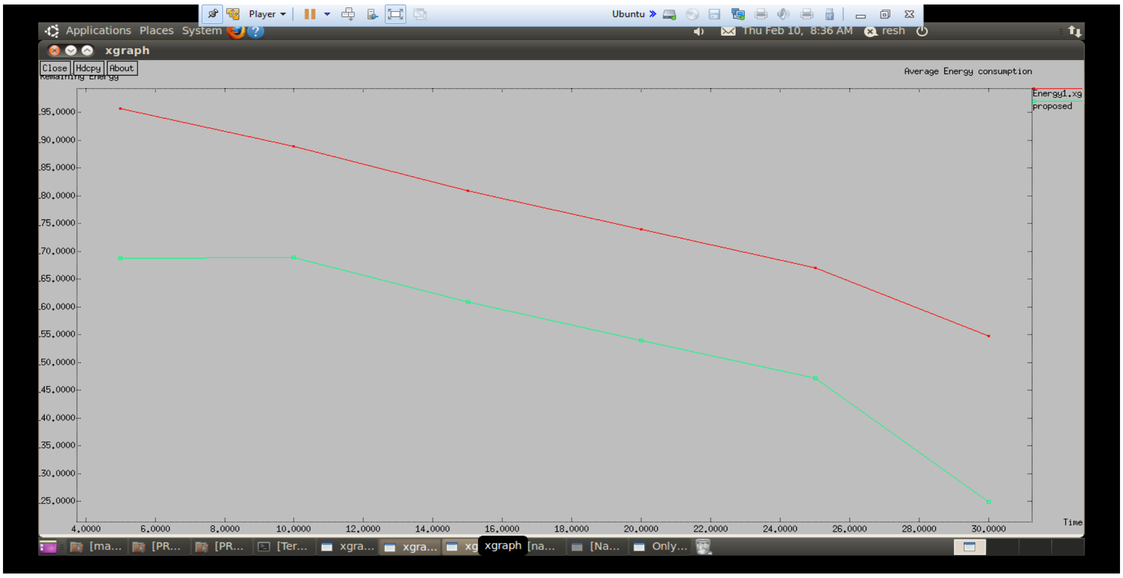


**Figure 6.8** Packet Delivery Ratio

The packet delivery ratio can be obtained from the total number of data packets arrived at destinations divided by the total data packets sent from sources. In other words Packet delivery ratio is the ratio of number of packets received at the destination to the number of packets sent from the source.

## IX. CONCLUSION

In this project an improved MANET routing authentication technique. To accomplish isolation, high performance, and improved anomaly detection, a 3DES technique is presented. The techniques for encryption and decryption are more effective. Three keys have been created in this system, resulting in three alternative key configurations for the 3DES implementation. The CNN (Convolutional Neural Network) technique is used to implement the routing mechanism. The MANET operation is successfully realised by this CNN algorithm. The primary benefit of adopting CNN is speed. The time it takes for CNN to make a decision is constant. The findings demonstrate that the CNN is capable of accelerating packet delivery with an average rise in networks with some malicious nodes. It simultaneously boosts the network's connection rate in the face of several attacks. PDR, throughput, and latency have been used as the metrics for performance analysis.

## X. REFERENCES

[1]. L. Lei Deng; Fang Liu; Yijin Zhang; Wing Shing Wong, 2021, “Delay-Constrained Topology-Transparent Distributed Scheduling for MANETs”, IEEE Transactions on Vehicular Technology, vol: 70, no: 01, pp: 1083 – 1088.

[2]. Carlo Kleber da Silva Rodrigues; Vladimir Emiliano Moreira Rocha, 2019, “BT-MANET: A Novel BitTorrent-Like Algorithm for Video On-Demand Streaming over MANETs”, IEEE Latin America Transactions, vol: 17, no: 01, pp: 78 – 84.

[3]. Taj Rahman; InamUllah; Ateeq Ur Rehman; Rizwan Ali Naqvi, 2020, “Notice of Violation of IEEE Publication Principles: Clustering Schemes in MANETs: Performance Evaluation, Open Challenges, and Proposed Solutions”, IEEE Access, vol: 08, pp: 25135 – 25158.

[4]. Ruo Jun Cai; Xue Jun Li; Peter Han Joo Chong, 2019, “An Evolutionary Self-Cooperative Trust Scheme against Routing Disruptions in MANETs”, IEEE Transactions on Mobile Computing, vol: 18, no: 01, pp: 42 – 55.

[5]. Masood Ahmad; Abdul Hameed; Ataul Aziz Ikram; Ishtiaq Wahid, 2019, “State-of-the-Art Clustering Schemes in Mobile Ad Hoc Networks: Objectives, Challenges, and Future Directions’, IEEE Access, vol: 07, pp: 17067 – 17081.

[6]. TaoufikYeferny; Sofian Hamad; Sadok Ben Yahia, 2019, “Query Learning-Based Scheme for Pertinent Resource Lookup in Mobile P2P Networks”, IEEE Access, vol: 07, pp: 49059 – 49068.

[7]. BurhanUl Islam Khan; Farhat Anwar; Rashidah F. Olanrewaju; Miss LaihaBinti Mat Kiah; Roohie N. Mir, 2021, “Game Theory Analysis and Modeling of Sophisticated Multi-Collusion Attack in MANETs”, IEEE Access, vol: 09, pp: 61778 – 61792.

[8]. Nousheen Akhtar; Muazzam A. Khan; Ata Ullah; Muhammad YounusJaved, 2019, “Congestion Avoidance for Smart Devices by Caching Information in MANETS and IoT”, IEEE Access, vol: 07, pp: 71459 – 71471.

[9]. Osamah Ibrahim Khalaf; F. Ajesh; Abdulsattar Abdullah Hamad; GiaNhu Nguyen; Dac-Nhuong Le, 2020, “Efficient Dual-Cooperative

Bait Detection Scheme for Collaborative Attackers on Mobile Ad-Hoc Networks", IEEE Access, vol: 08, pp: 227962 – 227969.

[10]. Jae Seang Lee; Yoon-SikYoo; HyungSeok Choi; Taejoon Kim; Jun Kyun Choi, 2019, "Energy-Efficient TDMA Scheduling for UVS Tactical MANET", IEEE Communications Letters, vol: 23, no: 11, pp: 2126 – 2129.

[11]. BabatundeOjetunde; Naoki Shibata; JuntaoGao, 2019, "Secure Payment System Utilizing MANET for Disaster Areas", IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol: 49, no: 12, pp: 2651 – 2663.

[12]. Fifi Farouk; Yasmin Alkady; RawyaRizk, 2020, "Efficient Privacy-Preserving Scheme for Location Based Services in VANET System", IEEE Access, vol: 08, pp: 60101 – 60116.

[13]. Jae Seang Lee; Yoon-SikYoo; Hyungseok Choi; Taejoon Kim; Jun Kyun Choi, 2020, "Group Connectivity-Based UAV Positioning and Data Slot Allocation for Tactical MANET", IEEE Access, vol: 08, pp: 220570 – 220584.

[14]. M. Sivaram; V. Porkodi; Amin Salih Mohammed; V. Manikandan; N. Yuvaraj, 2019, "Retransmission DBTMA Protocol with Fast Retransmission Strategy to Improve the Performance of MANETs", IEEE Access, vol: 07, pp: 85098 – 85109.

[15]. Bin Yang; Zhenqiang Wu; Yuanyuan Fan; Xiaohong Jiang; Shikai Shen, 2019, "Non-Asymptotic Capacity Study in Multicast Mobile Ad Hoc Networks", IEEE Access, vol: 07, pp: 115109 – 115121.

[16]. BurhanUl Islam Khan; Farhat Anwar; RashidahFunkeOlanrewaju; BismaRasoolPampori; RoohieNaaz Mir, 2020, "A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission with Optimized Network Operations in Futuristic Mobile Adhoc Networks", IEEE Access, vol: 08, pp: 124097 – 124109.

[17]. Jingwen Bai; Yan Sun; Chris Phillips; Yue Cao, 2018, "Toward Constructive Relay-Based Cooperative Routing in MANETs", IEEE Systems Journal, vol: 12, no: 02, pp: 1743 – 1754.

[18]. Waheb A. Jabbar; WasanKadhimSaad; Mahamod Ismail, 2018, "MEQSA-OLSRv2: A Multicriteria-Based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT", IEEE Access, vol: 06, pp: 76546 – 76572.

[19]. Rutvij H. Jhaveri; Narendra M. Patel; YubinZhong; Arun Kumar Sangaiah, 2018, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT", IEEE Access, vol: 06, pp: 20085 – 20103.

[20]. Zhinan Li; Yinfeng Wu, 2017, "Smooth Mobility and Link Reliability-Based Optimized Link State Routing Scheme for MANETs", IEEE Communications Letters, vol: 21, no: 07, pp: 1529 – 1532.

**Cite this article as :**

Sathish Kumar R, Ravi Shankar R, Sathish Kumar S,