International Journal on Applications in Information and Communication Engineering
Volume 9 : Issue 2 : July 2023, pp 75 – 85 www.aetsjournal.com ISSN (Online) : 2394 - 6237

Collaborate Framework Based on Software Defined Network in MANET

Dr. S. Mohanasundaram
Department of Information Technology
Government College of
Engineering
Erode, Tamilnadu, India
Email: smohanirtt@gmail.com

Dr. P. Thangavel
Department of Information Technology
Government College of
Engineering
Erode, Tamilnadu, India
Email: thangsirtt@gmail.com

Abstract

Design a new network model for mobile ad-hoc network (MANET) nodes and actors in wireless sensor networks collaboration to optimize the processing in event areas. Distributed algorithms have been developed, consisting of two phases: set-up phase and negotiation phase. The former is based on the weighted proportional max-min fairness to initially distribute the MANET nodes over the event areas, while the latter based on the market-based technique is used to re-distribute the number of MANET nodes depending on the current and new events. A mechanism for detecting malicious packet dropping attacks in MANETs. In the proposed algorithm Is Collaborative Convolutional Neural Network (CCNN) is the mechanism is depending on a trust module on each node, which is based on the reputation value computed for that node by its neighbors. The reputation value of a node is computed based on its packet forwarding behavior in the network. The reputation information is gathered, stored and exchanged between the nodes, and computed under different scenario. The proposed protocol has been simulated in a network simulator. The simulation results show the efficiency of its performance. Our solution incurs minimal overhead in terms of network bandwidth and latency even in the presence of cryptographic operations. Furthermore, we show that the protection remains effective even in the presence of misbehaving nodes and routing changes due to mobility. While further work is needed to fully evaluate our scheme, we believe that the notion of collaborative security in MANETs is a promising direction for future.

INTRODUCTION

A Mobile Ad hoc Network (MANET) is a peer-to-peer network of mobile nodes capable to communicate with each other without an underlying infrastructure. Nodes can communicate with their own neighbors (i.e., nodes in radio range) directly by wireless links. Anyway, non-neighboring nodes can equally communicate by using other intermediate nodes as relays which forward packets toward destinations. The lack of a fixed infrastructure makes this kind of network suitable in all scenarios where it is needed to deploy quickly a network but the presence of access points is not guaranteed. Examples are military applications, and more recently, cooperative systems for emergency management or pervasive healthcare, as well as many other scenarios, which require highly dynamic node mobility.

In traditional networks, malicious nodes and traffic are kept away from a set of nodes belonging to an organization or a group using firewalls. This is feasible because of the existence of a well-defined network perimeter. All incoming and outgoing

traffic needs to transit through these firewall nodes, which enforce the policies at the perimeter. Within the perimeter, smaller sub-groups can have more stringent policies by deploying their own firewalls. Unfortunately, the concept of a network perimeter does not exist in MANETs, and policies need to be enforced in a distributed manner while taking into consideration node mobility. To address this, recently, we proposed a deny-by-default architecture that enforces trust relationships and traffic accountability between mobile nodes through a distributed policy enforcement scheme for MANETs. In that architecture, we extended the network capability framework and tailored it to the resource-constrained MANET environment.

A capability is a token of authority that has associated rights. The capabilities propagate both access control rules and traffic shaping parameters that should govern a node's traffic. In the deny-by-default, model nodes can only access the services and hosts they are authorized for by the capabilities given to them. The enforcement of the capability is done in a distributed manner by all the nodes in the path from the source to the destination. Compromised or malicious nodes cannot exceed their authority and expose the whole network to an adversary. Upon detection, we can prevent a compromised node from further attacking the network simply by revoking its capabilities. Moreover, that architecture helps mitigate the impact of denial of service (DoS) attacks because excess or unauthorized packets are dropped closer to the attack source. Thus, we avoid unnecessary data processing and forwarding at the target node and the network itself.

Collaborative Application is based on the idea that people can share information. It is becoming more and more important everyday within all environments ranging from social to topical. The collaborative application can be used at emergency search and rescue operations, sharing of ideas and information in meeting or conferences, field survey operations at remote places, Group activity where no visual contact, security purpose, military operations and more. So people required different mobile applications for different purpose. The mobile application market is moving fast as more powerful phones are introduced. This short renewal time speeds up the adoption of new technology and creates a demand for applications utilizing new technology. If developing time for a new application is too long then, it will most probably out of date by the time is will finished. On need and designing a collaborative application framework using which different application can be developed rather than design a single application every time. It might require a significant larger amount of time to develop a framework rather than a single application. But a completed framework enables higher productivity and shorter development time for the actual applications, because of its capability of code and design reuse. This paper also discussing the related work done in this area and propose a prototyping model for developing collaborative application framework.

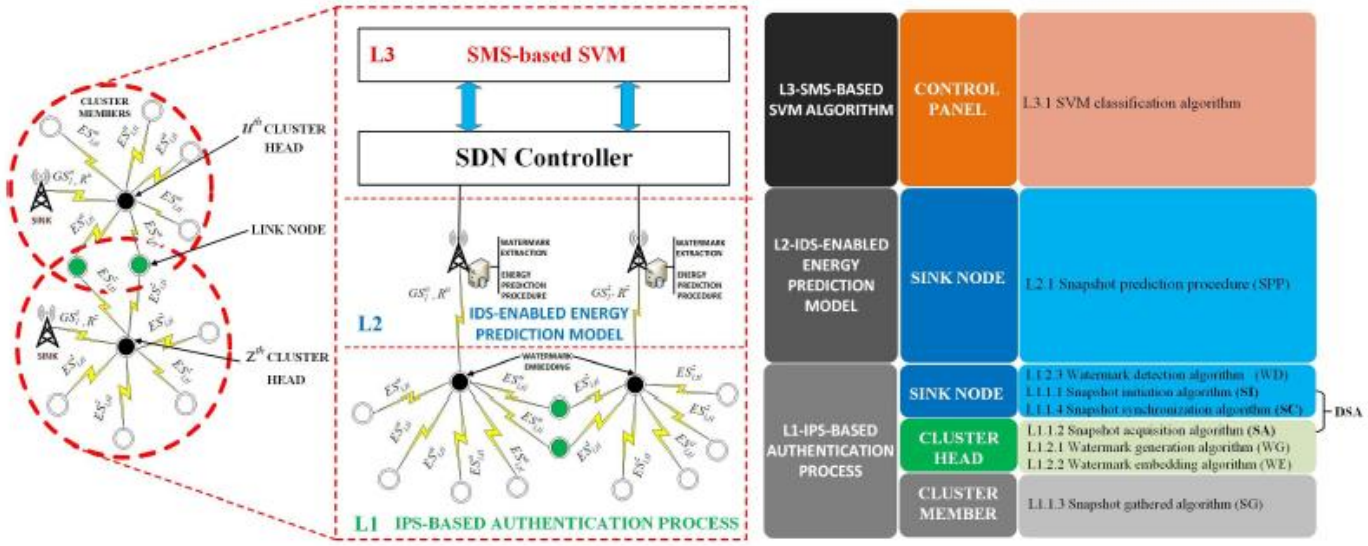
Due to the non-availability of central authority and the unreliability of wireless links, the routing protocols in mobile ad hoc networks (MANETs) are vulnerable to various types of security threats. The resource-constrained nature of MANETs with continuously evolving topology and frequent network partitioning complicates the security challenges in MANETs' routing. Most of the secure routing protocols for MANETs utilize some form of cryptography to ensure the network security. However, there are scenarios, where cryptography techniques fail to capture malicious behavior of a node. For example, (a) to disrupt the network topology, a node may provide falsified routing information to other nodes, (b) to preserve the battery, a node may not participate in the routing functions, and (c) a node may drop data packets instead of forwarding because of the malicious intention. To address these issues, trust-based security schemes [5–10] have been proposed to augment the security of traditional cryptography-based approaches.

In MANETs, trust can be defined as to what extent a node can fulfill the expectations of other node(s) as per the specification of an underlying communication protocol. In trust-based security schemes, each node within the network manages an independent trust table to compute and store the trust values of other nodes. The routing decisions are based on the computed trust values of the nodes. Although a lot of research work has been carried in the field of trust and reputation based systems in MANETs, however, almost all the proposed schemes suffer from one basic problem known as

bootstrapping problem. It refers to the time required by the trust-based scheme to build trust and reputation among nodes in the network. Such delay in accumulation of trust and reputation is often not acceptable in time-critical applications.

Due to the slow trust building process, a misbehaving node may have more opportunities to drop packets before being detected as malicious. One of the basic reasons for the aforementioned bootstrapping problem is that in most of the trust-based security schemes, an evaluated node's trust is computed based on a single trust attribute, such as data forwarding. Moreover, using single trust attribute may not effectively deal with the problem of selective misbehavior. A smart malicious node may misbehave in the context of one network function and behave properly for other network functions. For example, a node may misbehave in the context of data forwarding while demonstrating good behavior when dealing with the control packet forwarding. As the existing schemes use single trust attribute, the aforementioned selective misbehaving node is declared as malicious node and isolated from the routing path, hence no longer will be available to be used for other network functions.

In trust-based security schemes, each node collects two major types of information about other nodes: first-hand information (based on self-observations) and second-hand information (based on the other node observations). In literature, efforts have been made to minimize the bootstrapping time and to increase the detection rate by using second-hand information to evaluate the trustworthiness of the nodes. However, the aforementioned schemes still suffer from data sparsity problem. In trust-based security schemes, data sparsity is a situation where lack of information or insufficient interaction experience makes it difficult to evaluate the node's trust, especially in the early time of network establishment.



(a) SDN-based three layers' framework

(b) Security framework stack

SYSTEM STUDY

Existing System

The construction and running of hydropower plants does not merely involve hydropower generation itself but also facilities observation, quality monitoring, harmful creatures tracking, etc., thus requiring mobile and collaborative monitoring capabilities. MANET (Mobile Ad Hoc Networks), with its mobility, not flexibility, and robustness in volatile networking environment, is a competitive candidate to fulfill such tasks. Nevertheless, its distributed structure prevents the ineffective collaboration between MANET nodes. SDN (Software-Defined Networking) provides the centralized control over the network underlay.

Disadvantages

- Wasted band width
- Delay
- Increasing Network congestion

- External sources for destination location

Proposed system

The ad hoc network provides the facility to connect in a heterogeneous environment without a centralized approach. It is created automatically when two or more device has an active connection. Mobile Ad-hoc Networks (MANETs) allow the wireless network to establish communications without the need for infrastructure by allowing the nodes to deliver each other's packets to their destination. Such networks increased flexibility but require more-complex routing methods. In this study, we proposed a new routing method, based on Collaborative Convolutional Neural Network (CCNN), that distributes the computations in a Software Defined Network (SDN) controller and the nodes, so that, no redundant computations are executed in the nodes to save the limited resources available on these nodes. The proposed method has been able to significantly increase the lifetime of the network, while maintaining a high Packet Delivery Rate (PDR) and throughput. The results also show that the End-to-End delay of the proposed method is slightly larger than existing routing methods, according to the need for longer alternative routes to balance the loading among the nodes of the MANET.

Advantages

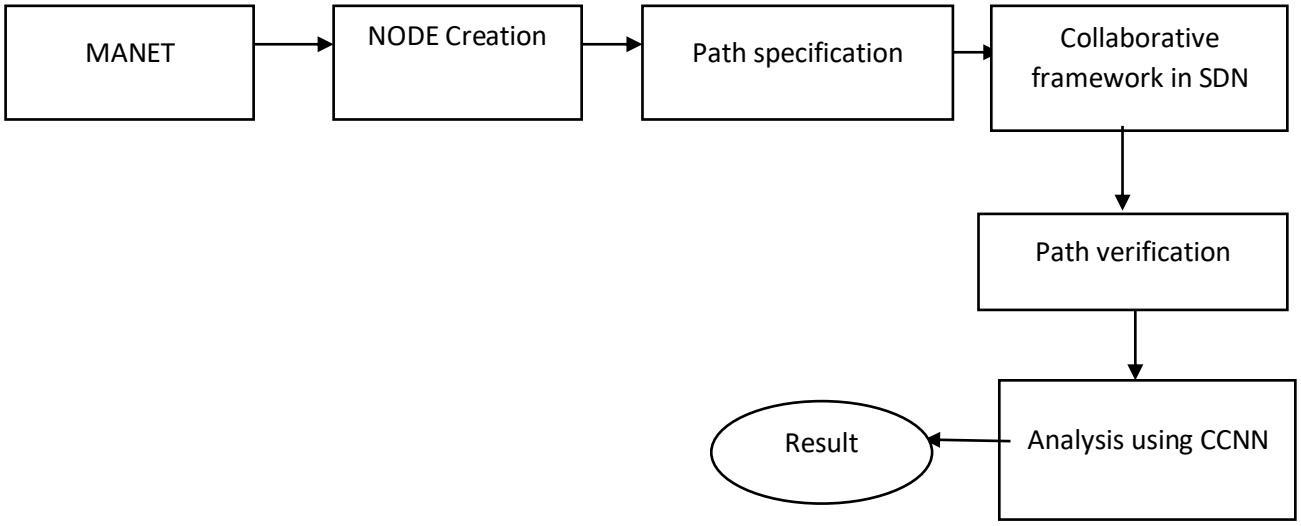
- Data security and safety
- Efficient to manage the traffic
- Low routing Latency
- State Information

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 u^{th} cluster head are represented as follows.

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

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

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



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 li

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 datasetto execute the SVM classification algorithm.As a

result, the malicious misclassified nodes will be segregated from thedata plane by removing them from the Open Flow table.

Therefore, the set of data received by the control plane islinearly 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 limitations.

MODULES DESCRIPTION

Source Node

Protection of the source of location privacy has a relatively low-security period, based on the source's location privacy protection algorithm, which is expected on the phantom source node. The coordinates of the source node and the sink node, the algorithm, provide a node selected at random in the elliptic and direction to establish the common phantom sound source node of the ellipse used phantom sound source node.

Routing Path

Routing is one of the most critical issues in the telecommunications network. It is one of the fundamental characteristics of both mobile radio networks and fixed networks. Underwater communication network, centralized command, you can achieve a share of the overall offense and defense and resources. It has played a vast and vital role in improving combat effectiveness. Wireless sensor networks are typically in harsh environments or developed in this area; wireless communication's broadcast characteristics do not match.

Collaborative Convolutional Neural Network

General network information security technology, firewall technology, intrusion detection technology, and anti-virus technology contain internal and external network isolation technology and e-mail security. Intrusion detection technology is the last line of defense for the defense of network security. For example, to disconnect the network connection, to adjust the entering packet out the access control strategy and filter tells the firewall system.

Secure Communication

The above algorithm will extract the analytical model's abnormal features of the time series and intrusion statistics, decomposing the multiple non-linear components of the transmission stream in a wireless network, no high detection accuracy. The type and the detection principle of a wireless network intrusion detection are analyzed. It uses a statistical analysis method information to detect network intrusion and build a traffic statistical analysis model for abnormal network intrusion by combining the signals to establish a network intrusion signal. Model method.

Destination Node

The destination node does not have sufficient resources to run together, encoding, and decoding. Also, many terminals destination node, computing power, and storage capacity are limited. Simulation results show that it is possible to improve decoding schemes to reduce the decoding load to the destination node effectively. Possession of all the nodes of the resource is not equivalent. Some of the terminal node, but it is not convenient to replace or upgrade.

SYSTEM DESIGN

Introduction

Framework configuration report depicts the framework necessities, the construction of the work and subsystems, documents, information base plan, input design, yield format, Human Machine Interfaces, point-by-point configuration, handling rationale, and an outside interface.

Executive summary of the project

In this section, a project for the preparation of a framework and overview from management's point of view provides a conceptual system design. If appropriate, it contains information that is described in a later section of the abstract.

Process of System overview

This part, utilizing non-specialized terms, portrays the organizational story of the framework. Where appropriate, it should give a general framework design graph representing a subfield framework. Figure level frameworks design or

subsystem, if relevant, ought to show the interface to outside frameworks. If material, and gives a setting block chart of undeniable level frameworks and subsystems. To decide the useful necessities allotted to each side of the plan documentation, kindly allude to the Requirements Traceability Matrix (RTM) by Functional Requirements Document (FRD).

Constraints on the design

This section (a trade-off, productivity with other systems, and analysis of competitive estimates of this utilization and resources) will introduce the limitations of the system design is a design that the project team has developed. The system will include the following assumptions.

Planning for software design

The programming module is the most minimal level of the plan molecule size of the framework. As indicated by the diverse programming advancement technique, at least one module of this framework exists. This part ought to give rationale, adequate subtleties of composing every one of the modules needed for the information in the source code in the framework (or coordinated COTS programming program).

If there are various modules or the record is a wide reach, or on account of addendum referred to another document. Each module, its functions, and a hierarchical structure are described. It is added to information to other drawings when necessary to follow the specifications of the industry-standard module. In the case of the detailed module design, it contains the following information.

Each module of the story description, the overall function process, logic, are connected (scheduled calls or invocations) interfaces, and other modules of the external conditions of the system, such as the security requirements use through the algorithm used in the detailed module.

Received drawing method (equal, for example, a structure diagram, action diagrams, flowcharts,) module handle graphical representation using logic, flow control, and algorithm.

To information and information yield realistic definition or related information components the off chance that it is depicted in detail in a complex or module plan for a huge scope, when joined into a solitary document, it very well may be rehashed a fitting screen data part.

Process of Input design

Design, data entered by the user is a computer-based format that has begun to enter the process. The easy input validation of the design of the input screen, without violating it, needs to see the entire screen in this way. Incorrect input data is the most common cause of error in data processing.

Gathering and ordering the info information into a bunch of comparative information. When recognized, the media dial input is chosen for handling.

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

The fundamental goal of planning input centers on:

- 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.

Enter the plan objective is to make the information section simple and legitimate as conceivable from errors and opportunity. In entering the information passage, the administrator has to realize each field's space, the field dispersion of the request, and source documents should coordinate. The processor breaks down the information required at that point, and it is acknowledged or dismissed.

Process of output design

A typical strategy in the improvement framework is to plan the originally itemized yield is to get back to the information. The yield is as remarks and reports yield from the framework, need

to move to the client. They additionally can be utilized later as a perpetual duplicate for the check.

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 portrays the plan for the client/yield of the working framework; shows planning to the significant level information stream depicted in the segment. The framework incorporates a reported yield, information show screen and a graphical User Interface, the inquiry result, etc. Yield record as portrayed in segment 3, and can be referred to in this segment is Presently it be given below:

- Unmistakable verification of codes and names for reports and data show screens.
- Depiction of report and screen substance (give a sensible depiction of each arrange and portray all data segments related with the plan or reference the data word reference)
- The portrayal of the reason for the yield, including distinguishing proof of the essential clients
- Report dispersion necessities, assuming any (incorporate recurrence for occasional reports)
- Depiction of any entrance limitations or security contemplations.

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. Configuration designs, engineers make it conceivable to examine their work at a more elevated level of deliberation, essentially can't be forestalled rehash an already solved problem learned.

The configuration model has consistently been available in my programming curse. I experience difficulty learning and recollecting that. On the one hand, I have followed this example before in my whole vocation, and even article situated language. Then again, I have not had the option to get a sufficient hold example and wording to have the option to visit unreservedly with their associates.

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.

Qualities of an average framework are characterized at the hour of a plan to fabricate the working framework; it has been bundled in a significant plan sub-frameworks of the computerization framework. Info and yield of every subsystem are planned interface with an outside framework is set up administration exercises are characterized.

A more itemized design of the framework is then based on subsystems, for the most part, recognized by the component creation. Every subsystem is separated into at least one unit, or module planned. An arrangement graph of the technique for the flowchart, the activity outlines, pseudo code, or other adequate organization for each planning unit or module portrayed. Itemized

rationale determination is composed as an actual component level is characterized for every module and an information portrayal. Requires client information and endorsement work in this finish of the occasion.

A movement of assigned spots and study measure all through the arrangement stage. The arrangement review affirms that it has the going with features.

- 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

Framework testing is the execution stage, which guarantees that the framework is exact before it is delivered to run effectively. Testing is basic to the achievement of the framework. Arrangement of perplexing test information, the test framework and the test information. Brought up a blunder in the testing cycle and has been fixed. Run client-created frameworks prepared. Equipment and programming security is intended to create and run the framework later on effectively.

TESTING STEPS

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

UNIT TESTING

Unit testing focuses on the software design and verification module of the smallest unit of work. It is called the "test module." During the programming period itself, this test has been completed. The modules have been individually tested. In this inspection process, each module is found to function well concerning the expected output from the module.

Integration test

Integration test system technology is based on the interface of errors found in the test and associated with it. In this project, all modules are then tested and combined as a whole program. As a result, errors in the actual test integration process have been corrected in the next test phase.

Verification test

Establishing validation tests is part of the software validation test requirements for embedded software requirements analysis. The software provided by the test meets all the features, behavior and performance requirements of the Ultimate. Errors found during integration testing have been fixed at this stage.

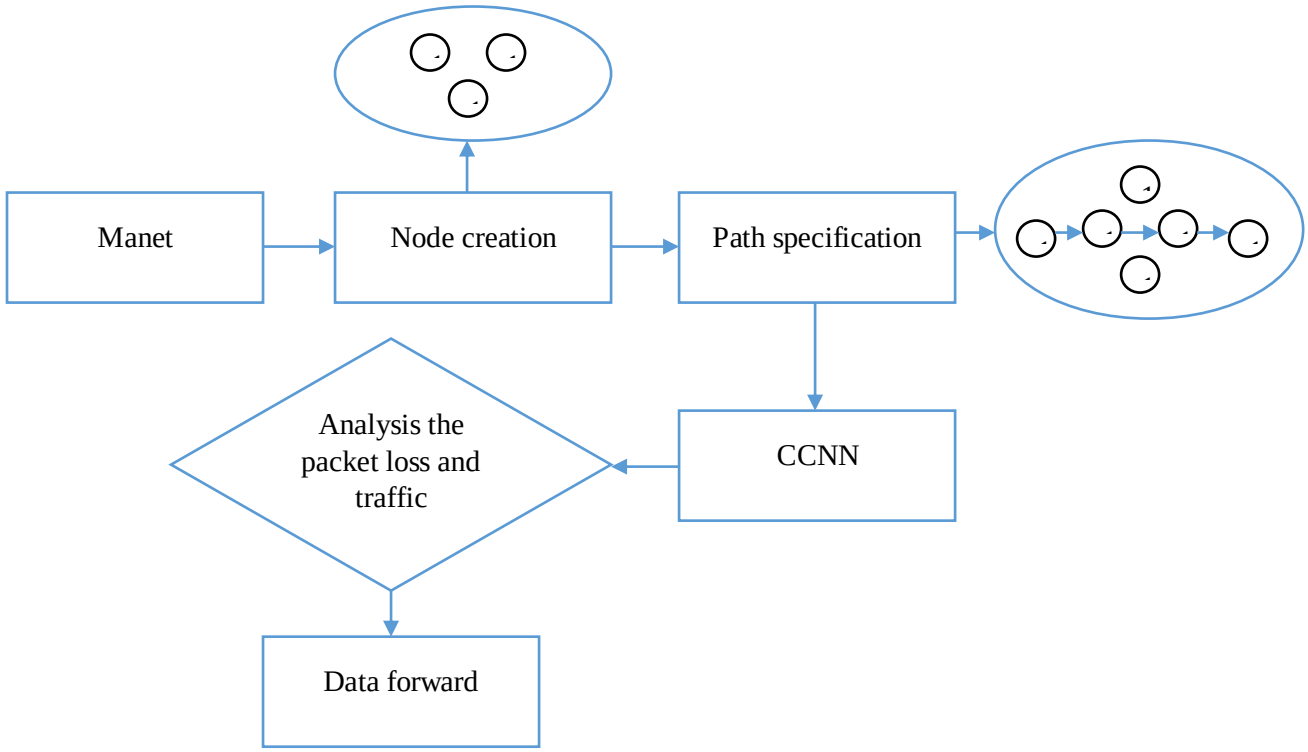
Output test

After running the validation test, the next step is to develop a system to output the test, as it cannot be useful in any system if it does not generate a particular output format. Or displayed by the output generated by the system under consideration, after which the user test requests the format request. On the screen, in addition to the print format, the output is considered in two aspects.

It turns out that the output format on the screen is dedicated to the hard copy format, according to the user's exact needs. The user test output specifies the output does not cause any connection in the system.

User acceptance test

Software testing begins coding design is completely object-oriented, so it is the first developed and tested interface. Each line of code accepts at least one key factor in the success of any system user and then tests the unit that inputs each of the various software modules. The system is running. Imagine that your system constantly evolves, creating proxy servers and keeping users testing their acceptance with future systems and touches.



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.

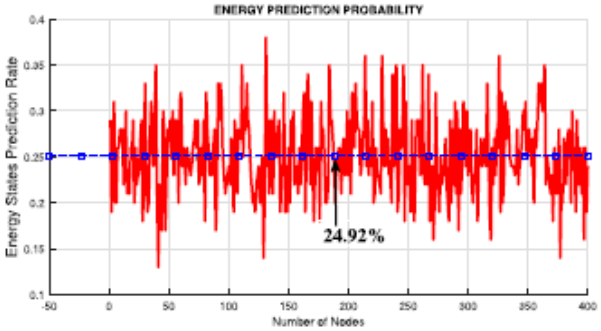
The system runs in parallel with the existing system and is tested with sampled data to find inconsistencies in user requirements. During the training, the user enjoyed the operating mode of the system.

At this stage, it's about user training, site preparation and file conversion. It may be necessary, depending on the nature of training for large users.

Step-by-step evolution of technology in passive roles. After development and testing are complete, we can start to implement the information system. During the software development stage, the project team ended the struggle during testing and development. However, a wide range of representatives of the organization offers very effective and simple mounting techniques. The project team completes the development of the project by implementing the system development cycle.

In the proposed work, we employed MATLAB to simulate various DoS attacks such as Black hole, Selective Forwarding,Hello Flood, and Sybil attacks in SDN setups. During thesesimulations, we compared the energy state transitions with thepredicted results using the Markov chain model. Towardsthis end, we employed different network parameters to depictthe SDN data plane characteristics as shown in Table II.

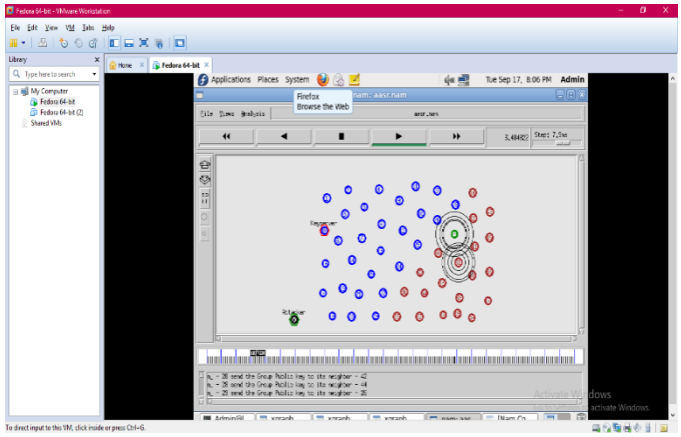
The obtained results illustrate thedifferences between the energy state transitions of a trustednode and the malicious one across the SDWSN. In black holeattacks, the malicious node maximizes its broadcast range aswell as the signal strength.

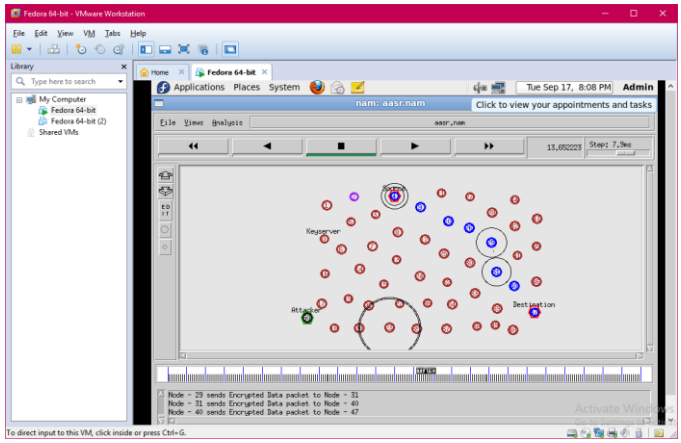


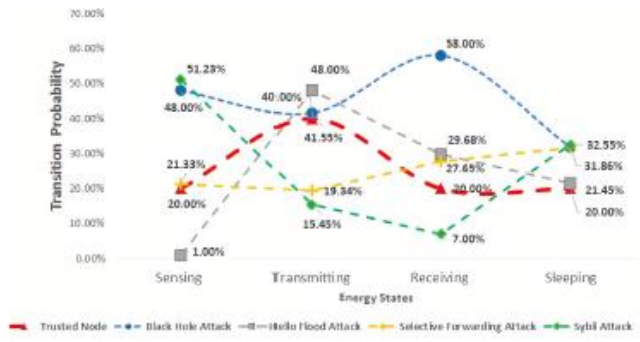
Thus, the energy consumption issignificantly larger than the energy predicted.

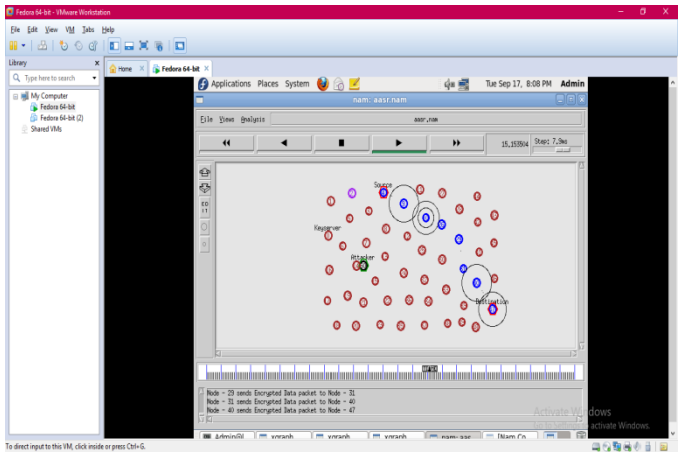
Subsequently,in Hello Flood attacks, the malicious node attracts the communications of cluster heads coming from the cluster nodes. Thus,the gap between the energy state of Hello Flood attack andthe predicted result is higher at the beginning but it decreasesgradually through the simulation.

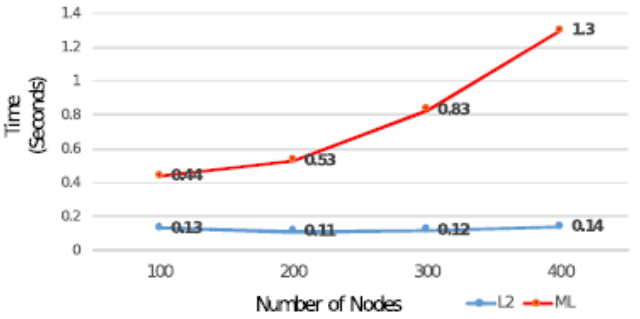
Moreover, the layer L2 of ourframework recognizes Selective Forwarding attacks as well,where the malicious node could be undetected at the beginningof the simulation but the probability of being inferred increasesdue to its signal strength variation in a given time.

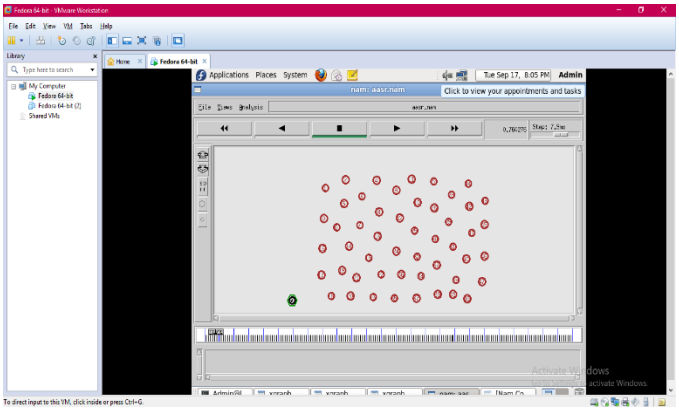


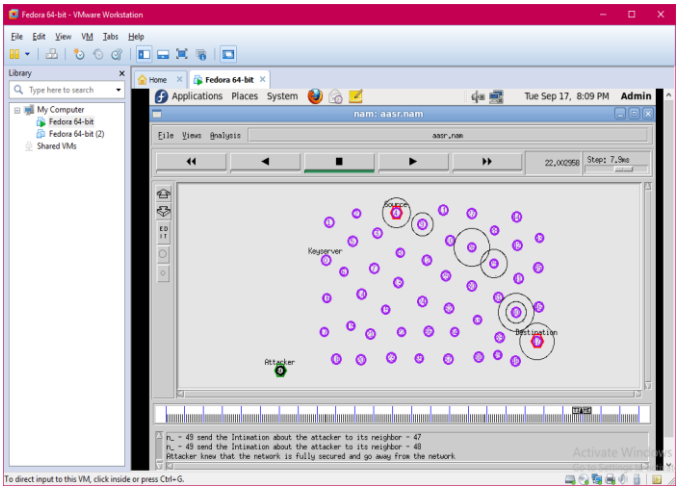


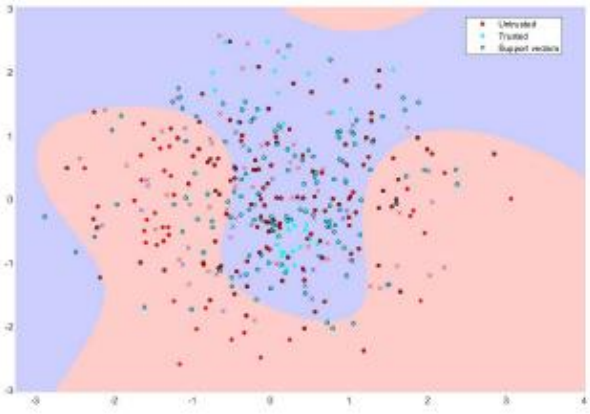












Conclusion

With the rapidly growing reliance on wireless communications to establish different types of connections and access a variety of services, the predefined infrastructure of these networks has become the limit to their operation. Ad-hoc networks have emerged as a solution for this problem by allowing the nodes in the network to establish communications by delivering each other's packets.

However, the absence of infrastructure and the ability of the nodes in the network to move has brought significant challenges toward routing the packets in the network. One of the main concerns in these networks is the efficient use of the limited resources on the nodes, in order to extend the lifetime of the network.

As for future work, we will implement the proposed security Moreover, our research will explore deep learning techniques to accurately classify framework in an IoT-centric testbed can be extended further for many applications in real time environment.

Further studies on improving the encryption technique is needed. it is time consuming process for reconstructing the message, which can be reduced further. The optimized routing techniques can be incorporated the finding shortest path.

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.

8. L. Deng, F. Liu, Y. Zhang and W. S. Wong, "Delay-Constrained Topology-Transparent Distributed Scheduling for MANETs," in IEEE Transactions on Vehicular Technology, vol. 70, no. 1, pp. 1083-1088, Jan. 2021, doi: 10.1109/TVT.2020.3046856.

9. D. O. Akande and M. F. Mohd Salleh, "A Network Lifetime Extension-Aware Cooperative MAC Protocol for MANETs With Optimized Power Control," in IEEE Access, vol. 7, pp. 18546-18557, 2019, doi: 10.1109/ACCESS.2019.2895342.

10. Y. Song, H. Luo, S. Pi, C. Gui and B. Sun, "Graph Kernel Based Clustering Algorithm in MANETs," in IEEE Access, vol. 8, pp. 107650-107660, 2020, doi: 10.1109/ACCESS.2020.3001137.