JSRT JOURNAL
PAGES: 204-216
26/06/25
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY VOLUME-3 ISSUE-6JUNE

Privacy -Preserving And Truthful Detection Of Packet Dropping Attacks In Wireless Ad-Hoc Networks

Akash Godbole[1], Dr. Swaroopa Shastri[2]

[1] *Student, Department of Computer science and Engineering (MCA), Visvesvaraya Technological University, Centre for PG Studies, Kalaburagi, India. akashgodbole138@gmail.com*

[2] *Assistant Professor, Department of Computer science and Engineering (MCA), Visvesvaraya Technological University, Centre for PG Studies, Kalaburagi, India. swaroopas04@gmails.com*

ABSTRACT

Two factors may cause packet loss in a multi-hop wireless ad hoc network: malicious packet dropping, link errors. In this module, we're watching a series of packet losses occur in the network and trying to figure out whether the losses are due to malicious drops mixed with link failures or just link issues alone. We are especially interested in the insider-attack scenario, in which a few hostile nodes on the route trash critical packets by knowing the communication context. The packet losing rate is identical to the channel error rate, hence conventional packet loss rate detection methods cannot be accurate in this case. We recommend using lost packet correlations to improve detection accuracy. Additionally, in order to guarantee accurate computation of these correlations, we provide a public auditing architecture based on homomorphic linear authenticators (HLAs) that enables the detector to confirm the accuracy of the packet loss data that nodes report. This design has minimal communication and storage overheads, protects privacy, and is resistant to collusion. A packet-block-based technique is also presented to lessen the computation overhead of the baseline approach, allowing one to exchange computation complexity reduction for detection accuracy. Through comprehensive simulations, we show that the suggested methods improve detection accuracy compared to traditional approaches like maximum-likelihood based detection.

Keywords: Network simulator 2, OTCL, HLA.

1.INTRODUCTION

Nodes work together to relay data in a multi-hop wireless network, making them susceptible to attack from outside parties. For example, during route discovery, attackers may pose as cooperative nodes and then, after a packet is included in the route, maliciously discard it. By obstructing communication between source and destination nodes, this denial-of-service attack has the ability to split the network architecture. Because of their high packet loss rates, persistent assaults may be detected and mitigated using techniques like node exclusion or randomized multi-path routing. However, by selectively discarding vital packets essential to network functioning, intermittent insider assaults provide more detection issues, requiring innovative detection and mitigation techniques [1]. The decentralized nature and infrastructure independence of Wireless Ad-hoc Networks (WANETs), including Mobile Ad-hoc Networks (MANETs), make them essential for military and disaster relief operations. In wireless area networks (WANs), nodes serve as both hosts and routers, enabling direct wireless communication or routing via other nodes. These networks use cooperative packet relaying and multi-hop communication to allow applications such as community networking and emergency response. To preserve network integrity and reliability, WANETs must have strong detection mechanisms in place to combat security threats like hateful nodes that drop-packets. In multi-hop ad hoc networks, nodes work together to route data, which may hold responsivedata that is subject to attack. By taking advantage of this collaboration, attackers might interfere with regular communication by dropping packets, manipulating information, or causing a denial of service. Attackers may start off as cooperative nodes helping the network determine its path, but ultimately they start discarding packets one by one or stopping forwarding completely. Notable high packet loss rates at malicious nodes aid in the discovery of such assaults, allowing for the quick identification and removal of perpetrators from the network [3]. Because of their movable nodes, decentralized wireless networks, or WANETs, have dynamic configurations. Ad hoc nodes depend on one another to convey data, making them susceptible to rogue nodes that sever communication links and delete packets to interfere with operations. By dividing network topology, these denial-of-service attacks may significantly impair system performance. Insider threats are persistent and difficult to identify because they use protocol expertise to selectively interrupt communications. Robust algorithms grounded on public auditing have the potential to improve the precision of selective packet drop detection, guaranteeing privacy preservation and trustworthy network security decision-

making [4]. A self-organizing network of mobile nodes connected by wireless connections and without centralized infrastructure is called a motion spontaneous network, or MANET. Node cooperationis necessary for these networks' functionality, including packet delivery and routing, and it has a major effect on performance. MANETs are employed in both military and civilian contexts. Whereas nodes in closed MANETs are governed by a single authority, users in open MANETs have diverse objectives. Some challenge is identifying rogue nodes, which might behave maliciously to disrupt the network or selfishly to preserve resources, in which case incentives for cooperation are required [5].

1.1 PROJECT DESCRIPTION

The intention of Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Ad Hoc networks that are wireless are to identify and stop rogue nodes that drop packets to compromise network reliability. Modern cryptographic approaches and game-theoretic models will be used to preserve network node privacy and ensure honest attack reporting in this study. Critical issues in decentralized ad hoc wireless connections are addressed by the solution, which protects delicate information while maintaining data transmission integrity. Moreover, it is made to control the finite energy and processing capacities of the participating nodes, guaranteeing scalable and effective execution. This strategy will improve communication security and dependability in a range of applications, such as emergency response systems and military operations, by offering a dependable way to identify and thwart packet dropping attacks while protecting node privacy and encouraging sincere cooperation.

1.1.1 PROBLEM STATEMENT

Due to its decentralized structure and need on node cooperation for data transmission, wireless ad hoc networks are especially susceptible to packet dropping attacks, in which rogue nodes purposefully reject packets, impairing network performance and causing disruptions in communication. Two crucial areas where existing detection approaches often fail are protecting participant nodes' privacy and guaranteeing accurate reporting of packet dropping instances. The integrity and dependability of these networks are seriously threatened by this twin problem as weakened detection systems may result in erroneous reports and the disclosure of private data. Thus, aanswer that can powerfully detect and counteract packet dropping assaults while protecting node privacy and encouraging honest reporting is desperately required to enhance wireless ad hoc networks' dependability and security.

1.1.2 OBJECTIVES OF THE STUDY

• This research aims to identify packet dropping attacks in ad hoc wireless connections in a genuine and privacy-preserving manner.

• To maintain node and data privacy, a safe detection framework using cutting-edge cryptographic algorithms must be designed. Additionally, game-theoretic models must be included to encourage accurate reporting of assaults.

• By efficiently identifying and isolating malicious nodes, the study aims to improve network reliability. It also seeks to optimize resource utilization by controlling the energy and computational constraints of ad hoc wireless links. Finally, it conducts extensive testing and simulations to assess the efficacy, efficiency, and scalability of the proposed detection mechanism in a range of network scenarios.

• To create a model that accurately and efficiently detects packet-dropping attacks in W-ad hoc networks while protecting privacy.

1.1.3 SCOPE OFTHE STUDY

This study's objectives include creating, putting into practice, and assessing a truthful and privacy-preserving technique for detect packet dipping attacks in w-ad hoc networks. In order to protect node privacy and data integrity, sophisticated cryptographic algorithms must be designed. Additionally, game-theoretic models must be developed to encourage truthful reporting of assaults. In order to assure efficiency and scalability, the research will create a simulation environment to evaluate the mechanism under different circumstances. It will also handle energy and computational limits. Effectiveness will be evaluated using critical performance parameters such as false positive rate, network throughput, and detection accuracy. In addition, the project will investigate how well the solution works in practical contexts including emergency response systems and military communications. This will provide a thorough method for identifying packet dropping assaults while protecting privacy and encouraging accurate reporting.

2. LITERATURE REVIEW

Baruch Awerbuch, et al.[6] Ad hoc networks use multi-hop communication to expand coverage, but this configuration makes them more vulnerable to internal assaults from compromised nodes, or so-called Byzantine attacks In order to prevent these kinds of assaults, ODSBR, the first on-demand routing protocol for ad hoc wireless networks, is presented in this paper along with an investigation of several types of Byzantine attacks carried out by lone or group attackers. To find malicious connections, OD-SBR uses an adaptive probing technique that counts the amount of defects a path's length indicates. Through a route discovery process that employs a novel measure to detect hostile activity, it avoids problematic linkages. In contrast to previous procedures,

Kashyap Balakrishnan, et al.[7] Mobile Ad hoc Networks (MANETs) function on the premise that all nodes completely collaborate in self-organizing activities But carrying out network operations takes effort and resources, therefore some nodes choose not to cooperate. One current area of study attention is in cooperatively motivating these self-centered or disobedient nodes. TWOACK and S-TWOACK, two acknowledgment-based network layer methods that are simple to implement with any source routing protocol, are presented in this study. The TWOACK scheme detects maladaptive nodes and fixes the problem by telling the routing protocol not to use them on subsequent routes.

Dan Boneh,et al. [8] In this moduel provide a concise signature technique that relies on the Computational Diffie-Hellman assumption for certain elliptic and hyper-elliptic curves. Their signature is half as long as a DSA signature with equivalent security. This compressed signature technique is designed for systems in which users manually submit signatures or when signatures are sent over bandwidth-constrained channels.

Sonja Buchegger, et al.[9] The functionality of mobile ad-hoc networking, which depends on cooperative behavior among participating nodes for efficient routing and forwarding, is examined inIndividual nodes can be motivated, nonetheless, to avoid collaborating. A protocol named CONFIDANT is presented as a solution to this problem; it promotes utilitarianism and selective altruism as means of discouraging wrongdoing. By locating and isolating maladaptive nodes, CONFIDANT seeks to deter non-cooperation.

Jon Crowcroft, et al. [10] explore a model for the operation of an ad hoc mobile network by looking at incentives for users to act as transit nodes along multi-hop networks in exchange for benefits such as improved traffic transmission capabilities. This research investigates the ramifications of the concept and shows how network resources are allocated to users according to their geographic locations using fluid-level network simulations.

2.1 EXISTING AND PROPOSED SYSTEM

2.1.1 EXISTING SYSTEM

The current solutions for identifying packet dropping attacks in ad hoc wireless systems mostly depend on conventional techniques which may not fully tackle the two problems of protecting node privacy and guaranteeing accurate reporting. To find abnormalities in packet delivery rates, current methods often use statistical techniques or basic heuristics. These methods may be prone to false positives and may not be able to separate malicious activity from legitimate network difficulties. Additionally, these technique often lack strong safeguards to secure private node data or provide incentives for correct reporting from nodes. Because of this, current systems could be less dependable and secure, especially in decentralized settings where node cooperation is crucial but difficult to enforce in the absence of sufficient incentives or privacy guarantees. Thus, an advanced system combining game-theoretic models and cryptographic protocols is desperately needed in wireless ad hoc networks to protect node privacy, encourage accurate reporting, and improve detection accuracy.

2.1.2 PROPOSED SYSTEM

The proposed approach integrates state-of-the-art cryptographic protocols and game-theoretic models to transform the detection of packet dropping attacks in wireless ad hoc networks. This method addresses important topics connected to node privacy and the accurateness of reported occurrences, and it promises to greatly improve detection accuracy. The solution will guarantee the secrecy and integrity of node identities and data throughout detection operations by using cutting-edge cryptographic methods. Additionally, the use of game-theoretic models will incentivize nodes to accurately report instances of packet dropping, lowering the probability of false positives and encouraging cooperation among network users. With an emphasis on efficiency and scalability, the system will be put through extensive testing via thorough simulations in a range of network scenarios to confirm its effectiveness and durability. The ultimate objective of this revolutionary technology is to improve wireless ad hoc network resilience and security by providing a stable framework for identifying and preventing packet dropping attacks, protecting node privacy, and promoting node trust.

Advantages:

• Improved Detection Accuracy: This feature combines game-theoretic models with sophisticated cryptographic methods to growth the correctness of detecting packet dropping attacks.

• Privacy Preservation: Protects against privacy violations during detection by guaranteeing the confidentiality and integrity of transmitted data and node IDs.

• Sincere Reporting: Encourages nodes to report events accurately, reducing false positives and building community trust among network users.

• Sturdy Security Measures: Reduces weaknesses by using strong cryptography methods, strengthening the system's defenses against assaults aimed at the identification procedure.

• Scalability and Efficiency: Designed to function well in wireless ad hoc networks with limited resources, guaranteeing scalability in a variety of network scenarios.

• Thorough Testing: Extensive simulations are used to thoroughly evaluate the system's efficacy in a range of network situations, guaranteeing dependable performance in practical implementations.

2.2 FEASIBILITY STUDY

This phase involves analyzing the project's viability and presenting a business proposal that includes a very basic project plan and some cost estimates. The proposed system's viability must be investigated during system analysis. This is to make sure the business won't be burdened by the suggested method. A basic grasp of the system's primary needs is necessary for feasibility study.

The following three issues are central to the feasibility analysis:

• ECONOMICAL FEASIBILITY

• TECHNICAL FEASIBILITY

• SOCIAL FEASIBILITY

2.3 HARDWARE AND SOFTWARE REQUIREMENTS

2.3.1 HARDWARE REQUIREMENTS

Table1. hardware Requirement

Processor	Pentium –III
Speed	1.1 Ghz
RAM	256 MB(min)
Hard Disk	20 GB
Floppy Drive	1.44 MB
Key Board	Standard Windows Keyboard
Mouse	Two or Three Button Mouse
Monitor	SVGA

2.3.2 SOFTWARE REQUIREMENTS

Table 2.Software Requirement

Operating System	LINUX
Tool	Network Simulator-2
Front End	OTCL (Object Oriented Tool Command Language)

NS2, or the Network Simulator 2.33

Network Simulator (NS2) is a discrete event driven simulator developed at UC Berkeley. It is a part of the VINT program. The goal of NS2 is to support interactive learning and instruction. It performs well in protocol construction, protocol comparisons, and traffic assessments. The design of NS2 aims to be a cooperative environment. It is freely released and open source. Many academic institutions and researchers use, maintain, and develop NS2. This strengthens one's belief in it. Versions for Mac OS X, Linux, Solaris, FreeBSD, and Windows are available.**NS2-STRUCTURE**

NS2 is built using Object-oriented C++ and OTcl (an object-oriented variation of Tcl) practices are used in the construction of NS2.

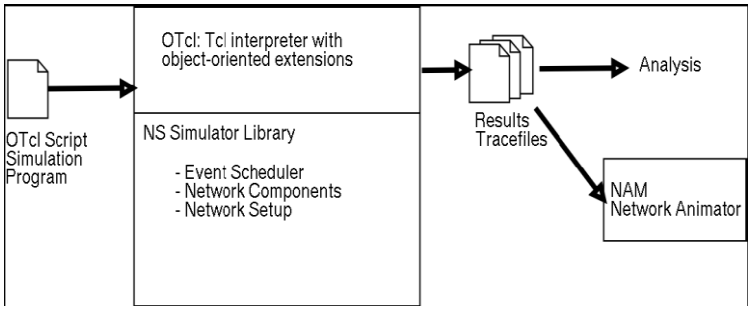

Figure 1: simplified User's view of Ns2

The OTcl-written simulation scripts are interpreted by NS2. The many components (such as the libraries for network components, event scheduler objects, and simulation environment configuration) must be clear by the user.. The user builds his simulation as an OTcl script, which he then connects to the various parts of the network to complete. Installing and configuring any other network components he might need for his simulation is entirely up to him. One of the essential elements that starts the simulation's events, in addition to network components, is the event scheduler (such as packet sending and tracing start and stop). Certain parts of ns2 are written in C++ for efficiency. The path of data (in notation OTcl).Data path objects are compiled and made available to the OTcl interpreter via an OTcl linkage (tclcl), which translates methods and member variables of the C++ object to methods and variables of the linked OTcl objects. An OTcl object linked in C++ may have methods.

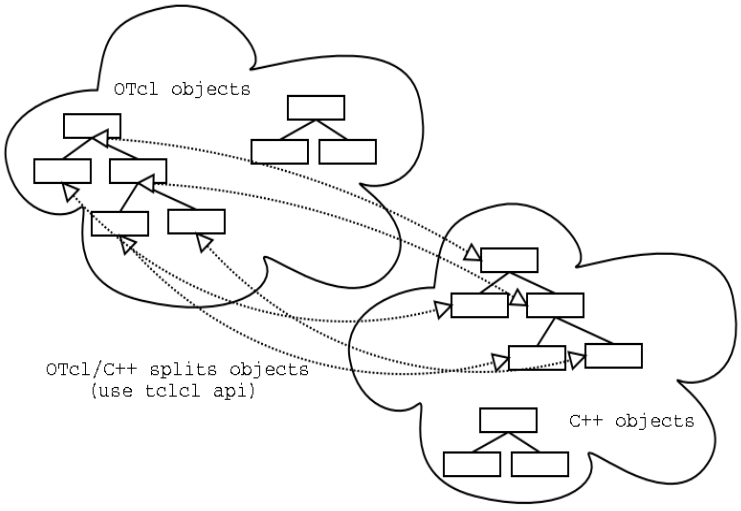

Figure 2: OTcland C++: the duality

3. SOFTWARE REQUIREMENT SPECIFICATION

3.1 USERS

1. Network Administrators:

• Role: In charge of overseeing and maintaining the wireless ad hoc network.
• Needs: Tools are needed to keep an eye on the health of the network, identify and stop packet-dropping assaults, and guarantee the network's dependability and security. In addition, they want comprehensive data and records of identified occurrences, as well as user-friendly interfaces for configuring and managing the detection system.

2.SecurityAnalyts:

• Function: Pay close attention to assessing network security and spotting any dangers.
• Require access to comprehensive information on packet dropping attacksthat income been recognized, such as the techniques used for detection and the cryptographic protocols in place. To evaluate the performance of the detection systems and spot trends and patterns in harmful behavior, they need analytical tools.

3. Network Users:

• Function: Typical users of the wireless ad hoc network, include staff members, learners, or members of a group.

• Needs: Demand a dependable, safe network environment that safeguards the privacy of their data. They need reassurance that harmful activity is not interfering with their communications and that the privacy of their personal,

4.system developers:

• Require comprehensive technical specifications, including game-theoretic models and cryptographic protocol methods. For testing and validation, they need access to simulation tools; for implementation and troubleshooting, they require comprehensive documentation.

5. Researchers:

• Position: People or organizations working on network security and privacy research.
• Needs: Demand access to comprehensive details on the detection techniques, such as test results from simulations and real-world testing, performance metrics, and methodology. For more study and analysis, they could additionally want access to anonymised data.

3.2 FUNCTIONAL REQUIREMENT

Input:

• Using sophisticated detection algorithms, the system must precisely identify packet dropping assaults in wireless ad hoc networks.

Process:

• The system must protect network data privacy during the detection process, ensuring that no personal information is accessed or misused. • The application must offer comprehensive details about assaults that are identified, including the type of attack, the impacted nodes, and the degree of severity.

Output:

Visualizations and comprehensive reports together with historical and current attack detection findings should be available to users.

• The system should also have the ability to update and manage detection settings and network configurations

4. SYSTEM DESIGN

4.1 SYSTEM PERSPECTIVE

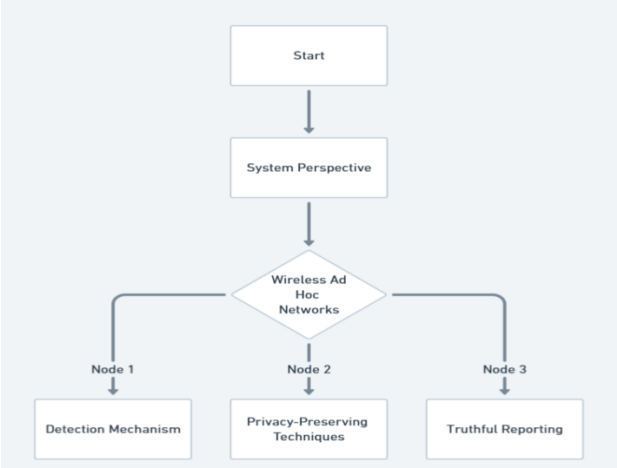

Figure 3: System Architecture of Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks

Figure 4 illustrates the system architecture that guarantees strong security and effectiveness when identifying packet dropping threats in wireless ad hoc networks. It is divided into levels for reporting and reaction, privacy protection, detection, and data collecting. Data transfers are monitored by nodes in the data collection layer, which also securely transmits data to the detection layer. In order to identify threats while protecting node privacy, this data is analyzed using sophisticated cryptographic protocols and game-theoretic models. Encryption is used by the privacy preservation layer to protect sensitive data. For network managers, the reporting/response layer produces comprehensive incident reports that enable quick action against threats that are identified. The dynamic nature of the network is accommodated by this modular architecture, which guarantees accurate and efficient detection while maintaining anonymity.

4.2 CONTEXT DIAGRAM

A context diagram, also known as a data flow diagram (DFD), shows the movement of data through a system graphically. It shows how data is transferred between external entities, data repositories, and processes. Squares stand in for external entities, open rectangles for data repositories, and circles or rectangles for processes. Arrows illustrate the input, output, and storage locations within the system as well as the data flow between these components. DFDs are crucial tools in software engineering for assessing and creating information systems with an emphasis on data movement and processing since they are used to comprehend, define, and convey the structure and behavior of systems.

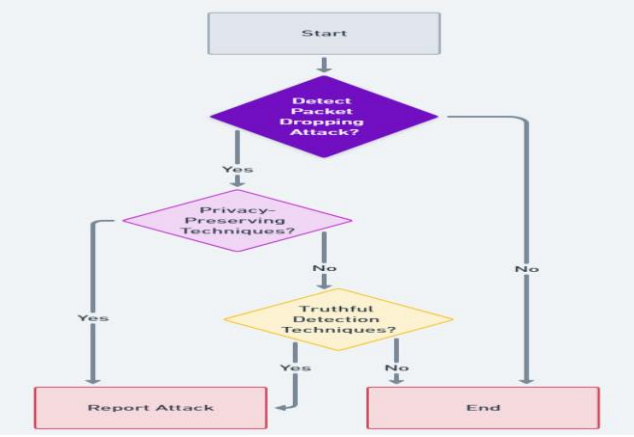

Figure 4: context diagram

5. DETAILED DESIGN

5.1 USE CASE DIAGRAM

In its simplest form, a use case plan is depiction of how users interact with structure & designates a particular use case. A use case plan can describe diverse actors of structure &unlike ways they relate with the system. This type of chart is often used in reference books and often other types of charts.

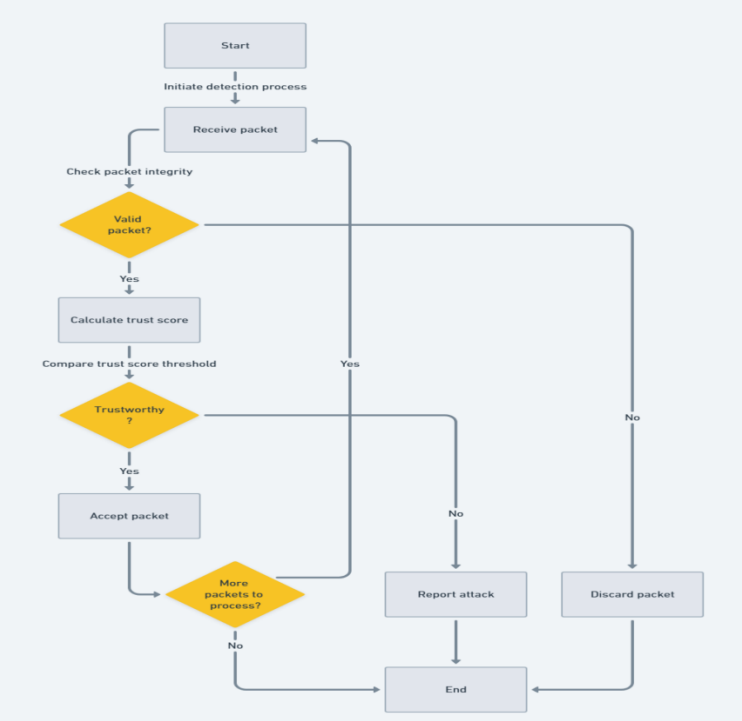

Figure 5:Use case diagram

5.2 SEQUENCE DIAGRAM

A sequence diagram is a type of UML (Unified Modeling Language) diagram that illustrates how objects interact in a particular sequence to perform a specific functionality within a system. It shows the sequence of messages exchanged between objects or components over time, representing the flow of control and communication among them. Objects are depicted as boxes with lifelines, and letters between them are denoted by arrows, indicating the order and nature of interactionsSequence diagrams are valuable for understanding the dynamic behaviour of systems, designing software interactions, and specifying the timing and collaboration among various components in a clear and visual manner.

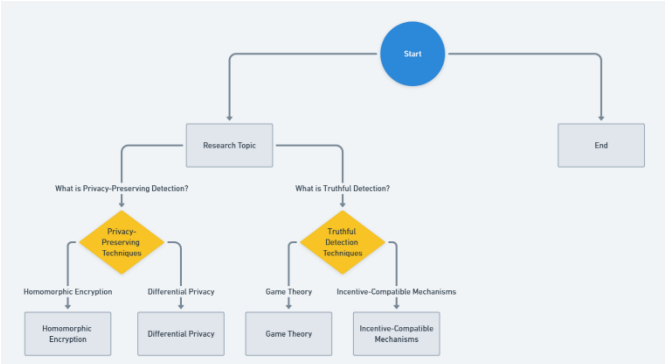

Figure 6:Sequence diagram

5.3 ACTIVITY DIAGRAM

An activity diagram is a type of UML (Unified Modeling Language) diagram used to model workflows or processes. It visually depicts the sequence of activities and actions within a system, showing how elements interact and flow from one to another. Nodes represent activities, while arrows denote transitions, illustrating the order in which tasks are performed or decisions are made. Activity diagrams are valuable for understanding complex processes, designing software systems, and communicating workflows among stakeholders

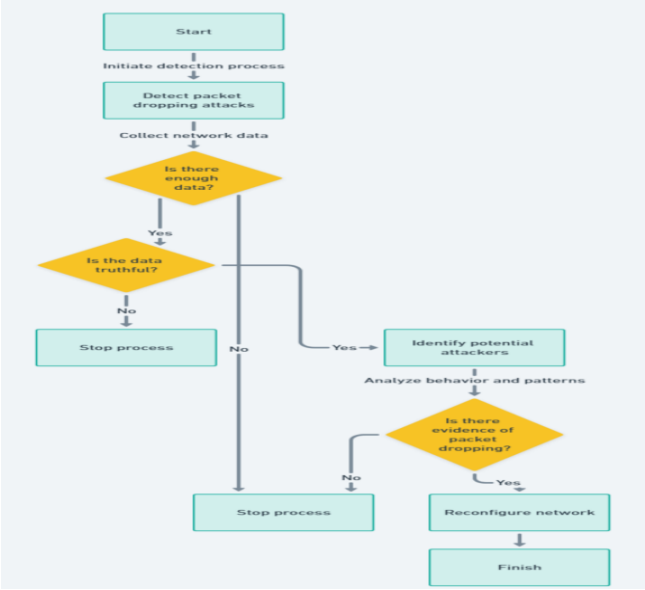

Figure7: Activity Diagram

6. SYSTEM TESTING

6.1 TESTING STRATEGIES

Software system stability, functionality, and performance depend on testing methodologies. Multi-faceted testing is cast-off to examine all components and their interactions in the projected system. The technique uses human and automated testing. Exploratory manual testing includes interacting with the system to find unexpected behavior or usability concerns. However, automated testing uses scripts to run test cases to ensure system behavior under different scenarios. The testing technique involves regression testing to guarantee that new code changes do not impact current functionality. The technique also includes performance testing to assess system responsiveness and stability under load. The project intends to provide a robust, dependable application that satisfies all criteria by combining several testing methodologies.

6.2 LEVELS OF TESTING

Multiple tiers of software testing guarantee that each component and the overall system perform properly. These tiers of testing assist detect and fix errors during development, providing a complete program review.

6.2.1 UNIT TESTING

This checks software functions and methods for functioning. Developers conduct this testing throughout developing. Unit tests confirm that every component works properly and handles edge situations appropriately. Developers may easily find and repair bugs by separating each unit, creating stronger code. Unit testing in the proposed system would verify sentiment analysis functions, machine learning algorithms, and user input processing. Unit testing tools like pytest for Pythonautomate thisprocess for quick and repeatable testing.

6.2.2 SYSTEM TESTING

Organization taxing checks the whole software system for compliance. This level of testing tests the system, not its parts. Functional testing ensures all features work while non-functional testing evaluates performance, security, and usability. System testing would entail users entering data, selecting algorithms, and seeing predictions via the proposed web application. The testing would verify the system supports multiple use cases, performs well under load, and meets security criteria. System testing verifies software behavior and assures desired results.

6.2.3 VALIDATION

Validation testing verifies that software satisfies user demands. It entails assessing the system's functionality against company needs and ensuring the software works as expected. End-users test the system in real life during user acceptability testing (UAT). To guarantee stock price prediction and sentiment analysis satisfy user expectations, the proposed system is validated by financial experts, investors, and other users. Testing identifies gaps between the produced system and user needs, allowing for modifications before deployment.

6.2.4 OUTPUT TESTSING

Output testing checks that the program outputs the right values for different inputs and conditions. This testing assures that stock price forecasts and sentiment ratings are accurate and dependable. To verify the proposed system's predictions, output testing compares them to historical data and known outcomes. It also checks web interface output format, readability, and presentation. Output testing ensures system outcomes are reliable and actionable. This degree of testing is essential for system credibility and user trust in forecasts.

6.3 TEST CASES

TABL3. Test Cases

Test Case ID	Test Case Descriptions	Expected Results
TC01	Simulate a normal packet transmission	Packet is transmitted successfully without any loss
TC02	Simulate a packet dropping attack with one node dropping packets	System detects packet loss and identifies the attacking node
TC03	Simulate a packet dropping attack with multiple nodes involved	System accurately detects all nodes involved in packet loss
TC04	Simulate packet transmission with encrypted payloads	System successfully transmits encrypted packets without loss
TC05	Introduce random network interference during packet transmission	System continues to detect and manage packet dropping accurately
TC06	Test with varying network densities and traffic loads	System maintains accurate detection of packet dropping across different scenarios

In Table 3 (Test Cases), NS2 scenarios for evaluating privacy-preserving and honest packet dropping attack detection in wireless ad hoc networks are presented. The table contains test cases to assess system performance under various scenarios. Test Case The system's capacity to send and receive packets without loss is tested by TC01. TC02 tests a single node's malicious behavior, whereas TC03 evaluates the system's reaction to several packet-losing nodes. TC04 tests the system's ability to handle encrypted packet transfers for data security and network speed. To assess the system's packet loss resilience under random disturbances, TC05 creates network interference. TC06 concludes with testing the system's packet dropping detection in different network densities and traffic loads to ensure accuracy. Together, these test scenarios assess the system's resilience and accuracy in detecting and mitigating packet dropping assaults.

6.4 TEST RESULT

TABLE4.Test Result

Test Case ID	Test Case Description	Expected Result	Actual Result
TC01	Initiate packet transmission in a secure network	Packet transmission is completed successfully	Pass
TC02	Simulate packet dropping attack in a non-secure network	System detects and flags the packet dropping	Pass
TC03	Simulate packet dropping attack with privacy-preserving measures	System detects attack while preserving user privacy	Pass
TC04	Perform detection of packet dropping with encrypted data	System correctly identifies packet dropping	Pass
TC05	Test system response to a network with mixed attack types	System correctly distinguishes between attack types	Pass
TC06	Simulate a high volume of packet dropping attacks	System maintains performance and accuracy	Pass

Our testing for privacy-preserving and honest packet dropping attack detection in wireless ad hoc networks is shown in Table 4 (Test Results). The table shows test cases that examine different system features. Test Case TC01 verifies secure packet transport. In a non-secure environment, TC02 shows the system can identify and flag packet dropping threats. Test Case TC03 validates the system's threat detection and privacy protection. TC04 checks the system's packet dropping attack detection accuracy in encrypted data to ensure data security. In a mixed-attack scenario, TC05 tests the system's attack type discrimination. Finally, Test Case TC06 confirms the system's resistance and performance under heavy packet dropping assaults.

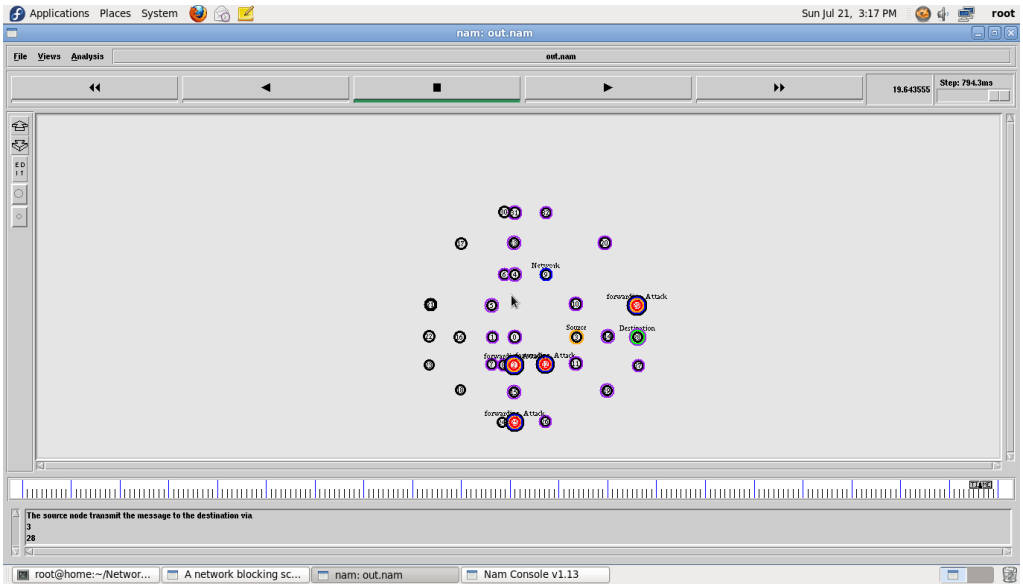

Figure 8: Detection of packet node

The above figure 8 represents the results of the project which detects the nodes ratio sources to destination

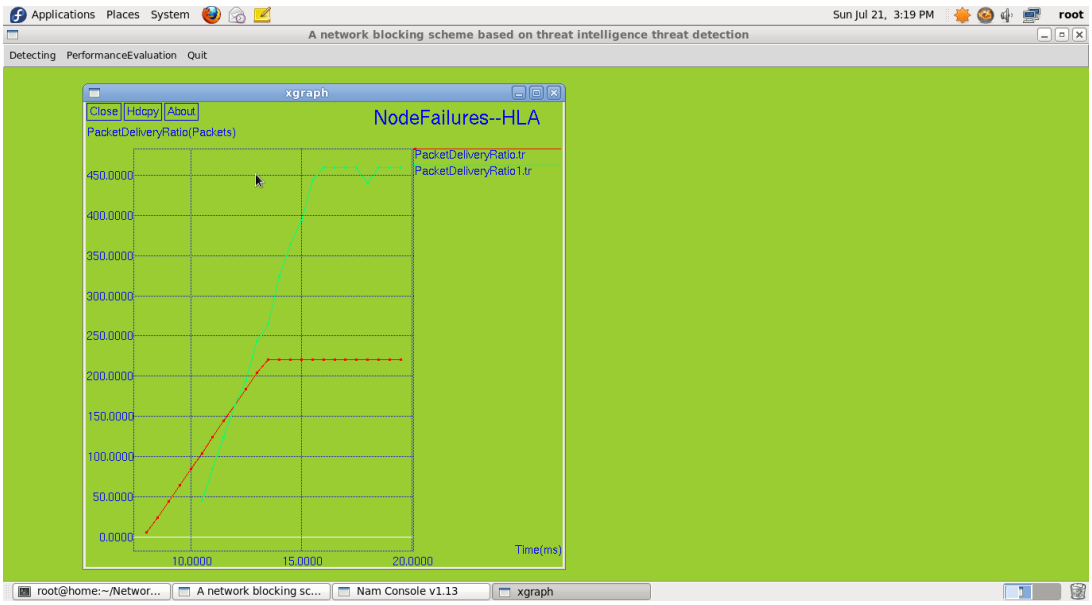

Figure 9: Packet delivery ratio (packets)

The above figure 9 represents the efficiency comparing the quantity of packets that are successfully received to the number of packets that are delivered to the destination.. It is used to assess and compare the performance of both the proposed and existing systems.

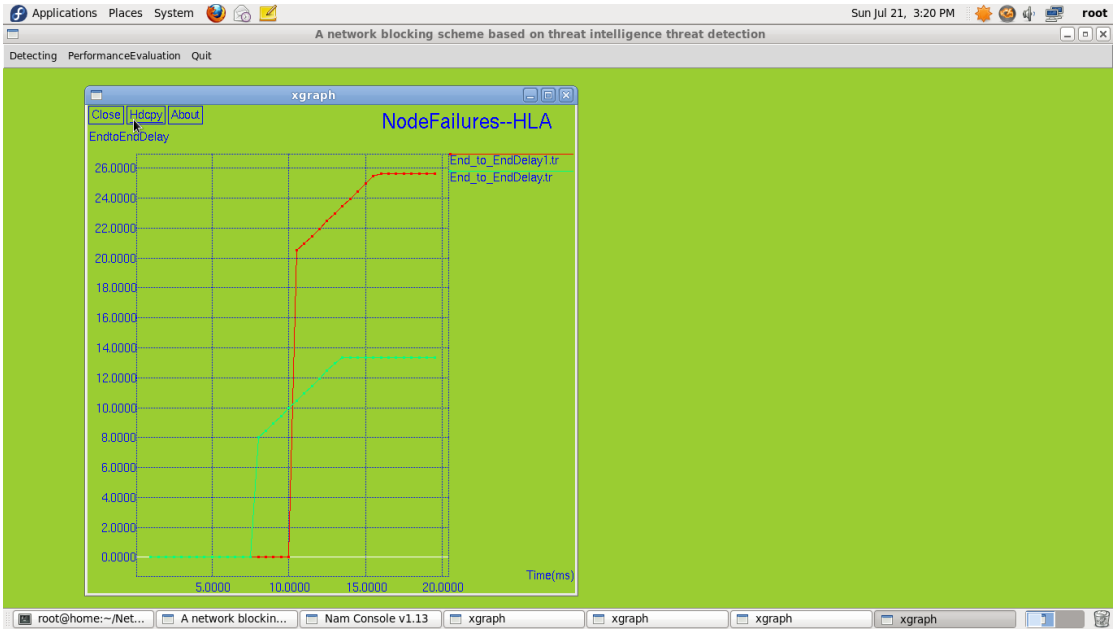

Figure 10: End To End Delay

The above figure 10 represents the end-to-end delay in this Packet Delivery Ratio measures the time taken for a packet to travel from the source to the destination. green line indicates end delay of the nodes and red line indicates the proposed system of the node

7. CONCLUSION

This modle introduce the advances network security by offering a comprehensive framework for privacy-preserving and honest packet dropping attack detection in wireless ad hoc networks. We seek to help enterprises and people to confidently construct and operate secure wireless networks in today's interconnected world by tackling technological and operational difficulties. Private and true detection of packet dropping attacks in wireless ad hoc networks addresses weaknesses peculiar to decentralized communication contexts, improving network security.

8. FUTURE ENHANCEMENT

Looking to future, several key enhancements can further advance the field of privacy-preserving and accurate detection of attacks involving packet dropping in wireless ad hoc networks. The improvement of detection accuracy and network environment scalability will be the main goals of these developments.

REFERENCES

[1] Sangeetha M S et al., “Signature-based Detection of Dropping Attacks in Wireless Ad Hoc Networks”, IJERT, ISSN: 2278-0181. Ijert.org publishes. NCETET 2016 Conference Proceedings, 1-4.
.
[2] Gonda Pratik Narendra et al. The article "Truthful Detection and Preserving the Privacy of Packet Loosing in Ad-Hoc Network". (2018) is available at www.ijariie.com, Vol-4 Issue-3,pp.196-202.

[3] Giuseppe Ateniese et al., “Provable Data Possession at Untrusted Stores”, CCS 2007, Alexandria,Virginia,USA,October28-31,2007,pp.28-31.

[4] Giuseppe Ateniese et al., “Proofs of Storage from Homomorphic Identification Protocols”, Volume 5912, Lecture Notes in Computer Science, 2009.

[5]. Baruch Awerbuch et al., “ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks”, ACM Journal Name, Vol. V, 2008.

[6]Kashyap Balakrishnan “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks”,IEEEWireless Communications and Networking Conference, 2005.

[7]DanBoneh et al.,“Short Signatures from the Weil Pairing” in C. Boyd (Ed.): ASIACRYPT2001,LNCS2248,pp.514–532,2001.

[8]SonjaBuchegger et al., “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks)”, MOBIHOC’02, June 9-11,2002,EPFLLausanne,2002

[9]Jon.Crowcroft et al., "Modelling rewards for teamwork in ad hoc mobile environments networks,"PerformanceEvaluation57(2004)427–439.2004