VDES Data Transmission Encryption Based on ECC Algorithm

Zhen Kang, Jiaxuan Yang and Zuohuan Chen

Navigation College, Dalian Maritime University Key Laboratory of navigation Safety guarantee of Liaoning Province, Dalian, 116026
Email:451077779@qq.com

Abstract-VDES communication system as the next-generation ship communication system currently lacks necessary information security protection measures so that VDES communication systems can easily cause loss or theft of data information during information transmission. In order to improve the security of the data information transmission in VDES communication system, the VDES communication system data transmission need to be encrypted. A data transmission encryption method for VDES communication system based on Elliptic Curve Cryptography(ECC) encryption algorithm is proposed that is public-key cryptosystem. The ECC encryption algorithm simulation test results show that ECC is used for VDES communication system data transmission for encryption, data information encryption is better, encryption efficiency is higher, and data information security is improved.

1. Introduction

Vessels need to communicate between shore-ship, ship-ship and ship-to-shore during the navigation. In the process of ship communication and information exchange, the safety of data information is crucial, and the ship’s information security will be the key to winning the war in the country and winning business opportunities. Studying the security of the VHF Data Exchange System(VDES) communication system will be of great significance in preventing ship information leakage and improving information security [1]. Therefore, the design of VDES communication system encryption has attracted people's attention. VDES is an enhanced and upgraded version of the Automatic Ship Identification System (AIS) in the field of maritime mobile services [2]. It has the biggest feature of the Internet that is openness. However, VDES communication system as the next-generation ship communication system currently lacks necessary information security protection measures. Therefore, VDES communication system has great security risks. In order to ensure the security, real-time and accuracy of VDES communication system transmission information, VDES communication system data transmission encryption will become an important research direction.

ECC has extremely high security in protecting digital communication services, and has short data encryption/decryption time, high implementation and security. Therefore, this paper uses ECC encryption algorithm to encrypt the data information with high confidentiality between shore-ship, ship-ship and ship-shore, which can effectively prevent the VDES data information from being falsified and forged. ECC encryption algorithm is of great significance in ensuring the ship safe sailing and efficient navigation are of great significance.

2. VDES Communication System

VDES communication system as the next-generation ship communication system, its function is shown in Figure 1. Based on the integration of existing AIS functions, the VDES communication
system adds special application messages (ASM) and VHF data exchange (VDE) functions, and is capable of ship identification, ship position reporting and ship navigation data exchange [3]. The VDES communication system is operated in the VHF (156.025-162.025 MHz) frequency band and is used to implement shore-ship, ship-ship and ship-to-shore data and information communication and satellite data information communication, which can effectively relieve pressure on the AIS communication system. The main purpose of the VDES communication system design is to meet e-NAV (e-Navigation) requirements and increase the safety of ships at sea.

2.1 VDES System Introduction

The specific system architecture is as shown in Figure 1.

2.1.1. VDES: data exchange between terrestrial stations
(1) AIS 1 (channel 2087) and AIS 2 (channel 2088) are AIS channels, in accordance with Recommendation ITU-R M.1371;
(2) ASM 1 (channel 2027) and ASM 2 (channel 2028) are the channels used for ASM;
(3) VDE1-A lower legs (channels 1024, 1084, 1025, 1085) are ship-to-shore VDE;
(4) VDE1-B upper legs (channels 2024, 2084, 2025, 2085) are shore-to-ship and ship-to-ship VDE.

![Figure 1. VDES Function Concept Figure](image)

2.1.2. VDES: data exchange between satellites and terrestrial stations
(1) AIS 1 (channel 2087) and AIS 2 (channel 2088) are terrestrial AIS channels that are also used as uplinks for receiving AIS messages by satellite;
(2) Long Range AIS using channel 75 and channel 76 that are specified channels to be used as uplinks for receiving AIS messages by satellite. SAT Up1 (channel 2027) and SAT Up 2 (channel 2028) are used for receiving ASM by satellite;
(3) SAT Up3 (channels 1024, 1084, 1025, 1085, 1026 and 1086) are used for ship-to-satellite VDE uplinks;
(4) SAT Downlink (channels 2024, 2084, 2025, 2085, 2026 and 2086) are used for satellite-to-ship VDE downlinks.

In summary, the VDES communication system will be able to meet the needs of all ship-ship, shore-ship, and ship-shore data exchange services in the future. The VDES communication system is designed to integrate AIS, ASM data exchange and e-Navigation, and enhance maritime
communications and GMDSS modernization. However, the VDES communication system has the greatest feature openness of the Internet which uses the common channel for all data exchange. At present, VDES communication system lacks necessary information security protection measures, which will lead to information loss or theft between ship-ship, shore-ship and ship-to-shore information in the process of transmission. Therefore, it is imperative to solve the hidden security problems in the VDES communication system.

3. Based on ECC encryption scheme

The VDES communication system as a next-generation ship communication system plays a crucial role in the e-Navigation strategy. Therefore, encrypting the VDES communication system data information will increase the safety of ships at sea service. Currently, ECC encryption algorithm is a relatively safe and efficient data encryption algorithm for communication systems that is currently widely used.

3.1. Implementation of Elliptic Curve Encryption Algorithm

The ellipse encryption algorithm mainly includes three sections: key generation, encryption, and decryption.

1) Key Generation

First select an elliptic curve based on a finite field and get \( E_p(a,b) \), the plaintext \( m \) is first converted to a single large integer plaintext point \( P_m \) and then mapped to the plaintext point \( P_m \) on the curve. Take a set of points in \( E_p(a,b) \) as generator \( G \), \( E_p(a,b) \) and \( G \) as public parameters. Ship \( A \) chooses a large integer \( n_A \) as private key and calculates \( P_A = n_A G \) as public key[5].

2) Encryption

When ship \( B \) want to dispatch the important ship message \( m \) to ship \( A \), ship \( B \) picks up a random number \( k \), then evaluates the two points \( C_1 = kG \) and \( C_2 = P_m + kP_A \), ship \( B \) sends a pair of point \( C_m = \{ kG, P_m + kP_A \} \) as cipher to ship \( A \).

3) Decryption

Ship \( A \) receives the cipher text \( C_m = \{ kG, P_m + kP_A \} \) from ship \( B \), ship \( A \) reconstructs the original important ship message \( P_m \) as follow:

Ship \( A \) multiplies \( C_1 \) by his private key \( n_A \) and subtracts it from \( C_2 \). The solution method is shown in Formula (1):

\[
P_m + kP_A - n_A (kG) = P_m + k(n_A G) - n_A (kG) = P_m
\]  \( \text{Formula (1)} \)

3.2. The Related Operation of Elliptic Curve Based On Finite Domain

Commonly used in cryptography is an elliptic curve based on a finite field. An elliptic curve based on a finite field is a curve equation. In definition (2), all coefficients are elements in a finite field \( GF(p) \) where \( p \) is a Large prime number[6][7]. The most commonly used one is the equation:

\[
\left\{ \begin{array}{ll}
    y' = (x' + ax + b)(\text{mod } p) \\
    [a, b \in GF(p), (4a^2 + 27b^2)(\text{mod } p) \neq 0]
\end{array} \right.
\]  \( \text{Formula (2)} \)

3.3. The defined elliptic curve.

Based on the finite field ECC algorithm mainly involves the following four operations:

Add to zero \( O \). For any given point \( P \) on the elliptic curve, there are \( P + O = P \).  
1) Add to the inverse element. For a point \( P = (x,y) \) on any given elliptic curve, its additive.  
2) Inverse is the symmetry point \( P' = (x,-y) \) of the point \( P \) with respect to the x-axis.  
3) Multiply rule on elliptic curve.

Make a tangent to point \( P \) on the elliptic curve. Let this tangent intersect the elliptic curve at point
Define \( 2P = P + P = -M \) [8]. Similarly, you can define \( P + P + P = 2P + P = 3P \) (The multiplication of an elliptic curve point by an integer is converted or transformed into many additions and doubling of many points). If there are \( k \) same points \( P \) added, it is called the multiplication of points, denoted as \( kP \).

4) Add any two points on the elliptic curve.

Let us take any two points, \( P(x_1, y_1) \) and \( Q(x_2, y_2) \) on elliptic curve \( y^2 = x^3 - 4x + 1 \), and \( P, Q \in GF(p) \). Then sum of \( P \) and \( Q \), i.e., \( P + Q = R(x_3, y_3) \), is defined as follows. First, you draw or sketch a straight line passing through the two points, \( P \) and \( Q \); This line will touch or intersect the elliptic curve at another point. This point is represented as \( R(x_3, y_3) \).

\[
x_3 = \frac{y_2 - y_1}{x_2 - x_1} (P \neq Q) \\
y_3 = \frac{3x_1^2 + a}{2y_1} (P = Q)
\]

(3)

Among them, \( \lambda \) is the slope of the straight line \( L \):

\[
\lambda = \begin{cases} 
\frac{y_2 - y_1}{x_2 - x_1} & (P \neq Q) \\
\frac{3x_1^2 + a}{2y_1} & (P = Q)
\end{cases}
\]

(4)

In the following, two arbitrary points \( P \) and \( Q \) on the elliptic curve will be respectively introduced to the solution of \( (x_1, y_1) \) in both cases of \( P = Q \) and \( P \neq Q \).

1) When any two points on the elliptic curve are \( P \neq Q \), the addition of any two points \( P \) and \( Q \), because the addition on the elliptic curve defines: If the three points on the elliptic curve are on the same line, then the sum of three points is \( O \). We can draw \( P + Q + (-R) = O \) [9], then \( P + Q = R \).

Known that the elliptic curve equation over a finite field is \( y^2 = x^3 + ax + b \), the straight line \( L \) passes over any two points \( P \) and \( Q \) on the elliptic curve over a finite field, and the equation of the straight line \( L \) is \( y = \lambda x + n \), then we can deduced:

\[
\lambda = \frac{y_2 - y_1}{x_2 - x_1}
\]

(5)

\[
n = y_1 - \lambda x_1
\]

(6)

Substituting the introduced \( \lambda \) and \( n \) into the elliptic curve equation \( y^2 = x^3 + ax + b \) over a finite field, the elliptic curve equation is obtained by:

\[
x^3 - (\lambda x + n)^2 + ax + b = 0
\]

(7)

Assuming that there are three roots in the unitary cubic equation (7), respectively \( x_1, x_2, x_3 \), according to the monad cubic equation coefficient and the root of the equation there is available:

\[
x_1 + x_2 + x_3 = \lambda^2
\]

(8)

Then it can be shown/proven that:
The coordinates of the point \( R(x_3, y_3) \) obtained by adding any two points \( P \) and \( Q \) on the elliptic curve are obtained.

(2) When any two points \( (P = Q) \) on the elliptic curve, any two points \( P \) and \( Q \) on the elliptic curve are added, i.e. the point is self-incremented with itself. The curve of the elliptic curve equation represents the tangent of the elliptic curve of the point \( P \). Then, the tangent equation of the elliptic curve can be obtained, and \( \lambda \) can be obtained by the following steps.

For the elliptic curve equation on the finite field \( y^2 = x^3 + ax + b \) derivative on \( x \), available:

\[
\frac{dy}{dx} = \frac{(3x^2 + a)}{(2y)}
\]  
(10)

At point \( P \), the derivative is:

\[
\frac{dy}{dx} \bigg|_{x=x_1} = \frac{(3x_1^2 + a)}{(2y_1)}
\]  
(11)

Suppose the tangent equation of \( P \) point on the elliptic curve is \( y = \lambda x + n \), then the slope \( \lambda = \left(3x_1^2 + a\right) / (2y_1) \) of the tangent equation can be known by formulas (10) and (11). Similarly, from equation (7), when \( (P = Q) \), \( P + Q = P + P = 2P = R \) and \( R(x_3, y_3) \) are the coordinates of point \( 2P \). The geometric meaning of the elliptic curve point self-addition.

\[
\begin{align*}
x_3 &= \lambda^2 - 2x_1 \\
y_3 &= 3\lambda x_1 - \lambda^3 - y_1
\end{align*}
\]  
(12)

3.4. Calculation of Point Sets Based on Elliptic Curves over Finite Fields

Let \( E_p(a, b) \) be the set of all points on the elliptic curve defined by the elliptic curve equation (2) \( \{ (x, y) | 0 \leq x < p, 0 \leq y < p, (x, y \in Z) \} \) and the point at the infinity \( O \) [10]. First, determine whether each \( x \) \( \{0 \leq x < p, x \in Z\} \) calculates the square root of the \( (x^3 + ax + b)(mod \ p) \) value in the modulo \( p \). If it does not exist, then there is no point on the curve corresponding to this one \( x \); If it does exist, then find if its two square roots are equal to \( Y \). The set of points that satisfy all the points of the equation is denoted as \( E_p(a, b) \).

| \( a \) | \( b \) | \( x \) | \( y \) |
|---|---|---|---|
| 0 | 22 | 0 | 22 |
| 0 | 19 | 4 | 7 |
| 9 | 21 | 10 | 15 |
| 12 | 18 | 15 | 21 |
| 16 | 13 | 17 | 19 |
| 21 | 1 | 22 | 21 |

As an example, consider the elliptic curve \( y^2 = x^3 - 4x + 1 \), defined over GF(23). This curve is represented by \( E_{23}(-4, 1) \).
4. Design and implementation of VDES encryption based on ECC

In the VS2015 environment, the ECC algorithm is encapsulated based on MFC, and the ECC encryption algorithm is used to encrypt the files (AIS data, packets, videos, and images, etc.) transmitted by the VDES. The result of the operation of the encryption algorithm is shown in Figure 2, in which, the finite field $P < 200$ byte, the parameters $A$ and $B$ of the elliptic curve satisfy $4A + 27B \neq 0 \pmod{P}$.

In order to verify the feasibility and security of the ECC algorithm, the AIS data is encrypted in this paper. The above content completes the simulation test of AIS data transmission encryption based on VDES between ECC ships. The overall operation results are shown in Figure 2. The system simulation results show that the ECC encryption algorithm can be safely and efficiently encrypted in the VDES for ship information with higher confidentiality. The smaller the number of bytes of data information shown in Figure 3, the higher the encryption/decryption efficiency. Suitable for encryption processing of important data information between ships and shores.

![Figure 2](image)

Figure 2. Specifies the file name of the AIS data to be decrypted and the AIS data after decryption

The security of the ECC encryption system is based on the elliptic curve of the discrete logarithm problem (ECDLP) [11]. The best algorithm to solve the elliptic curve discrete logarithm problem is the factorization algorithm, but it is the full exponential time complexity algorithm. The security of RSA and DSA based on the decomposition of two large prime numbers. The general method for solving such problems is the algorithm of sub-exponential time complexity. Therefore, the ECC encryption algorithm is currently the most secure asymmetric cryptosystem. TABLE 2 shows that the security of
the encryption algorithm is proportional to the key length. By comparing the RSA encryption algorithm with the ECC encryption algorithm in the table, it can be seen that if the security level is the same, the ECC encryption algorithm can use a shorter key to achieve the same encryption strength as the RSA algorithm. In addition, as the key length increases, the computational efficiency of encryption will decrease, and more storage space will be needed. Therefore, the ECC algorithm has the characteristics of strong anti-attack ability, small amount of calculation, fast processing speed, and small storage space. ECC encryption algorithm will be widely used in wireless communication security, data encryption and other fields.

![Figure 3. Relationship between ECC encryption/decryption and encrypted data size](image)

| Breakdown time (MIPS year) | RSA/DSA (key length) | ECC key length | RSA and ECC key length ratio |
|---------------------------|----------------------|----------------|-----------------------------|
| $10^4$                    | 512                  | 106            | 5:1                         |
| $10^8$                    | 768                  | 132            | 6:1                         |
| $10^{11}$                 | 1024                 | 160            | 7:1                         |
| $10^{20}$                 | 2048                 | 210            | 10:1                        |
| $10^{78}$                 | 21000                | 600            | 35:1                        |

5. Conclusion

ECC encryption algorithm is a relatively safe and efficient data encryption algorithm used in communication systems. In the communication system, only the users participating in the two parties can obtain and read the data transmitted by the communication. The ECC encryption algorithm allows VDES to be "selectively" encrypted between shore-ships, ship-ships, and ship-to-shore for a variety of confidential data (text files, data information, etc.), which will make the flexibility of VDES encrypted has increased dramatically. The ECC encryption algorithm simulation test results show that the amount of data information involved in the ECC encryption algorithm is very small, so the amount of resources used in the entire encrypted transmission process is not large, and the encryption/decryption efficiency is high. In addition, the comparison between the ECC algorithm and the RSA algorithm shows that the ECC algorithm has extremely high security. Therefore, the ECC encryption algorithm will play a crucial role in the future safe and efficient digital navigation strategy.

6. Acknowledgement

Fund Project: Liaoning Natural Science Foundation Project (201602082).
7. References

[1] Jiang Huifang. Design and implementation of ship security system [J]. Ship Science and Technology. 2017, 6: 146-149.

[2] Sun Zhu. Research on Modulation and Demodulation Algorithm of ASM Baseband and Implementation by FPGA [D]. Dalian: Dalian Maritime University, 2017.

[3] Xiong Yaying. Maritime Communication Technology New Development - VDES System [J]. Satellite Application. 2016(2):37.

[4] Lu Yao, Feng Lin, Zhang Rui. A physical layer design and implementation of VDES communication terminal, Aerospace Electronics and Military Integration Forum and Academic Exchange, 2017.

[5] Meng Xuemei. Exploring how to implement an encryption algorithm for encryption key disclosure [J]. Consumer Electronics Magazine, 2013(16): 65-65.

[6] SR Singh, AK Khan, TS Singh. A Critical Review on Elliptic Curve Cryptography, International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016.

[7] Hao Xiaojin. An Elliptic Curve Threshold Group Signature Scheme Based on Chinese Remainder Theorem [D]. Beijing: Minzu University of China, 2011.

[8] Wu Yuhua, Huang Yun, Li Yanjun, et al. The FPGA design of ECC encryption algorithm [J]. Microcomputer Information, 2007, 23(11): 236-237.

[9] Huang Fang. Realization of System Privilege Setting Based on Elliptic Curve Cryptography [J]. Network Security Technology & Application, 2008(10): 83-84.

[10] Li Yuejian, Zhu Changwon. Study and Improvement on System Architectures of Larbin Web Crawler [J]. Computer Technology And Development, 2012(7), 147-150.