Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 734768, 7 pages
http://dx.doi.org/10.1155/2014/734768

Research Article

Performance Improvement Based Authentication Protocol for Intervessel Traffic Service Data Exchange Format Protocol Based on U-Navigation System in WoT Environment

Byunggil Lee[1] and Namje Park[2]

[1] *Electronics and Telecommunications Research Institute (ETRI), 218 Gajeong-ro, Yuseong-gu, Daejeon 305-700, Republic of Korea*
[2] *Department of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju-do 690-781, Republic of Korea*

Correspondence should be addressed to Namje Park; namjepark@jejunu.ac.kr

Received 15 March 2014; Accepted 4 June 2014; Published 7 August 2014

Academic Editor: Young-Sik Jeong

International Association of Lighthouse Authorities (IALA) is developing the standard intersystem VTS exchange format (IVEF) protocol for exchange of navigation and vessel information between VTS systems and between VTS and vessels. VTS (vessel traffic system) is an important marine traffic monitoring system which is designed to improve the safety and efficiency of navigation and the protection of the marine environment. And the demand of Inter-VTS networking has been increased for realization of e-Navigation as shore side collaboration for maritime safety. And IVEF (inter-VTS data exchange format) for inter-VTS network has become a hot research topic of VTS system. Currently, the IVEF developed by the International Association of Lighthouse Authorities (IALA) does not include any highly trusted certification technology for the connectors. The output of standardization is distributed as the IALA recommendation V-145, and the protocol is implemented with an open source. The IVEF open source, however, is the code used to check the functions of standard protocols. It is too slow to be used in the field and requires a large memory. And the vessel traffic information requires high security since it is highly protected by the countries. Therefore, this paper suggests the authentication protocol to increase the security of the VTS systems using the main certification server and IVEF.

1. Introduction

The vessel traffic system (VTS) field that is about maritime safety has mostly relied on overseas technology, unlike the shipbuilding industry that has recently retained the leader's position in the global market as a traditional industry. The VTS technology in the maritime safety field consists of maritime IT technology and has desperately required the grafting with the up-to-date IT technology [1, 2].

In the maritime field, the concept of "e-Navigation" for the grafting of the electronic information technology was introduced into Europe, and the popularity of this concept has been rising internationally in recent two to three years. The e-Navigation promoted by IMO is about collecting/integrating/expressing/analyzing the marine data between ships and the land in harmony through the electronic method with the purpose of marine safety/security and marine environment protection through the improvement of the sailing-related services.

VTS plays the following key roles with the purpose of materializing the e-Navigation in the marine environment: collecting/integrating/analyzing the various data related to marine traffic control and then providing the data to the applicable ships. The VTS Committee (a professional IALA group) has been actively discussing VTS' role, VTS service, and so forth, in order to establish the new concept suitable for the e-Navigation environment [2, 3].

Internationally, there is a trend that VTS has been evolving to vessel traffic management (VTM) recently and VTS' overall concept has expanded as the framework of the methods and services to enhance the following: the safety in the sailable water, the efficiency in security and shipping, and the marine environment protection. In other words, this service architecture has been changing into a new service

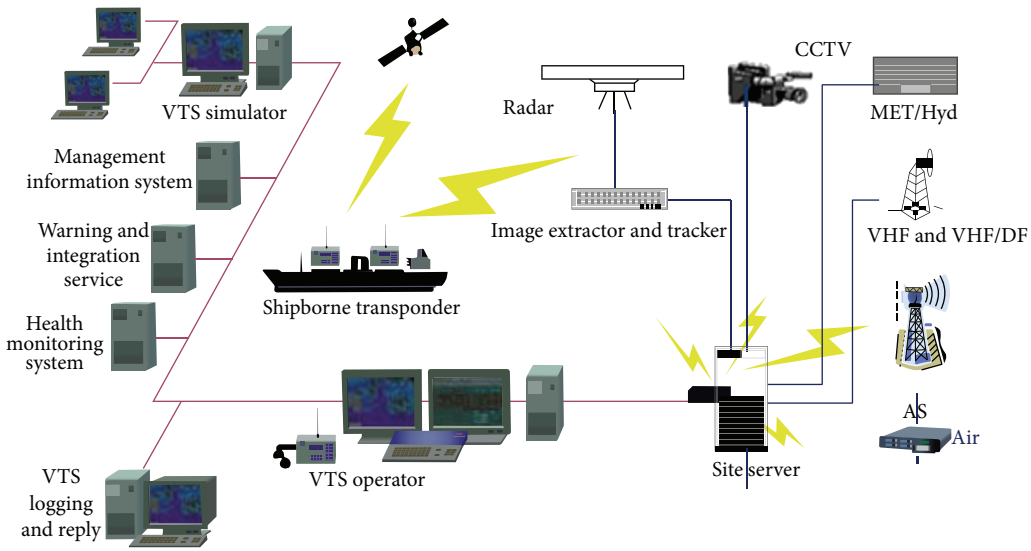


Figure 1: System architecture of VTS service.

type, not only in the maritime traffic safety and business service, but also in the maritime computing environment, and foretells the change in the existing VTS and its concept.

In general, the elements composing VTS are shown in Figure 1. VTS is the system in which the followings are connected to one another: the VTS center on the land, the base station site on which various sensors (sensing devices such as CCTV, Radar, DF, MET, etc.) and AIS are installed, the control center that actually operates VTS, and it is a complicated system consisting of various types of telecommunications networks that connect ships, satellites, and sensing devices [4–6].

As for the VTS-related study overseas, through the Framework Programme (FP) project, they promoted various studies whose objects include the next-generation technology of VTS, vessel traffic management and information system (VTMIS), and port control management service (PCS). As the MarNIS project is to be implemented between 2012 and 2020, this study is marked by providing the VTM and search and rescue (SAR) services through collecting various information such as the ship's dynamic/static data and water climate/geography/environment by means of various media and processing the data safely and efficiently. Besides, in the MarNIS project, they have been conducting the aids-to-navigation study (including the marine mobile communication network technology) for the enhanced multimedia telecommunication. In particular, they applied the enhanced controlling function, multimedia telecommunications function, and so forth and have been conducting the follow-up studies and developments continuously for the actual service implementation and the international standardization [7–9].

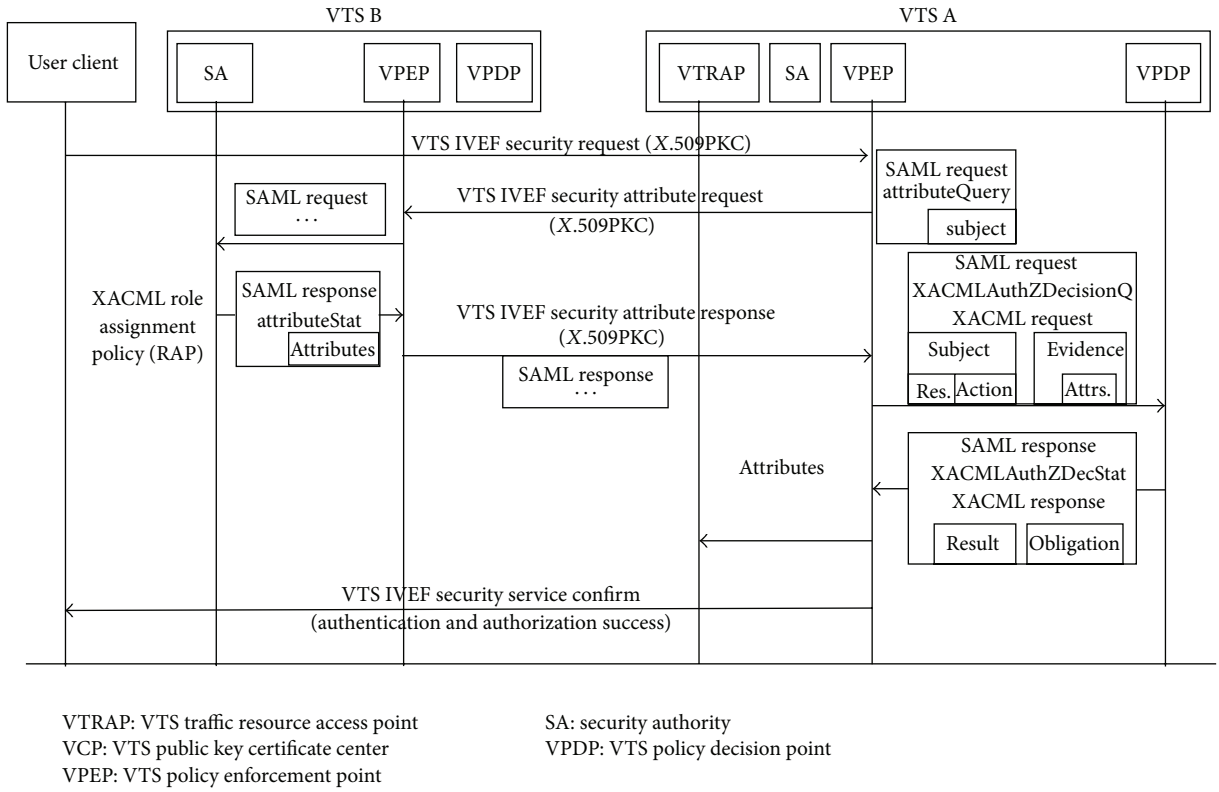
International Association of Lighthouse Authorities (IALA) is developing the standard intersystem VTS exchange format (IVEF) protocol for exchange of navigation and vessel information between VTS systems and between VTS and vessels. The output of standardization is distributed as the IALA recommendation V-145, and the protocol is implemented with an open source. The IVEF open source, however, is the code used to check the functions of standard protocols. It is too slow to be used in the field and requires a large memory [10–12].

Secure communication systems among the network enabled devices are significant concern in mobile environments [1].

2. Overview of IVEF Protocol

The VTS Committee of IALA is a framework of methods and services to promote the safety, security, efficiency, and environment protection in all transportable water that is evolving from a traditional VTS to an e-Navigation service. In other words, this service structure is advanced from the vessel traffic monitor and control to business service and e-Navigation in vessel computing environment as a new service form. The various information collection and management in the sea encountered a rapid development in its technology, which aims to provide the information service for the vessels during their voyage, such as sea situations and sea map vessel support. At this time, the vessel information collection/management/production/sharing/provision services should be enabled through the information collection from vessels or trusted information exchange between the land systems.

IVEF service is a gateway service in the currently developing land system structure by IALA-AISM's e-Navigation working group. In other words, the IVEF service can have an external third party system linking structure as the client that requests the service and the mutually trusted network gateway security service is required. The traffic information provides the necessary information to the nearby system through the IVEF service. IVEF service should be defined as a mutually linked service between domains. In addition, for a safe IVEF service, the land systems of regional VTS,



VTRAP: VTS traffic resource access point
VCP: VTS public key certificate center
VPEP: VTS policy enforcement point
SA: security authority
VPDP: VTS policy decision point

Figure 2: IVEF security protocol process.

national VTS, related institutions, and companies should be interconnected in a safe structure.

IVEF service is a server/client model serving as a protocol to exchange traffic information between VTS systems. Its development based on open source is underway by IALA and its protocol and sample program can be checked by downloading SDK in OpenIVEF website [2]. Basic actions to provide service between server/client take three steps as follows. In the first step, a client requests server certification and receives login reply if he/she is a legitimate user. In the second step, the server provides a certain service for the specific user only if it has such service. If it does not offer such service, it provides a basic service defined in the standard called BIS (basic IVEF services). In this step, the client can designate area of interest, data renewal period, or data form based on his/her preference. In the third step, the client sends logout message to the server in order to end use of IVEF service. Since the server does not give a separate reply on the logout message, all the client has to do is just cancel access to server when he/she sends the message [10].

IALA, which is the basic protocol to provide IVEF service between VTS centers, defines nine messages as shown in the Notions and Acronyms section. Definition of these messages is composed of XML-type schema and all messages are composed of subelements of MSG_IVEF, which is the most significant element. Message of each subelement also has its own sub-elements based on message characteristics. IVEF messages are broadly divided into control information message and real-time information message. The former consists of user certification and termination, service request to the server and its reply message, and others to provide information on server status. The latter controls ship's current location, expected route, destination port, and other physical information in an object data.

3. IVEF Security Process

This clause defines the mutual security factors between domains and detailed procedures using the defined security messages. In other words, Figure 2 shows the security management flow map on the linking areas with the security messages where the VTS domain B approaches VTS domain A. The basic security structure uses the XML based standard protocols and the characteristics for IVEF are expanded using the IVEF security message characteristic exchange protocol. The approach management procedures according to the procedures and authorities for the policy management within a domain when the domains are linked are shown in Figure 4. After the IVEF service between the domains is requested, the VTS IVEF service basic certification mechanism based on ID/Password with the access limitation based authority function is as follows.

(1) The user sends the access request to use the system resources or application service. At this time, the access request is same as the existing methods with user ID and password.

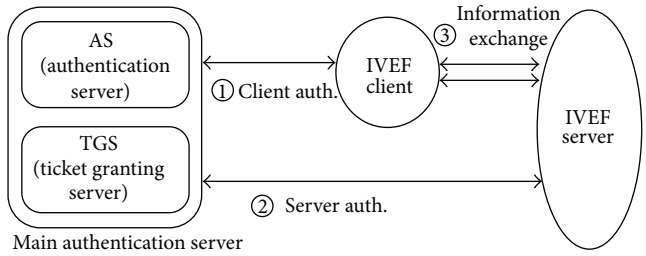


Figure 3: Main authorization scheme for user authentication in IVEF.

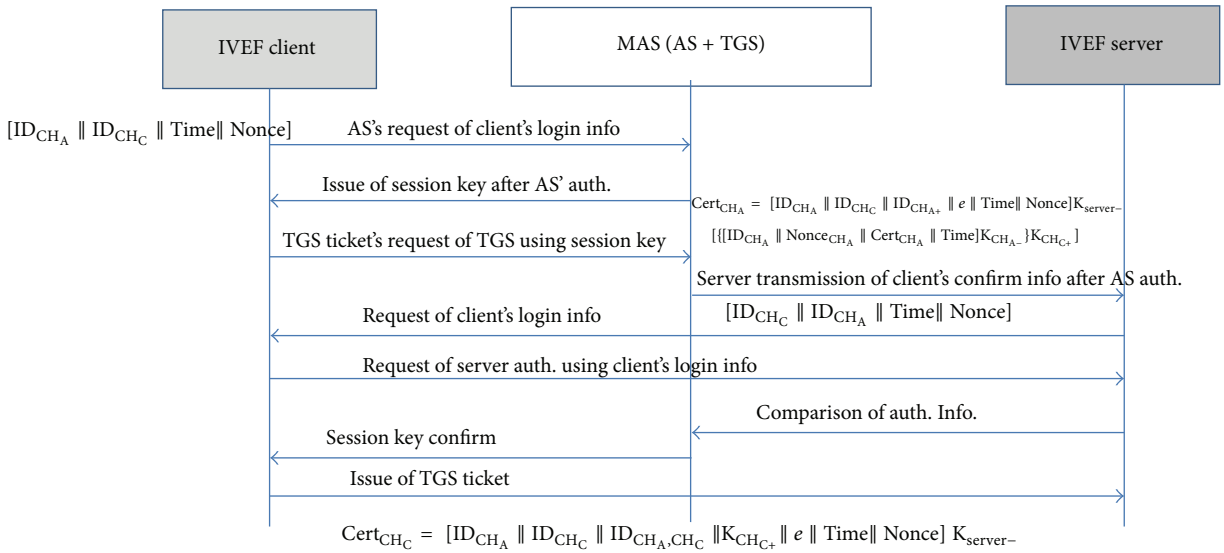


Figure 4: Secure protocol between IC, IS, and MAS.

(2) The PEP of the access control receives the access request and confirms the user's ID and password with the access control list. This is same as the previous method.

(3) Once the VPEP (VTS policy enforcement point) confirms the user ID and password, it will transmit the user ID and the requested items (read, write, and execute) to VPDP (VTS policy decision point).

(4) VPDP loads the policy from VPAP (policy administration point) and determines whether the user has the appropriate authorities for the requested actions. For this, the user, resource, environmental characteristics, and policy are used to determine whether to approve.

(5) VPDP delivers the result to VPEP. In other words, approval/denial is delivered to VPEP. When it is "approved," the user certificate is examined and if it is valid, then the user request is approved.

(6) VPEP downloads the user certificate from the storage and checks for validity. If it is valid, it approves the access.

4. Security Enhancement of User Authentication Scheme

IVEF is an open-source SDK for VTS information exchange that is being developed by IALA and is almost complete in its international standardization as a gateway. The official IVEF technology documents provided by IALA specify that the data security except for authentication and authorization is out of the IVEF scope. The IVEF security suggested at this point only codes the user authorization information in an open key method. However, when the physical link is terminated and then reconnected between VTSs, the VTS system may be delayed from temporary traffic overload. This may lead to data leakage. A solution requires studies on the main authorization server. This section suggests the main authorization server for user authentication as shown in Figure 3.

Figure 4 briefly summarizes the information exchange system after authentication for the main authentication server with the IVEF client (IC) and IVEF server (IS). The MAS is comprised of AS (authentication server) and TGS (ticket granting server).

Figure 4 shows the protocol between IC, IS, and MAS. Step 1 in Figure 4 shows how IC requires to confirm the user from the AS in MAS using the login information. Step 2 is the

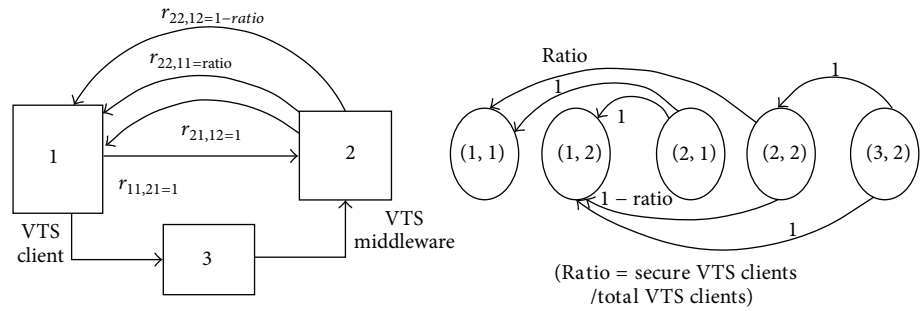


Figure 5: Multiple class queuing systems in the secure VTS push scenario.

issuing of the session key after the certification of the IC in AS. Step 3 is the request of the TGS ticket issuing from TGS with the issued session key. TGS ticket holds the client ID, IP address, ticket issue time, and ticket validity information. Step 4 sends the IC confirmation certified in AS in MAS to IS. Step 5 requests the login information from IC by IS directly. Step 6 is the request of the server authentication with the client login information. Step 7 is the result delivery after the comparison of the confirmation from AS in Step 4 and the client login result. Step 8 confirms the issued session key in Step 2. Lastly, Step 9 certifies IC an IS by issuing the same TGS ticket if there were no errors in all steps.

Therefore, MAS can authenticate IC and IS at the same time to sense the link termination in certain areas. In addition, the TGS ticket IP address and ticket valid time information can prevent the illegal access and replay attack of the attackers.

5. Security and Performance Discussion of Improved Protocol

We modelled our architecture as a closed queuing system, as in Figure 5, and performed the approximate mean value analysis (MVA) described in [13–15]. In the scenario of Figure 5, the secure mobile VTS procedure has two job classes: the initial secure location update step and secure mobile VTS service step. $r_{im,jn}$ means the probability that a class m job moves to class n at node j after completing service at node i. And ratiorepresents the ratio of total users to secure mobile VTS service users [15]. The analysis steps for the class switching closed queuing system are as follows.

Step 1. Calculate the number of visits in the original network by using

$$e_{ir} = \sum_{j=1}^{K} \sum_{s=1}^{C} e_{js} r_{js,ir}, \tag{1}$$

where K is total number of queues and C is total number of classes.

Step 2. Transform the queuing system to a chain.

Step 3. Calculate the number of visits, e_{iq}^{*}, for each chain by using

$$e_{iq}^{*} = \frac{\sum_{r \in \pi_q} e_{ir}}{\sum_{r \in \pi_q} e_{1r}}, \tag{2}$$

where r is queue number in chain q and q is total queue number.

Step 4. Calculate the scale factor α_{ir} and service times s_{iq} by using (3) with (1):

$$s_{iq} = \sum_{r \in \pi_q} s_{ir} \alpha_{ir}, \quad \alpha_{ir} = \frac{e_{ir}}{\sum_{s \in \pi_q} e_{is}}. \tag{3}$$

Step 5. Calculate the performance parameters for each chain using MVA.

Figure 6 showed difference for 4 seconds that compare average transfer time between client and mobile VTS middleware of middleware filtering and unfiltering by network. According as increase tag number on the whole, showed phenomenon that increase until 4 seconds.

Figure 7 showed average transmission time accordingly as increased client number in nonfiltering protocol environment. If client number increases, we can see that average transfer time increases on the whole. And average transfer time which increases rapidly in case of client number is more than 45. Therefore, tag number that can process stably in computer on testbed environment grasped about 40 EA (at the same time). When comparing difference of filtering time and protocol time, time of mobile middleware platform's filtering module is occupying and shows the importance of signature module about 32% of whole protocol time. In this paper's supplementary material (see Photos S1 and S2 available online at http://dx.doi.org/10.1155/2014/734768), we derive a protocol performance of functions of IVEF client/server.

6. Conclusion

These days, the latest electronic technologies and IT are being employed for safer ship operation and efficient control of marine traffic. e-Navigation relies on IVEF service as the standard to exchange data between VTS centers. IVEF,

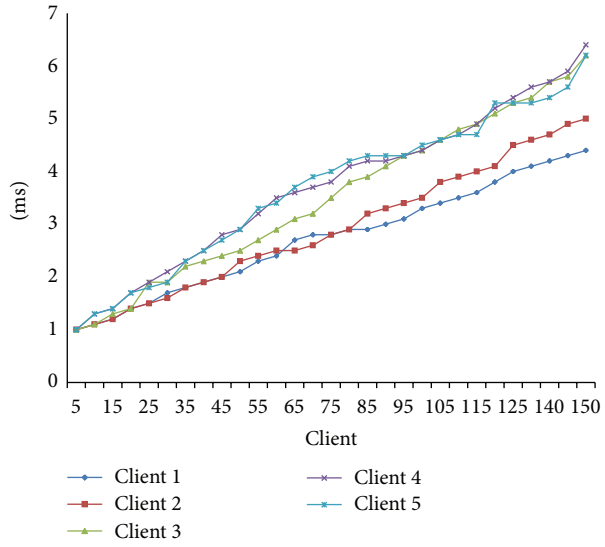


Figure 6: Simulation result of mobile VTS middleware filtering.

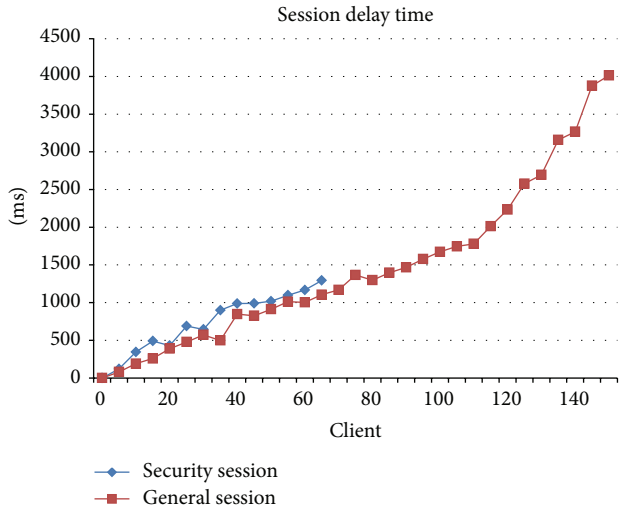


Figure 7: Simulation result of mobile VTS middleware nonfiltering.

however, is still a program under development and thus its actual implementation and performance have not been fully verified.

This paper provides an overview of the vulnerability introduced by an attack, as well as the countermeasures to mitigate the threat. Our analysis demonstrates that the Tsai et al.'s protocol does not provide known key security which is a fundamental requirement for secure communication. Our future work is undertaken to protect privacy for mobile stations and improve authentication efficiency.

Notation and Acronyms

CH_A: Cluster head A
ID_X: Identification X
$K_{S,CH}$: Confidential key shared between session key S and CH or S and CH
Time: Current time
S: CH_A member client
X: CH_B member client
K_{A+}: Public key of client A
K_{A-}: Private key of client A
$cert_A$: Certification of client A
e: Effective date of authentication
$Nonce_A$: Client A nonce generation.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This paper is extended and improved from accepted paper of CSA 2012 conferences. This work was supported by ETRI through Maritime Safety and Maritime Traffic Management R&D Program of the MOF/KIMST (2009403, development of next generation VTS for maritime safety), and this research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A4A01013587).

References

[1] IALA Recommendation V-145 on the Inter-VTS Exchange Format (IVEF) Service, June 2011.

[2] http://en.wikipedia.org/wiki/E-Navigation.

[3] OpenIVEF, http://openivef.org/.

[4] N. Park, S. Cho, B.-D. Kim, B. Lee, and D. Won, "Security enhancement of user authentication scheme using IVEF in vessel traffic service system," in *Computer Science and its Applications*, vol. 203 of *Lecture Notes in Electrical Engineering*, pp. 699–705, 2012.

[5] K. Kim, B. D. Kim, B. Lee, and N. Park, "Design and implementation of IVEF protocol using wireless communication on Android mobile platform," *Communications in Computer and Information Science*, vol. 339, pp. 94–100, 2012.

[6] T. Kang and N. Park, "Design of J-VTS middleware based on IVEF protocol," in *Grid and Pervasive Computing*, Lecture Notes in Computer Science, 2013.

[7] B. Arifin, E. Ross, and Y. Brodsky, "Data security in a ship detection and identification system," in *Proceedings of the 5th International Conference on Recent Advances in Space Technologies (RAST '11)*, pp. 634–636, Istanbul, Turkey, June 2011.

[8] N. Park and H.-C. Bang, "Implementation of vessel traffic system's mobile middleware platform for secure IVEF service," Security and Communication Networks, 2014.

[9] D. Frejlichowski and A. Lisaj, "Analysis of lossless radar images compression for navigation in marine traffic and remote transmission," in *Proceeding of the IEEE Radar Conference (RADAR '08)*, pp. 1–4, Rome, Italy, May 2008.

[10] "A Security Architecture of the inter-VTS System for shore side collaboration of e-Navigation," 2012.

[11] International Association of Lighthouses and Aids-to-Navigation Authorities (IALA), "Interface Control Document for IVEF," Release 0.1.7.

[12] http://en.wikipedia.org/wiki/e-Navigation.

[13] N. Park, J. Kwak, S. Kim, D. Won, and H. Kim, "WIPI mobile platform with secure service for mobile RFID network environment," in *APWeb Workshops 2006*, H. T. Shen, J. Li, M. Li, J. Ni, and W. Wang, Eds., vol. 3842 of *Lecture Notes in Computer Science*, pp. 741–748, Springer, Heidelberg, Germany, 2006.

[14] N. Park, "Implementation of terminal middleware platform for mobile RFID computing," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 8, no. 4, pp. 205–219, 2011.

[15] Z. C. Taysi and A. G. Yavuz, "ETSI compliant GeoNetworking protocol layer implementation for IVC simulations," in *Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS '12)*, pp. 1–5, Amman, Jordan, May 2012.