International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.97-110
http://dx.doi.org/10.14257/ijsia.2015.9.2.10

S3 (Secure Ship-to-Ship) Information Sharing Scheme using Ship Authentication in the e-Navigation

Seung-hee Oh, Daehee Seo and Byunggil Lee

Cyber Security Department, SW Content Research Laboratory,
Electronics and Telecommunications Research Institute, Republic of Korea
{seunghee5, dhseo, bglee}@etri.re.kr

Abstract

Recently, the e-Navigation is main flow of worldwide maritime communications. The e-Navigation suggested by the International Maritime Organization (IMO) and International Association of Lighthouse Authorities (IALA) is about collecting/integrating/expressing /analyzing/exchanging the marine data between ships and the land in harmony through the electronic method for protecting marine environment, keeping safe navigation, and maintaining marine safety/security [2]. However, the e-Navigation is concentrated only the maritime service and a common data structure to share maritime information, so security considerations especially when ship starts to communicate other ships is insufficient. In this paper, we analyze the e-Navigation Maritime Service Portfolios (MSPs) and ship-to-ship information sharing protocol. We propose security requirements of MSPs and secure ship-to-ship information sharing scheme to provide reliable communication between ships based on the analysis results. Our proposed scheme has 3 steps to authenticate each other using the each ship's Maritime Mobile Sevice Identify (MMSI) is a unique key of each ship and increases the security of reliable ship-to-ship communication.

Keywords: *e-Navigation, Authentication, Ship-to-ship, AIS*

1. Introduction

The e-Navigation suggested by IMO and IALA is discussed on the importance of collecting/integrating /expressing/analyzing/exchanging the marine data for the safe navigation and marine environmental protection in maritime communications. In particular, the e-Navigation focuses on developing data structure and services for the marine data exchange between the ship and the shore-side systems (for example Vessel Traffic Service (VTS)). However, the e-Navigation is the lack of security considerations for reliable information sharing. Therefore, the consideration of the security aspects has emerged as an important problem to be leading.

We deduce the security requirements by analysis of the possible security threats and vulnerabilities in the e-Navigation environment and propose reliable ship-to-ship communications scheme using mutual authentication mechanism which consists of 3 steps.

This paper is organized as follows. In section 2, we introduce the architecture and service portfolios of the e-Navigation and Automatic Identification System (AIS) communication. Section 3 analyses existing ship-to-ship information sharing schemes and the proposed secure ship-to-ship information sharing scheme for the e-Navigation is addressed in section 4. Section 5 describes the analysis of proposed S3 (Secure ship-to-ship) information sharing scheme. Finally, section 6 gives conclusion and directions for future works.

ISSN: 1738-9976 IJSIA

2. The Overview of the e-Navigation Architecture and AIS

In this sector we look at the structure of the e-Navigation, MSPs (Maritime Service Portfolios), and AIS which is the standard communication method between ships. After then, we analyze the requirements for the MSPs [16].

2.1. The e-Navigation

The e-Navigation is an ongoing standardization strategy to the 2018 target co-organized by IMO, IALA, IHO (International Hydrographic Organization). Its purpose is to provide data exchange between ship-to-ship and between shore-side systems (for example VTS) for better safety and more various maritime services expansion of the existing marine vessels and shore-side VTS. This is the definition of e-Navigation [18].

The e-Navigation is the harmonized collection, integration, exchange, presentation and analysis of marine information onboard and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment.

The e-Navigation would help reduce navigational accidents, errors and failures by developing standards.

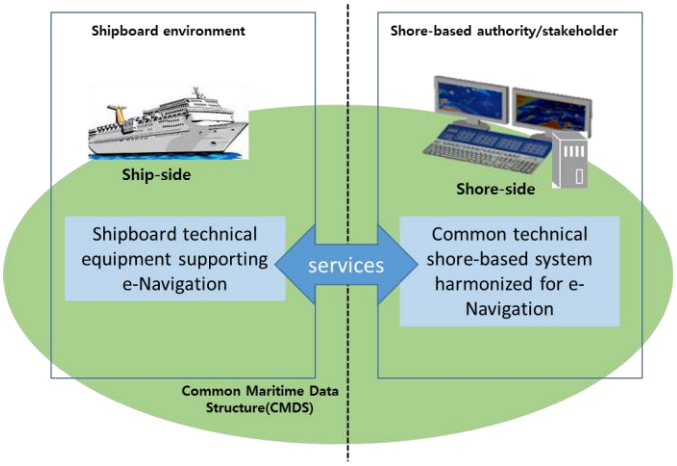
Shipboard environment
Shore-based authority/stakeholder
Ship-side
Shore-side
Shipboard technical equipment supporting e-Navigation
services
Common technical shore-based system harmonized for e-Navigation
Common Maritime Data Structure(CMDS)

Figure 1. The Architecture of CMDS in e-Navigation

In other words, the e-Navigation focus on not only integration of equipment but also integration of information. In addition, the e-Navigation contains information service structure to provide safe navigation, and marine environment and resources protection using exchanging, sharing, and integrating of a variety of marine–related information from marine and land [19]. The CMDS (Common Maritime Data Structure) is to send and receive the e-Navigation data in order to exchange information in heterogeneous equipment for next generation maritime network.

It is organized into 17 major services for the e-Navigation MSPs shown as below Table 1 and MSP 1, 2, 3, and 5 are related to ship-to-ship communication.

Table 1. The MSPs Related to Ship-to-ship Communication

MSP No.	Identified Services
MSP1	VTS Information Service(INS)

MSP2	Navigation Assistance Service(NAS)
MSP3	Traffic Organization Service(TOS)
MSP4	Local Port Service(LPS)
MSP5	Maritime Safety Information(MSI) Service
MSP6	Pilotage Service
MSP7	Tugs service
MSP8	Vessel shore reporting
MSP9	Remote monitoring of ships systems
MSP10	Telemedical Assistance Service(TMAS)
MSP11	Maritime Assistance Service(MAS)
MSP12	Nautical Chart Service
MSP13	Nautical publications service
MSP14	Ice navigation service
MSP15	Meteorological information service
MSP16	Real-time hydrographic and environmental information services
MSP17	Search and Rescue(SAR) service

2.2. Ship-to-Ship information Sharing

The AIS was developed primarily as a tool for maritime safety - vessel collision avoidance, use by VTS and as a means for littoral states to get information on vessels operating near their coasts.

The IMO recommends to install AIS equipment in ship typically more than 300-ton, depending on Safety of Life at Sea (SOLAS) Convention since 2005. The AIS equipment installed on ships continuously and autonomously transmits ship information including its identity, position, course and speed to enhance safety. The technology characteristic of the AIS is according to ITU-R recommendation M.1371-4 [20] and the user and operator requirements referring to IMO Resolution MSC.74 (69) [17]. However, these documents do not include the security threats and method for providing safety.

Currently, AIS message defined 1~27 types and 1, 2, 3 messages are used to exchange the information about current location of ship. When sending and receiving position information between ships, inaccurate location information or malicious forgery /modification of location information is an important threatening factor of maritime. Therefore, it is the one of the most urgent issue and must be handled as soon as possible to prevent security threats. In addition, AIS 1, 2, and 3 messages should be used to support MSP 1, 2, 3, and 5 referred to in Section 2.1.

2.3. Basic Requirements (BR) and Security Requirements (SR) in MSPs

In this section, we analyze basic requirements and security requirements for supporting MSP 1, 2, 3, and 5 services to exchange information securely between ships in the e-Navigation. The SRs are the same as the security requirements on the wireless network [2, 9-11].

These are the BRs in MSPs (for the e-Navigation).

● BR1-MSPs: Requires the network to collect and exchange the information of ships.

- BR2-MSPs: Requires the information about the individual ship's location, speed, route and the peripheral ships information.
- BR3-MSPs: Require the essential information for the control area within the ship.
- BR4-MSPs: Require a network connection to the service internationally for exchanging information on the safety.

These are the Security Requirements in MSPs for exchange maritime information in the e-Navigation environment.

- SR-1: The wired/wireless network between ship-to-ship, ship to shoreside system or shoreside systems must be connected seamlessly and should be able to trust each other.
- SR-2: The ship information including basic information/location information/emergency warning/signal and traffic control information should be trusted between ship-to-ship, ship to shoreside system or shoreside systems.
- SR-3: The information between ship-to-ship, ship to shoreside system or shoreside systems should not be forged or tampered during send and receive.
- SR-4: The information between ship-to-ship, ship to shoreside system or shoreside systems should not be exposed to the user that is not allowed during send and receive (including other ships, agencies, and etc).

Table 2 is shown the relationships between the security requirements and the need for MSPs.

Table 2. Security Requirements in MSPs

Security Requirements	MSP
SR-1. Reliable Network for connectionless and mutual trust	BR1-MSPs, BR2-MSPs, BR3-MSPs, BR4-MSPs
SR-2. Trusted ship information between ships or ship-to-shore system or shore systems	BR1-MSPs, BR2-MSPs, BR3-MSPs, BR4-MSPs
SR-3. Maintain integrity of the receiving information against malicious forgery or modification	BR1-MSPs, BR2-MSPs, BR3-MSPs, BR4-MSPs
SR-4. Maintain confidentiality of the receiving information for only authorized user	BR1-MSPs, BR2-MSPs

The required security technologies for trusted/reliable communication in general digital communication are below.

- Authentication: Especially, Extensible Authentication Protocol (EAP) is an authentication framework frequently used in wireless networks and point-to-point connections and is defined in RFC 5247 [21].
- Authorization: It is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular.
- Transferring Data Encryption: It is the function of preventing transmitted data forgery or modification.
- Network Security: It is the function of maintaining data network without interruption to be sent and received.

3. Analysis of Existing Ship-to-Ship information Sharing Schemes

This sector analyzes existing two ship-to-ship information sharing schemes. One is Nerea Toledo's scheme and the other is polish approach to the e-Navigation scheme.

3.1. Nerea Toledo's Scheme

The Nerea Toledo's paper analyses the requirements of maritime communication for e-navigation strategy implementation. Nerea Teledo's suggested enhanced ship-shore communications, always-best-connected procedures as shown Figure 2 [13].

In that paper, the Host Identity Protocol (HIP) as the mobility management protocol are applied for secure mobility while enhancing performance of handover processes. It mentions secure communication in ship-shore communication environment not ship-to-ship communication.

The integration of the HIP protocol and the always-best connected mechanisms leads to an architecture which supports secure and seamless mobility while covering ship-shore communications in an efficient and affordable manner.

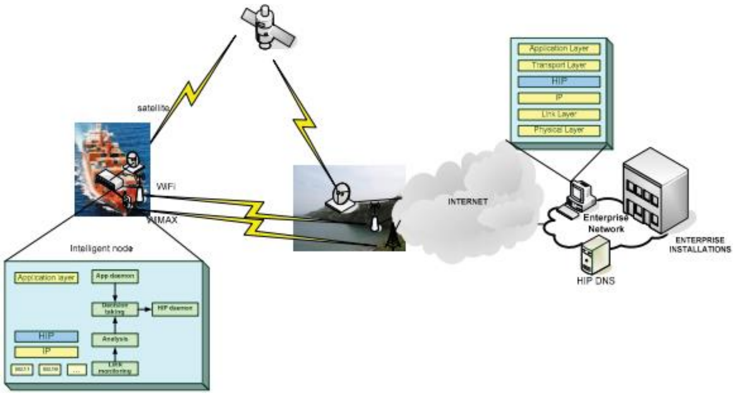

Figure 2. Architecture to cover ship-shore communications in Nerea toledo's scheme

This paper is a system architecture for communication between ship and shore systems. Neraa Toledo's scheme can be applied BR1-MSPs, BR2-MSPs, and BR3-MSPs in Section 2.3, can, but are excluded BR4-MSPs. In addition, it supports SR-1, but it does not support SR-2, SR-3, and SR-4.

3.2. Polish Approach to the e-Navigation Scheme

The A. Weintrit's paper predicts future e-navigation system deployment as two main directions shown like Figure 3 [14]. One is integrated system where information from ships will be send to shore data processing centers and the main decisions about the ship navigation assist will be made onshore; and the other is distributed system based on development of ship intelligent self-organizing systems which will be able to exchange the information between the other ships and will be able to process the information and to support the decision of navigators.

It also presents that the e-navigation systems will be most likely developed in two stages:

- First stage: It will be totally based on existing bridge and communication systems (AIS, Electronic Chart Display & Information System (ECDIS) and voice Very High Frequency (VHF)) only development of shore navigation

- Final stage: The dedicated system based on created ship e-navigation support platform where satellite communication will be applied.

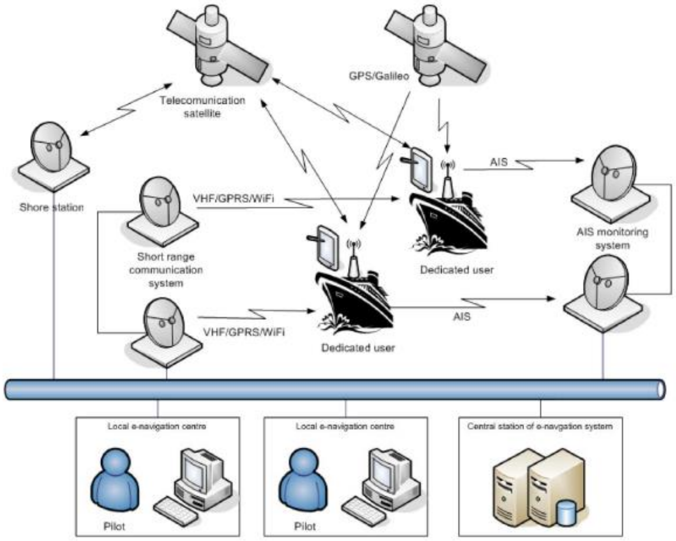
Telecomunication satellite
GPS/Galileo
Shore station
VHF/GPRS/WiFi
AIS
Short range communication system
Dedicated user
AIS monitoring system
VHF/GPRS/WiFi
AIS
Dedicated user
Local e-navigation centre
Pilot
Local e-navigation centre
Pilot
Central station of e-navgation system

Figure 3. Polish e-Navigation System Configuration

It is addressed as one of the issues about the protocol to prevent unauthorized access to safety or security-critical, real-time data transmissions. However, it did not mention the detail security mechanism.

This paper concerned BR1-MSPs, BR2-MSPs, BR3-MSPs, and BR4-MSPs in Section 2.3. It refers to SR-1 which is the communication security between ships, but it do not include SR-2, SR-3, and SR-4, and the method how to apply other security requirements.

4. Proposed S3 (Secure Ship-to-Ship) Information Sharing Scheme

In this section, the default scenario, assumptions, and authentication 3 steps of the proposed mutual authentication method for providing secure communications between ship-to-ship in the e-Navigation environment are described. The data communications in the e-Navigation environment are divided into (1) ship-to-ship communication; (2) a communication between ships and shoreside systems; (3) a communication between shoreside systems.

We limited only (1) ship-to-ship communication which is wireless communication using AIS in proposed scheme. The proposed scheme applies trusted third party (TTP) based authentication using MMSI as a unique key before starting the communication and it has three steps to provide authentication as such Pre-Authentication, Mutual Authentication, Multi_Ship Group Authentication [4-5].

4.1. Scenario of S3 Information Sharing Scheme

The security threats such as unauthorized access, Denial of Service (DoS) attack, the message modulation/forgery, replay attack are possible in the communication between ships. We mentioned related technical security elements that support to send and receive information safely between the domains as described in Section 2.3 [1, 3, 7-8].

In this paper, we propose the communication scheme including reliable authentication process between ships before starting ship communication using AIS network layer. Our authentication scheme focus on MSP1, 2, 3, and 5 as described in Section 2.1. It follows the authentication process to each other via the TTP as shown in Figure 4, to configure the e-Navigation environment that is mutual trust between ships.

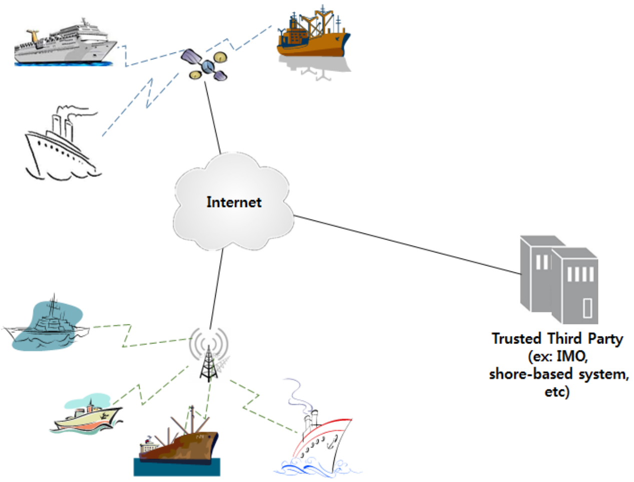

Figure 4. Explicit Authentication between Ships using TTP in the e-Navigation Environment

The proposed S3 information exchange scheme assumes the following:

- To communicate with ships, AIS equipment is provided.
- A ship is connected to the Internet via a AIS base station or Global Positioning System (GPS).
- TTP is possible to communicate with the ship via the Internet.
- The provided ship network is reliable.
- The integrity of exchanging information between ships is provided.

4.2. Scenario of S3 Information Sharing Scheme

The exchange of information between ships using existing AIS did not go through the authentication process under the assumption of mutual trust. Therefore, information exchange has been carried out without being able to confirm such as the value modulation or malicious AIS default setting error. The e-Navigation environment, as described in section 2, important information exchanges between ship-to-ship communications, so that authentication process is required to prevent malicious access and attack [6, 12, 15].

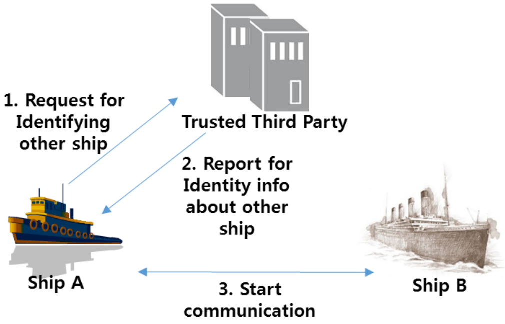

Figure 5. S3 Information Sharing Authentication Scheme

In this paper, we provide the explicit authentication scheme between ships using the TTP based on the MMSI which is unique key of each ship in consideration of the AIS communication characteristics. The proposed S3 authentication scheme is divided into three steps, parameters of the system are as follows.

- H(): secure hash function
- h: reliable hash value which is calculated using H()
- $MMSI_x$: the Identifier to be used in each ship
- X: Ship A(A), Ship B(B)…
- r: random value
- T_x: timestamp
- TTP: Trusted third party needed for mutual authentication between ships

Step 1: Pre-Authentication

A ship provides a MMSI to the TTP before performing mutual authentication between ships, and receives r and T required for the mutual authentication process shown as Figure 6.

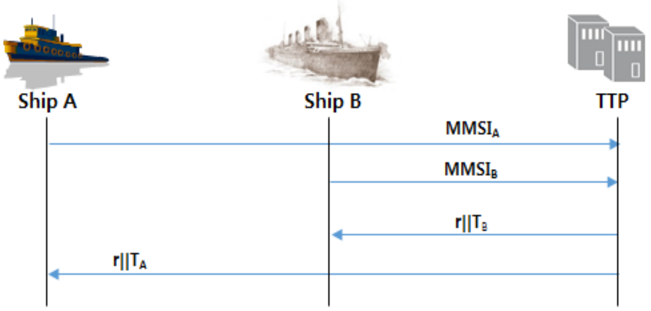

Figure 6. S3 Information Sharing Pre-Authentication

1. Ship A and Ship B transmit its $MMSI_x$ to TTP and then TTP manages them.
2. TTP send shared random value r and each timestamp T_x to Ship A and Ship B.

Step 2: Mutual Authentication:

In the process of mutual authentication between the ships is performed via the TTP, if the ship A is to communicate with the ship B will go through the following steps.

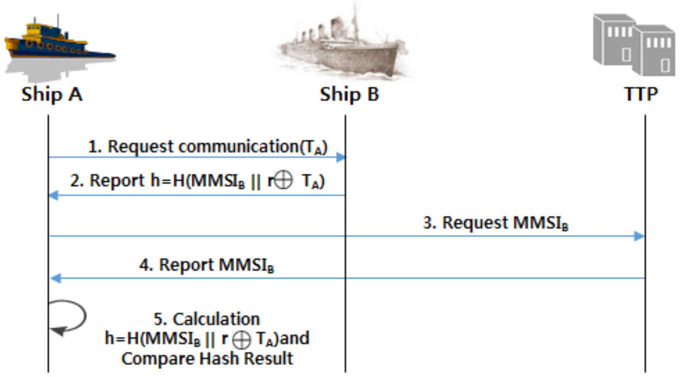
Ship A
Ship B
TTP
1. Request communication(T_A)
2. Report h=H($MMSI_B$ || r$\oplus$ T_A)
3. Request $MMSI_B$
4. Report $MMSI_B$
5. Calculation
h=H($MMSI_B$ || r $\oplus$ T_A)and
Compare Hash Result

Figure 7. S3 Information Sharing Mutual Authentication

1. Ship A requests communication to Ship B and sends timestamp T_A to Ship B.
2. Ship B makes hash value using $MMSI_B$, r (by TTP), and T_A (by ship A).
3. Ship A requests $MMSI_B$ (other ship's MMSI) to TTP.
4. TTP reports $MMSI_B$.
5. Ship A compares the two hash values that one is received from Ship B, the other is the calculated value using $MMSI_B$ received from TTP.

Step 3: Multi_Ship Group Authentication

Multi_ship group authentication is the method between ship groups instead of ships. When a ship is required to communicate with other ships after making mutual authentication between other ships, a ship should authenticate other ships one by one. However, this method is very inefficient if there are many ships already performed mutual authentication and a ship needs to authenticate all of other ships. Therefore, we propose Multi-Ship Group Authentication which offers integrated management by complementing the inefficiency of individual ship management.

- Initial Group Creation: If at least two ships is successful mutual authentication, TTP manages to generate a group key for the two ships. Example: If the ship A and the ship B that they do not belong to any group are successful mutual authentication, the ship A and the ship B become the group a and share GID (Group ID) a = {$MMSI_A$, $MMSI_B$, GKey (Group Key)$_a$}. The TTP manages the ship A and the ship B as a group.

- Added a new ship in the group: If the ship C which does not belong to any group requires mutual authentication to the ship A as shown Figure 8, the ship C becomes a member of the Group a and can communicate with certified group communication after successful mutual authentication.

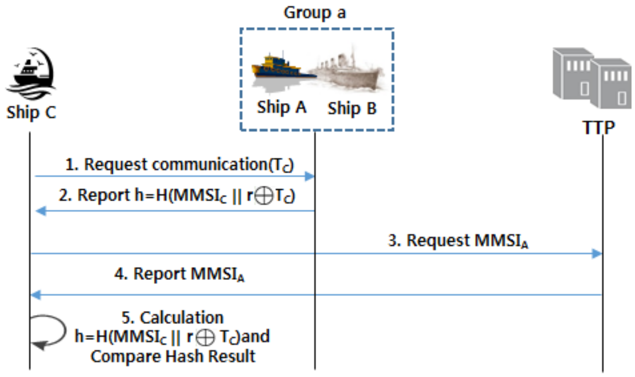

Figure 8. The Process of Adding New Ship in the Group

- Mutual authentication between the groups: It processes for example as like Figure 9, the Ship A in the Group a needs to communicate with the Ship D in the Group b, the Ship A processes mutual authentication to the Group b instead of the Ship D. After successful mutual authentication, the Ship A can communicate with not only the Ship D but also the Ship E in Group b. the Ship D also can communicate with not only the Ship A but also the Ship B and the Ship C without additional authentication process.

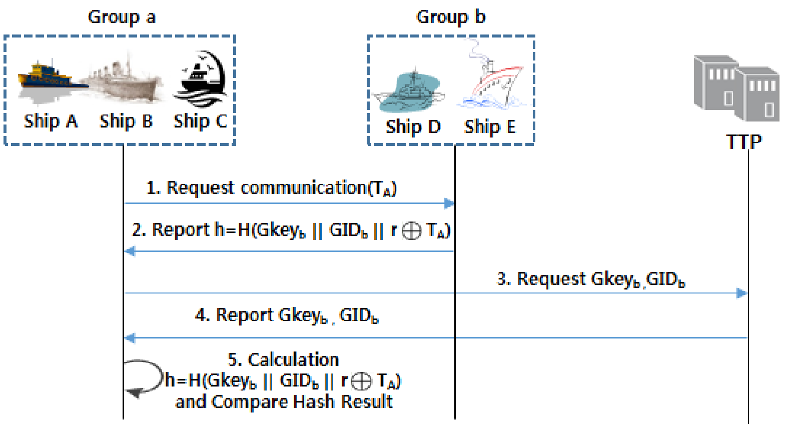
Group a
Ship A
Ship B
Ship C
Group b
Ship D
Ship E
TTP
1. Request communication(T_A)
2. Report $h=H(Gkey_b \,||\, GID_b \,||\, r \oplus T_A)$
3. Request $Gkey_b$,GID_b
4. Report $Gkey_b$, GID_b
5. Calculation
$h=H(Gkey_b \,||\, GID_b \,||\, r \oplus T_A)$
and Compare Hash Result

Figure 9. S3 Information Sharing Group Authentication

With an explicit authentication, it is possible to prevent attempts to communicate by changing the information on the ship with malicious intent as well as providing a reliable communication environment among ships. Additionally, the proposed scheme also presented a methodology for performing authentication between the ships through the efficient 3 steps authentication process.

5. Analysis of Proposed Scheme

In this section, we compare the exchange of information between the traditional methods in Section 3 and the proposed S3 information sharing scheme. Table 3 can be summarized as items that support the proposed scheme is based on the BRs and SRs in that analysis in section 2.3.

The proposed S3 information sharing scheme unlike a conventional method are concentrated in the network security is providing reliability using mutual authentication between ship-to-ship and is ensuring confidentiality by transmitting only authenticated ships. Our scheme assume that the network among ships is reliable and the messages between ship-to-ship are guaranteed integrity.

Table 3. Analysis of Security Requirements

	Nerea Toledo's Scheme	Polish approach to e-Navigation scheme	Suggested S3 information sharing scheme
SR-1. Reliable network	O	O	X
SR-2. Trusted ship information	X	X	O
SR-3. Maintain integrity	X	X	X
SR-4. Maintain confidentiality	X	X	O

(O: Support, X: Not support)

The proposed scheme is satisfied the MSP 1, 2, 3, and 5 in the e-Navigation environment and it is expandable structure so that it can apply to between shore-side systems (*e.g.* VTS) and between shore-side system and ship. In addition, it's one of key feature is easy to apply to the existing AIS environment.

6. Conclusion and Future Works

In this paper, we analyzed for AIS, ship-to-ship communication and the e-Navigation architecture and proposed 3 steps mutual authentication scheme to provide enhanced security at the ship-to-ship communication which is suitable for the e-Navigation environment. The e-Navigation environment is expected to be made of more various types of information exchange between the ships, should be preceded by a cross-check in order to trust the information sent and received between the ships.

We propose the information sharing scheme which has 3 steps (Pre-Authentication, Mutual Authentication, Multi_Ship Group Authentication) to authenticate between ships using MMSI which is the unique key of each ship. In addition, proposed scheme can be applied MSP 1, 2, 3, and 5 among 17 MSPs of the e-Navigation and support SR-2 and SR-4 under the condition that SR-1 and SR-3 are provided.

In the future, we will be carried out the dedicated encryption algorithm for maritime data and network security methods to support the reliable/trusted communication between the ship and shoreside systems. In addition, we keep following additional security requirements in the e-Navigation and maritime data communication.

Acknowledgements

This work was supported by ETRI through Maritime Safety & Maritime Traffic Facilities Management R&D Program of the MOF/KIMST (2009403, Development of next generation VTS for maritime safety).

This paper is a revised and expanded version of a paper entitled "Mutual authentication between ships in the e-Navigation environment" presented at SecTech 2014, Hainan, China, 20-23 Dec.2014.

References

[1] A. Irshad, W. Noshairwan, M. Shafiq, S. Khurram, E. Irshad and M. Usman, "Security Enhancement in MANET Authentication by checking the CRL status of Servers", International Journal of Advanced Science and Technology(IJAST), vol. 1, (**2008**) December, pp. 91-98.

[2] B. Lee and N. Park, "Performance Improvement based Authentication Protocol for Inter-Vessel Traffic Service Data Exchange Format Protocol based on U-navigation System in WoT Environment", Journal of applied mathematics, vol. 2014, (**2014**) August.

[3] E.-S. Lee, H.-J. Lee, K. Lee and J.-H. Park, "Automating Configuration System and Protocol for Next-Generation Home Appliances," ETRI Journal, vol. 35, no. 6, (**2013**) December, pp. 1094-1104.

[4] H. Modares, A. Moravejosharieh, R. B. Salleh and J. Lloret, "Enhancing Security in Mobile IPv6", ETRI Journal, vol. 36, no. 1, (**2014**) February, pp. 51-61.

[5] J.-H. Park, Y.-H. Jung, K.-H. Lee, K.-W. Lee and M.-S. Jun, "An Enhanced Light-weight Anonymous Authentication and Encryption Protocol in Wireless Sensor Network," International Journal of Database Theory and Application (IJDTA), vol. 5, no. 1, (**2012**) March, pp. 1-20.

[6] J. Ok Kwon and Ik Rae Jeong, "Relations among Security Models for Authenticated Key Exchange," ETRI Journal, vol. 36, no. 5, (**2014**) October, pp. 856-864.

[7] K. Sharma and M. K. Ghose, "Cross Layer Security Framework for Wireless Sensor Networks," International Journal of Security and Its Applications (IJSIA), vol. 5, no.1, (**2011**) January, pp. 39-52.

[8] K. Sharma, M. K. Ghose, D. Kumar, R. P. Kumar Singh and V. K. Pandey, "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", International Journal of Advanced Science and Technology (IJAST), vol. 17, (**2010**) April, pp. 31-44.

[9] Md. S. Islam and S. A. Rahman, “Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches,” International Journal of Advanced Science and Technology (IJAST), vol. 36, (**2011**) November, pp. 1-8.
[10] P. Kumar, A. Gurtov, M. Ylianttila, S.-G. Lee and H. Lee, “A Strong Authentication Scheme with User Privacy for Wireless Sensor Networks,” ETRI Journal, vol. 35, no. 5, (**2013**) October, pp. 889-899.
[11] T. Wenjun and H. Bin, “A Stronger Formal Security Model of Three-party Authentication and Key Distribution Protocol for 802.11i,” International Journal of Security and Its Applications (IJSIA), vol. 6, no. 4, October (**2011**), pp. 163-174.
[12] T.-H. Chen and W.-K. Shih, “A Robust Mutual Authentication Protocol for Wireless Sensor Networks,” ETRI Journal, vol. 32, no. 5, (**2010**) October, pp. 704-712.
[13] A. Weintri, R. Wawruch, C. Specht, L. Gucma, and Z. Pietrzykowski, “Polish Approach to e-Navigation Concept,” TransNav, International Journal on Marine Navigation and Safety of Sea Transportation, vol. 1, no. 3, September (**2007**), pp. 261-269.
[14] N. Toledo, M. Higuero, E. Jacob and M. Aguado, “A Novel Architecture for Secure, Always-Best Connected Ship-Shore Communications,” Intelligent Transport Systems Telecommunications (ITST), (**2009**) October, pp. 192-197.
[15] R. M. Savola, “Node Level Security Management and Authentication in Mobile Ad Hoc Networks,” 2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, MDM, (**2009**), pp. 449-458.
[16] S.-h. Oh, D. Seo, B. Lee and B. Chung, “Mutual authentication between ships in the e-Navigation environment”, Proceeding of Computer and Computing Science (COMCOMS) 2014, (**2014**) December.
[17] B. J. Tetreault, “Use of the Automatic Identification System (AIS) for maritime domain awareness (MDA)”, OCEANS, Proceedings of MTS/IEEE, (**2005**).
[18] IMO NAV 53/13, “Development of an E-Navigation Strategy. Report of the Correspondence Group on e-navigation (Submitted by the United Kingdom),” International Maritime Organization (IMO), London, 20 (**2007**) April.
[19] IMO’s Sub-Committee of Safety of Navigation (NAV) “Draft Strategy for the Development and Implementation of e-Navigation”, (**2008**) September.
[20] Recommendation ITU_R M.1371-4, “Technical characteristics for an automatic identification system using time-division multiple access in the VHF maritime mobile band”, (**2010**) April.
[21] http://en.wikipedia.org/

Authors

Seung-Hee Oh, she received the B.S. degree in Computer Science from Chonbuk National University, Republic of Korea, in year 1999. She received the M.S. degree in Computer Science and Engineering from Ewha Womans University, Republic of Korea, in 2001. She is working as a Senior Member of Engineering Staff in Electronics and Telecommunications Research Institute (ETRI), Republic of Korea since 2001. Her research interests include information security, network security, security management, air traffic control, and vessel traffic control.

Dae-Hee Seo, he received the Ph.D. degree from Soonchunhyang University, Choongnam, Korea. He is currently a Senior Member of Engineering Staff with the Electronics and Telecommunications Research Institute, Daejeon, Korea. He has published many research papers in international journals and conferences. His research interests include key management, network management, wireless security, and ubiquitous computing. Dr. Seo is a member of the International Academy, Research, and Industry Association; the Association for Information, Culture, Human, and Industry Technology; and the Science and Engineering Research Support Society.

Byunggil Lee, he received his Ph.D. degree in electrical engineering from the Kyungpook National University in 2003. In 2001, he joined the ETRI (Electronics and Telecommunications Research Institute), Republic of Korea and he is working as principle member of engineering staff in software ･ contents research laboratory of ETRI. He is currently a project leader of maritime - ICT convergence research project. His research interests include vehicle to vehicle network based converged security, vessel traffic management, maritime safety and e-navigation.