Security Analysis of the SEAT Authentication Protocol for Maritime Traffic Management

Nai-Wei Lo
Department of Information Management
National Taiwan University of Science and Technology
Taipei, Taiwan
nwlo@cs.ntust.edu.tw

Cih-Sheng Li
Department of Information Management
National Taiwan University of Science and Technology
Taipei, Taiwan
M11109129@mail.ntust.edu.tw

***Abstract*—Maritime transportation is vital for global commerce, requiring secure communication systems for vessel monitoring and management. This paper presents a comprehensive security analysis of the SEAT protocol, recently proposed by Jegadeesan et al., which enhances the security of maritime traffic management. Our study identifies critical vulnerabilities against the SEAT protocol, including a flawed design of mutual authentication, a vulnerable mechanism to defend against replay attacks, exposure to man-in-the-middle attacks, and loopholes in the defense scheme against message modification attacks.**

Keywords—Identity Authentication, Maritime Traffic Management, Anonymity, Unlinkability, Privacy Preservation

I. INTRODUCTION

Maritime transportation is vital for global commerce and travel, with oceans serving as primary channels for trade and economic growth [1]. The marine transport sector is transforming into intelligent traffic management systems that incorporate digital technologies, introducing new security challenges [2].

The Automatic Identification System (AIS), mandated by the International Maritime Organization in 2004 and used by approximately 570,000 ships, lacks essential security measures. Its authentication protocol exhibits significant weaknesses, particularly with Maritime Mobile Service Identity (MMSI), which can be manipulated, compromising maritime security [3]. In 2022, Jegadeesan et al. proposed the SEAT protocol to secure maritime traffic management systems, which supports the preservation of trajectory privacy and anonymous authentication [1]. In this study, security analysis is conducted to evaluate the security robustness of the SEAT scheme.

II. SYSTEM MODEL

The system model proposed by Jegadeesan et al. in [1] consists of three main components and other possible entities such as satellites SA_n, as shown in Figure 1:

A. Maritime traffic controller (MTC)

A trusted entity that handles system initialization, generates public parameters, and registers ships and base stations.

B. Base station (BS_j)

It is a part of fixed coastal infrastructure, responsible for monitoring ships in its coverage range, providing docking information, and route guidance.

C. Ship (S_i)

Standard vessels are equipped with AIS technology for exchanging maritime data with other ships and shore stations.

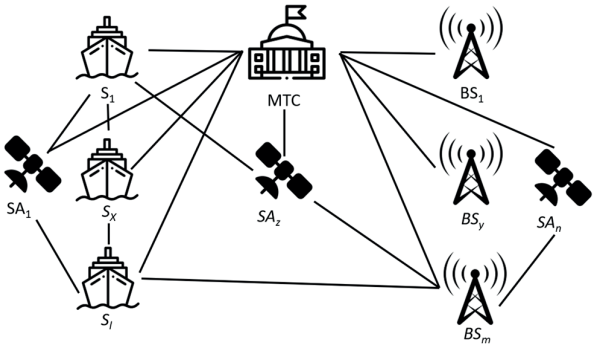

Figure 1. The system model of the SEAT protocol.

The proposed system operates under three distinct communication modes:

1) Private Communication Mode: Within custom management regions, the system employs private communication mode. This mode facilitates network access through secure channels, ensuring data integrity and confidentiality for sensitive operations.

2) Satellite Communication Mode: If a Base Station is not available in a specific region, the system switches to satellite communication mode. This mode ensures continuous communication capability across broader geographic areas where direct terrestrial infrastructure may be lacking.

3) VHF Frequency Channel Mode: This mode is utilized for data communication over short distances, typically within 20 to 30 nautical miles. It is selected to transmit traffic data between Ships and Base Stations for effective maritime traffic management.

III. THREAT MODEL

The SEAT protocol encompasses both internal and external attacks. An internal attack occurs when a ship fabricates its own identity information or impersonates another vessel to transmit deceptive data. Similarly, even a legitimate but inquisitive AIS center may engage in an internal attack by collecting and analyzing ships' trajectory information. In contrast, adversaries who attempt to uncover the identities or trajectories of ships, base stations, and related entities are classified as external attackers.

IV. OVERVIEW OF THE SEAT PROTOCOL

The SEAT protocol comprises five main stages, and the corresponding protocol notations are shown in Table I.

A. System initialization

MTC selects the random numbers msk, $S_{mtc} \in Z^*_q$ as the master secret and private keys. Compute the public key U_{mtc}

$= g_1^{S_{mtc}}$ and the parameter $SP = g_1^{\frac{1}{2S_{mtc}+msk}}$. Select the collision-resistant one-way hash function H : $\{0,1\}^* \rightarrow Z^*_q$. Announce the system parameters $\{q, e, g_1, g_2, G_1, G_2, G_T, msk, U_{mtc}, H(\cdot)\}$ to the public.

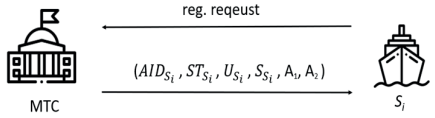

Figure 2. Registration and secret key generation for ship S_i.

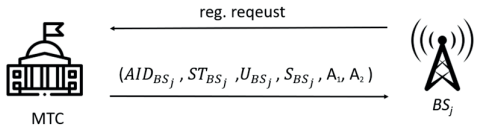

Figure 3. Registration and secret key generation for base station BS_j.

Table I. Notations of the SEAT protocol.

Notation Table	
MTC	Maritime traffic controller
S_i	Ships, $i \in Z^*_q = \{1,..x,...,l\}, 1 \le x \le l$
BS_j	Base station, $j \in Z^*_q = \{1,..y,...,m\}, 1 \le y \le m$
SA_k	Satellite, $k \in Z^*_q = \{1,..z,...,n\}, 1 \le z \le n$
msk	Master secret key for MTC
S_{mtc}, U_{mtc}	Private/ public key for MTC
S_{S_i}, U_{S_i}	Private/ public key for S_i
S_{BS_j}, U_{BS_j}	Private/ public key for BS_j
SP	security parameter
$r_{1\sim6}$	random numbers
$MMSI_{S_i}$	Maritime Mobile Service Identity
AID_{S_i}	Anonymous identity for S_i
AID_{BS_j}	Anonymous identity for BS_j
ST_{S_i}	Ship tracking parameter
ST_{BS_j}	Base station tracking parameter
A_1, A_2	Secret parameter
$H(\cdot)$	Secure one-way hash function

B. Registration and secret key generation

Ships and base stations provide documentation to MTC, generating private keys, public keys, anonymous identities, and tracking parameters. The detailed steps shown in Figures 2 and 3 are as follows:

- MTC generates a random number $r_1 \in Z^*_q$ .Compute the private key $S_{S_i} = g_1^{\frac{1}{r_1+S_{mtc}}}$ and public key $U_{S_i} = g_1^{r_1}$ .Assign a unique nine-digit Maritime Mobile Service Identity.Create an anonymous identity AID_{S_i} for the ship as $AID_{S_i} = g_1^{S_{mtc}+msk+r_1}$ .Compute ship tracking parameter $ST_{S_i} = g_1^{msk+r_1}$. Stores the values (U_{S_i}, S_{S_i}, AID_{S_i}, $ST_{S_i}^{S_{mtc}}$) in the database.Selects two confidential parameters $A_1, A_2 \in Z^*_q$ where $A_1, A_2 > 18000$. MTC transmits the values (AID_{S_i}, ST_{S_i}, U_{S_i}, S_{S_i}, A_1, A_2) to the S_i.
- MTC generates a random number $r_2 \in Z^*_q$ .Compute the private key $S_{BS_j} = g_1^{\frac{1}{r_2+S_{mtc}}}$ and public key $U_{BS_j} = g_1^{r_2}$ .Create an anonymous identity AID_{BS_j} for the base station as $AID_{BS_j} = g_1^{S_{mtc}+msk+r_2}$ .Compute base station tracking parameter $ST_{BS_j} = g_1^{msk+r_2}$ .Store the values (U_{BS_j}, S_{BS_j}, AID_{BS_j}, $ST_{BS_j}^{S_{mtc}}$) in the database.Select two confidential parameters $A_1, A_2 \in Z^*_q$ where $A_1, A_2 >$ 18000.MTC transmits the values (AID_{BS_j} , ST_{BS_j} , U_{BS_j} , S_{BS_j} , A_1, A_2) to the BS_j.
- The MTC securely transmits the following data (AID_{S_i}, ST_{S_i}, U_{S_i}, S_{S_i}, A_1, A_2) to the S_i . Similarly, the MTC securely sends (AID_{BS_j}, ST_{BS_j}, U_{BS_j}, S_{BS_j}, A_1, A_2) to the BS_j.

C. Anonymous authentication

To verify its identity to nearby ships or Base Stations, the ship generates an authentication certificate shown in Figure 4 as follows:

- The S_i randomly selects four values $r_3, r_4, r_5, r_6 \in Z^*_q$ to serve as one-time session keys. Here, r_3 is designated as the ship's one-time private key, and y_1 is its corresponding one-time public key. Using these values, it computes: $y_1 = g_1^{r_3}$, $y_2 = ST_{S_i} \times AID_{S_i}$, $x_1 = g_1^{r_3+r_6}$, $x_2 = g_1^{r_5-r_6+r_4}$, $x_3 = g_1^{r_3+r_4}$.
- S_i computes the challenge value (C) value as $C = H(x_1 \| x_2 \| x_3 \| y_1)$. Subsequently, the Si calculates the $F_1 = g_1^{r_4+r_6}$, $F_2 = g_1^{-r_4}$, $F_3 = g_1^{r_4-r_6}$, $F_4 = g_1^{r_4+r_5}$ as fake security parameters.
- The ship S_i then constructs the authentication certificate AC by concatenating the following values: F_1, F_2, F_3, F_4, y_1, C, and AID_{S_i}. Therefore, $AC = \{F_1 \| F_2 \| F_3 \| F_4 \| y_1 \| C \| AID_{S_i}\}$.

To safeguard the integrity of the AIS data, the ship S_i computes an anonymous signature σ as follows: $\sigma = g_2^{\frac{1}{r_3+AC}}$. The ship then combines this signature with the AIS information D_i, the current timestamp TS_1, and the trajectory privacy information TPI. TPI is calculated as $TPI = y_2 \times S_{S_i}$. Finally, the ship broadcasts the following message to nearby ships or base stations: $\{\sigma \| D_i \| TPI \| y_1 \| TS_1\}$.

Upon receiving the message $\{\sigma \| D_i \| TPI \| y_1 \| TS_1\}$ from ship S_i, the receiving entity performs the following verification steps. Timestamp Validation: The receiver checks the timestamp TS_1 against its own timestamp TS_2. If the difference $TS_2 - TS_1$ exceeds the agreed-upon time delay threshold ΔT, a replay attack is suspected, and the verification

process terminates. The receiver verifies the integrity of the received AIS information D_i by performing the following pairing operation: Calculate e ($y_1 \times g_1^{AC}$, σ). Compare the result with e (g_1, g_2). If the two values do not match, the signature is invalid, and the verification process terminates. If both the timestamp check and the data integrity check pass, the receiver proceeds to the next authentication steps.

Upon successful anonymous signature verification, the receiving entity proceeds to validate the authentication certificate AC as follows. The receiver calculates the following values using the received components of the AC: $x_1 = y_1 \times F_1 \times F_2$, $x_2 = F_2 \times F_3 \times F_4$, and $x_3 = y_1 \times F_1 \times F_2 \times F_3$. Then the receiver computes the challenge value $C' = H(x_1 \| x_2 \| x_3 \| y_1)$. The calculated challenge value C' is compared with the received challenge value C. If they match, the authentication certificate is considered valid. Otherwise, the authentication process is terminated.

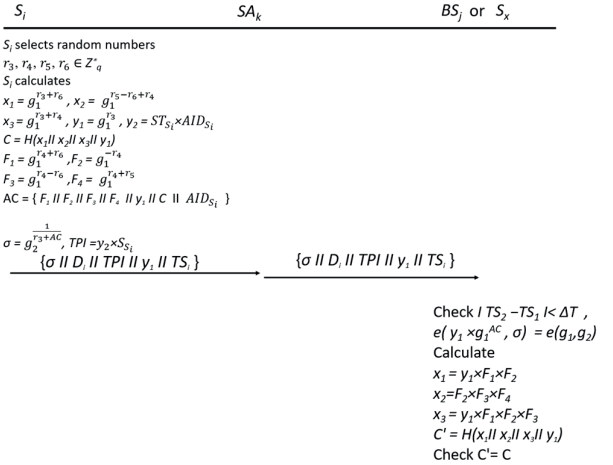

Figure 4. Anonymous authentication.

D. Conditional Tracking

In the event of a dispute, such as ship S_i transmitting falsified data to another ship or base station, which could potentially lead to maritime accidents, the proposed system includes mechanisms to address such issues as shown in Figure 5. The MTC can track the misbehaving ship S_i by submiting its AID_{S_i} value. Using this identifier, the MTC calculates $ST_{S_i}^{S_{mtc}}$, a security parameter, and correlates it with S_i's actual identity through a tracking mechanism.

Upon confirming S_i's misbehavior, the MTC takes decisive action by revoking *Si's* access to the system. This removal prevents further risks and disruptions to maritime operations. By swiftly addressing such incidents, the system aims to maintain safety within maritime traffic management.

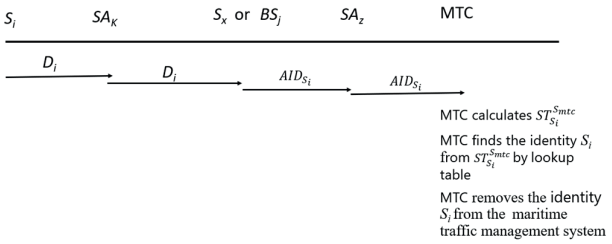

Figure 5. Conditional tracking.

E. Trajectory Privacy Preservation

In emergencies, the protocol maintains trajectory privacy while enabling services such as search and rescue positioning, as shown in Figure 6.

- If the emergency or critical situation of the S_i is identified through the received D_i, then the receiver sends the Trajectory Privacy Information (*TPI*) to the *MTC* along with the anonymous identity.
- Upon receiving the *TPI*, the *MTC* performs the following steps. The *MTC* calculates ST_{S_i} by the received *TPI* value $ST_{S_i} = TPI/(AID_{S_i} \times S_{S_i})$. The *MTC* computes P_i as the product of A_1 and A_2, ensuring both A_1 and A_2 are greater than 18000.The MTC determines P_1 and P_2 as $P_1 = (P_i)/A_1$ and $P_2 = (P_i)/A_2$. The MTC calculates Q_1 and Q_2 as the modular multiplicative inverses of P_1 and P_2 respectively, such that:$Q_1 \times P_1 \equiv 1 \pmod{A_1}$ and $Q_2 \times P_2 \equiv 1 \pmod{A_2}$. The *MTC* generates anonymous geographical coordinates (R_1, R_2) for ship S_i using the following formulas: $R_1 = P_1 \times Q_1 \times u_i' \pmod{P_i}$ and $R_2 = P2 \times Q_2 \times v_i' \pmod{P_i}$. The *MTC* sends the calculated anonymous geographical coordinates (R_1, R_2) to the Base Station or the nearby ship.
- Upon receiving the anonymous geographical coordinates (R_1, R_2), the Base Station or nearby ship can calculate the ship's (S_i) actual geographical coordinates (u_i, v_i) as follows: $u_i' = R_1 \times K_1$ and $v_i' = R_2 \times K_2$. Here, (u_i', v_i') represents the result of an accuracy calculation applied to the actual geographical coordinates of Ship S_i.

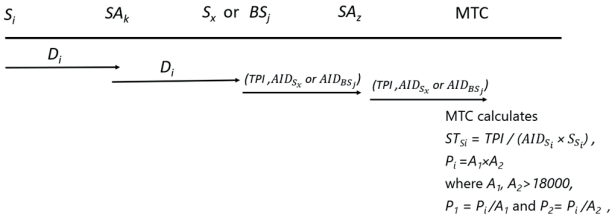

Figure 6. Trajectory privacy preservation.

V. Security Analysis of the SEAT Protocol

Our comprehensive security analysis of the SEAT protocol reveals several significant vulnerabilities that could compromise maritime communication systems. The following sections depict identified security flaws:

A. Parameters Not Transmitted

In the anonymous authentication section, we found that the authentication parameters are not transmitted. S_i transmits {σ ‖ D_i ‖ *TPI* ‖ y_1 ‖ TS_1} to BS_j or S_x which does not contain the authentication certificate AC, so in addition to not being able to verify that e ($y_1 \times g_1^{AC}$, σ) = e (g_1, g_2), it is not possible to confirm that $C' = C$, because the values of F_1, F_2, F_3, and F_4 are not known.

B. Vulnerable to Replay Attack

In the Anonymous Authentication section, the attacker can listen to the message $\{\sigma \| D_i \| TPI \| y_1 \| TS_1\}$, then modify the TS_1 to TS_1', and then replay the message $\{\sigma \| D_i \| TPI \| y_1 \| TS_1'\}$ sent to BS_j or the S_x.

C. No Mutual Authentication

In the protocol, only BS_j or S_x has verified S_i, but S_i has not been given any parameters to verify BS_j or S_x. Hence, the process is not mutual authentication.

D. Vulnerable to Man-in-the-Middle Attack

1) Man-in-the-middle attacks by outsiders: In this case, outsiders can get message $\{\sigma \| D_i \| TPI \| y_1 \| TS_1\}$, they can modify the information of D_i, TPI and TS_1 as they like, and then send the message to BS_j or S_x, in this case, since it does not modify the values of y_1 and σ required for the validation, it can be successfully validated.

2) Man-in-the-middle attacks by insiders: In this case, insiders can do anything that man-in-the-middle attacks by outsiders can do, and in addition, because they are the internal legitimizer, they can modify σ and y_1.

E. Vulnerable to Message Modification Attacks

As discussed in point parameters not actually transmitted, the absence of crucial parameters in the transmitted data renders the anonymous signature method ineffective against message modification attacks, despite the original author's claims.

F. No Explanation on How to Identify Fake Information in Conditional Tracking

At this stage, *MTC* can receive the AID_{S_i} value and use it to calculate the ST_{Si}^{Smtc} to find out the real identity. Still, there is no way to check the correctness of the data, and even if it receives the fake D_i and AID_{S_i} values, the situation remains unchanged.

VI. Conclusion

Our security analysis of the protocol proposed by Jegadeesan et al. reveals several critical vulnerabilities that could significantly compromise the security and reliability of maritime communication systems. The identified issues include incomplete parameter transmission, inadequate protection against replay and man-in-the-middle attacks, lack of mutual authentication, and ineffective message integrity verification and conditional tracking mechanisms. These findings underscore the need for more robust and comprehensive security solutions in maritime traffic management systems. Future protocols should address these vulnerabilities by ensuring complete parameter transmission, implementing stronger protections against replay attacks, establishing mutual authentication, hardening defenses against man-in-the-middle attacks, enhancing message integrity verification, and improving conditional tracking mechanisms.

Acknowledgment

This work was partially supported by the National Science and Technology Council of Taiwan, under grants NSTC 114-2221-E-011 -115 and NSTC 114-2634-F-011-002-MBK.

References

[1] S. Jegadeesan, M. S. Obaidat, P. Vijayakumar, and M. Azees, "SEAT: Secure and Energy Efficient Anonymous Authentication With Trajectory Privacy-Preserving Scheme for Marine Traffic Management," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 2, pp. 815-824, June 2022, doi: 10.1109/TGCN.2021.3126618.

[2] D. P. F. Möller, I. A. Jehle, J. Froese, A. Deutschmann, and T. Koch, "Securing Maritime Traffic Management," 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 2018, pp. 0453-0458, doi: 10.1109/EIT.2018.8500147.

[3] I. Rudan, V. Francic, M. Valcic, and M. Sumner, "Early detection of ship collision situations in a ship traffic services area," Transport, vol. 35, no. 2, pp. 121–132, 2019, doi: 10.3846/transport.2019.11464.