2026 Volume: 02 Issue: 05 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-31

DEVELOPMENT AND SIMULATION OF AN IMPROVED ALGORITHM FOR INTRUSION DETECTION IN MOBILE ADHOC NETWORKS (MANETS)

*Angbianshio Erdoo, Dr. T. Gbaden, Alex Akimwade, Akase Jude Saater

Nigeria.

Article Received: 19April 2026
Article Revised: 09 May 2026
Published on: 29 May 2026

***Corresponding Author: Angbianshio Erdoo**
Nigeria.

DOI: https://doi-doi.org/101555/ijrpa.6733

ABSTRACT

This study presents an improved algorithm for intrusion detection in Mobile Ad-hoc Networks (MANETs), aimed at enhancing the security and efficiency of decentralized wireless communication systems. MANETs are highly dynamic and infrastructure-less networks, making them vulnerable to a variety of security threats such as black hole, wormhole, and denial-ofservice attacks. Existing cryptographic approaches like RSA have provided partial solutions but remain limited by computational inefficiency and vulnerability to advanced attacks. The research employed an object-oriented design methodology and developed a hybrid encryption model combining RSA (asymmetric) and 3DES (symmetric) encryption techniques to strengthen data confidentiality and computational performance. The system was simulated using Python, with MANET nodes representing network entities capable of detecting file modifications, triggering encrypted alerts, and transmitting them securely through the network to an admin node. The hybrid approach utilized 3DES for fast encryption of alert messages and RSA for secure key exchange, ensuring both security and performance balance. Findings from the simulation revealed that the improved intrusion detection algorithm effectively detected file alterations and securely transmitted alert messages without compromising performance. The integration of RSA and 3DES provided a robust encryption mechanism that improved key management, minimized computational overhead, and enhanced message confidentiality across MANET nodes. The study concludes that hybrid encryption significantly strengthens MANET security by combining the speed of symmetric encryption with the reliability of asymmetric key exchange. It recommends the adoption of hybrid cryptographic models for securing decentralized networks, the extension

of the framework for real-time applications, and further evaluation using larger and more complex MANET environments to enhance scalability and resilience.

KEYWORDS: Mobile ad-hoc Networks (MANETs), Rivest, Shamir and Adleman algorithm (RSA), Tripple Data Encryption Alogrithm (3DES), Hybrid Encryption, Intrusion.

1.0 INTRODUCTION

1.1 Background of the Study

Wireless networks employ wireless media for inter-entity (node or device) communication (Khan *et al.,* 2020). These networks are incredibly crucial for communication around the globe, be it in people's homes, workplaces, or organizations. The ability of wireless networks to link numerous portable devices across the Internet forms the basis for several crucial networking, real-time multimedia, and surveillance applications (Yan *et al.,* 2019). In the light of classification, wireless networks are typically categorised into Infrastructure-based Wireless Networks, and Wireless Ad-hoc Networks (Khan *et al.,* 2020).

The Wireless Ad-hoc Networks are Local Area Networks (LANs) that are built to allow the connection of two or more wireless devices over a medium. Because the communication nodes of these networks do not require any form of fixed infrastructure, they are sometimes referred to as "Infrastructure-less" Wireless Networks (Khan *et al.,* 2020).

Wireless Ad-hoc Networks, which allow any node to connect to any other node within the communication range and relay data to the destination node, have emerged from literature as potential research areas particularly the Mobile Ad-hoc Networks (MANETs). Through its numerous applications in the majority of fields, Ad-hoc Networks have been useful over the last two decades. However, because of their characteristics, which include hostile deployments, high levels of mobility, a lack of resources, and physical insecurity, they are at the forefront of attacks. Research has provided different mechanisms such as cryptographic methods (a method of encryption and decryption that employs a mathematical formula to convert plain text to cipher text and back) and intrusion detection system – IDS (software or hardware system that automate the process of monitoring the occurrence of attacks over a network) to halt some of these attacks (Kumar and Dutta, 2016). Mobile Ad-hoc Networks (MANETs) are wireless multi-hop networks that have the ability to broadcast data via a network of intermediary nodes (Muruganandam *et al.,* 2022).

Because of its application and adaptability in various applications, MANETs has lots of security problems. Links are open and actively movable here thus malicious nodes take

advantage of this facility and starts controlling nodes available in the network or starts receiving information packets after pretending as authenticated nodes (Manmohan *et al.,* 2020).

Due to the dynamic nature of MANETs that makes prevention methods insufficient to secure the networks, Randeep and Bakal (2016) suggested that it is necessary to include intrusion-detection system for MANETs as an additional layer of defence to check attacks. This additional layer of defence will check attacks to avoid overall system breach (Xenakis *et al.,* 2011; Muruganandam *et al.,* 2022).

In order to increase the security of MANET, intrusion prevention systems (software or hardware system used in MANETs to prevent the occurrence of attacks) and intrusion detection systems (software or hardware system that automate the process of monitoring the occurrence of attacks over a network) must all be in place. Muruganandam *et al.* (2022) offer an alternative approach for identifying hostile nodes in mobile ad-hoc networks with the construction of intrusion detection and prevention schemes. In order to detect malicious activity in a MANET environment, Muruganandam *et al.* (2022) present a dynamic algorithm and undertake experiments to compare the program's effectiveness with other algorithms.

All these studies have been targeted at building robust systems that could prevent attacks and safeguard MANETs.

1.2 Statement of the Problem

Intrusion detection and the absolute prevention of attacks for MANETs is a sensitive and complex task. This is because MANETs are mostly affected by several internal or external attackers. One of the most common attacks in MANETs comes from malicious nodes, such as the Black hole attack (Muruganandam *et al.,* 2022). Researchers agreed however, that improved security for MANETs is always possible with the use of intrusion detection algorithms. In order to provide security against multi-level attacks, Lalli and Jothi (2019), presented a solution to prevent and detect these attacks in MANETs using Rivest, Shamir and Adleman algorithm. However, since its initial publication, the MANETs have been utilising the RSA algorithm as a security layout has been attacked. The RSA algorithm has been analysed for vulnerability by many other researchers such as Chen *et al.* (2023), aiming to improve the RSA algorithm for better performance.

As an added solution to the problem of RSA's vulnerability, this work will highlight some of the attacks on the RSA algorithm and propose a new framework to improve the RSA algorithm for securing MANETs.

1.3 Aim and Objectives of the Study

The aim of this research was to develop and simulate an improved algorithm for intrusion detection in Mobile Ad-hoc Networks (MANETs).

The specific objectives of the study are to:

1. Design a hybrid encryption technique that integrates RSA and 3DES to enhance security and computational efficiency.
2. Simulate the algorithm developed in (i) in a network environment to examine its ability to detect intrusion attacks involving modifications such as file updates and deletions.
3. Evaluate the effectiveness and efficiency of the simulated hybrid algorithm in detecting intrusion attacks over MANETs.

2.0 LITERATURE REVIEW

2.1 The Concept of Intrusion Detection System

The concept of intrusion detection in mobile networks generally is hovered around the identification of activities (intrusions) on mobile networks which targets the altering of the standard operations of such a mobile network. Generally, any attempt that prevents a technology system from functioning properly or normally is classified as a security intrusion (Khraisat *et al.,* 2019). This includes, but not limited to, denial of service attacks, easter eggs, trojan horses, worms, time bombs, malicious code, keystroke loggers, social engineering, piggybacking, coat-tailing, and back doors (Insider, 2023). Intrusion detection systems (IDSs) are software or hardware devices that automate the process of tracking and examining network or computer system activity for indications of security issues (Randeep and Bakal, 2016).

Intrusion detection systems have two broad categories; Anomaly-based Intrusion Detection System (AIDS) and Signature-based Intrusion Detection System (SIDS) (Khraisat *et al.,* 2019).

2.1.1 Signature-based Intrusion Detection Systems

Signature Intrusion Detection Systems (SIDS), sometimes referred to as Knowledge-based Detection or Misuse Detection, are based on pattern matching approaches to locate a known attack. To locate a prior incursion in SIDS, matching techniques are used. In other words, an alarm signal is triggered when an intrusion signature coincides with an intrusion signature that already exists in the signature database. To detect malware, SIDS examines the host's

logs for patterns of commands or actions that have previously been recognized as malicious (Khraisat *et al.,* 2019).

For previously known incursions, SIDS typically provides good detection accuracy (Kreibich and Crowcroft, 2004). Due to the lack of a matching signature in the database until the new attack's signature is extracted and saved, SIDS struggle to identify zero-day assaults. Numerous widely used tools, such as Snort (Roesch, 1999) and NetSTAT Vigna and Kemmerer, (1999), use SIDS. Traditional methods for detecting SIDS go over network packets and attempt signature matching. These methods, however, are unable to recognize attacks that cover many packets. It could be necessary to extract signature information from numerous packets due to the sophistication of contemporary malware. In order to do this, the IDS must remember what was in prior packets. There have been various approaches to creating a signature for SIDS, including state machines (Meiners *et al.,* 2010) string patterns in formal languages, and semantic requirements (Lin *et al.,* 2011).

Since there is no known prior signature for any such attacks, the prevalence of zero-day attacks (Symantec, 2017) has made SIDS approaches progressively less effective. Malware with polymorphic versions and an increase in focused attacks may make this conventional paradigm less effective. Utilizing AIDS approaches, which focus on profiling normal behaviour rather than abnormal conduct, could be a solution to this issue (Khraisat *et al.,* 2019).

2.1.2 Anomaly-based Intrusion Detection Systems

Many researchers are interested in anomaly-based intrusion detection system (AIDS) since it can overcome SIDS's limitations. In AIDS, a typical model of a computer system's behaviour is built using machine learning, statistical analysis, or knowledge-based techniques. Anomalies are considered to be intrusions when there is a sizable difference between the observed behaviour and the model. This category of approaches is predicated on the idea that malevolent activity deviates from ordinary user behaviour.

The two stages that make up the development of AIDS are the testing phase and the training phase. As part of the testing phase, a fresh data set is utilized to determine the system's ability to generalize to previously unknown intrusions. During the training phase, the normal traffic profile is used to create a model of normal activity. According to the training methodology, AIDS can be divided into a variety of categories, including statistical, knowledge-based, and machine learning-based categories (Butun *et al.,* 2014).

Since AIDS does not rely on a signature database to detect irregular user behavior, its key benefit is its capacity to detect zero-day attacks (Alazab *et al.,* 2012). When the observed behavior deviates from the norm, AIDS raises a red flag. Moreover, AIDS offers a number of advantages. They are able to identify internal harmful activity, first. An alarm is raised if an intruder begins making transactions in a stolen account that aren't obvious from regular user activity. Second, because the system is built from personalized profiles, it is highly challenging for a cybercriminal to identify regular user behaviour without raising an alert.

Packet capture, NetFlow, and other network data sources are used by Network-based IDS to monitor network traffic that has been collected from a network. Many machines that are connected to a network can be monitored using network-based IDS. Before the risks propagate to another computer system, the Network-based IDS is able to monitor the external harmful actions that could be started from an external threat at an earlier stage. On the other hand, due to the volume of data travelling through contemporary high-speed communication networks, Network-based IDSs have a limited capacity to inspect all data in a high bandwidth network (Bhuyan *et al.,* 2014).

Network-based IDS deployed at different positions within a particular network topology, together with Host-based IDS and firewalls, can provide a better, resilient, and multi-tier protection against both external and insider attacks (Khraisat *et al.,* 2019). In order to increase detection rates while lowering false alarm rates, Creech *et al.* (2014), suggested a Host-based IDS methodology using discontinuous system call patterns (Creech, 2014). The fundamental concept is to understand abnormal program behaviour by applying a semantic structure to kernel-level system calls.

Anomaly-based intrusion systems can be implemented using one of three general approaches: machine learning-based Buczak and Guven (2016); Meshram and Haas (2017), knowledge-based Elhag *et al.* (2015), Can and Sahingoz (2015), or statistics-based Chao *et al.* (2015). The statistics-based approach entails gathering, analyzing, and creating a statistical model of typical user behaviour from each data record in a set of objects. The machine learning methods develop complicated pattern-matching skills from training data, while the knowledge-based approaches attempt to detect the requested actions from system data already present, such as protocol specifications and network traffic instances (Khraisat *et al.,* 2019).

2.2 The Concept of Mobile Ad Hoc Networks (MANETs)

The concept of mobile ad hoc networking is dated as far back as 1972 during the DARPA (Defence Advanced Research Projects Agency) Packet Radio Network project of 1972. A MANET is a self-configuring, infrastructure-less networks that consist of mobile nodes without a centralized administration, (Praveen *et al.,* 2022; Khudayer *et al.,* 2023). MANETs have emerged as a promising technology for various applications. Due to the nature of decentralized communication, MANETs have gained huge interest in different applications including emergency rescue operations, military operations, collaborative distributed computing, disaster management and some personal network applications (Walikar and Biradar, 2019) etc. Ad hoc network research was previously restricted to the military, and it wasn't until the middle of the 1990s, with the development of commercial radio technologies, that the wireless research community began to recognize the enormous potential and benefits of mobile ad hoc networks outside of the military context. This was evidenced by the establishment of the Mobile Ad hoc network Hoc Networking working group within the IETF (Hoebeke *et al.,* 2004).

Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. There are no base stations and every node must co-operate in forwarding packets in the network. Nodes can communicate directly and are in charge of dynamically discovering one another if they are within each other's transmit range. Intermediate nodes serve as routers that redirect packets generated by other nodes to their destinations, enabling communication between nodes that are not directly inside each other's transmit range. These nodes are frequently energy-constrained, battery-powered, and have a wide range of capabilities (Manmohan *et al.,* 2020).

In general, devices connected to a mobile ad hoc network are free to enter and leave the network, and they are also free to roam at will, which could lead to sudden and unforeseen changes in the topology. Nodes must organize themselves dynamically to offer the essential network functionality in this energy-constrained, dynamic, distributed multi-hop environment since there is neither fixed infrastructure nor centralized management.

Mobile ad hoc networks have several benefits despite the severe design limitations. First of all, this kind of network is ideal for usage in scenarios where a fixed infrastructure is unavailable, unstable, unreliable or too expensive. Ad hoc networks enable quick deployment with a minimum of user involvement because of its capacity for self-creation, self-organization, and self-administration.

Additionally, ad hoc networks can be connected to the Internet in order to integrate a variety of devices and make their services accessible to other users. This eliminates the requirement for ad hoc networks to function independently. Additionally, given that they can increase coverage and interconnectivity in conjunction with current cellular infrastructures, arguments based on capacity, range, and energy are made in favor of their adoption. Finally, MANETS do not need intricate wiring or base station installation design (Agrawal *et al.,* 2023).

2.3 Related Literature Review

Sivapriya and Mohandas (2022) presented an overview of various topics that have been discussed on MANET security. This effort led to the identification of elements contributing to threat scenarios, a summary of network security requirements, and the categorization of attacks based on the communication protocol stack. The article also presents potential research directions for developing promising future security systems for MANETs and related application paradigms.

Murugeshwari *et al.* (2023) conducted research on a hybrid key authentication scheme to ensure privacy in Ad-hoc communication. The Trust Aware Privacy-Preserving Protocol (TAP3) is a mechanism for supporting the origin in proactively selecting a trust-able target and doing privacy-preserving route verification. Nodes use their features to discover their fellow node and use the trust to create strong connections with the random node via a multi-hop trusting chain by identifying the secure location. The verification duties are then spread among the nodes and validate the log updates without exposing the nodes.

Islabudeen and Kavitha (2020) proposed a new method for improving MANET intrusion detection and prevention systems to prevent security attacks. The technique involves creating and implementing a MANET-specific intrusion detection and prevention system by using four entities: Packet Analyzer, Preprocessing Unit, Feature Extraction Unit and Classification Unit.

Ghodichor *et al.* (2023) conducted research on securing MANET against attacks using a blockchain-based Secure Routing Algorithm (SRA). MANET, being an infrastructure-less network with a dynamic topology, is highly vulnerable to attacks. The secure routing algorithm (SRA) proposed by blockchain technology safeguards control and data flow against threats. This is achieved by generating a Hash Function for every transaction.

Khan *et al.* (2021) built a mechanism to analysed the performance of Adhoc on-demand Distance Vector Protocol (AODV), a reactive routing protocol under the influence of Black

hole, Gray hole and Worm hole attacks in MANET. They proposed a security mechanism that is based on two techniques, namely: cryptography-based, and trust-based.

Regassa and Yeom (2021) implemented an IDS mechanism along with the OLSR (Optimized Link State Routing) protocol to accurately detect misbehaving nodes in a MANET. The mechanism validates the path and detects attackers, isolating them through an alternative path for End-to-End communication. Although this approach adds some network overhead, it significantly improves network security.

Torky *et al.* (2022) proposed a new drone charging system management method. System was simulated on a generated dataset consisting of 300 drones and 50 charging station points to evaluate its performance. The optimization of the proposed scheduling methodology was based on the particle swarm optimization (PSO) algorithm and game theory-based auction model. In addition, authenticating and verifying drone charging transactions were executed using a proposed blockchain protocol.

Kaur and Kakkar (2022) proposed a new routing security method for Vehicular Ad Hoc Networks. Their approach combines hybrid optimization and deep learning-based attack detection. The hybrid optimization-based Deep Maxout Network (DMN) was developed for attack classification in VANET. The Cluster Head (CH) selection and routing process was performed using designed hybrid optimization algorithm.

Pooja, Kavita, and Gia (2020) proposed a protective mechanism against dual attacks in MANET with specific focus on Black Hole Attack and Gray Hole attacks by using the concept of Artificial Neural Network (ANN) as a deep learning algorithm along with the swarm-based Artificial Bee Colony (ABC) optimization technique. For the network designing and simulation purposes, MATLAB software was used with communication and neural network toolboxes.

Korir and Cheruiyot (2022) suggest a survey to assess MANET routing protocol security risks. Implementation involves collecting data from relevant literature and analyzing MANET routing protocols. MANET routing protocol security, vulnerabilities, and deficiencies are examined in the output values.

Srilakshmi *et al.* (2022) presented a MANET-specific safe optimization routing method. The Bacteria for Aging Optimization Algorithm (BFOA), which finds the ideal hops in advancing the routing, was utilized to offer a trust-based protected and energy-efficient navigation in MANETs. The fuzzy clustering algorithm was activated first, and the Cluster Heads (CHs) were selected depending on the value of indirect, direct, and recent trust that each CH had.

Abdan and Seno (2022) proposed machine learning to detect MANET wormhole attacks. Implementation involves training machine learning models to identify and classify wormhole attacks and deploying the detection system in a MANET.

Alsarhan *et al.* (2021) proposed a machine learning-based optimization strategy to improve VANET IDS performance using Support Vector Machines (SVM). Machine learning models improve intrusion detection precision and effectiveness.

Khalifa, Nuri and Ali (2021) proposed an Intrusion Detection System (IDS) using three Machine Learning (ML) techniques: Random Forest (RF), Support Vector Machines (SVM), and Naive Bayes (NB). These techniques were applied to classify nodes in MANET using the Dynamic Source Routing (DSR) protocol.

3.0 METHODOLOGY

3.1 Overview

Methodology is the overall approach to the software development process that guides the team on how to plan, design, implement, and maintain the system. In this study, Object-oriented design (OOD) methodology is employed.

The use of an object-oriented design technique in the context of designing an intrusion detection and prevention algorithm for Mobile Ad-hoc Networks (MANETs) is deliberate and advantageous. By reducing large systems down into modular and encapsulated components, object-oriented modeling excels at simulating them. This method is consistent with the intricate structure of cryptographic algorithms, allowing for the depiction of key cryptographic components like keys, encryption processes, and network nodes as discrete, interconnected objects.

The object-oriented model acts as a template for the algorithm's design and implementation, fostering a clear and organized architecture. Classes are developed to encapsulate the attributes and behaviors of cryptographic pieces, allowing them to be reused and modularized. For example, in the MANET environment, network nodes are represented as objects, each with its own set of attributes and functionalities. This abstraction facilitates in the management of MANETs' essential complexity, as well as the cryptographic operations requiring RSA and 3DES.

Aside from the conceptual advantages, the choice of simulating MANET nodes using Python's object-oriented capabilities improves the study's practicality. The simulation environment provides a controlled environment in which to test and validate the generated method. It enables the simulation of real-world MANET situations such as node mobility and

changing network topologies, giving a realistic foundation for assessing the algorithm's performance under various scenarios.

3.2 Analysis of the Existing System

The RSA technique is widely used in the Intrusion Detection System (IDS) that is currently being used in the Mobile Ad-Hoc Network (MANET). Even with RSA's contribution to strong security base, issues still arise, especially with computational efficiency. This is especially clear in Mobile Ad-Hoc Network (MANET) circumstances where resources are limited.

The importance of the RSA algorithm in enhancing MANET security is highlighted by recent study, which places it as the main security mechanism (Sankarayanan *et al.,* 2017). Though the study recognizes the restrictions imposed by the inherent limitations on resources of MANET systems, it also recognizes the importance of addressing computational efficiency concerns.

To achieve improved communication security in MANETs, researchers have been investigating better or different algorithms. The goal of research into novel cryptographic techniques is to reduce the computational burden that the RSA algorithm alone bears. Examples of these techniques include hybrid cryptographic techniques that incorporate several algorithms, such as DES and RSA.

3.3 Analysis of the Developed System

The system is a significant development in improving network security. The system was designed to imitate five nodes, which presents an enhanced algorithm for intrusion detection in the MANET network. In this approach, the last node, considered to be the admin node or intended receiver, serves as the heart of the network for secure communication. Meanwhile, the first four nodes work as MANET nodes, actively monitoring specific directories. When changes are detected in these directories, the sender node sends an encrypted alert message using the hybrid encryption techniques. This encrypted message proceeds through a network of connected nodes until it reaches the admin node, ensuring a safe and robust communication channel. An important part of the developed system was the establishment of a network upon the creation of each node, which serves as a means for nodes to interconnect and share their respective public keys. This critical step ensures that each node possesses the necessary public keys to facilitate secure communication within the MANET.

The application of a hybrid encryption technique, which involves combining the strengths of both the Triple Data Encryption Standard (3DES) and the Rivest-Shamir-Adleman (RSA) algorithms, distinguishes this developed system. Each simulated MANET node actively monitors its specified directory, sending an alert message as soon as any file alterations are detected. This decentralized alerting mechanism ensures quick intrusion detection within the dynamic MANET network, which is crucial for improving security in resource-constrained environments.

The alert message is encrypted using a refined hybrid encryption technique that strategically uses the admin node's public key to encrypt the 3DES key used in encrypting the alert message. This approach protects against potential interception by intermediary nodes, ensuring the utmost level of confidentiality during the message transport.

The alert message is first symmetrically encrypted using the 3DES technique, assuring efficiency and speed. Following that, the 3DES key, which is also used to decrypt the alert message, is asymmetrically encrypted using the admin node's public key using the RSA technique. This hybrid encryption solution makes use of the speed of symmetric encryption while also increasing the security of the key exchange process via asymmetric encryption.

The admin node's public key is important in this hybrid encryption process since it serves as a secure route for transferring the encrypted 3DES key. This means that only the admin node, possessing the corresponding private key, can successfully decrypt the asymmetrically encrypted 3DES key, subsequently allowing the deciphering of the original alert message. This dual-layered encryption methodology forms the backbone of the system's resilience against unauthorized access and ensures a confidential and secure communication environment within the MANET. The architecture of the developed system is shown in Figure 6.

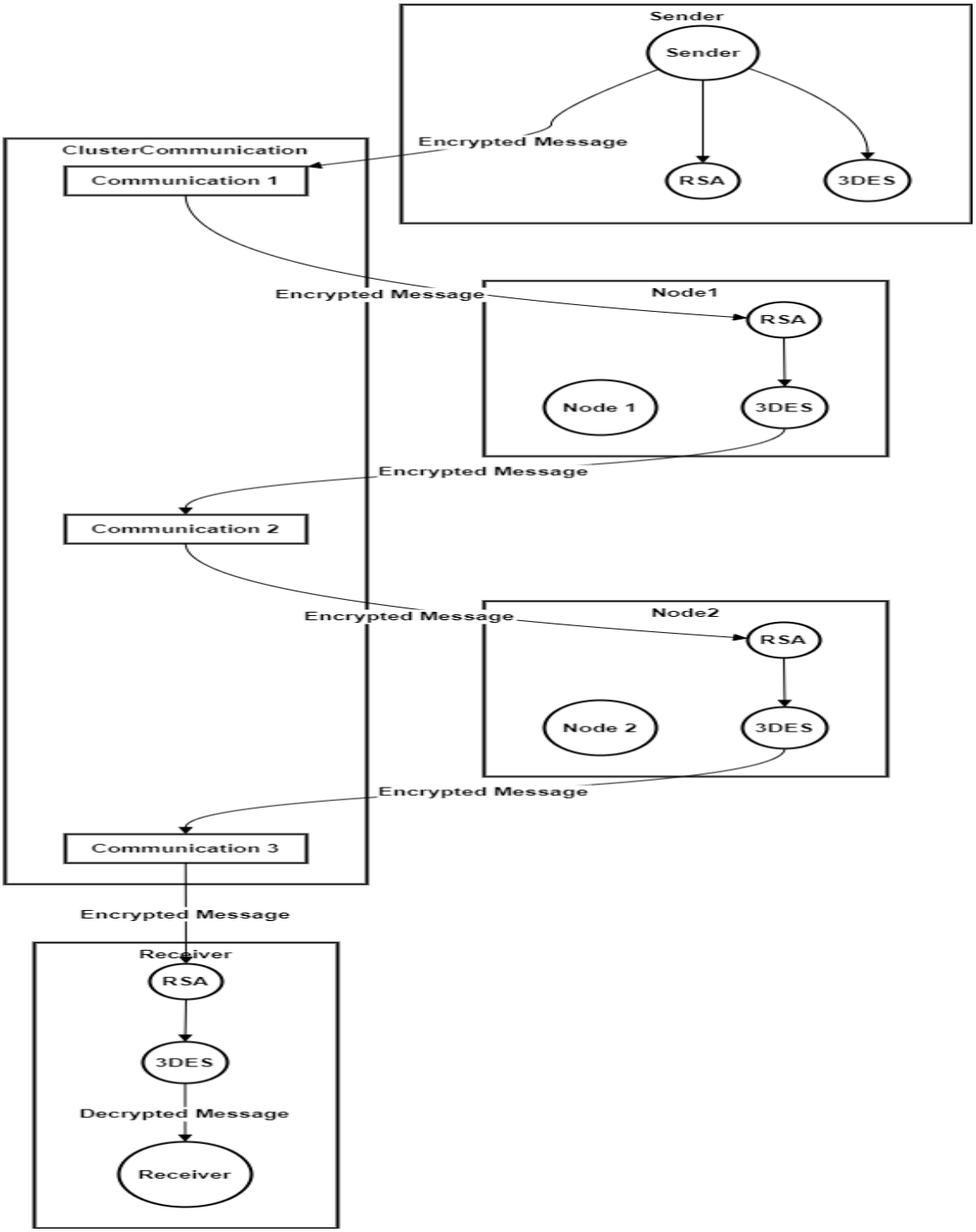

FIGURE 6: Developed System Architecture

3.4 Design of the Developed System

The cryptographic approach employed in this system plays a pivotal role in ensuring the confidentiality and security of communication within the Mobile Ad-Hoc Network (MANET). The chosen cryptographic method is the hybrid encryption approach, seamlessly

integrating the strengths of both the Triple Data Encryption Standard (3DES) and the Rivest-Shamir-Adleman (RSA) algorithms.

3.4.1 Symmetric Encryption with 3DES

Symmetric encryption is a cryptographic approach that uses the same key for both data encryption and decryption. In the context of the developed system, the symmetric encryption algorithm is 3DES (Triple Data Encryption Standard).

Triple Data Encryption Standard (3DES) is an evolution of the original Data Encryption Standard (DES) algorithm. DES, while widely used, became vulnerable to brute-force attacks due to its relatively short key length. 3DES addresses this vulnerability by applying the DES algorithm three times in succession.

3DES Algorithm:

- **Key Generation:** 3DES uses three 56-bit keys, providing a total key length of 168 bits. The three keys are derived from a longer key through a process called keying option 1, where the same key is used for each of the three steps.
- **Encryption:** 3DES encrypts data in three stages: an encryption operation (E), a decryption operation (D), and another encryption operation (E). The algorithm encrypts the plaintext, decrypts the result, and then encrypts it again (Srinivasa, 2015).
  Ciphertext = E (K1, D (K2, E (K3, Plaintext)))
- **Decryption:** The decryption process is the reverse: it decrypts (D), encrypts (E), and then decrypts (D) the data.
  Plaintext = D (K3, E (K2, D (K1, Ciphertext)))

3.4.2 Asymmetric Encryption with RSA

The RSA algorithm, chosen for its key exchange capabilities, facilitates the secure transmission of the 3DES key. This asymmetric encryption process adds an extra layer of security by ensuring that only the intended recipient, possessing the corresponding private key, can successfully decrypt the key and subsequently access the encrypted alert message.

RSA Encryption Steps:

- **Key Generation:** Generate Prime Numbers: Select two large prime numbers, p and q. Calculate Modulus (N): Compute $N=p\times q$. Compute Euler's Totient Function $\phi(N)$: Calculate $\phi(N)=(p-1)\times(q-1)$. Select Public Exponent (e): Choose e such that $1<e<\phi(N)$

and e is coprime to ϕ(N). Calculate Private Exponent (d): Compute d such that d ≡ e−1(mod ϕ(N)).

- **Encryption:** Message Representation: Represent the message M (3DES key) as an integer where 0 <M <N. Compute Ciphertext (C): C ≡ M^e (mod N).
- **Decryption:** Compute M ≡ C^d (mod N). The resulting M is the decrypted message, which is the 3DES key in the context of this study (Tahir, 2015).

3.4.3 Hybrid Encryption Design

The design of the hybrid encryption mechanism involves a combination of symmetric and asymmetric encryption algorithms. At its core, the developed system leverages the efficiency of 3DES for symmetric encryption, ensuring swift and secure encryption of alert messages. Simultaneously, the RSA algorithm is employed for asymmetric encryption, specifically for securing the 3DES key used in the encryption process.

The developed system was designed with the aid of a pseudocode shown below:

Start

Procedure Node Initialization ():

Generate public-private key pair (PK, SK) using RSA algorithm

Establish connection with neighboring nodes

Share public key (PK) with neighboring nodes

Procedure Monitor Directory ():

While True:

Check for any changes in specified directory

If changes detected:

Generate alert message

Encrypt alert message using 3DES algorithm

Encrypt 3DES key using admin node's public key (RSA)

Send encrypted alert message to neighboring nodes

Procedure ForwardMessage(encrypted_alert_message, target_node):

If current node is not the target_node:

Find nearest neighboring node to target_node

Forward encrypted_alert_message to nearest neighboring node

Else:

Receive Alert Message (encrypted_alert_message)

Procedure Receive Alert Message (encrypted_alert_message):
Decrypt 3DES key using admin node's private key (RSA)
Decrypt alert message using decrypted 3DES key
If alert message is intended for current node:
Process alert message
Else:
Forward Message (encrypted_alert_message, target _node)

Procedure Admin Node Processing ():
While True:
Receive encrypted alert messages from neighboring nodes
Decrypt alert messages using admin node's private key
Process alert messages and take appropriate action

Procedure Main ():
Initialize node
Monitor directory for changes
If node is admin node:

Admin Node Processing ():
Else:
ReceiveAlertMessage(encrypted_alert_message)
End

3.6 Choice of Programming Language

Programming languages have strengths in different areas. Some languages are powerful but can be bug-prone and difficult to work with, while others are simpler but can be limiting in terms of functionality or performance (Ben *et al.* 2001). In this research work, python is used. Python is a high level, interpreted and general-purpose dynamic programming language. The syntax in python helps the programmer's code in fewer steps as compared to other programming languages. It is used in to carry out this study because; it supports web applications, it has many in built functions, it has extensive support libraries and it has user friendly data structures.

3.7 System Requirements

The system requirements are essential for the efficient running of the file sharing application and the file encryption and decryption modules.

Hardware requirements:

1. 64-bit PC
2. Hard drive of at least 500MB free space

Software requirements:

1. Operating system: Windows 10 or later, macOS 10.12 or later, or Linux
2. Python 3.6 or later
3. PyCrypto module for generating the 3DES and RSA algorithm
4. Socket: to perform network initialization and communication
5. Colorama: Colorama python library efficient in visually representing the test results, particularly in highlighting the different types of file intrusions such as creation, deletion, and modification.

4.0 RESULTS

4.1 Implementation and Results

The secure network intrusion detection system in Mobile Ad hoc networks (MANETs) was implemented using Python version 3.11.5 as the programming language. The design specifications carried out in the previous chapter were implemented into a functional software application using an object-oriented programming paradigm.

4.1.1 Implementation of the AdminNode Class

The AdminNode class was implemented into a functional module responsible for decrypting and recording incoming messages from the MANETNode. It features a decryptMessage() method that utilizes the DecryptionHandler class to decrypt alert messages received from the MANETNode. Additionally, the recordMessage() method is responsible for saving decrypted messages, which aids future analysis and traceability.

By using these methods, the AdminNode effectively monitors, secures, and processes alert messages. This collaborative approach ensures a secure and efficient system for detecting and responding to potential threats within the network.

4.1.2 Implementation of the MANET Node Class

The MANET Node class was implemented into a module consisting of several methods that perform essential tasks for maintaining network security:

- The monitor Directory () method uses the Directory Monitor class to continuously watch directories for file changes. This method is responsible for detecting any modifications within assigned folders and helps maintain an active intrusion detection system.
- The trigger Alert () method employs the Alert Message class to generate alerts when an intrusion or file modification is detected in the monitored directory. This method ensures that potential threats are swiftly identified and reported.
- The encrypt Message () method uses the Encryption Handler class to secure alert messages before they are transmitted to the Admin Node. This method employs encryption techniques to protect the content of the alert messages, ensuring the confidentiality of the information being communicated.

These methods work together within the MANET Node class to create a robust system that monitors, identifies, and encrypts critical alert messages to maintain security and effectively manage potential threats within the network.

4.2 Program Testing

Following the implementation of the secure network intrusion detection system in MANETs, thorough program testing was conducted to ensure its functionality, reliability, and security. The testing phase encompasses various methodologies and techniques to validate the system's performance under different scenarios and conditions.

4.2.1 Unit Testing

Unit testing involves testing individual components or units of the system in isolation to verify their correctness and functionality. Each module, class, or function within the system was tested independently to ensure that it behaved as expected. For example, unit tests were conducted to verify the encryption and decryption processes, folder monitoring functionality, and message routing mechanisms.

4.2.2 Integration Testing

Integration testing was performed to validate the interactions between different components or modules of the system. This testing phase ensures that the integrated system functions as intended and that data flows correctly between various modules. Integration tests verify the

seamless communication between nodes, proper encryption and decryption of messages, and the routing of alert messages through the network.

4.2.3 System Testing

System testing evaluates the entire system to ensure it meets the specified requirements and objectives. This phase involves comprehensive end-to-end testing, simulating various intrusion scenarios, file modifications, and network conditions to assess the system's ability to detect and respond to security threats effectively.

The test cases cover essential processes such as key management, intrusion detection, and encryption, secure message routing, decryption, and overall system performance. By integrating RSA and 3DES encryption, the system ensures secure communication while efficiently detecting and responding to unauthorized modifications within the network. The objectives and expected outcomes of the test cases are detailed in Table 4 below.

Table 1: Test Cases.

No.	Test Case	Test Objectives	Expected Outcomes
1	TC1	To test if the system can successfully initialize the Key Manager for secure key distribution	The system initializes the Key Manager Node, which generates RSA key pairs fundamental for the hybrid encryption technique
2	TC2	To test if nodes can securely connect to the MANET network via the Key Manager	Nodes successfully connect to the MANET network and exchange RSA public keys with the Key Manager Node
3	TC3	To test if the system can detect file modifications and trigger an encrypted alert message	The system detects file modifications in monitored directories and triggers an alert message encrypted using 3DES
4	TC4	To test if alert messages are encrypted using the 3DES algorithm	The system encrypts alert messages using the 3DES algorithm, demonstrating the symmetric encryption component of the hybrid technique
5	TC5	To test if the system can securely route encrypted alert messages to the admin node	The encrypted alert messages are securely transmitted through the MANET network to the admin node, leveraging RSA for key exchange and 3DES for message encryption
6	TC6	To test if the admin node can decrypt received alert messages and record them for further analysis	The admin node successfully decrypts alert messages using its private RSA key, completing the hybrid encryption process
7	TC7	To evaluate the overall functionality, security, and efficiency of the system under normal operating conditions	The system is tested under various conditions, ensuring it operates efficiently, detects intrusions in real-time, and maintains optimal performance

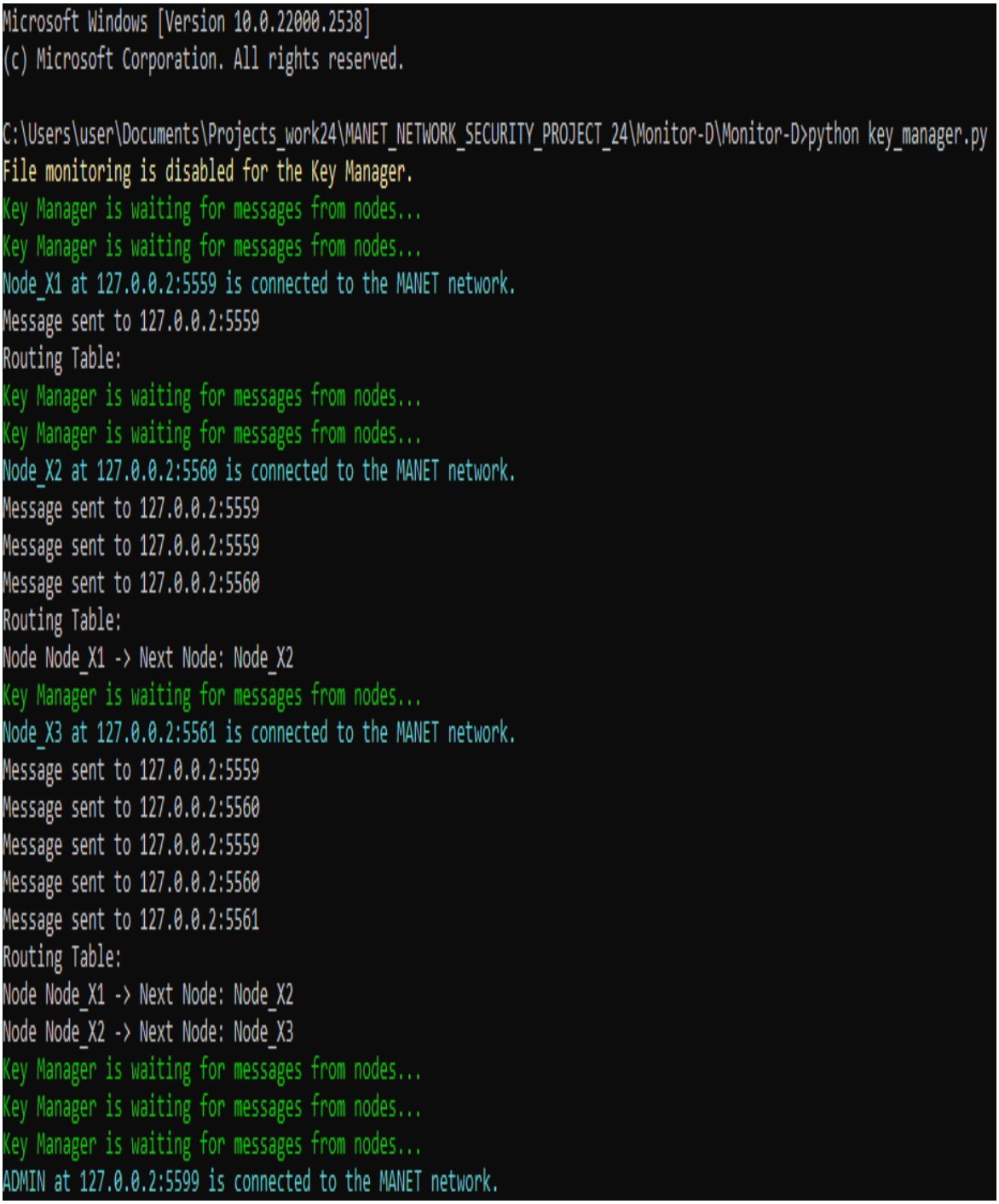

FIGURE 2: Initialization of Key Manager Node.

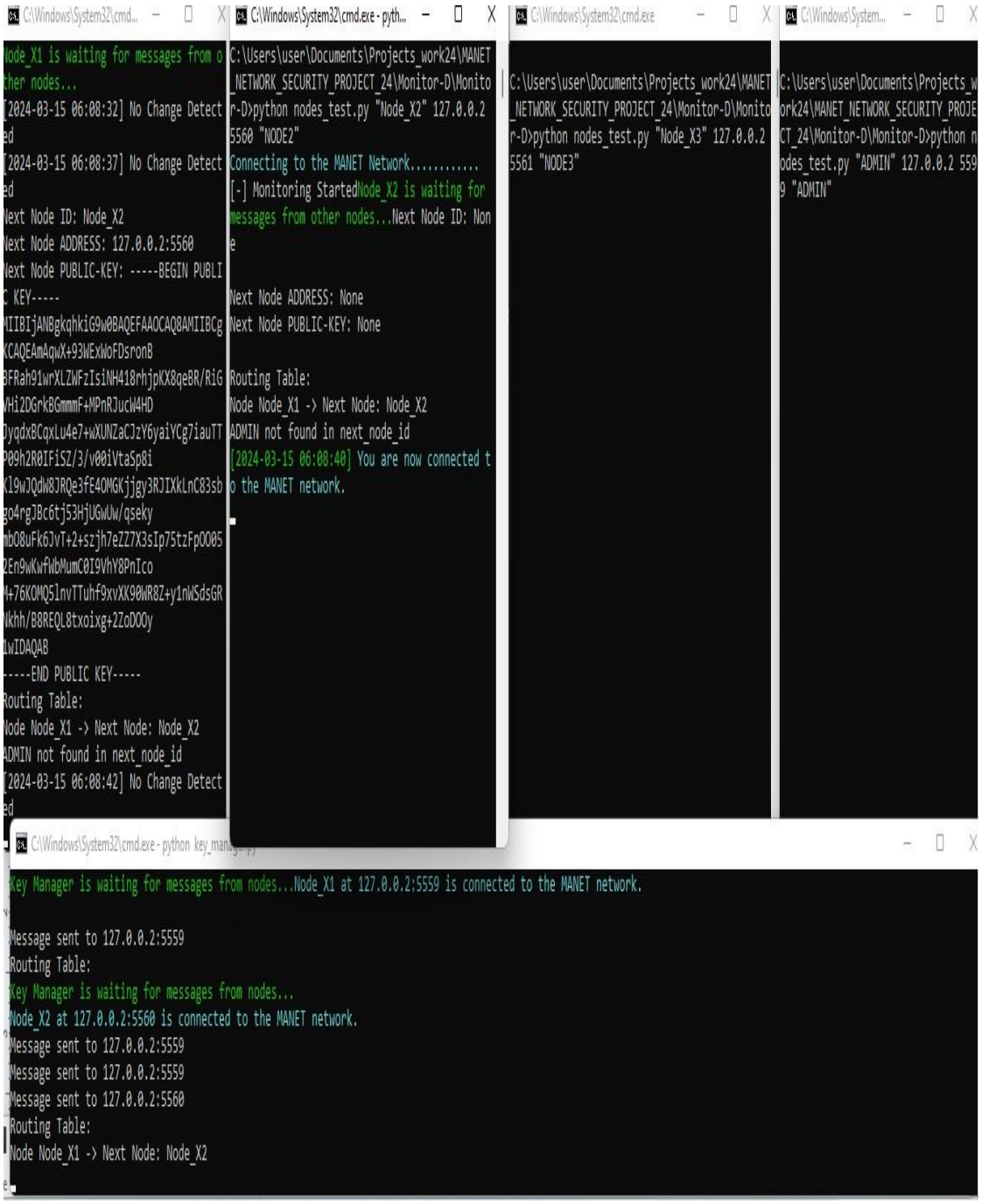

FIGURE 3: Node Connection to MANET Network.

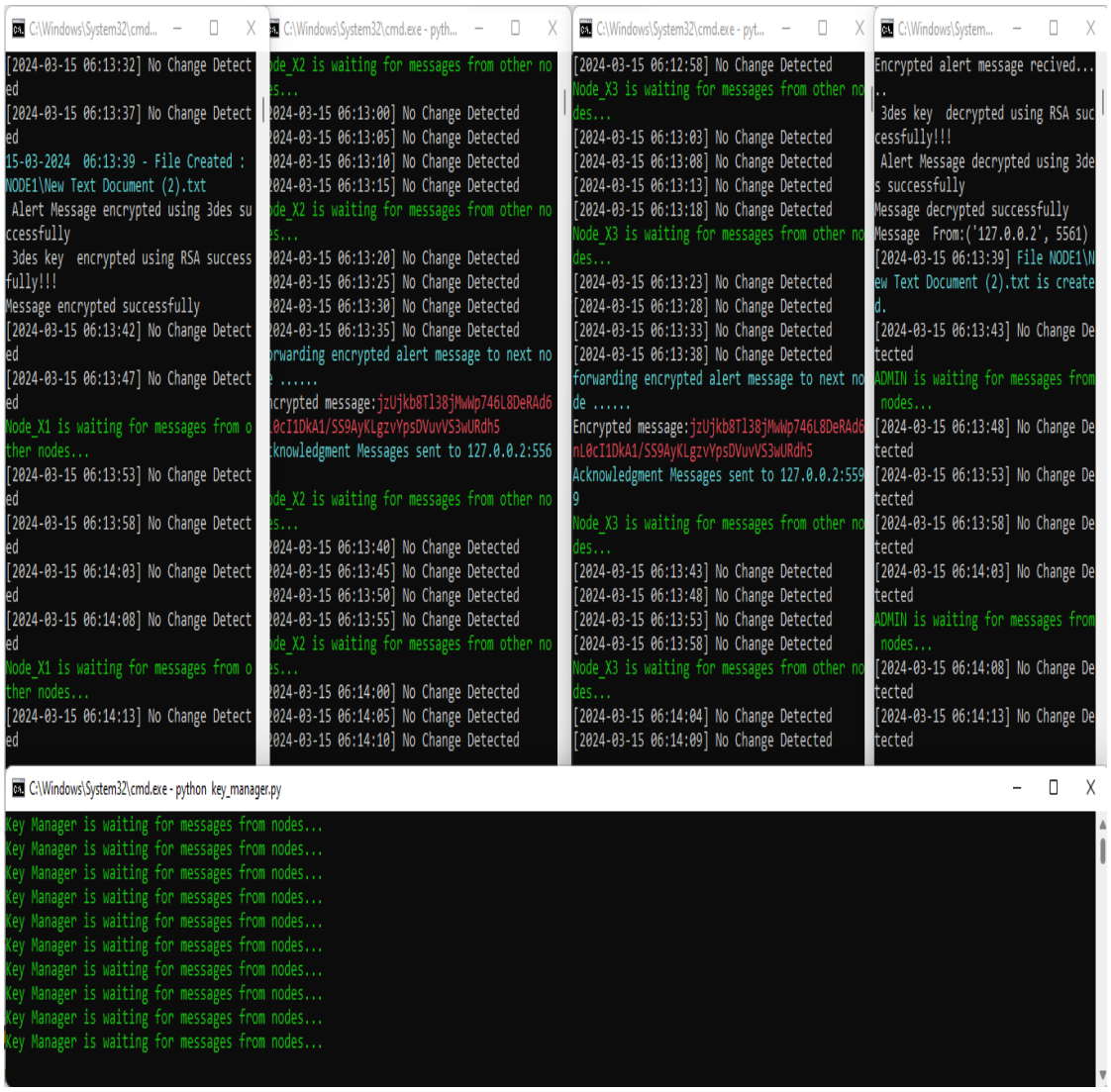

FIGURE 4: HERE: Alert Message Triggering.

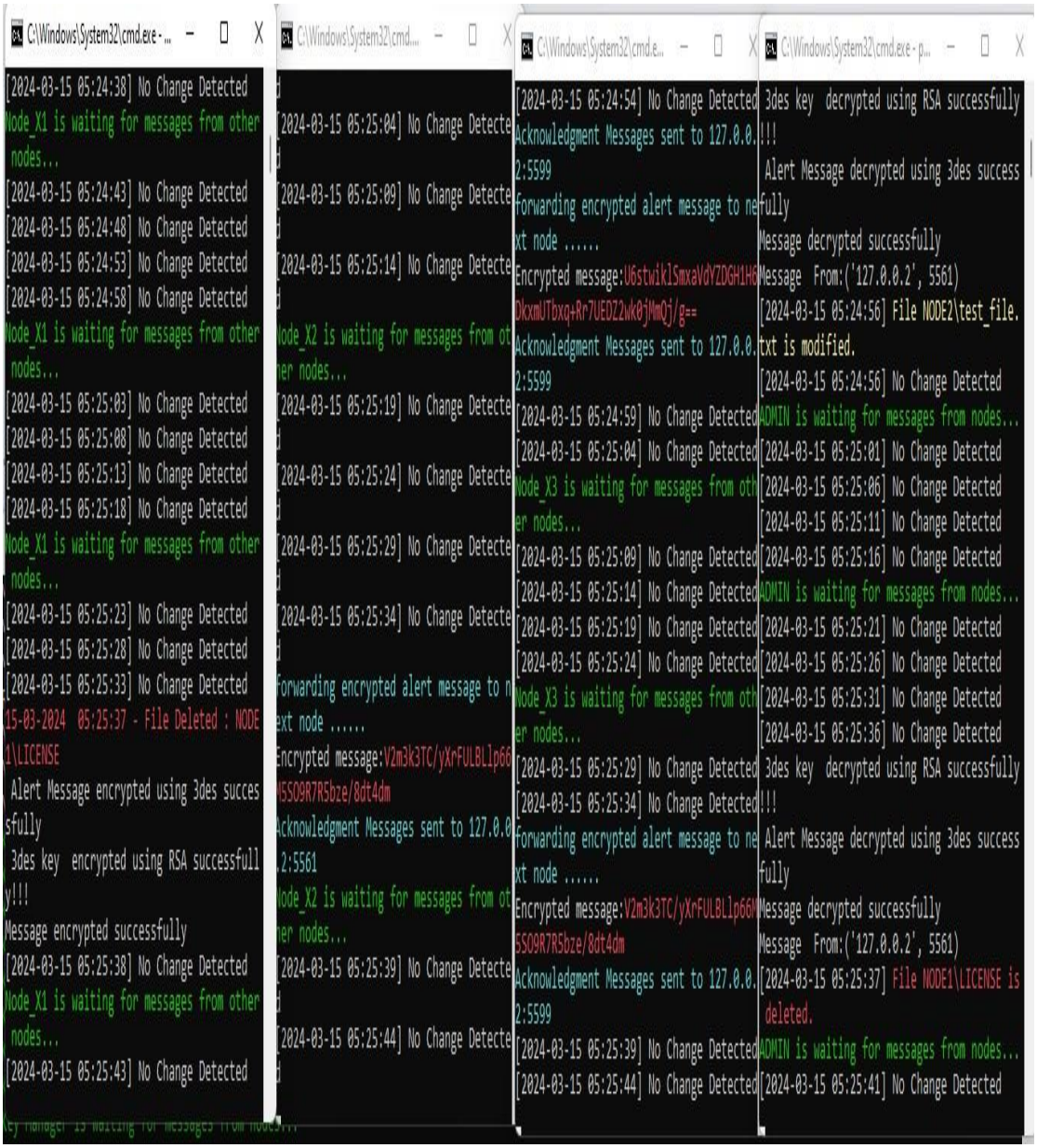

Figure 5: Secure Message Routing through node2 and node 3.

5.0 DISCUSSION

5.1 Discussion of Test Results

The results of the testing phase demonstrate the functionality and performance of the Secure Network Intrusion Detection System in Mobile Ad-Hoc Networks (MANETs). The outputs obtained from the various test-cases were carefully analyzed and each test case was executed to assess specific aspects of the system's behavior and capabilities. Below are the findings from each test case.

5.1.1 Test Case 1: Initialization of Key Manager Node

In Test Case 1 (TC1), the initiation of the Key Manager Node proceeded smoothly, resulting in successful outcomes. Specifically, the system efficiently kick-started the Key Manager Node, accomplishing vital tasks like generating RSA key pairs and establishing connections with other nodes in the MANET network. This effective initialization establishes a sturdy basis for secure communication within the network, showcasing the system's adeptness in setting up crucial components.

The observed outcomes affirm that the system executed the initiation process effectively, ensuring the Key Manager Node's preparedness to facilitate secure communication. Through the generation of RSA key pairs and the establishment of connections with other nodes, the system showcased its proficiency in laying the groundwork for secure interactions within the MANET environment. Overall, this test case confirms the system's ability to initialize essential components accurately, underscoring its readiness for secure network operations. The result of Test-Case 1 is shown in Figure 2.

5.1.2 Test Case 2: Node Connection to MANET Network

Test Case 2 (TC2) shows that the system efficiently allowed nodes to join the MANET network through the Key Manager Node, where they could exchange their RSA public keys. This process helped in building a network where communication between nodes could be trusted. The outcomes observed indicate that the system effectively managed node connections, ensuring that nodes seamlessly became part of the MANET network.

By enabling nodes to connect and exchange their RSA public keys, the system proved its ability to create secure communication paths within the network. This successful integration of nodes into the MANET environment highlights the system's effectiveness in fostering reliable connections and ensuring the network operates smoothly. Overall, TC2 confirms the system's proficiency in handling node connections and establishing secure communication channels, which are crucial for maintaining the MANET network's integrity and security. The result of Test-Case 2 is shown in Figure 2.

5.1.3 Test Case 3: Alert Message Triggering

Test Case 3 (TC3) shows how quickly the system can send out alert messages when it notices any changes to files in specific folders. This quick reaction means that the system is good at spotting possible security risks in the network. By letting administrators know right away about any file changes, the system helps improve the network's security. It acts like an early

warning system for any attempts to break into the network or access files without permission. TC3 proves that the system can detect and deal with security issues as they happen, making the network stronger and able to handle potential threats. The result of Test-Case 3 is shown in Figure 3.

5.1.4 Test Case 4: Alert Message Encryption

Test Case 4 (TC4) shows that the system adeptly encrypted alert messages using the 3DES algorithm and a shared secret key, ensuring robust security measures for message transmission. This encryption process effectively scrambles the content of alert messages, rendering them unreadable to unauthorized entities and bolstering the confidentiality of communication within the MANET network.

By employing encryption, the system significantly enhances the security of alert messages, mitigating the risk of interception or tampering during transit. This cryptographic technique adds an extra layer of protection, safeguarding sensitive information against potential threats and contributing to the overall resilience of the network. The result of Test-Case 4 is shown in Figure 3.

5.1.5 Test Case 5: Secure Message Routing

Test Case 5 (TC5) shows that the Encrypted alert messages were securely routed through the MANET network to the admin node, demonstrating the system's proficiency in maintaining message confidentiality and integrity. Through robust routing mechanisms, the system ensured that encrypted messages reached their intended destination without compromising data security. The successful routing of encrypted messages underscores the system's capability to establish and maintain secure communication channels within the MANET environment. By preserving the confidentiality and integrity of message transmission, the system fosters trust among network nodes, facilitating reliable information exchange and effective collaboration. The result of Test-Case 5 is shown in Figure 4.

5.1.6 Test Case 6: Admin Node Decryption and Analysis

Test Case 6 (TC6) demonstrates that the admin node effectively decrypts the encrypted alert messages and saved them for later reference, allowing constant monitoring and examination after security incidents. This decryption process ensures that authorized personnel can access and analyze alert messages promptly, facilitating timely responses to security threats and enhancing overall network defense. With its decryption and analysis capabilities, the admin node plays a crucial role in finding and dealing with security problems in the MANET

network. By recording decrypted messages, the system creates a track record of security events, making it easier to investigate and fix problems when needed. The result of Test-Case 6 is shown in Figure 4.

5.1.7 Test Case 7: System Functionality and Performance

Test Case 7 (TC7) demonstrates that the system operates optimally, accurately detecting and responding to security threats within the MANET network. This high level of functionality ensures that the system effectively fulfills its role in safeguarding network integrity and protecting against potential intrusions or malicious activities. The system's exceptional performance and scalability demonstrate its readiness to handle the dynamic nature of MANET environments. By efficiently detecting and addressing security threats, the system enhances the resilience of the network and instills confidence in its ability to maintain secure operations under various conditions. The result of Test-Case 7 is shown in Figure 5.

6.0 CONCLUSION AND RECOMMENDATION

6.1 Conclusion

In this study, the researchers have developed and evaluated an improved Algorithm for Intrusion detection in Mobile Ad-hoc networks. Through a series of test cases, the researcher assessed critical functionalities such as initialization, encryption, decryption, and overall system performance. The results demonstrate the system's effectiveness in detecting and responding to security threats, thus enhancing the overall security posture of MANETs.

The successful completion of test cases validates the system's capability to establish secure communication channels, detect file modifications, trigger alert messages, and securely route encrypted messages within the network. Moreover, the system's decryption and analysis capabilities at the admin node enable real-time monitoring and post-incident investigation, further strengthening the network's resilience against potential security breaches.

6.2 Recommendations

While the current system shows promising results, there are several avenues for future research and development to enhance its capabilities and address potential limitations:

- **Performance Optimization:** Optimize system performance to reduce resource consumption and improve scalability, particularly in large-scale MANET deployments. Techniques such as parallel processing, distributed computing, and network optimization can enhance system efficiency and responsiveness.

- **Real-world Deployment:** Conduct real-world deployment trials to evaluate the system's performance under diverse environmental conditions and network topologies. Collaborate with industry partners and government agencies to assess the system's practicality, usability, and effectiveness in real-world scenarios.
- **User Education and Training:** Provide comprehensive user education and training programs to network administrators and end-users to enhance awareness of security best practices and promote proactive security measures. Empowering users with the knowledge and skills to identify and respond to security threats can significantly improve the overall security posture of MANETs.

6.3 Contributions to Knowledge

1. The algorithm provides a secure and efficient method for monitoring and protecting decentralized Mobile Ad-hoc Networks (MANETs). It strengthens the overall security architecture by ensuring the integrity and confidentiality of data transmissions within dynamic and infrastructure-less environments.
2. A major contribution of this work is the integration of RSA and 3DES encryption algorithms. This hybrid approach leverages the advantages of both symmetric (3DES) and asymmetric (RSA) encryption techniques, offering robust protection for sensitive information and secure key management across the network.
3. The project introduces a detailed framework for testing and evaluating intrusion detection systems in MANETs. This framework provides standardized guidelines and methodologies that can assist researchers and developers in assessing the performance, effectiveness, and reliability of various security measures in dynamic network environments.
4. The system and methodologies establish a foundation for future advancements in MANET security. The hybrid encryption model and evaluation framework can be extended or adapted for other wireless or decentralized network environments, promoting continued innovation in intrusion detection and data protection technologies.

In conclusion, the development of a robust and secure system for intrusion detection in MANETs is essential for safeguarding critical infrastructure and ensuring reliable communication in dynamic network environments. By addressing the aforementioned research directions, we can further strengthen the system's security capabilities and pave the way for the widespread adoption of MANET technology in various domains, including military operations, disaster response, and emergency communication systems.

REFERENCES

1. Abdan, M., and Seno, S.A.H. (2022). Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). *Wireless Communications and Mobile Computing*, 2022, 1-12.
2. Abhiram Shashank, N., and Bharathi, C. (2019). Secure Intrusion Detection System for MANETs Using Triple-DES Algorithm. *Proceedings of Engineering and Technology Innovation, 12*, 39-46.
3. Abid, R., Iwendi, C., Javed, A. R., Rizwan, M., Jalil, Z., Anajemba, J. H., and Biamba, C. (2021). An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Personal and Ubiquitous Computing*, 1-14.
4. Albers, P. Camp, O. (2002). "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches". Proceedings of the 1st *International Workshop on Wireless Information Systems*, (pp. 1-12).
5. Alsarhan, A., Alauthman, M., Alshdaifat, E.A., Al-Ghuwairi, A.R., and Al-Dubai, A. (2021). Machine Learning-driven Optimization for SVM-Based Intrusion Detection System in Vehicular Ad hoc Networks. *Journal of Ambient Intelligence and Humanized Computing*, 1-10.
6. Axelsson, S. (1998). Research in Intrusion-Detection Systems: A Survey. Technical Report 98–17. Department of Computer Engineering, Chalmers University of Technology.
7. Axelsson, S. (2000). Intrusion Detection Systems: A Survey and Taxonomy.
8. Bace, R. G., and Mell, P. (2001). Intrusion Detection Systems.
9. Buczak, A. L., and Guven, E. (2015). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys and Tutorials*, 18(2), 1153-1176.
10. Chen, Z; Liu, F; and Sonia, C. Security Analysis of another Vulnerability to RSA Algorithm. 13th *International Conference*.
11. Freebersyser, J. A., and Leiner, B. (2001). A DoD Perspective on Mobile Ad-hoc Networks. *In Ad hoc networking* (pp. 29-51).
12. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., and Vázquez, E. (2009). Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges. *Computers and Security*, 28(1-2), 18-28.

13. Ghodichor, N., Sahu, D., Borkar, G., and Sawarkar, A. (2023). Secure Routing Protocol To Mitigate Attacks By Using Blockchain Technology In Manet. *arXiv preprint arXiv:2304.04254*.
14. Hoebeke, J., Moerman, I., Dhoedt, B., and Demeester, P. (2004). An Overview of Mobile Ad-hoc Networks: Applications and Challenges. *Journal-Communications Network*, 3(3), 60-66.
15. Hosein, M., and Jedidiah, A. (2023). Mobile Adhoc Networks and Networking–An Overview of Existing Intrusion Prevention Techniques and Predictive Intrusion Prevention. *Global Journal of Computer Science and Technology: Network, Web and Security*.
16. Islabudeen, M., and Kavitha Devi, M.K. (2020). A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks against Security Attacks. *Wireless Personal Communications*, 112:193-224.
17. Karthik S, Kannan S., Arunachalam V. P., Ravichandran T., and Valarmathi M. L.. (2010). An Investigation about Performance Comparison of Multihop Wireless Ad-Hoc Network Routing Protocols in MANET, *International Journal of Computer Science Issues (IJCSI)*, 7(3), pp. 35-41.
18. Kaur, G., and Kakkar, D. (2022). Hybrid Optimization Enabled Trust-Based Secure Routing with Deep Learning-Based Attack Detection in VANET. *Ad Hoc Networks*, 136.
19. Kaur, S., and Kaur, H. (2015). Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature. *International Journal for Advance Research in Engineering and Technology*, 3, 24-28.
20. Khalifa M. M., Nuri O., Ali Alheeti K. M., (2021). New Intrusion Detection System to Protect MANET Networks Employing Machine Learning Techniques, *International Conference of Modern Trends in Information and Communication Tech. Industry (MTICTI) IEEE*.
21. Khan A. U., Chawhan M. D., Mushrif M. M., Neole B., (2021). Performance Analysis of Adhoc On-demand Distance Vector Protocol under the influence of Black-Hole, Gray-Hole and Worm-Hole Attacks in Mobile Adhoc Network, *Proceedings of the Fifth Int. Conf. on Intelligent Computing and Control Systems (ICICCS 2021), IEEE Xplore*.
22. Khraisat, A., Gondal, I., Vamplew, P., and Kamruzzaman, J. (2019). Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges. *Cybersecurity*, 2(1):1-4.
23. Khudayer, B. H., Alzabin, L. R., Anbar, M., Tawafak, R. M., Wan, T. C., AlSideiri, A., and Al-Amiedy, T. A. (2023). A Comparative Performance Evaluation of Routing

Protocols for Mobile Ad-hoc Networks. *International Journal of Advanced Computer Science and Applications*, 14(4):2-7.

24. Korir, F., and Cheruiyot, W. (2022). A Survey on Security Challenges in the Current MANET Routing Protocols. *Global Journal of Engineering and Technology Advances*, 12(01), 078-091.
25. Kumar S., and Kumar J. (2012). Comparative Analysis of Proactive and Reactive Routing Protocols in Mobile Ad-Hoc Networks (MANET), *Journal of Information and Operations Management*, 3(1):92-95.
26. Lalli, M., and Jothi, S. A. (2019). Detecting and preventing black hole attack in manet using rsa algorithm. *International Journal of Computing*, 3(6):1-4.
27. Manmohan. S, Mamoon. R (2020). "Security Attacks in MANET-A Comprehensive Study", *International Conference on Intelligent Communication and Computational Research (ICICCR-2020)*.
28. Milanov, E. (2009). The RSA algorithm. *RSA laboratories*, 1-11.
29. Murugeshwari B., Saral Jeeva Jothi D., Hemalatha B., Neelavathy Pari S. (2023). Trust Aware Privacy Preserving Routing Protocol for Wireless Adhoc Network, *International Journal of Engineering Trends and Technology*, 70(9):362-370.
30. Pooja Rani, Kavita, Sahil Verma and Gia Nhu Nguyen, (2020). Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network, *IEEE*, 12(2):111-113.
31. Prasath, N., and Sreemathy, J. (2019). Optimized dynamic source routing protocol for MANETs. *Cluster Computing*, 22(5):12397-12409.
32. Praveen Bondada, Debabrata Samanta, Manjit Kaur and Heung-No Lee (2022). Data Security-Based Routing in MANETs Using Key Management Mechanism, *Applied Sciences*, 12(3):1041.
33. Randeep.K, Bakal.J (2016). "H-EAACK-An Intrusion Detection System using Hybrid Cryptography for MANET", *International Research Journal of Engineering and Technology (IRJET)*.
34. Regassa D., Yeom H. Y., Son Y., (2022). Efficient Attacker Node(s) Detection and Isolation Schemes in MANETs OLSR Protocol, *Int. Conf. on Information Networking (ICOIN) IEEE*.
35. Sankaranarayanan, S., and Murugaboopathi, G. (2017). Secure Intrusion Detection System in Mobile Ad Hoc Networks using RSA Algorithm. *Second International Conference on Recent Trends and Challenges in Computational Models*.

36. Singh, A. (2024). UML Class Diagram Explained with Examples.
37. Sivapriya, N., and Mohandas, R. (2022). Analysis on Essential Challenges and Attacks on MANET Security Appraisal. *Journal of Algebraic Statistics*, 13(3):2578-2589.
38. Smaha, S. E. (1988, December). Haystack: An Intrusion Detection System. In *Fourth Aerospace Computer Security Applications Conference* (Vol. 44, p. 37).
39. Srilakshmi, U., Alghamdi, S.A., Vuyyuru, V.A., Veeraiah, N., and Alotaibi, Y. (2022). A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks. *IEEE Access*, 10, 14260-14269.
40. Srinivas, B.V., Mandal, I., and Keshavarao, S. (2022). Virtual machine migration-based Intrusion Detection System in Cloud Environment using Deep Recurrent Neural Network. *Cybernetics and Systems*, 1-21.
41. Srinivasa, R. (2015). Performance Analysis of DES and Triple DES. *International Journal of Computer Application*, 130(14).
42. Tahir, A.S. (2015). Design and Implementation of RSA Algorithm using FPGA. *International Journal of Computers and Technology*, 14(12):1-12.
43. Torky, M., El-Dosuky, M., Goda, E., Snášel, V., and Hassanien, A.E. (2022). Scheduling and Securing Drone Charging System Using Particle Swarm Optimization and Blockchain Technology. 6(9):1-26.
44. Umesh K. S., Mewada S., Iaddhani L., and Bunkar K. (2011). An Overview and Study of Security Issues & Challenges in Mobile Ad-Hoc Networks (MANET), *International Journal of Computer Science and Information Security*, 9(4):106-111.
45. Walikar, G. A. Biradar, R. C. (2017). A Survey on Hybrid Routing Mechanisms in Mobile Ad Hoc Networks, *Journal of Network and Computer Applications*, 77:48-63.