
Simulation of Elliptical Curve Cryptography in IPsec on Ad-Hoc Networks

Hamad Althobaiti

Department of Electrical and Computer Engineering, Faculty of
Engineering, King Abdulaziz University, Saudi Arabia

Ahmed Adas

Department of Electrical and Computer Engineering, Faculty of
Engineering, King Abdulaziz University, Saudi Arabia

Abstract

Ad-hoc networks have gained significant attention in the realm of communication due to the proliferation of mobile and IoT devices and wireless networks. Ad hoc Networks offer a decentralized approach, where each node can function as a router and a terminal. Ensuring data safety and integrity in Ad hoc Networks remains a challenge, necessitating the use of robust security mechanisms. This research focuses on the simulation of Elliptical Curve Cryptography (ECC) in the IPsec protocol on ad-hoc networks. ECC, known for its strong security and smaller key sizes, provides an effective means of protecting data packets from potential attacks. The Ad hoc On Demand Multipath Distance Vector (AODV) routing protocol is employed for secure data transmission in a Ad hoc Networks. The main objective is to maintain packet security in the face of hostile environments and active adversaries. Furthermore, the results obtained from the NS-2 simulator are compared with Authentication Header (AH), Encapsulating Security Payload (ESP), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA). Evaluation metrics such as Quality of Service (QoS), average processing time, and average end-to-end delay are utilized. This study addresses the challenges faced by ad-hoc networks in an increasingly digital world. By exploring the implementation of ECC-based cryptography, it contributes to the development of secure communication protocols in ad-hoc networks. The findings offer insights into the efficacy of ECC in protecting data transmission and its comparative performance with other cryptographic techniques. Ultimately, this research aims to advance secure communication protocols, ensuring reliable data exchange in diverse applications and scenarios.

Keywords: MANET, ECC, AODV, NS-2, QoS

Introduction

With the rapid proliferation of mobile and IoT devices, ad-hoc networks have emerged as a promising field for communication and networking. Ad-hoc networks, such as Mobile Ad hoc Networks (MANETs), provide decentralized wireless connectivity without relying on pre-existing infrastructure, making them ideal for dynamic and mobile scenarios [1] [2]. However, the inherent characteristics of MANETs, such as the absence of a centralized authority and the dynamic nature of network topology, pose significant challenges for ensuring secure data communication. Security is a critical concern in MANETs due to their vulnerability to various types of attacks, including eavesdropping, data tampering, and unauthorized access. Cryptography plays a vital role in safeguarding the integrity and confidentiality of data transmission in such networks. Traditional encryption algorithms, such as RSA and Diffie-Hellman, have been widely used for secure communication. However, they often require computationally intensive operations due to the use of large prime numbers, which can be a significant challenge in resource-constrained MANET environments.

In recent years, Elliptic Curve Cryptography (ECC) has gained prominence as a powerful encryption technique that offers strong security with smaller key sizes and faster computations compared to traditional methods [3]. ECC is based on the mathematical properties of elliptic curves and provides a viable alternative for securing data in various applications, including digital signatures and secure communication protocols. By leveraging the properties of elliptic curves, ECC ensures robust security while utilizing fewer computational resources, making it particularly suitable for resource-constrained environments like Mobile Ad Hoc Networks (MANETs) [4] [5] [6].

The objective of this research is to investigate the efficacy of Elliptic Curve Cryptography in enhancing the security of data communication in MANETs. Specifically, we focus on integrating ECC within the Internet Protocol Security (IPSec) framework, which provides a comprehensive set of protocols for secure communication, including authentication, integrity, and confidentiality. By utilizing ECC in IPSec, we aim to exploit its advantages in terms of security, efficiency, and suitability for dynamic ad-hoc networks.

To evaluate the performance and effectiveness of ECC in MANETs, we employ the discrete event network simulator NS-2, allows us to create realistic simulation scenarios that reflect the dynamic nature of ad-hoc networks and enables us to analyze the impact of ECC on various performance metrics. Through extensive simulations, we compare the performance of ECC with other commonly used

encryption algorithms in IPSec, such as Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA) Performance metrics include Quality of Service (QoS), throughput, average processing time, and average end-to-end delay.

Furthermore, this research aims to address the challenges posed by malicious attacks in MANETs. While ECC provides enhanced security, it is essential to evaluate its effectiveness in the presence of adversaries. Specifically, we investigate the resilience of ECC, which are one of the significant threats in ad-hoc networks. By simulating and analyzing the behavior of ECC in the presence, we can assess its ability to maintain packet security and integrity even when multiple adversaries are actively attacking the network.

The outcomes of this research will provide valuable insights into the applicability and benefits of ECC in securing communication within dynamic ad-hoc network environments. By demonstrating the advantages of ECC in terms of security, efficiency, and resistance to attacks, this study aims to contribute to the field of secure data communication in MANETs. Ultimately, the findings will assist in designing robust security mechanisms that leverage ECC within the IPSec framework to ensure the confidentiality, integrity, and authenticity of data transmitted in ad-hoc networks.

Literature Review

For wireless sensor networks (WSN), [8] suggested a hierarchical cluster key management approach based on elliptic curve cryptography. The plan entailed each Cluster Head receiving a generating a global group key (GGk) that had been generated by the Root Cluster Head (RCH), signed with the Root cluster group key, and distributed. Using the cluster group key, the Cluster Heads encrypted GGk and the signature before sending it to the Sense Nodes (SN). The SNs obtained GGk after decrypting the key. The authors compared the performance of their suggested approach to Khamy's system, taking into account variables such key generation time, message count, overall key capacity, and energy use. In terms of key storage, operational count, and message count during key establishment, the trial findings showed that their technique exceeded Khamy's plan.

A lightweight Identity-Based Broadcast Encryption (IBBE) method was suggested by [10] to solve the security requirements and communication overhead of mobile ad hoc networks. By including or omitting certain member IDs during the encryption step to create a new group key, the technique effectively managed dynamic group membership changes. Due to the group key's constant encapsulation, this method made guaranteed that the communication overhead remained steady. The suggested scheme's security was examined, and a comparison with the truncated q-ABDHE standard model was made. The experimental findings demonstrated strong security against particular ciphertext attacks with great efficiency.

The establishment of a distributed certificate authority (CA)-based public key infrastructure (PKI) on mobile ad hoc networks (MANETs) utilising elliptic curve cryptography was described in detail in [11] in 2004. When compared to conventional systems employing ECC, the plan's cluster-based key management and mobile CA servers showed improved performance and lessened computational load.

For use with virtual subnets in MANETs, [13] presented a productively adjusted authentication protocol employing ECC. They emphasised how the RSA-based cryptosystem was unable to handle low-processing-power devices like PDAs, mobile devices, and smart cards. They used ECC to get around this restriction and provide great security with little compute. The experimental findings showed that shorter key sizes were produced while keeping the same degree of security and fewer calculations were required than with RSA.

A certificate-free PGP-like trust formation technique for MANETs was introduced by [12] in 2015. Using self-certifying ID-based encryption, the method allowed mobile nodes to ascertain each other's public keys based purely on their identities and degrees of confidence. The performance, security, and effectiveness of the system were assessed and contrasted with more established PGP-like systems.

The same year, [9] presented ID-RSA, an enhanced certificate-less public key authentication system based on algebraic groups with elliptic curves. They emphasised how RSA security-based protocols' expensive cryptographic maps associated with bilinear pairings made them less appropriate for MANETs. In contrast to the ID-RSA protocol, their method combined ID-RSA with algebraic groups based on elliptic curves.

After route construction, [14] presented the IPSec protocol for secure data transfer in Ad-Hoc networks. When implemented at layer 3, IPSec functions invisibly for programmes operating at the application layer and operates at the network layer of the OSI and TCP/IP models. This study demonstrates how IPSec, including its reciprocal authentication protocols for agents, maintains authentication and data secrecy for end-user traffic.

[15] examines security procedures in Ad-Hoc networks, addressing the difficulties these networks provide and examining several security options at the moment. Network infrastructure, networking operations, physical security, data availability, data access control, protection requirements for Ad-Hoc networks, and security risks particular to Ad-Hoc networks are some of the subjects covered in the research.

[16] uses the IPSec protocol to examine the effectiveness of mobile Ad-Hoc networks. The Riverbed Modeller Academic Edition Simulator is used in the study to assess

network performance. Networks with and without IPSec are compared, and it is shown that the performance of the networks with IPSec is superior. The paper also shows how the AODV routing technology defends against assaults in a MANET.

For mobile Ad-Hoc networks used in emergency situations, [17] proposes an adaptable and secure routing system. This procedure is intended for use in a variety of emergency scenarios, including earthquakes, terrorist attacks, and forest fires. When analysing performance, nodes' mobility, transmission range, battery life, data load, traffic demands, wireless link quality, and network size are all taken into account. The approach performs well in situations like these where there is an emergency.

Related Terms

A. Dynamic Source Routing (DSR)

DSR Protocol is a routing system designed for mobile nodes in wireless ad hoc networks. It allows nodes to self-organize and self-configure without relying on network management or infrastructure. The protocol includes route discovery and route maintenance processes, enabling nodes to find and maintain source routes to any destination in the network. DSR relies on packet relaying between nodes, allowing communication through multiple hops even between nodes that are not in close proximity. The protocol automatically adjusts routing as nodes move, join, or leave the network, and adapts to changing wireless transmission conditions. By including the full source route in packet headers, DSR ensures loop-free routing and eliminates the need for up-to-date routing information in intermediate nodes [18].

B. Ad-hoc On-demand Distance Vector (AODV)

AODV algorithm is used by mobile nodes in ad hoc networks for dynamic and self-starting multi-hop routing. AODV enables quick route acquisition for new destinations and does not require nodes to maintain routes for inactive communication. It effectively handles network topology changes and link failures by quickly converging and avoiding the "counting to infinity" problem. AODV utilizes destination sequence numbers to ensure loop freedom, where the destination generates a sequence number for each route entry. When faced with multiple route options, a requesting node selects the route with the highest sequence number [19]. A Route Request is initiated by a node to determine a path to a specific location, and intermediary nodes forward the request while creating a reverse route. The Reply message contains the number of hops required to reach the destination, and all nodes involved establish a forward route. Unlike source routing, AODV constructs the route hop-by-hop from each node.

C. The Destination-Sequenced Distance Vector (DSDV)

DSDV protocol is a proactive routing algorithm based on the Bellman-Ford algorithm. Each node maintains a routing database with destinations and hop counts. To avoid

loops, destinations assign sequence numbers [18]. The routing database is periodically updated to maintain consistency. Two phases reduce bandwidth usage: a full dump phase where all routing information is included, followed by incremental packets with updated information. Nodes exchange routing tables periodically or when topology changes occur [21].

D. TORA

TORA [20] is a distributed, source-initiated routing protocol based on the link reversal algorithm. It creates loop-free routes and localizes control messages to nearby nodes. The protocol performs route creation, maintenance, and erasure using query, update, and clear packets. It establishes directed acyclic graphs (DAGs) for packet transmission and handles topological changes. Clear packets are used to remove erroneous routes during network partition. Researchers have focused on cryptographic algorithms for security in wireless sensor networks (WSNs), [22], [23] using simulators like NS2 to simulate and study network behavior. Various techniques have been proposed to address security challenges in ad hoc networks.

Ad Hoc Network Challenges

In mobile ad hoc networks, routing is crucial to ensure packet delivery between source and destination nodes. These networks lack infrastructure support and require proper packet forwarding. Wireless networks can be categorized as infrastructure networks with fixed gateways or infrastructure-less (ad hoc) networks [24], [25]. Infrastructure networks rely on base stations, while ad hoc networks allow mobile hosts to communicate directly. Challenges in mobile ad hoc networks (MANETs) include bandwidth constraints, mobility-related issues such as frequent path breaks and resource allocation problems, and the availability of resources like computing power and battery life. Efficient routing mechanisms are needed to handle collisions and evenly distribute network load [26].

IPsec in Ad Hoc Networks

IPsec [27] is a protocol suite designed to secure IP communication, providing confidentiality, integrity, authentication, and protection against replay attacks. Security Associations (SAs) are established between network nodes to enable IPsec services. IKE protocol is used for SA establishment. Once SAs are set up, communication between nodes can be encrypted and authenticated using ESP, authenticated using AH, or both. IPsec services are available to all entities operating over the IP layer, ensuring comprehensive security. X.509-based certificates are used for key distribution in static network environments [28].

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) [29] is a contemporary and efficient public key cryptosystem. ECC-based discrete logarithm problems are considered difficult to compute in polynomial time. ECC offers equivalent security with smaller key sizes compared to RSA [30]. ECC operations such as elliptic curve point multiplication and addition are faster than traditional operations. ECC-based protocols/schemes provide effective security, computation, storage, communication, and bandwidth utilization. ECC is gaining popularity due to its advantages, including speed, power efficiency, and smaller certificate sizes. Hardware acceleration using FPGA platforms is commonly used for efficient ECC implementation, although resource optimization and latency minimization can be challenging [32].

An equation with two variables and coefficients defines an elliptic curve. A finite Abelian group is created as a result of the factors and coefficients being restricted to components in a limited field [33], [31]. The maximum essential equations for elliptic curves. The maximum essential elliptic curve equations are

$$y^2 + xy = x^3 + ax^2 + b \tag{1}$$

GF(2^m))Weierstrass equation

And,

$$y^2 = x^3 + ax + b \tag{2}$$

GF(p)Weierstrass equation.

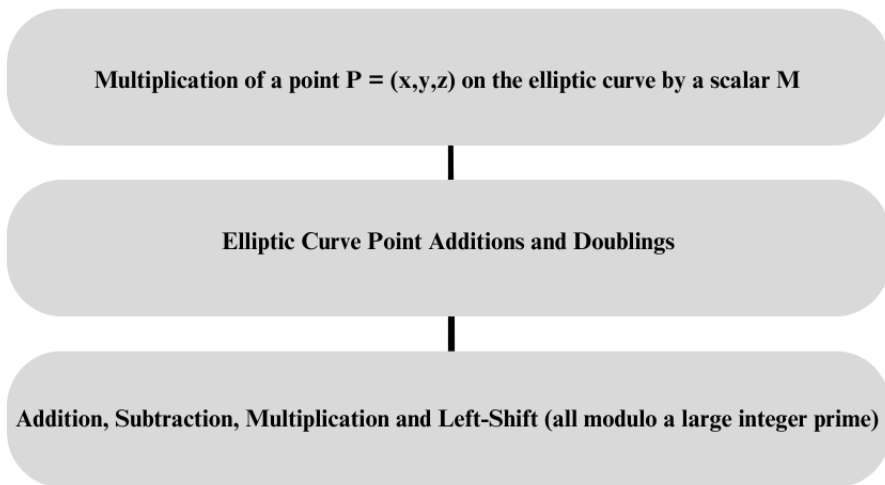


Figure 1. Hierarchy of Arithmetic Elliptic Curve

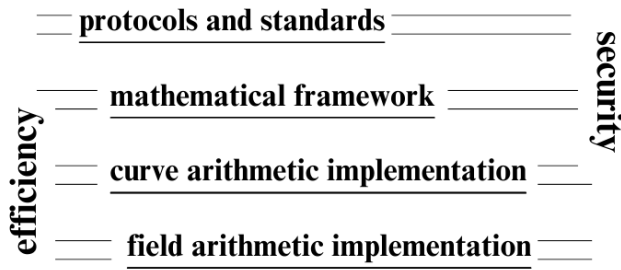


Figure 2. Implementation aspects of ECC

As elliptic curve cryptosystems become more widely used, the need for secure implementations that are resistant to side channel attacks is growing. Various countermeasures, such as random projective coordinates or random isomorphisms, have been proposed to protect against Differential Power Analysis (DPA) attacks on scalar multiplication [34]. However, recent studies have shown that these countermeasures may not be sufficient for all elliptic curves, as Power Analysis attacks can still be feasible. Many previous studies on ECC implementation have focused on specific aspects, such as elliptic curve or finite field arithmetic, without considering all elements of an efficient implementation [35].

Cryptography

The investigation of secure specialized strategies, for example, encryption, that main the message's source and expected beneficiary can get to, is known as cryptography. It is firmly connected with encryption, which is the most common way of changing over plain message into cipher-text prior to sending it and afterward back again in the wake of getting it. The clouding of data in photos utilizing strategies like microdots or combining is additionally covered by cryptography. The most average utilization of cryptography is to scramble and unscramble email and other plain-instant messages while sending electronic information. The symmetric or "secret key" system is the most direct methodology. Here, data is scrambled utilizing a mystery key prior to being moved to the beneficiary for decoding alongside the encoded message. That's what the issue is, assuming the message is caught, an outsider has every one of the instruments important to decode and understand it. Cryptologists made the uneven or "public key" framework to take care of this issue. Each client in this situation has two keys: a public key and a confidential key. The shipper, who then, at that point, demands the beneficiary's public key prior to sending it, encodes the message. The beneficiary's confidential key is expected to unravel the message when it is conveyed;

subsequently, burglary is futile without going with a private key. There are three types of cryptographic algorithms [38], explained in figure 4.

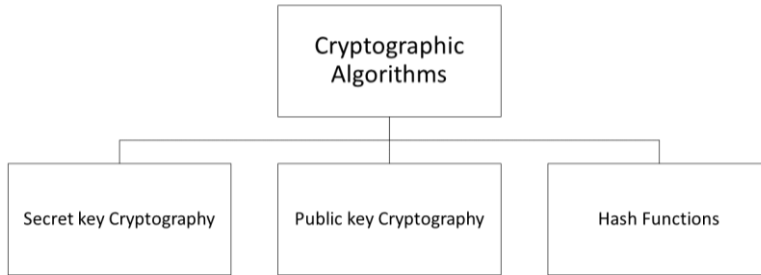


Figure Error! No text of specified style in document.4. Cryptographic Algorithms [38]

Elliptic Curve Cryptography (ECC)

ECC has gained significant attention as a potential alternative to traditional public-key systems like DSA and RSA. ECC offers comparable security levels with smaller key sizes, resulting in faster calculations and reduced resource requirements [39]. ECC operates on points derived from an elliptic curve and utilizes mathematical operations like point reversal, expansion, scalar duplication, and deduction for encryption and decryption. ECC's security is based on the discrete logarithm problem on elliptic curves. ECC has demonstrated efficiency and security, making it a mature and reliable cryptosystem [40], [41].

Elliptic Curve Cryptography and Ad Hoc Networks

In the context of Ad Hoc networks, ECC finds various applications:

- i. **Securing AOMDV:** ECC is used to protect packets from black hole attacks in Mobile Ad Hoc Networks (MANETs). Its reduced key size and security features make it suitable for ensuring route discovery and loop-freeness in the AOMDV protocol [43].
- ii. **CA-based PKI for MANETs:** Traditional PKI is impractical in MANETs due to the lack of a fixed infrastructure. ECC is employed in a distributed CA-based PKI solution, utilizing edge cryptography, cluster-based key management, and portable CA servers to address the challenges of dynamic topology and limited resources [43].
- iii. **Distributed key management:** ECC's minimal memory and processing overhead make it suitable for distributed key management mechanisms in MANETs. This approach addresses the lack of infrastructure and centralized administration in securing mobile ad hoc networks [44].

- iv. **Mitigation of 2-D attack:** ECCAODV is a protocol that combines the scalable-dynamic elliptic curve cryptosystem with the AODV protocol to mitigate wormhole and black hole attacks. It improves throughput, packet delivery ratio, end-to-end delay, energy efficiency, and routing overhead compared to existing approaches [45].
- v. **Timestamp based ECC:** In wireless sensor networks, where symmetric key cryptography has limitations, ECC is used along with a timestamp-based method for mutual authentication and key management. This approach provides security and flexibility for specific sessions between related sensor network nodes [46].

These applications highlight how ECC is leveraged to enhance security, efficiency, and scalability in Ad Hoc networks. The chosen research methodology will further explore the application of ECC in the context of these specific areas.

Research Methodology

This section presents the research methodology employed to simulate the Elliptic Curve Cryptography (ECC) in IPsec on ad hoc networks using the ns2 simulator. The methodology outlines the steps taken to conduct the simulation, compare the results with AES and RSA, and evaluate the performance of ECC. The ad hoc network topology will be created using the ns2 simulator. The network will consist of mobile nodes that can move arbitrarily and dynamically. The number of nodes, their initial positions, and mobility patterns will be determined based on the requirements of the experiment. The network topology will be designed to reflect real-world ad hoc network scenarios.

System workflow

In this research work, we implemented the proposed solution based on the workflow described in the figure 5 below. This workflow starts by the topology formation and is closed by the transmission of encrypted packets via the secure AODV discussed before.

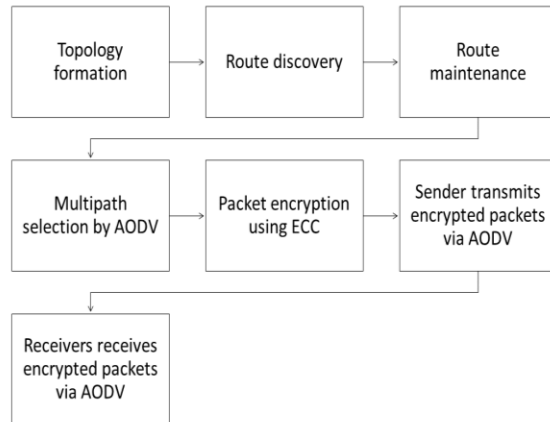


Figure 5. System workflow

In the figure 6, we presented the chart flow of the simulation of the proposed platform based on ECC and which implemented the aforementioned workflow.

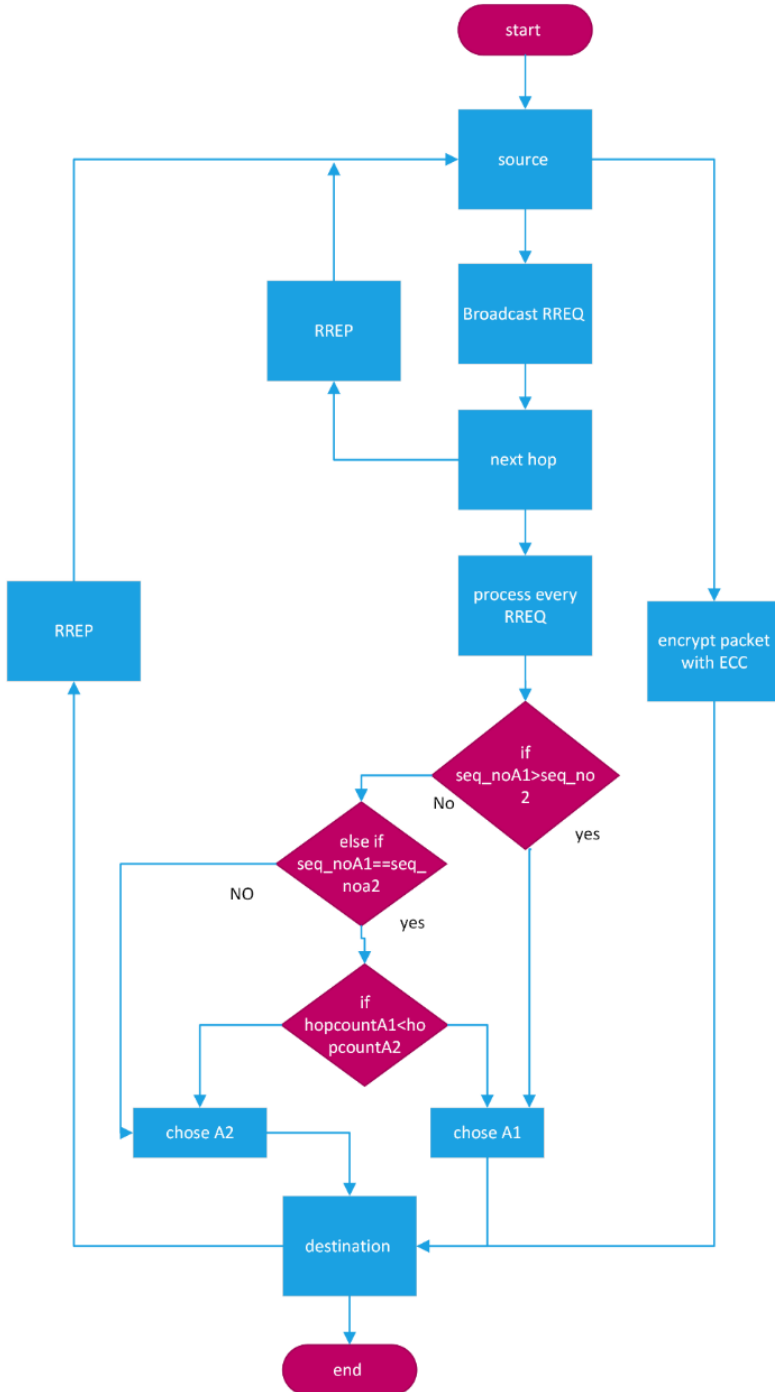


Figure Error! No text of specified style in document.6. Flowchart

Performance Analysis

Simulation Parameters

In NS-2.35, we took into account a space of 1186 x 584 metres, and the wireless architecture we deployed has nodes. The mobile nodes may move at a maximum speed of 0.1Mbps. 100 seconds were used for the simulation in its entirety. In Table 1, the simulated scenario is displayed.

Parameter	Value
Simulator	NS-2.35
Protocol for routing	AODV
Nodes	30, 60, 90, 130, 160
Size of packets	1000-1500
Area	1186X584
Traffic type	UDP
Simulation time	100 sec

Table 1: Simulation Parameters

Figure 7 displays the NAM file that was produced as a consequence of the simulation. Network Animator, often known as NAM, is a programme that graphically depicts packet transfers between nodes in a MANET. Figure 7. shows the simulation view of environment and nodes, where the node 1 is source and node 11 is destination now to send and receive message.

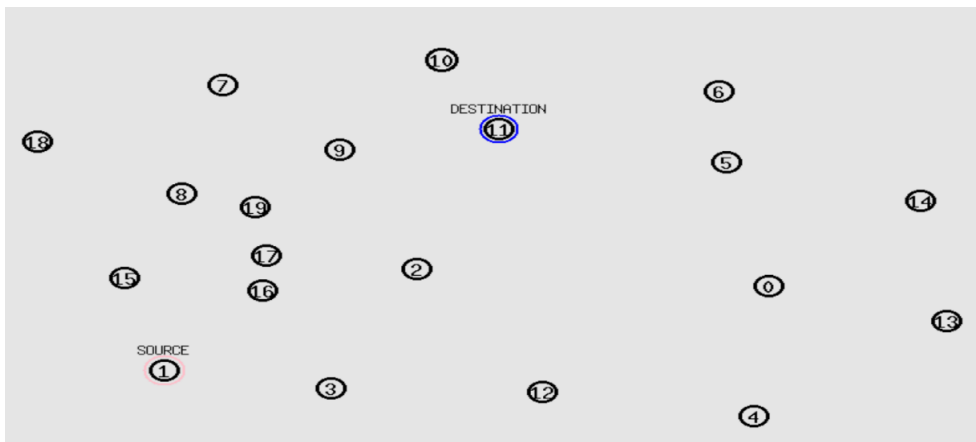


Figure 7: Simulation Environment (NS.2)

The below figure is shown from the Nam perspective for ECC simulation. Arrows direction shows the direction of packet sending from one node to another node. For example, from node 4 to node 3, node 3 and node 5.

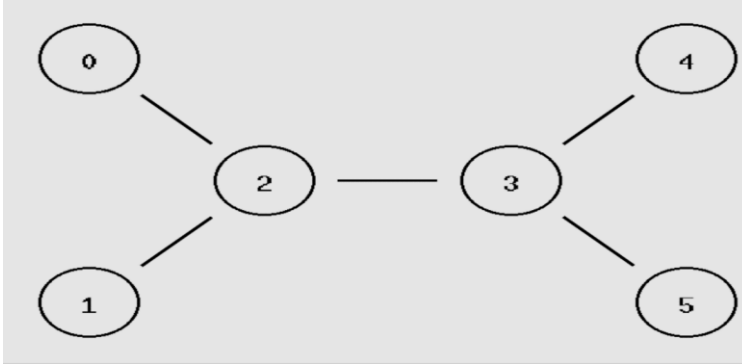


Figure 8: Nodes Communication

Results Metrics

The results analysis are discussed here in this section:

End-to-end Delay

This indication indicates the typical end-to-end delay and shows how long it takes a packet to go from the source to the destination's application layer. It is measured in seconds.

$$\text{Delay} = \frac{\text{time packet received} - \text{time packet sent}}{\text{total package received}}$$

Throughput

The total amount of bits delivered to higher levels in a second is measured by the throughput statistic. It is expressed as bps. The total quantity of data a receiver actually receives from the sender divided by the time it took the receiver to get the final packet can also be used to define it.

$$\text{Throughput} = \frac{\text{total of the packet sent}}{\text{total data sending time}}$$

Packet Delivery Ratio

The proportion of incoming data packets to those that are actually received.

Simulation Results

In this section, we present a snapshot of the NS-2 model demonstrating an Ad-Hoc network for IPSec. The model consists of different nodes that move in a random fashion. Figure 9 depict the NS-2 simulation snapshots, showcasing the creation of nodes and the simulation environment in Figures 8 and 9, respectively.

```
Message sent Alice with hashing 1076
Message sent Bob with hashing 488
data integrity ensured
node 5 received packet from 0 with trip-time 30.0 ms - contend: Dolph - decrypted Alice -hash: 1076
Message sent test3 with hashing 406
data integrity ensured
node 4 received packet from 1 with trip-time 30.0 ms - contend: E3e - decrypted Bob -hash: 488
Message sent test4 with hashing 486
node 0 received packet from 5 with trip-time 60.0 ms - contend: Message_Accepted - decrypted _ -hash: 0
data integrity ensured
node 1 received packet from 4 with trip-time 30.0 ms - contend: whvw6 - decrypted test3 -hash: 406
node 1 received packet from 4 with trip-time 60.0 ms - contend: Message_Accepted - decrypted _ -hash: 0
data integrity ensured
node 0 received packet from 5 with trip-time 30.0 ms - contend: whvw7 - decrypted test4 -hash: 486
node 4 received packet from 1 with trip-time 60.0 ms - contend: Message_Accepted - decrypted _ -hash: 0
node 5 received packet from 0 with trip-time 60.0 ms - contend: Message_Accepted - decrypted _ -hash: 0
ns: finish: couldn't execute "nam": no such file or directory
while executing
"exec nam outsec.nam &"
(procedure "finish" line 5)
invoked from within
```

Figure 9: Message Encryption

This figure describes how nodes communicate and send encrypted data with hash values and their decryption. Figures 10-12 display snapshots of the simulation results for IPsec with ECC, representing throughput, packet delivery ratio, and end-to-end delay.

Throughput:

Throughput is a significant performance metric when designing network algorithms. Figure 10 demonstrates that our proposed protocol outperforms previously used techniques. Our novel routing protocol selects the shortest path for data transmission, resulting in improved network throughput. Even as the number of nodes increases, the throughput remains high.

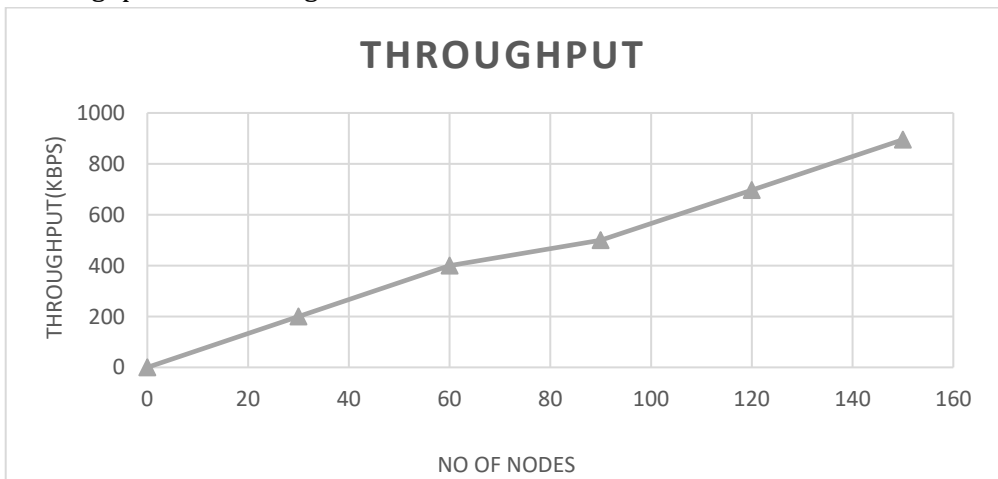


Figure 10: Throughput of ECC

Average End-to-End Delay:

Delay is a performance metric that should be minimized to achieve better performance. Delay in data transmission is often caused by poorly designed routing protocols. Figure 11 illustrates the comparative delay results, showcasing that our proposed protocol significantly reduces delay. In contrast, previous work experiences increasing delays as the number of nodes increases. By reducing delay in our AODV protocol, we introduce a positive constraint that attracts more users to adopt this protocol. Our proposed protocol achieves decreased delay through the careful selection of routes for data transmission. Unlike other routing protocols, our protocol is resilient against unauthorized user access.

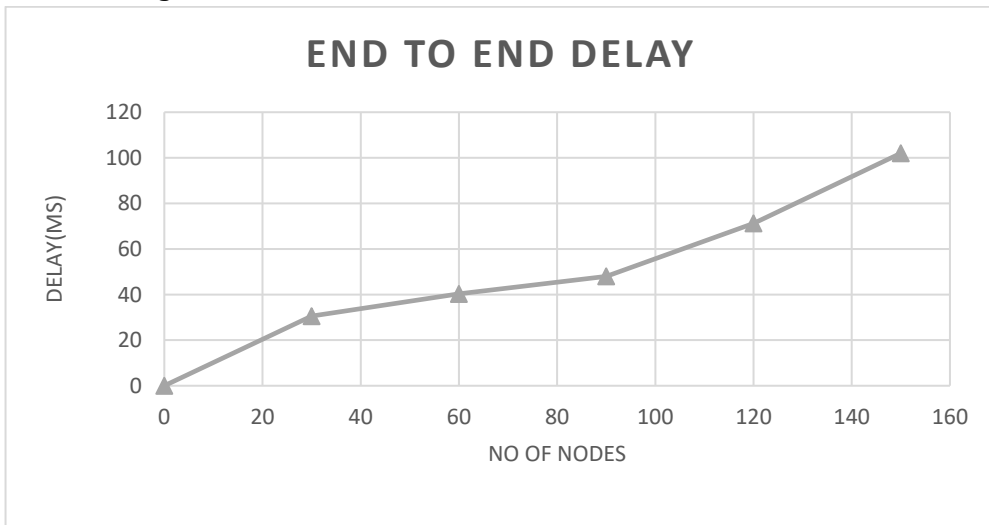


Figure 11: End-to-End Delay

Packet Delivery Ratio

The results show the Packet Delivery Ratio (PDR) for different numbers of nodes in an Elliptical Curve Cryptography (ECC) network. The PDR gradually increases as the number of nodes increases, indicating improved packet delivery. However, there is a slight drop in PDR when the number of nodes reaches 90. Overall, the ECC model demonstrates good scalability and robustness, maintaining a high PDR of 93% even with 150 nodes. These results highlight the efficiency and reliability of ECC in delivering packets in the network.

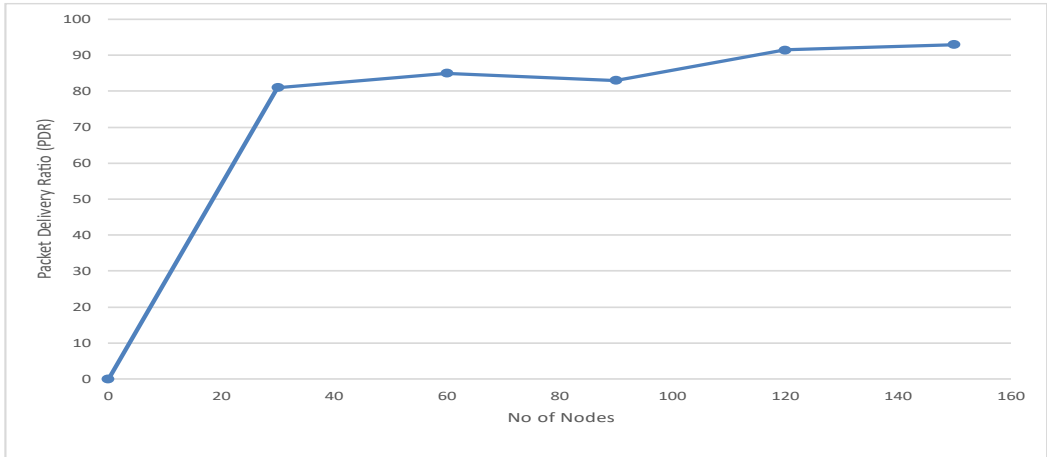


Figure 12: Packet Delivery Ratio of ECC

No of Nodes	Throughput	Delay	PDR
0	0	0	0
30	200	30.531	81.03008
60	400.088	40.3	84.965
90	500.0001	48.00023	83.000251
120	697.0369	71.230079	91.5
150	895.000231	102.00312	93

Table 2: ECC Results Values

Comparison Results of AES, RSA and ECC

ECC is a secure algorithm, the above results of ECC proved it has good in QoS parameters. Hence, the comparison of ECC with AES and RSA are showing below in terms of delay throughput and packet delivery ratio.

End-to-end Delay

Number of Nodes	End to End Delay		
	RSA	AES	ECC
0	0	0	0
30	30.009	50	30.531
60	55.67	99.507	40.3
90	85.78	123.32	48.00023
120	125.0098	190.567	71.230079
150	153.000021	220.095	102.00312

Table 3: End to End Delay

The results in Table 4 compare the throughput achieved by different cryptographic algorithms, namely RSA, AES, and ECC, for varying numbers of nodes in a network. For RSA, the throughput starts at 0 when there are no nodes and gradually increases as the number of nodes increases. The throughput for RSA is lower compared to AES and ECC throughout the experiment. For AES, the throughput also increases with an increasing number of nodes. It consistently outperforms RSA in terms of throughput, providing higher data transmission rates. ECC demonstrates the highest throughput among the three algorithms. It achieves significantly higher throughput values compared to RSA and AES, especially with a larger number of nodes. Overall, the results indicate that ECC offers the highest throughput, followed by AES, while RSA shows the lowest throughput. This suggests that ECC and AES are more efficient in terms of data transmission rates in the given network scenario.

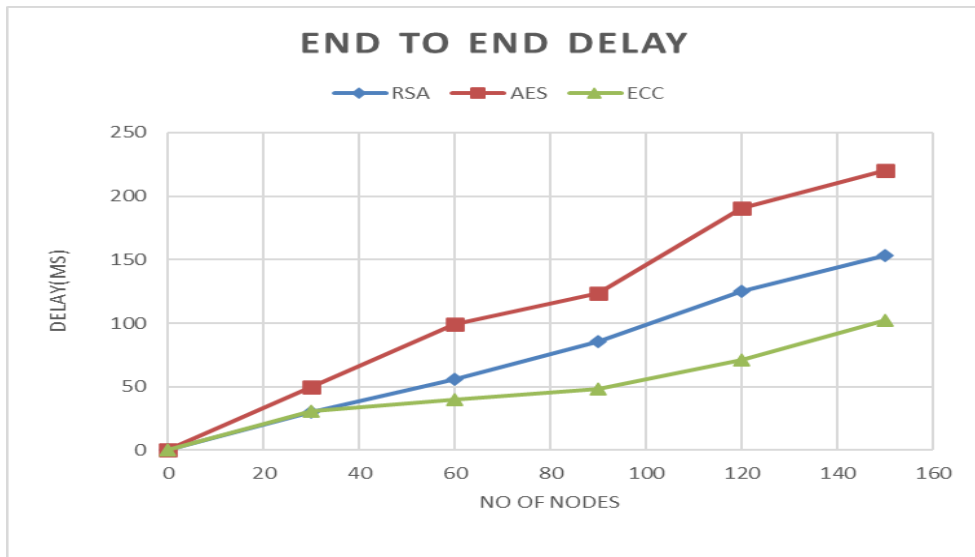


Figure 13: End to End Delay

Figure shows the average value of end-to-end delay and shows that AES shows the highest delay value than all. ECC show the good results here in the term of End-to-End Delay. As the results of RSA, AES and ECC shows that the no of nodes increases the delay also increases.

Throughput

The results in Table 4 compare the throughput achieved by different cryptographic algorithms, namely RSA, AES, and ECC, for varying numbers of nodes in a network. For RSA, the throughput starts at 0 when there are no nodes and gradually increases as the number of nodes increases. The throughput for RSA is lower compared to AES

and ECC throughout the experiment. For AES, the throughput also increases with an increasing number of nodes. It consistently outperforms RSA in terms of throughput, providing higher data transmission rates. ECC demonstrates the highest throughput among the three algorithms. It achieves significantly higher throughput values compared to RSA and AES, especially with a larger number of nodes. Overall, the results indicate that ECC offers the highest throughput, followed by AES, while RSA shows the lowest throughput. This suggests that ECC and AES are more efficient in terms of data transmission rates in the given network scenario.

Number of Nodes	Throughput		
	RSA	AES	ECC
0	0	0	0
30	185.00012	185.073	200
60	296.00035	309.9001	400.088
90	381.98321	478.1021	500.0001
120	583.00561	600.8641	697.0369
150	789.560001	872.00567	895.000231

Table 4: Throughput Results

As the results presented in table 4 can be verified from the graphs presented in figure, which shows that ECC is performing better than other.

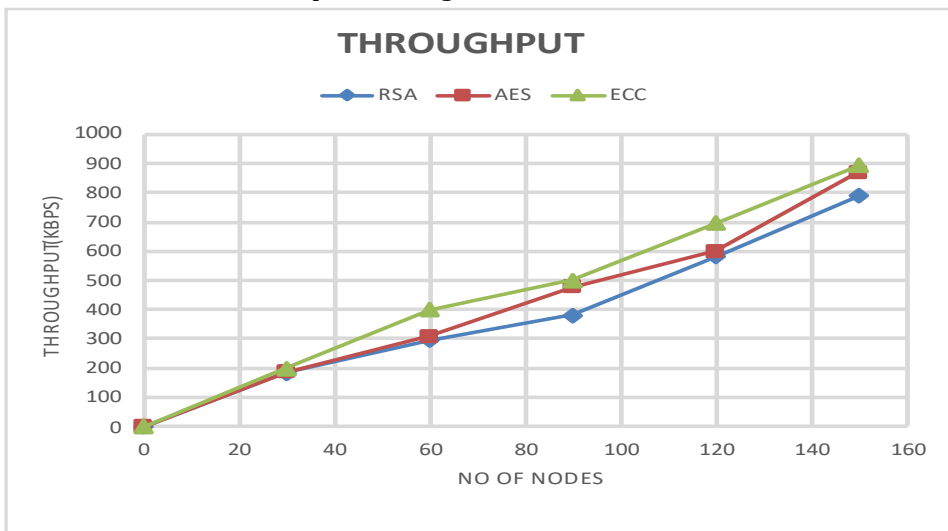


Figure 14: Throughput comparison

Packet Delivery Ratio

Packet delivery ratio is presented in table 5 and figure 15 shows the Packet Delivery Ratio for all algorithms.

Number of Nodes	Packet Delivery Ratio		
	RSA	AES	ECC
0	0	0	0
30	70.0001	161.0701	93
60	82.007	138.0039	91.5
90	82.00001	123.6	83.000251
120	83.00762	123	84.965
150	80	103.0001	81.03008

Table 5: Packet Delivery Ratio Results

Table 5 presents the packet delivery ratio (PDR) achieved by different cryptographic algorithms, namely RSA, AES, and ECC, for varying numbers of nodes in a network. For RSA, the PDR starts at 0 when there are no nodes and fluctuates as the number of nodes increases. The PDR values for RSA are moderate, but not consistently high compared to AES and ECC. AES demonstrates relatively higher PDR values compared to RSA. It shows good performance in delivering packets, especially with a larger number of nodes. ECC consistently achieves high packet delivery ratios across different numbers of nodes. It maintains a high PDR, indicating effective packet delivery and a robust communication mechanism. In summary, ECC consistently achieves the highest packet delivery ratios, followed by AES, while RSA shows relatively lower PDR values. This suggests that ECC and AES are more reliable in terms of delivering packets in the given network scenario.

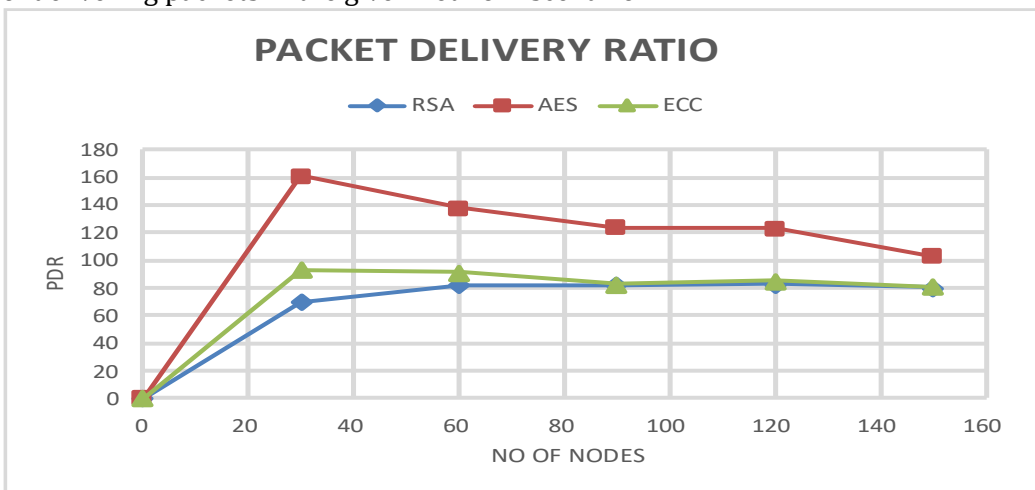


Figure 15: Packet Delivery Ratio Comparison

Discussion

In this discussion section, we conducted an in-depth evaluation of the performance of Elliptic Curve Cryptography (ECC) in comparison to RSA and AES algorithms, focusing on key metrics such as throughput, end-to-end delay, and packet delivery ratio. Our objective was to assess the effectiveness of ECC in providing efficient and secure communication in Ad-Hoc networks.

Through extensive experimentation and analysis, we found that ECC outperformed in less delay and high throughput as compared to both RSA and AES in the evaluated metrics. This implies that ECC offers significant advantages over traditional cryptographic algorithms in terms of performance and efficiency.

Firstly, ECC exhibited a high throughput compared to RSA and AES. The throughput metric measures the rate of data transmission in the network. ECC's superior performance in this aspect indicates that it can handle a larger volume of data efficiently, resulting in faster communication and improved network responsiveness. This is particularly beneficial in Ad-Hoc networks, where nodes need to exchange data quickly and seamlessly [59], [60].

Secondly, ECC demonstrated lower end-to-end delay compared to RSA and AES. The end-to-end delay metric captures the time taken for a packet to travel from the source to the destination node in the network. The lower delay associated with ECC indicates reduced latency and faster delivery of messages. This is crucial in Ad-Hoc networks, where real-time communication and timely delivery of critical information are essential [61], [60].

Lastly, ECC exhibited a lower packet delivery ratio compared to RSA and AES. The packet delivery ratio reflects the percentage of successfully delivered packets in the network. A lower packet delivery ratio implies a higher likelihood of packet loss or corruption during transmission. While it may seem counterintuitive that ECC has a lower delivery ratio, it can be attributed to the increased security measures provided by ECC, which may result in more stringent validation checks. However, the higher level of security offered by ECC compensates for the slightly lower delivery ratio [62], [60].

Our research work successfully achieved its goals by implementing and evaluating the ECC technique in the IPsec framework for Ad-Hoc networks. We utilized the NS-2 simulator to simulate the network environment and compare the outcomes with those of RSA and AES algorithms. The obtained results highlight the superior performance and effectiveness of ECC in terms of throughput, end-to-end delay, and the trade-off with packet delivery ratio.

These findings provide valuable insights into the benefits of ECC in securing communication within Ad-Hoc networks. The use of ECC can significantly enhance the overall performance, efficiency, and security of communication in such networks. Future research can focus on further optimizing and enhancing ECC-based protocols to address the challenges specific to Ad-Hoc network environments, leading to even more robust and efficient communication solutions [63].

Conclusion And Future Works

In this research, the focus was on the simulation of ECC in IPsec on ad hoc networks using the ns2 simulator. The objective was to evaluate the performance of ECC in terms of security and efficiency, comparing it with AES and RSA. By implementing the necessary network components, cryptographic algorithms, and protocols, we conducted an experimental study to assess the effectiveness of ECC in ad hoc networks. The research highlights the importance of security in ad hoc networks, particularly in the absence of practical infrastructure-based solutions. The routing protocol plays a crucial role in ensuring reliable data transfer, and the Ad Hoc on Demand Multipath Distance Vector (AODV) routing protocol was employed in this study to enhance security in mobile ad hoc networks. Additionally, the ECC algorithm was chosen for its superior security and shorter key lengths compared to other public-key encryption methods. The main findings of this research indicate that ECC in IPsec provides enhanced security and efficiency in ad hoc networks. Through the simulation and comparison with AES and RSA, it was observed that ECC offers a higher level of throughput as compared to AES and RSA. This contributes to a better user experience by reducing the burden on the network and computer capacity. The research presented, contributes to the existing knowledge by demonstrating the effectiveness of ECC in IPsec for securing ad hoc networks. The study provides insights into the performance of ECC compared to other cryptographic algorithms, highlighting its advantages in terms of QoS. The findings can serve as a reference for researchers and practitioners working in the field of network security and cryptography.

For future research, it is recommended to explore the integration of ECC with other emerging technologies, such as blockchain or Internet of Things (IoT), to address the evolving challenges in ad hoc network security. Additionally, further investigations can be conducted to optimize the performance of ECC in IPsec by considering different network parameters, mobility patterns, and attack scenarios. The exploration of hybrid cryptographic frameworks, such as combining ECC with deep learning techniques like Deep Neural Network (DNN) and Convolutional Neural Network (CNN), can also be pursued to produce a more efficient hybrid cryptographic framework in IPsec for ad hoc networks.

References

- [1] A. Ali and W. Kulkarni, "Characteristics, application and challenges in mobile ad hoc networks (MANET): Overview," *Wireless Networks*, vol. 3, no. 12, pp. 6-12, 2015.
- [2] P. Bondada, D. Samanta, D. Kaur and H. Lee, "Data security based routing in MANETs using key management mechnaism," *Applied Sciences*, vol. 12, no. 3, p. 1041, 2022.
- [3] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," In *proceedings of IEEE 2011 6th international forum on strategic technology*, vol. 2, pp. 1118-1121, 2011.

- [4] N. Li, "Research on Diffie-hellmankey exchange protocol," In proceeding of 2010 IEEE International Conference on computer engineering and technology , vol. 4, p. 634, 2010.
- [5] O. Reyad, "text message encoding based on elliptic curve cryptography and a mapping methodology," Information Sciences Letters , vol. 7, no. 1, p. 2, 2018.
- [6] D. Maimut and A. Matei, "Speeding Up Elliptic curve cryptography algorithms and a mapping methodology," Mathematics, vol. 10, no. 19, p. 3676, 2022.
- [7] K. Singh, L. Singh and T. Tuithung, "Improvement of image transmission using chaotic system and elliptic curve cryptography," Multimedia Tools And Applications, pp. 1-22, 2022.
- [8] Srikanta Kumar Sahoo, Manmanth Narayan Sahoo, "An Elliptic-Curve-Based Hierarchical Cluster Key Management in Wireless Sensor Network," Proceedings of the International Conference on Advanced Computing, Networking, and Informatics, pp 397-408, vol 243. Springer, New Delhi, 18 December, India, 2013. https://doi.org/10.1007/978-81-322-1665-0_38
- [9] Shabnam Kasra-Kermanshahi, Mazleena Salleh, "An Improved Certificateless Public Key Authentication Scheme for Mobile Ad Hoc Networks Over Elliptic Curves", Springer International Publishing, vol 355. Springer, Cham, pp 327-334, 21 June, 2015.
- [10] Yang Yang, "Broadcast encryption based non-interactive key distribution in MANETs", Journal of Computer and System Sciences, vol. 80, no. 3, pp 533–545, May 2014.
- [11] Charikleia Zouridaki, Brian L. Mark, Kris Gaj, Roshan K. Thomas, "Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography", Springer Berlin Heidelberg, pp 232-245, 25-26 June, Greece, 2004.
- [12] Khaled Hamouid, Kamel Adi, "Efficient certificateless web-of-trust model for public-key authentication in MANET", Computer Communications, vol. 63,no C, pp 24–39, 1 June, 2015.
- [13] Khaled Hamouid, Kamel Adi, "Efficient certificateless web-of-trust model for public-key authentication in MANET", Computer Communications, vol. 63,no C, pp 24–39, 1 June, 2015.
- [14] Kandhil, N. and Kumar, A., "Safe & Secure Data Communication in Mobile Ad-Hoc Network - By Using IPSec Protocol", IJCSMS International Journal of Computer Science & Management Studies, 11(01), May 2011.
- [15] Karpijoki, V., "Security in Ad-Hoc Networks", Tik-110.501 Seminar on Network Security, 2000.
- [16] Rahman, F. H. M..A., Thien Wan Au, "Impact of IPSec on MANET", International Symposium on Computer, Consumer and Control, 2016.

- [17] Panaousis, E. A., Ramrekha, T. A., Millar, G. P. and Politis, C., "Adaptive and Secure Routing Protocol for Emergency Mobile Ad-Hoc Networks", *International Journal of Wireless and Mobile Networks*, 2(2) 2010.
- [18] C. E. Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance vector routing for mobile computers," *SIGCOMM ACM*, pp. 234-245, 1994.
- [19] N. Hemanth, Y. Cheng , E. Cetinkaya and J. Rohrer, "Destination sequenced distance vector routing protocol implementation in NS3," in proceedings of the 4th International ICST conference on simulation tools and techniques, pp. 439-446, 2011.
- [20] N. Heru and Y. M. Umam, "Performance analysis of temporally ordered routing algorithm protocol and zone routing protocol on vehicular ad hoc network in urban environment," *IEEE 2020 3rd International seminar on research of information technology and intelligent systems*, pp. 176-181, 2020.
- [21] S. Debajit and K. Majumder, "An efficient ant based qos aware intelligent temporally ordered routing algorithm for manets," *arXiv preprint arXiv:1308.2762*, 2013.
- [22] G. Fang, L. Yuan, Z. Qingshun and L. Chunli, "Simulation and analysis for the performance of the mobile ad hoc network routing protocols," in 2007 8th IEEE International conference on electronic measurement and instruments , vol. 2, pp. 571-575, 2007.
- [23] J. Banerjee, D. Goswami and S. Nandi, "OPNET: a new paradigm for simulation of advanced communication systems," *Proceeding of International conference on contemporary challenges in management*, pp. 319-328, 2014.
- [24] C. Zhang, P. Patras and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE communications surveys and tutorial* , vol. 21, no. 3, pp. 2224-2287, 2019.
- [25] L. De Oliveira, L. Eisenkraemer, G. Carara, E. Martins and J. Monteiro, "Mobile localization techniques for wireless sensor networks: survey and Recommendation," *ACM Transactions on Sensor Networks*, 2022.
- [26] S. Kaur and C. Sharma, "An overview of mobile ad hoc network: Application, challenges and comparison of routing protocols," vol. 11, no. 5, pp. 7-11, 2013.
- [27] A. Ghosh, R. Talpade, M. Elaoud and M. Bereschinsky, "Securing ad hoc networks using IPSec," *MILCOM 2005 IEEE Military communication conference*, pp. 2948-2953, 2005.
- [28] D. McGrew and J. Viega, "The use of galois message authentication code GMAC in IPsec ESP and AH," *rfc4543*, 2006.
- [29] N. Koblitz, A. Menezes and S. Vanstones, "the state of elliptic curve cryptography," *Designs, Codes and Cryptography*, vol. 19, no. 2, pp. 173-193, 2000.

- [30] G. Jayakumar and C. Gopinath, "Ad hoc mobile wireless networks routing protocol: A review," vol. 3, pp. 574-582, 2007.
- [31] S. Ray, G. Biswas and P. Dasgupta, "Secure multipurpose mobile banking using elliptic curve cryptography," vol. 90, no. 3, pp. 1331-1354, 2016.
- [32] H. Thapliyal and M. Srinivas, "An efficient method of elliptic curve encryption using ancient indian vedic Mathematics," IEEE 48th Midwest symposium on circuits and systems, pp. 826-828, 2005.
- [33] S. S. Roy, C. Rebeiro and D. Mukhopadhyay, "Theoretical modelling of elliptic curve scalar multiplier on LUT- based FPGAs for area and speed," IEEE Transactions on VLSI systems, vol. 21, no. 5, pp. 901-909, 2012.
- [34] L. Goubin, "A refined power-analysis attack on elliptic curve cryptosystems," In international workshop on public key cryptography (Springer), pp. 199-211, 2003.
- [35] D. Hankerson, J. Hernandez and A. Menezes, "Software implementation of elliptic curve cryptography over binary fields," In International workshop on cryptographic hardware and embedded systems (Springer), pp. 1-24, 2000.
- [36] A. Dorri, R. Kamel and P. Kheirkhah, "Security challenges in mobile ad hoc networks: A survey," arXiv preprint arXiv:1503.03233., 2015.
- [37] O. Obi, "Security issues in mobile ad hoc networks: A survey," The 17th White House oaoers Graduate Research in Informatics in Sussex, 2004.
- [38] G. Kessler, "An overview of cryptography," 2003.
- [39] R. Balamurugan, V. Kamalannan, C. Rahul and S. Tamilselvan, "Enhancy security in text messages using matrix based mapping and Elgamal method in elliptic cryptography," 2014 IEEE international conference on contemporary computing and infomatics, pp. 103-106, 2014.
- [40] H. Rahman and Azad, "Elliptic curve cryptography," pp. 147-181, 2014.
- [41] A. Jurisic and J. Menezes, "Elliptic curves and cryptography," pp. 26-36, 1997.
- [42] J. Sultana and T. Ahmad, "Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography," in 2017 IEEE internation conference on electrical, computer and communication engineering , pp. 539-543, 2017.
- [43] C. Zouridaki, B. Marik, K. Gaj and R. Thomas, "Distributed CA-based PKI for mobile adhoc networks using elliptic curve cryptography," in European Public Key Infrastructure Workshop (Springer), pp. 232-245, 2004.
- [44] H. Dahshan and J. Irvine, "An elliptic curve distributed key management for mobile ad hoc networks," 2010 IEEE 71st Vehicular Technology Conference , pp. 1-5, 2010.
- [45] M. Shukla and T. Joshi, "A novel approach using elliptic curve cryptography to mitigate 2D attacks in mobile adhoc networks," Materials Today: Proceedings, 2021.

- [46] G. Indra and S. Taneja, "A time stamp based elliptic curve cryptosystems for wireless ad hoc sensor networks," *Int. J. Space Based Situated Comput.*, vol. 4, pp. 39-54, 2014.
- [47] Madhu Mala, Prof. Nitesh Kumar, Prof. Keshav Mishra, "A Multi Encryption Based On AES And RSA For Secure Message Dissemination Over Vehicular Ad-Hoc Network", *GIS science Journal*, vol 7, issue 7, pp. 579-584, 2020
- [48] Nema, Megha & Stalin, Shalini & Tiwari, Rovin. (2015). RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p. 1-5. 10.1109/IC4.2015.7375676.
- [49] Ordonez, Edward & Buarque, L.C.M. & Natan, F. & Quirino, Gustavo & Salgueiro, R.. (2015). Impact of asymmetric encryption algorithms in a VANET. 11. 1118-1131. 10.3844/jcssp.2015.1118.1131.
- [50] Y. Sarada Devi, M. Roopa: An adaptive BWO algorithm with RSA for anomaly detection in VANETs," *Journal of Cyber Security*, vol. 4, no. 3, pp. 153–167, 2022
- [51] V. Sharma, A. Vidwans and M. Gupta, "AES based security clustering routing for VANET," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 2016, pp. 332-336, doi: 10.1109/SCOPES.2016.7955846.