International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Secure Data Transmission Through Active Way Identifier (AWID) and Elgamal-Elliptic Curve Cryptosystem (E-ECC)

1st Geepthi D
Computer Science and Engineering,
PSN College of Engineering and Technology,
Tirunelveli, tamilnadu
geepthi.d@gmail.com

2nd Prof. Christopher Columbus C
Computer Science and Engineering,
PSN College of Engineering and Technology,
Tirunelveli, tamilnadu
christoccc@gmail.com

Abstract— Security is an important thing in network during data transmission. This work proposed a novel Active Way Identifier (AWID) for every paths to make a secure data transmission in network. In additionally, this AWID get changed dynamically based on timestamp parameter which provides high security from attackers and also helps for detecting attackers. Not only path, the transmitting message also secured by using public key cryptography. A novelty is made on developing an ElGamal cryptography with Elliptic Curve Cryptography (ECC). The ElGamal-Elliptic Curve Cryptosystem (E-ECC) uses the point addition, subtraction and doubling concepts of ECC for reducing time cost and ElGamal providing efficient group based security. The efficiency of proposed AWID is compared with existing D-PID and Color techniques in term of resource utilization and the efficiency of E-ECC in encrypted message size is compared with ElGamal and Paillier algorithms. It is proved that the proposed works are more efficient than others.

Index Terms— Active Way Identifier, The ElGamal-Elliptic Curve Cryptosystem, data transmission, public key cryptography

I. INTRODUCTION

The message or information communication technology is found in each half of human life. Information exchange became automated and frequently used in banking, commerce, government and hospitals. All these information need security to protect privacy, to prevent fraud and to defend against hacking [4].

In recent years, more works including the path identifiers PIDs that identify paths between network entities as inter-domain routing objects. There are two different use cases of PIDs in the

Aforementioned approaches. In the first case, the PIDs are globally advertised. As a result, an end user knows the PID(s) toward any node in the network. In the second case, conversely, PIDs are only known by the network and are secret to end users [3].

Elliptic curve cryptography (ECC) is a public key cryptography technique. It is based on the algebraic structure that uses finite keys. ECC requires smaller keys compared to non-EC cryptography to provide equivalent security [1].

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. ElGamal is a public key cryptography technique proposed by Taher ElGamal and is based on Diffie Hellman Key Exchange (DHKE). There is a possibility of using ElGamal with ECC, several researches have successfully conducted, and results are promising in terms of security analysis [1]. The security of the ElGamal scheme depends on the properties of the underlying group G as well as any padding scheme used on the messages.

In individual, both the ECC and ElGamal are the best cryptosystem but additionally which are combined in this work for improving efficiency of both techniques and also improving the group based security.

The contribution of this work is,

- Generate AWID and Individual Node Identifier (INID) for every transaction in the network
- Then find the shortest path for each transaction to get quick transmission
- After finding shortest path, perform public key cryptography using proposed E-ECC
- After cryptography send the data through shortest path and find attackers using AWID.

The introduction about path ID, ElGamal and ECC have described in section 1. The literature is stated in section 2 and the methodology of the proposed work is presented in section 3. The performance analysis of proposed work is showed in section 4 and section 5 concludes this work with its advantages.

II. LITERATURE SURVEY

Adeel et al. [1] presented a lightweight elliptic-ElGamal-based authentication scheme using PKI (FHEEP) in D2D communication to mitigate M-I-T-M and to reduce communication costs. Pollard's rho and Baby Step, Giant Step (BSGS) methods are used to evaluate the authenticity and secrecy of their proposed scheme.

Tanmoy et al. [2] proposed an ElGamal cryptosystem and biometric information along with a user's password-based authentication scheme for cloud-based IoT applications refereed as SAS-Cloud. Because they focused on the serious issues in cloud-based IoT applications like legitimacy of communicators during communication sessions through insecure channels and

authentication procedure is highly desirable to remove the unapproved access in IoT applications.

Hongbin et al. [3] presented the design, implementation, and evaluation of D-PID, a framework that uses PIDs negotiated between neighboring domains as inter-domain routing objects. In DPID, the PID of an inter-domain path connecting two domains is kept secret and changes dynamically. They describe in detail how neighboring domains negotiate PIDs, how to maintain ongoing communications when PIDs change.

Sagar and Ravikumar [4] focused on the security issues similarly as computing tie square measure two necessary factors for data technology applications, such as ATM, Smart cards and web. The elliptic curve algorithmic program contain cluster of the elliptic curve points forms associate degree Abelian group. They discussed about elliptic curve and a proposed algorithm which is useful for small device.

Ashok et al. [5] proposed a new certificate-based "lightweight access control and key agreement protocol in the IoT environment, called LACKA-IoT" that utilizes the elliptic curve cryptography (ECC) along with the "collision-resistant one-way cryptographic hash function". Through a detailed security analysis using the formal security under the "Real-Or-Random (ROR) model", informal security analysis and formal security verification.

III. METHODOLOGY

A. Network Model

In this work, every nodes in the network contains Individual Node Identifier (INID) and generate Active Way Identifier (AWID) for every path in the network for improving security. Generally the path ID is used for identifying the paths between network entities and those are static in existing works but this work contains dynamic AWID.

B. Overview of AWID

The overview of AWID is described in this section. AWID is same like path identifier, at first the router generates the AWID for every possible paths for improving the security. Here this AWID get changed dynamically based on the timestamp value in the packet which means every packet contains some timestamp value in the transmitting packet that denotes the lifetime of the AWID. After the timestamp get exceed the AWID get changed and the packet will be dropped. If the attacker get one AWID and transmit some malicious message through this AWID, the AWID get changed after certain period and the AWID will block that attacker as well as drop that malicious message.

C. AWID Generation

The Linear Congruential Generator (LCG) algorithm is used for generating this AWID in an efficient manner.

$$AWID_{k+1} = (IN_{ID}(AWID_i) + TS) \bmod S_N \quad (1)$$

Where AWID is the Active Way Identifier,

INID – Individual Node Identifier

TS – Time Stamp value

SN – Sequence Number of a Message

AWID0 – Initial value.

These values are generated by the router before starting data transmission and attach AWID and TS as a part of the transmitting packet header.

D. Shortest Path Finding

After generation of AWID, the router fined the shortest path for the destination node which sends request to the router. At first, every node send the resource request message to the router when it require any resource. Based on that request message, router finds the shortest path to that node from itself. This is the process done in the shortest path finding stage.

E. Public Key Cryptography

After finding shortest path, the router perform public key cryptography for improving the security of transmitting packet. A new ElGamal-Elliptic Curve Cryptosystem (E-ECC) is proposed for improving the efficiency of public key cryptography.

F. ElGamal-Elliptic Curve Cryptosystem (E-ECC)

- Generate Public key and Private Key (Sender)
- Chooses E(x, y) with an elliptic curve over F(p) or F(2n)
- Chooses a point on the curve, k1 (a1, b1) and choose an integer z.
- Calculate k2(a2, b2) = z × k1(a1, b1) (Multiple addition of points is denoted as multiplication)
- Declare E (x, y), k1(a1, b1) and k2(a2, b2) as public key
- z as private key.

(i) Identify Encryption (Sender)

- M is a point on the curve, as plaintext m
- Calculate the cipher texts

$$CT1 = r \times k1 \quad (2)$$

$$CT2 = M \times r \times k2 \quad (3)$$

(ii) Decryption (Receiver)

Calculate the plain text P using the following formula

$$M = CT2 - (z \times CT1) \quad (4)$$

IV. PROPOSED ALGORITHM

(iii) Generate Public key and Private key (Sender)

- Chooses E(x, y) with an elliptic curve over F(p) or F(2n)
- Chooses a point on the curve, k1(a1, b1)
- Chooses another point on the curve, k2(a2, b2)
- Calculate k3(a3, b3) = k1 + k2
- Announce E (x, y), k1(a1, b1) and k3(a3, b3) as his public key
- Keeps k2(a2, b2)as his private key.

(iv) Encryption (Sender)

- Sender Select P a point on the curve, as her plaintext m1 and m1 = M1(a4, b4), m2 = M2(a5, b5)

Sender Calculate

CT1 = M2 + k1 + 2M1
CT2 = M1 + k1 + 2M2
CT3 = M1 + k3 + M2
Sender define cipher text (CT1, CT2 and CT3).

(v) *Decryption (Receiver)*

The cipher text is decrypted by using private key e2
M1 = CT1 – CT3 + k2
M2 = CT2 – CT3 + k2.

G. *Attack Detection*

The attacks are detected in this work through AWID which is very helpful for identifying and reducing attacks. AWID is a part of sending message, if any attacker obtain this ID and perform any malicious activity through this ID, the AWID will block those attacker and discard that malicious activity when its timestamp get exceeds

H. *PERFORMANCE ANALYSIS*

a. *Active Way Identifier (AWID)*

The path is secured by the AWID during data transmission and here the efficiency of the proposed technique is compared with the existing D-PID and COLOR systems in term of resource utilization. Table 1 contains the Resource usage of three different techniques and Figure 1 shows the resource utilization comparison of AWID with D-PID and COLOR. Here the AWID is outperformed the COLOR and D-PID.

TABLE I

Resource Utilization Comparison between Three Different Techniques

Maximum Transmission Speed (Mbit/s)	Resource Usage %		
	AWID	COLOR	D-PID
100	5	7	6
200	9	14	12
300	11	16	14
400	12	18	16
500	13	20	18
600	14	22	20
700	14	25	23
800	14	31	28
900	14	38	30
1000	14	39	34

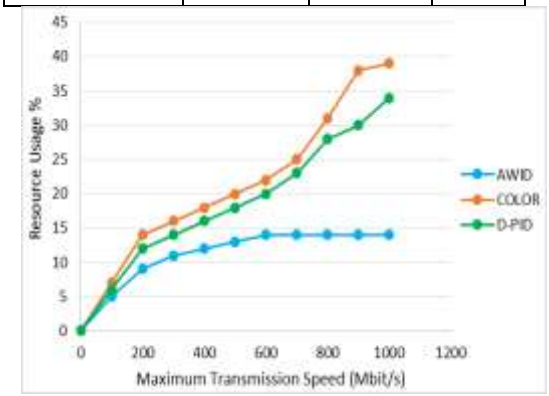

Fig. 1. Resource Utilization Comparison between Three Different Techniques

b. *ElGamal-Elliptic Curve Cryptosystem (E-ECC)*

The propose E-ECC is fully based on the point addition, subtraction and doubling concept of ECC that avoids scalar multiplication for reducing time cost because scalar multiplication consumes more time. Table 2 contains the Encrypted Message Size of E-ECC, ElGamal and Paillier and Figure 2 shows the Comparison of E-ECC, ElGamal and Paillier in Encrypted Message Size. Here the E-ECC is outperformed the ElGamal and Paillier.

TABLE 2

Encrypted Message Size of E-ECC, ElGamal and Paillier

Message Sizes (KB)	Encrypted Message Sizes (KB)		
	E-ECC	*ElGamal*	*Paillier*
80	250	500	1500
125	500	950	2100
162	750	1500	8500
245	2000	3500	12000

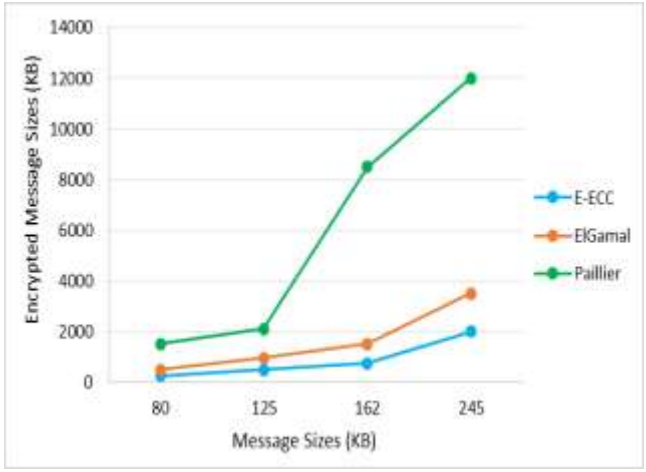

Fig. 1. Comparison of E-ECC, ElGamal and Paillier in Encrypted Message Size

V. CONCLUSION

In this work, the path has been secured by the proposed AWID technique which does not allows attackers and it helps to identify the attackers through its dynamically changing mechanism. The transmitting message get secured by using the proposed E-ECC which contains both ECC and ElGamal properties. In E-ECC, ElGamal does not allows unauthorized person to decrypt the message and ECC avoids scalar multiplication for reducing the time cost as well as computation complexity. The E-ECC provides secure group based data transmission in network.

REFERENCES

[1] Adeel Abro, Zhongliang Deng and Kamran Ali Memon, “A Lightweight Elliptic-Elgamal-Based Authentication Scheme for Secure Device-to-Device Communication”, Future internet, 2019.

[2] Tanmoy Maitra, Mohammad S. Obaidat, Debasis Giri, Subrata Dutta and Keshav Dahal, “ElGamal cryptosystem-

based secure authentication system for cloud-based IoT applications", IET Networks, Vol. 8, Issue. 5, pp. 289-298, 2019.

[3] Hongbin Luo, Zhe Chen, Jiawei Li and Athanasios V. Vasilakos, "Preventing Distributed Denial-of-Service Flooding Attacks with Dynamic Path Identifiers", IEEE Transactions on Information and Forensics Security, Vol. 12, Issue. 8, pp. 1801 - 1815, 2017.

[4] Sagar Shankarrao Dake and Ravikumar Uttamrao Ighare, "A Proposed ECC Algorithm for Smart Cards Cell Phones and Wireless Networks", International Conference on Nascent Technologies in the Engineering Field, 2017.

[5] Ashok Kumar Das, Mohammad Wazid, Animi Reddy Yannam, Joel J. P. C. Rodrigues and Youngho Park, "Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment", IEEE Access, Vol. 7, pp. 55382 - 55397, 2019.