IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

COLLABORATE FRAMEWORK BASED ON SOFTWARE DEFINED NETWORK IN MANET

[1]Mr.S.Praveen Kumar, [2]Mr.D.Magesh, [3]Ms.Priya.N, [4]Ms. Gomathy.A [5]Dr.S.Uma
[1]PG Scholar, [2-4]Assistant Professor, [5]Research Coordinator
[1-4]Departement of Computer Science,
Hindusthan College of Engineering and Technology, Coimbatore.

ABSTRACT

Create a novel network model for mobile ad hoc network (MANET) nodes and actors in wireless sensor networks to collaborate on event processing. There are two stages in the development of distributed algorithms: setup and negotiation. The first uses weighted proportional max-min fairness to initially allocate MANET nodes across event zones, whereas the latter uses a market-based method to re-distribute the number of MANET nodes based on existing and new events. A detection technique for malicious packet dropping attacks in MANETs. The mechanism of the suggested approach is Collaborative Convolutional Neural Network (CCNN), which is based on the reputation value computed for that node by its neighbours. A node's reputation value is determined by its network packet forwarding behaviour. The reputation information is collected, saved, and transferred between nodes before being calculated under various scenarios. A network simulator was used to test the proposed protocol. The simulation results demonstrate the effectiveness of its performance. Even in the presence of cryptographic procedures, our method incurs negligible network bandwidth and latency costs. Moreover, we demonstrate that the protection is still effective in the presence of misbehaving nodes and routing changes caused by mobility. While further research is needed to thoroughly evaluate our method, we feel that the concept of collaborative security in MANETs is a potential future area.

Key Words: MANET, TCP/IP, CCNN, ADHOC

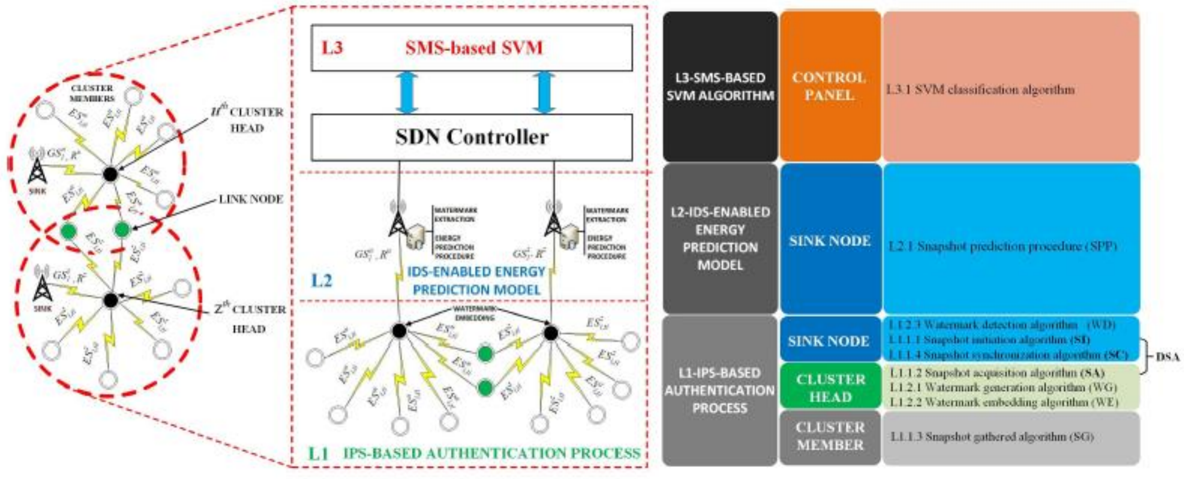
INTRODUCTION

A Mobile Ad hoc Network (MANET) is a peer-to-peer network of mobile nodes that may interact with one another without the use of an underlying infrastructure. Wireless connections let nodes to interact directly with their neighbours (i.e., nodes within radio range). In any case, non-neighboring nodes can interact as well by employing other intermediary nodes as relays that forward packets to destinations. Using firewalls, harmful nodes and traffic are kept away from a set of nodes belonging to an organization or a group in conventional networks. Because of the existence of a well-defined network boundary, this is possible. All incoming and outgoing traffic must pass via these firewall nodes, which enforce perimeter restrictions. To solve this, we have suggested a deny-by-default architecture for MANETs that enforces trust relationships and traffic responsibility across mobile nodes using a distributed policy enforcement system. The premise of a collaborative application is that individuals may exchange information. It is becoming increasingly relevant in all situations, from social to topical, on a daily basis. The collaborative application may be used for emergency search and rescue operations, idea and information exchange at meetings or conferences, field survey activities in remote locations, group activity when no visible contact is possible, security purposes, military operations, and more. As a result, numerous mobile applications were necessary for various purposes. This study also discusses previous research in this field and proposes a prototyping strategy for designing a collaborative application platform.

The Routing protocols in mobile ad hoc networks (MANETs) are subject to many forms of security risks due to the lack of central authority and the unreliability of wireless connectivity. The resource-constrained nature of MANETs, along with constantly altering topology and frequent network segmentation, adds to the security issues in MANET routing.

In MANETs, trust may be defined as the extent to which a node can meet the expectations of other nodes as specified by an underlying communication protocol. Each node in the network controls an individual trust table to compute and store the trust values of other nodes in trust-based security methods. The calculated trust levels of the nodes are used to make routing decisions.

Further, having a single trust characteristic may not properly address the issue of selective misbehaviour. Because existing schemes employ a single trust attribute, the aforementioned selectively misbehaving node is marked malicious and segregated from the routing path, and therefore no longer accessible for use in other network operations. Each node in a trust-based security system gathers two kinds of information about other nodes: first-hand information (based on self-observations) and second-hand information (based on the other node observations). Data sparsity is a scenario in trust-based security systems in which a lack of information or insufficient interaction experience makes evaluating the node's trust challenging, particularly during the early stages of network setup.


CLUSTER MEMBERS
Hth CLUSTER HEAD
LINK NODE
Zth CLUSTER HEAD
SINK
L3
SMS-based SVM
SDN Controller
L2
WATERMARK EXTRACTION
ENERGY PREDICTION PROCEDURE
IDS-ENABLED ENERGY PREDICTION MODEL
WATERMARK EMBEDDING
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
L1.2.3 Watermark detection algorithm (WD)
L1.1.1 Snapshot initiation algorithm (SI)
L1.1.4 Snapshot synchronization algorithm (SC)
DSA
CLUSTER HEAD
L1.1.2 Snapshot acquisition algorithm (SA)
L1.2.1 Watermark generation algorithm (WG)
L1.2.2 Watermark embedding algorithm (WE)
CLUSTER MEMBER
L1.1.3 Snapshot gathered algorithm (SG)

(a) SDN-based three layers' framework (b) Security framework stack

Figure 1.SDN Based Three layer and Security Framework Stack

The building and operation of hydropower plants involves not only hydropower generation but also facility observation, quality monitoring, dangerous creature tracking, and so on, necessitating mobile and collaborative monitoring capabilities. MANET (Mobile Ad Hoc Networks) are a viable alternative for such jobs due to their mobility, flexibility, and robustness in a turbulent networking environment. Nonetheless, its scattered topology precludes MANET nodes from collaborating ineffectively. SDN (Software-Defined Networking) enables centralized control over network infrastructure.

DISADVANTAGES

- Wasted band width
- Delay
- Increasing Network congestion
- External sources for destination location

PROPOSED SYSTEM

The ad hoc network allows you to connect in a diverse environment without relying on a centralised strategy. It is generated automatically when two or more devices are connected. Mobile Ad-hoc Networks (MANETs) enable wireless networks to establish connections without the requirement for infrastructure by allowing nodes to deliver packets to each other. Such networks provide greater flexibility but need more complicated routing strategies. In this paper, we proposed a new routing method based on Collaborative Convolutional Neural Network (CCNN) that distributes computations in a Software Defined Network (SDN) controller and the nodes so that no redundant computations are executed in the nodes, thereby conserving the limited resources available on these nodes.

ADVANTAGES

- Data security and safety
- Efficient to manage the traffic
- Low routing Latency
- State Information

In order to offer scalability for large-scale WSN and enhance the efficiency of the authentication operation, each link node must respond to all of them. The energy status of the cluster heads is integrated into the global energy state obtained by them prior to data transmission.

$$\mathbf{GS}_l^u = [ES_{1,t_1}^u, ES_{2,t_2}^u \ldots, ES_{i,t_i}^u],$$

The cluster head then averages the GS^u_l vector to generate the kth u fingerprint using the following equation.

$$k_u^{\text{th}} = \mathrm{E}[\mathbf{GS}_l^u],$$

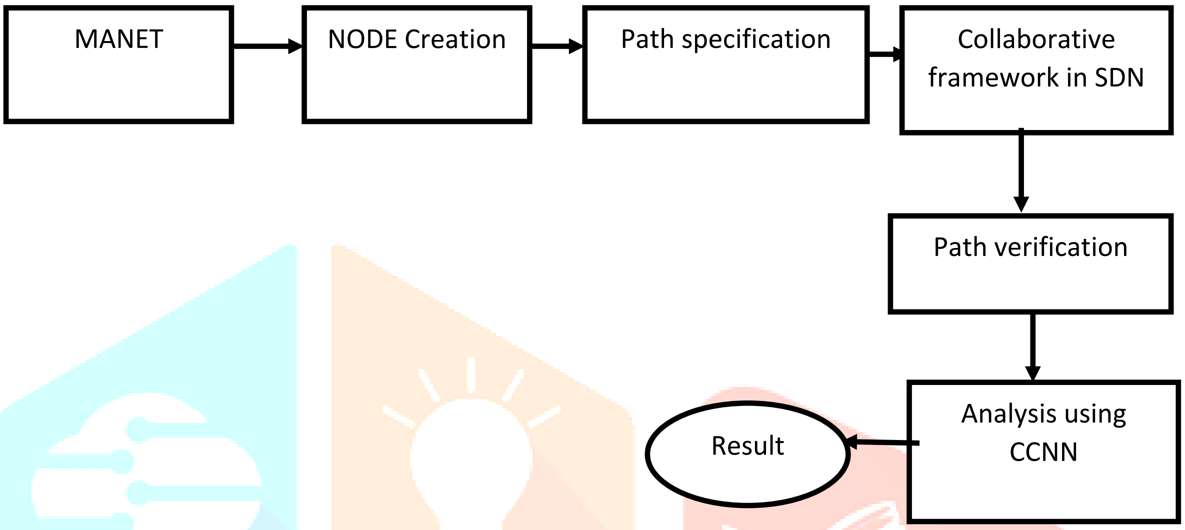


FIGURE 2 OVERALL PROPOSED SYSTEM ARCHITECTURE

The Random value of each snapshot is calculated by introducing the most significant bits of the sent data, GS^u_l and the kth u key into a random function. The kth u key is the same as in WG. The parameter vu Authorized verification. Nevertheless, once the control plane receives the watermarked dataset, Algorithm 7 is immediately executed to verify the sink node's authenticity and recover the labeled dataset to execute the SVM classification algorithm. As a result, the malicious misclassified nodes will be segregated from the data plane by removing them from the Open Flow table. Therefore, the set of data received by the control plane is linearly separable, where the distance between the hyperplane and the set of points Xi is 1/w . Therefore, the margin of the separation hyperplane is defined by 2/w . The learning problem is reformulated, since by minimizing w2 = wT , w becomes subject to the linear separation limitation

MODULES DESCRIPTION

SOURCE NODE

Based on the source's location privacy protection technique, which is predicted on the phantom source node, the source's location privacy protection has a relatively low security period. The algorithm uses the coordinates of the source and sink nodes to choose a node at random in the elliptic and direction to establish the common phantom sound source node of the ellipse utilised phantom sound source node.

ROUTING PATH

COLLABORATIVE CONVOLUTIONAL NEURAL NETWORK

SECURE COMMUNICATION

The aforementioned approach will extract the abnormal features of the time series and intrusion statistics from the analytical model, deconstructing the various non-linear components of the transmission stream in a wireless network with low detection accuracy. The kind and detection mechanism of a wireless network intrusion detection system are investigated. It employs a statistical analysis approach to gather data.

DESTINATION NODE

The destination node does not have enough resources to conduct both encoding and decoding concurrently. Furthermore, the destination node, computational power, and storage capacity of many terminals are restricted. The simulation results suggest that it is feasible to optimise decoding algorithms in order to effectively minimise the decoding burden to the destination node.

SYSTEM DESIGN

INTRODUCTION

The framework configuration report displays the framework requirements, work and subsystem construction, documents, information base plan, input design, yield format, Human Machine Interfaces, point-by-point configuration, handling reasoning, and an outside interface.

EXECUTIVE SUMMARY OF THE PROJECT

A project for the construction of a framework and overview from management's perspective provides a conceptual system design in this area. It may contain information that is described in a subsequent part of the abstract if applicable.

PROCESS OF SYSTEM OVERVIEW

This section depicts the framework's organizational narrative using non-specialized words. It should provide a generic framework design graph representing a subfield framework when suitable. Figure level frameworks design or subsystem, if applicable, should indicate the interface to external frameworks. If material, and provides a block diagram of high level frameworks and subsystems.

CONSTRAINTS ON THE DESIGN

This part (a trade-off, productivity with other systems, and analysis of competitive estimates of utilization and resources) will introduce the constraints of the system design, which is a design produced by the project team. The following assumptions will be made by the system.

PLANNING FOR SOFTWARE DESIGN

The programming module is the framework's most basic level of plan molecule size. At least one module of this framework exists, according to the various programming advancement approach. This section should provide reasoning and appropriate details for composing all of the modules required for the information in the source code in the framework (or coordinated COTS programming program).

PROCESS OF INPUT DESIGN

Design, user-entered data is a computer-based format that has begun to enter the process. The full screen must be seen in this manner for simple input validation of the design of the input screen without violating it. The most prevalent source of mistake in data processing is incorrect input data.

- Effectiveness
- Accuracy
- Ease of Use
- Consistency
- Simplicity
- Attractiveness

THE FUNDAMENTAL GOAL OF PLANNING INPUT CENTERS:

- Controlling the amount of input required
- Avoiding delayed response
- Controlling errors
- Keeping process simple
- Avoiding errors
- Delivering savvy technique for input.
- Accomplishing the most elevated conceivable degree of exactness.
- Guarantee that the information is satisfactory to and perceived by the staff.

PROCESS OF OUTPUT DESIGN

Returning to the information is a common method in the improvement framework. As comments and reports are generated by the framework, they must be sent to the client. They can also be used as a permanent replica for the check later on.

YIELD DESIGN CONSIDERATION

The motivation behind the yield is to be perceived; to examine the effectiveness of the contained data, it should be confirmed. From there on, the yield is characterized.

- Name of the Output
- Content
- Format
- Frequency

OUTPUTS

This segment depicts the client/yield of the working framework's plan; it demonstrates planning to the important level information stream represented in the segment.

- Unmistakable code and name verification for reports and data display displays.
- Illustration of report and screen content (give a sensible depiction of each arrange and portray all data segments related with the plan or reference the data word reference)
- The depiction of the explanation for the yield, incorporating differentiating proof of the key clientele
- Report any dispersion requirements (incorporate recurrence for occasional reports)
- Illustration of any admission restrictions or security concerns.

CODE DESIGN

Configuration design is this present reality normalized arrangements day-to-day programming configuration issues, and issues in the application advancement have happened off. The focal point of the example is the communication between the plan and the object on top of the line.

DATA SET DESIGN

Data set plans incorporate the formation of a clinical data table, communicated as the capacity of the actual information base. They have their quality. Each table can be viewed as a record containing the data that each line is important, segments can be viewed as a similar field of information, and it has been coordinated in lines and sections.

FRAMEWORK FOR SYSTEM DESIGN

Explicit and clear necessities of the plan work will change to a full and gritty particular for the direct turn of events and testing. A useful framework is characterized, the actual interface, point-by-point plan choices to meet the security and information necessities. The remainder of the plan of the plan.

- Is directly recognizable to the requirements.
- Describes how the limits portrayed by the essentials will execute.
- User, human/ interface plan
- System designing
- Detailed framework plan
- Database plan including an actual information model and information word reference.

SYSTEM TESTING

The execution stage of framework testing ensures that the framework is accurate before it is supplied to execute successfully. Testing is critical to the framework's success. Arrangement of puzzling test data, the test framework, and the test data.

TESTING STEPS

- Unit testing
- Integration Testing
- Verification Test
- Output test
- User Acceptance Testing

UNIT TESTING

Unit testing focuses on the smallest unit of work's software design and verification module. It's known as the "test module." This test was done during the programming time. Individual modules have been tested. During the inspection phase, each module is determined to perform properly in terms of the desired output.

INTEGRATION TEST

The technology of integration test systems is based on the interface of faults detected in tests and associated with them. All modules are then tested and merged as a whole software in this project. As a consequence, mistakes in the real test integration process were fixed in the following test phase.

VERIFICATION TEST

The software validation test requirements for embedded software requirements analysis include the establishment of validation tests. The programme produced by the test fulfils all of the Ultimate's functionality, behaviour, and performance criteria. At this point, all errors discovered during integration testing have been corrected.

OUTPUT TEST

Following the execution of the validation test, the next stage is to create a system to output the test, as it cannot be helpful in any system unless it generates a certain output format. Or shown by the system under consideration's output, following which the user test asks the format request. In addition to the print format, the output on the screen is examined in two ways.

USER ACCEPTANCE TEST

Because the coding architecture is entirely object-oriented, it is the first created and tested interface. Each line of code accepts at least one critical aspect in any system user's success and then tests the unit that inputs each of the many software modules.

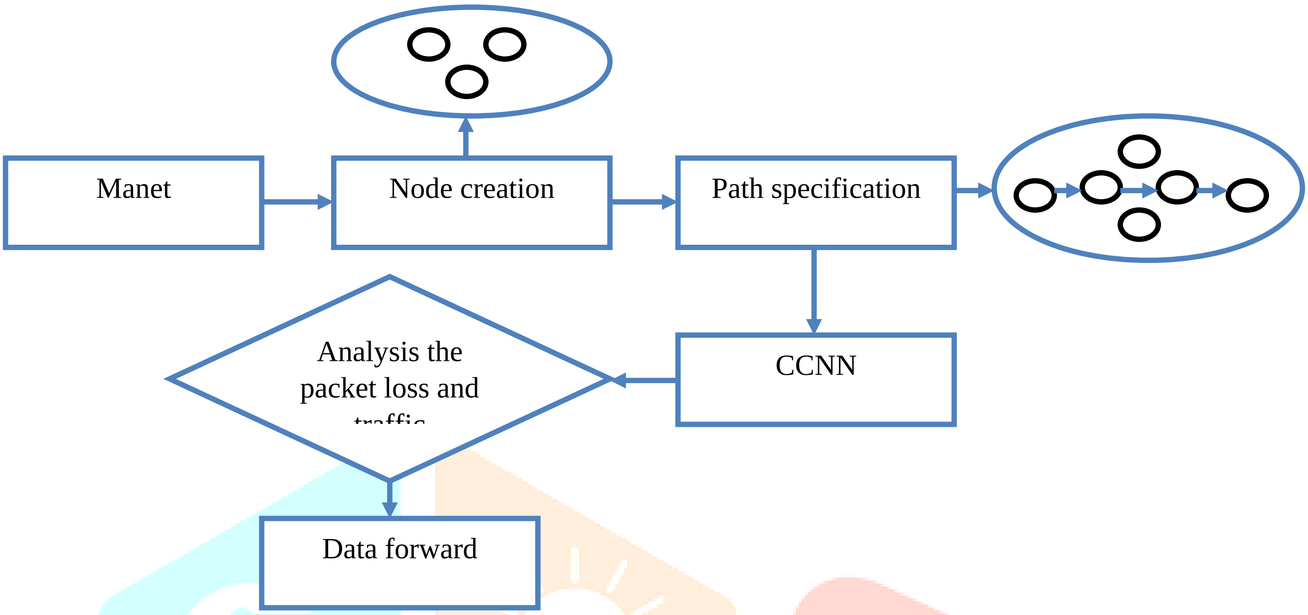
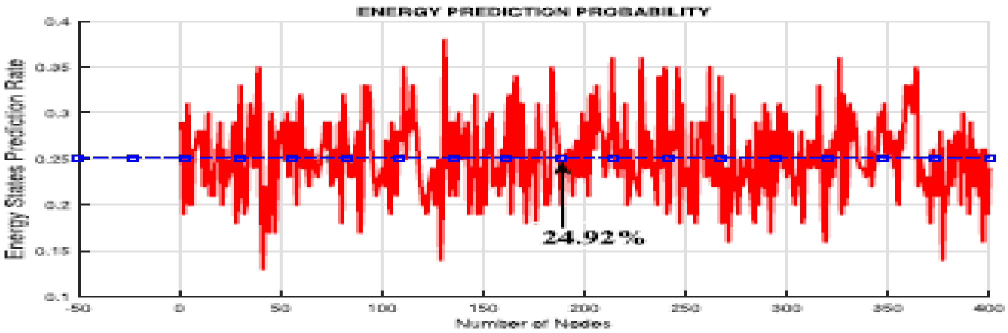


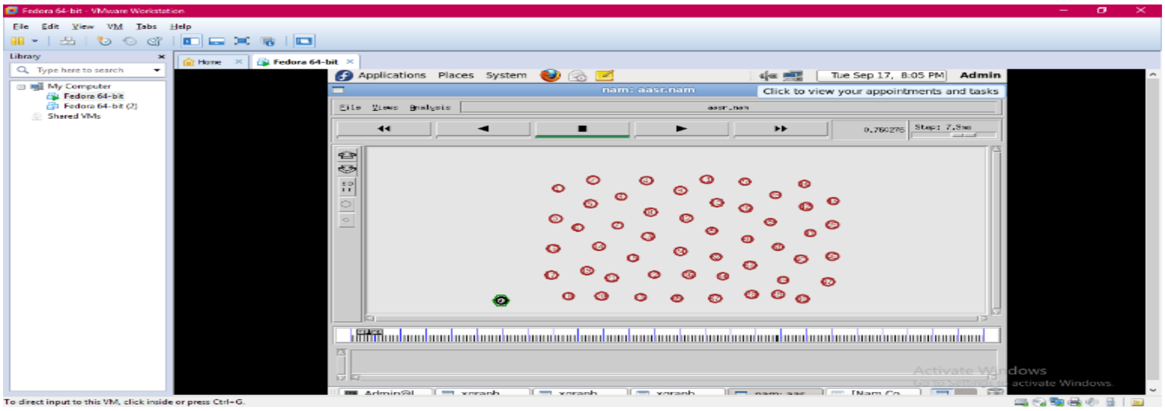
Figure 3 ER Diagram for Collaborate Framework

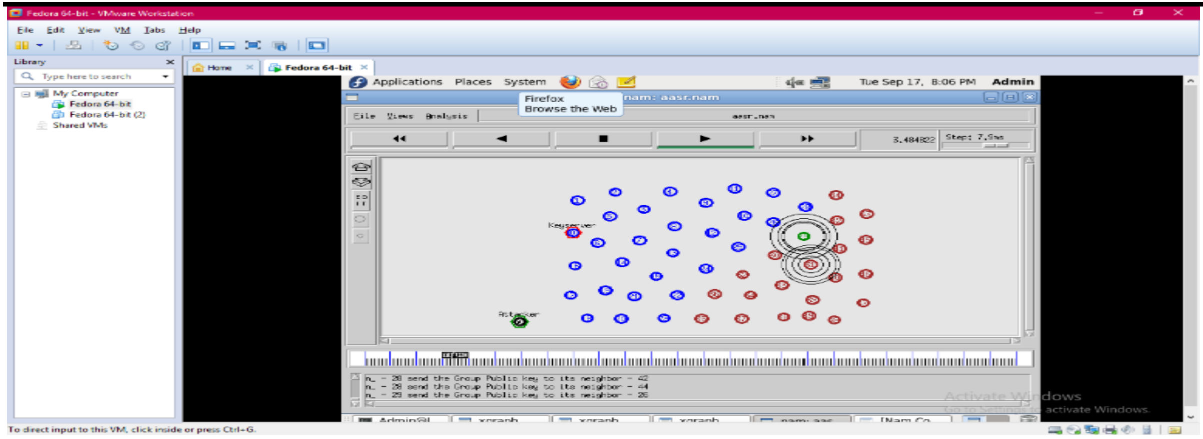
SYSTEM IMPLEMENTATION:

The implementation phase of the system includes the following steps.

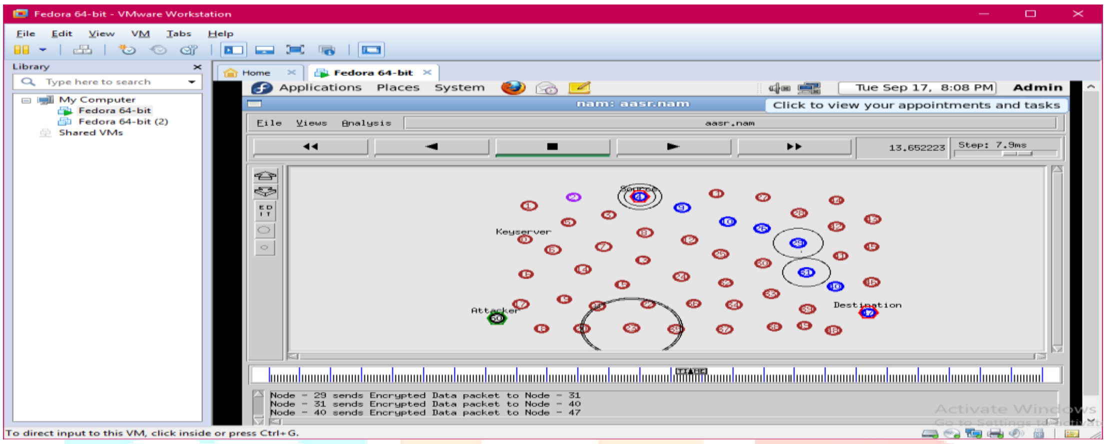
- Software development and test sample data.
- Correct and identify any errors.
- Create a file system using the actual data
- The system makes an error and makes the necessary corrections.
- Human resource development for users.



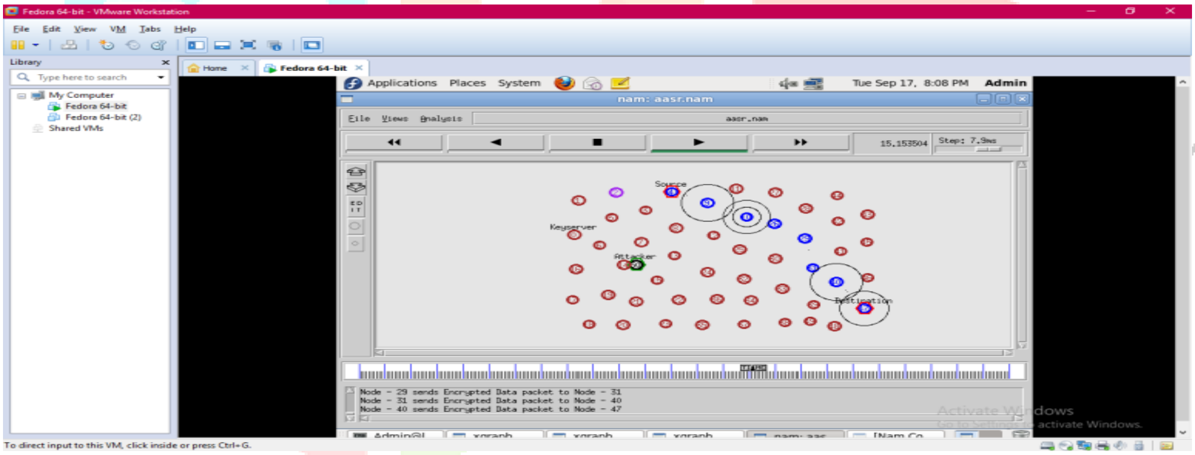

Fedora 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Fedora 64-bit
Fedora 64-bit (2)
Shared VMs
Home
Fedora 64-bit
Applications Places System
Tue Sep 17, 8:05 PM
Admin
nam: aasr.nam
Click to view your appointments and tasks
File Views Analysis
aasr.nam
0.760276
Step: 7.9ms
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, click inside or press Ctrl+G.


Fedora 64-bit - VMware Workstation
Applications Places System
Tue Sep 17, 8:06 PM Admin
Firefox
Browse the Web
nam: aasr.nam
File Views Analysis
aasr.nam
3.484822
Step: 7.5ms
Keyserver
Attacker
To direct input to this VM, click inside or press Ctrl+G.

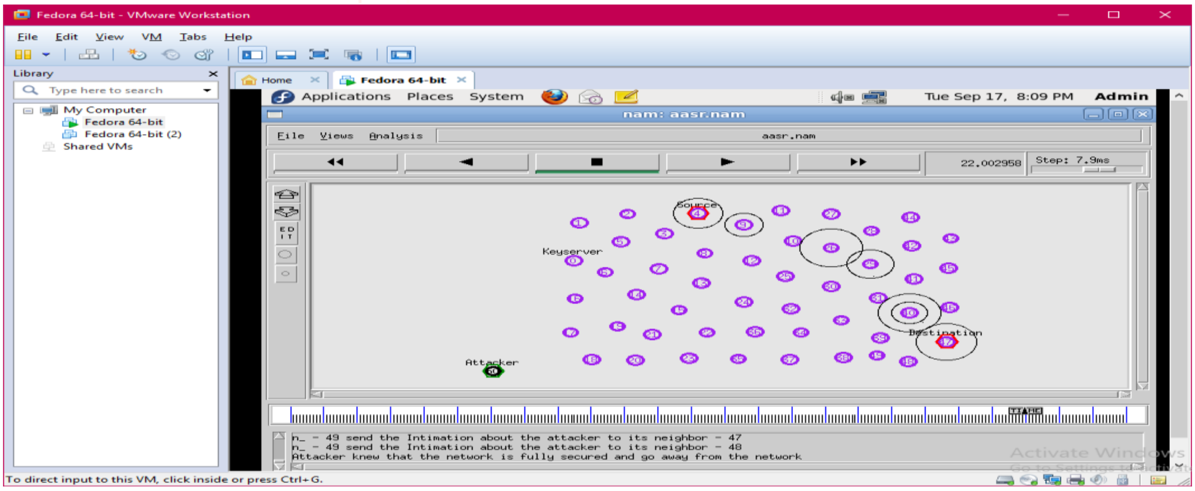
```
n_ - 28 send the Group Public key to its neighbor - 42
n_ - 28 send the Group Public key to its neighbor - 44
n_ - 29 send the Group Public key to its neighbor - 26
```


Fedora 64-bit - VMware Workstation
Applications Places System
Tue Sep 17, 8:08 PM Admin
nam: aasr.nam
Click to view your appointments and tasks
File Views Analysis
aasr.nam
13.652223
Step: 7.9ms
Source
Keyserver
Attacker
Destination
To direct input to this VM, click inside or press Ctrl+G.

```
Node - 29 sends Encrypted Data packet to Node - 31
Node - 31 sends Encrypted Data packet to Node - 40
Node - 40 sends Encrypted Data packet to Node - 47
```


Fedora 64-bit - VMware Workstation
Applications Places System
Tue Sep 17, 8:08 PM Admin
nam: aasr.nam
File Views Analysis
aasr.nam
15.153504
Step: 7.9ms
Source
Keyserver
Attacker
Destination
To direct input to this VM, click inside or press Ctrl+G.

```
Node - 29 sends Encrypted Data packet to Node - 31
Node - 31 sends Encrypted Data packet to Node - 40
Node - 40 sends Encrypted Data packet to Node - 47
```


Fedora 64-bit - VMware Workstation
Applications Places System
Tue Sep 17, 8:09 PM Admin
nam: aasr.nam
File Views Analysis
aasr.nam
22.002958
Step: 7.9ms
Source
Keyserver
Destination
Attacker
To direct input to this VM, click inside or press Ctrl+G.

```
n_ - 49 send the Intimation about the attacker to its neighbor - 47
n_ - 49 send the Intimation about the attacker to its neighbor - 48
Attacker knew that the network is fully secured and go away from the network
```

CONCLUSION:

With the increasing reliance on wireless communications to establish various sorts of connections and access a range of services, the predetermined architecture of these networks has become their operational limit. Ad-hoc networks have arisen as a solution to this challenge by allowing network nodes to initiate connections by delivering packets from one another. However, the lack of infrastructure and the freedom of network nodes to relocate has posed substantial obstacles to network packet routing. One of the primary problems with these networks is making the most use of the limited resources on the nodes in order to extend the network's lifetime. In terms of future work, we will put the planned security measures into action. Furthermore, our research will investigate deep learning approaches to effectively categorise framework in an IoT-centric testbed, which can then be expanded to numerous applications in a real-time context. More research towards refining the encryption technology is required. The process of recreating the message takes time, which can be decreased further. The shortest path may be found using improved routing algorithms.

REFERENCE

1. D. -K. Chae, J. A. Shin and S. -W. Kim, "Collaborative Adversarial Autoencoders: An Effective Collaborative Filtering Model Under the GAN Framework," in IEEE Access, vol. 7, pp. 37650-37663, 2019, doi: 10.1109/ACCESS.2019.2905876.

2. Y. Han, P. Zhang, T. Zhuo, W. Huang, Y. Zha and Y. Zhang, "Ensemble Tracking Based on Diverse Collaborative Framework With Multi-Cue Dynamic Fusion," in IEEE Transactions on Multimedia, vol. 22, no. 10, pp. 2698-2710, Oct. 2020, doi: 10.1109/TMM.2019.2958759.

3. M. Franzago, D. D. Ruscio, I. Malavolta and H. Muccini, "Collaborative Model-Driven Software Engineering: A Classification Framework and a Research Map," in IEEE Transactions on Software Engineering, vol. 44, no. 12, pp. 1146-1175, 1 Dec. 2018, doi: 10.1109/TSE.2017.2755039.

4. D. Tran, J. Du, W. Sheng, D. Osipychev, Y. Sun and H. Bai, "A Human-Vehicle Collaborative Driving Framework for Driver Assistance," in IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 9, pp. 3470-3485, Sept. 2019, doi: 10.1109/TITS.2018.2878027.

5. Y. Komai, Y. Sasaki, T. Hara and S. Nishio, "K Nearest Neighbor Search for Location-Dependent Sensor Data in MANETs," in IEEE Access, vol. 3, pp. 942-954, 2015, doi: 10.1109/ACCESS.2015.2445323.

6. C. K. da Silva Rodrigues and V. E. Moreira Rocha, "BT-MANET: A Novel BitTorrent-Like Algorithm for Video On-Demand Streaming over MANETs," in IEEE Latin America Transactions, vol. 17, no. 01, pp. 78-84, January 2019, doi: 10.1109/TLA.2019.8826698.

7. J. Liu, M. Sheng, Y. Xu, J. Li and X. Jiang, "End-to-End Delay Modeling in Buffer-Limited MANETs: A General Theoretical Framework," in IEEE Transactions on Wireless Communications, vol. 15, no. 1, pp. 498-511, Jan. 2016, doi: 10.1109/TWC.2015.2475258.