Route Plan Exchange Scheme based on Block Chain

Doyoung Chung, Hae Sook Jeon
Information Security Research Division
ETRI
Daejeon, Republic of Korea
thisisdoyoung@etri.re.kr

***Abstract*—** Route Plan describes recommended movement of vessels. It consists of waypoints, and each waypoint demonstrates expected arrival/depature times, angle, and direction. The importance of route plan is become more important as appearance of autonomous ship. To achieve safe and smart voyage, integrity of route plan is very important. To avoid forgery and temper of route plan, and clarify who is responsible, digital signature is one of reliable solution. In this study, we suggest route plan management scheme which demonstrates how to manage digital signature of route plan based on block chain.

Keywords—route plan; block chain; autonomouse vessel; pki

I. INTRODUCTION

The Route Plan means assembly of waypoints and the route described by these. Maritime navigation and radio communication equipment and systems, especially ECDIS(Electronic chart display and information system), display route to user by its display.

As the autonomous vessel is developed, route plan and its exchange is become important. The autonomous vessel decides its movement depends on route plan. The route plan is generated and updated, based on weather, ocean current, fuels and time schedule. In this case, due to the complexity of calculation and massive scale of required information, the control center on shore is expected to perform the generation and update of the route plan. The autonomous vessel receives the route plan from the control center, thus method for supporting authentication and integrity is required. Moreover it should be able to identify the author or modifier of route to clarify responsibilities in situations such as accidents that may arise.

Digital signature could be one of reliable solution to achieve above requirements. Block chain eases manage of digital signature and its infrastructure because of distribute characteristic.

II. ROUTE PLAN EXCHANGE FORMAT

A. IEC 61174 – Annex S

Route plan exchange format – RTZ is defined in IEC 61174:2015 – Annex S [1], currently. Although it is defined in Annex, but standardization activities are underway in IEC TC80 WG17.

```
<extensions>
  <extension manufacturer="Acme" version="2.1"
    name="AuxRouteInfo-9674F26E-EAFB-4319-AE24-08D5BA69D895">
    <property name="source"
value="http://services.acme.com/auto route/?id=3e891884e620970e5303fd2399427986"/>
    <property name="attachment" value="rtz://assignement-13.04.2013.docx"/>
    <property name="attachment" value="rtz://MFD original.rt3"/>
  </extension>
</extensions>
<extensions>
```

Fig. 1. Example of a RTZ format

The route exchange format is a file containing an XML coded version of the route plan. The XML route exchange file uses the extension .rtz. It also allows third-party extensions..

B. Route plan

A route plan is consists of waypoints. Each waypoint describes the leg between waypoints. For example, the leg between waypoint A and B represents the leg from waypoint A to B. It includes geographical coordinates, radius and calculated distance. It also includes more specific information, such as, vessel information, roll, wave, wind, speed, change history, etc,.

These information may cause critical accident for vessel sometimes. For example, if the route plan records a value larger than the turn-able radius that the vessel can afford, and the vessel trusts it and tries to rotate at that radius, an overturning accident may occur. Otherwise, if advisory forgery geographical coordinates of route plan, than he can induce vessel to move wrong position intentionally.

III. ROUTE PLAN VERIFICATION

Route Plan verification means confirm who generates and updates the route plan. In this paper, verification of correctness of the contents of route plan, such as correctness of weather forecast, is out of bound.

Integrity and non-repudiation are major requirements to trust received route plan. Auditing is also required to clarify responsibilities. The digital signature could be one of reliable solution to provide above requirements. Route Plan Exchange is performed by exchange file based on RTZ format. RTZ

format is based on XML. By adopt digital signature for XML files, integrity and non-repudiation is achieved.

To achieve auditing for clarify responsibilities, it requires other reliable solution. Block chain is one of most effective candidate. Block chain provides distributed ledger. The distributed ledger is stored by each client, and it has resistance against forgery attack and manipulation. The attacker should have more than 50% of computing power of whole stakeholder to manipulate distributed ledger as her/his intentions. The success of Bit-coin has proved its safety in practically.

By using digital signature and block chain we suggest reliable solution to achieve required security required, such as integrity, non-repudiation and clarification of reliabilities.

IV. Proposed Scheme

Our proposed scheme is consist with two parts. First, How to manage and design PKI to manage certificates for stakeholder of Route Plan. Second, we suggest how to improve legacy PKI to more efficient and distributed. This suggestion also provide the solution to audit operation on Route Plan in distributed way.

A. PKI for the stakeholders

In this section, we clarify who is stakeholder of Route Plan and who should have certificates and generate/verify digital signature.

- To identify the owner of digital signature, PKI is required. The structure of PKI is well defined in X.509 standards [2], thus in this paper we clarify who should be subject of PKI.
- The stakeholder of Route Plan is ship owner, shipping company, government operator such as VTS. These may include, but is not limited. For example, the operator of autonomous vessel control center should be one of stakeholder as development of autonomous vessel.

  The shipping company will be publisher of regular Route Plan. The government operator may be publisher of special Route Plan, which related with emergency situation or safety.

B. Distributed PKI and Auditing

The legacy PKI structure has centralized CA(Certificate Authority), RA, etc,. The legacy auditing system also has centralized structure. Because of its centralized structure, they exposed to single-point-failure problem and conflict of interest problem. Because of development of lots of redundancy method, single-point-failure problem is less critical than past. But conflict of interest problem is still existed. The main problem is that stakeholder performs management role. There is motivation for the stakeholder, to manage ledger or PKI in unfair direction.

In legacy PKI or auditing system solves conflict of interest by adopting 3rd trust party. But this occurs complexity of system, and additional cost. Block-chain and its successful example, Bit-coin, is specialized for managing distributed ledger. Block-chain is well suited to managing log of Route Plan Exchange in distributed way.

Block-chain is also helpful to manage certificate and its revocation status[3. 4]. Stakeholders write the information of certificate's subject in to the Block-chain with hash value which used to verify written information. The subject of certificate has right to write its certificate's revocation status – revocation time, reason, etc,.

The stakeholder who published new or modified Route Plan should record it on the distributed ledger. In this case, hash value is generated by using (Route Plan)|(CMS Signed Data of Route Plan).

We can separate our proposed scheme in two steps. First step is Block-chain based certificate management. Second step is recoding issuing or publishing or Route Plan on Block-Chain.

First step,

- The stakeholder requests to certificate issuer to create his certificate. In request, subject of certificate's information should be included.
- The certificate issuer issues requested certificate. After issuing certificate, the issuer discards subject's information and generate hash value of the certificate to record on Block-Chain. The reasons why using hash value of the certificate instead of certificate itself are further extensions of linkage with Bit-Coin and increase efficiency. The Block-Chain for Bit-Coin has small reserved field to record additional information related with its transaction.
- The subject of certificate has right to discard its certificate. When the subject decides to discard its certificate before certificate' expired date, the subject records on distributed ledger that discard time, discard reason, and hash value of the certificate.
- The stakeholder that receives Route Plan with digital signature should verify the digital signature with its certificate. During verification process, the stakeholder require to check whether the certificate is revoked or not. The stakeholder may verify it via above distributed ledger. If there is revocation information on the distributed ledger, then the stakeholder discard Route Plan with digital signature that generated by revoked certificate.

Second step,

- The stakeholder who published new or modified Route Plan should reveal its identity to other stakeholders. It should not be forged by other or repudiated by the publisher. The publisher recommend to XML's digital signature or CMS Signed Data. Otherwise the publisher should generate digital signature which included whole contents of the Route Plan, and provider reliable method to reveal its identity.

- The publisher should record published Route Plan on Block-Chain. For the security aspect, recording whole contents of Route Plan is recommended, but it is harm for availability. In this scheme, (ID of Route Plan, digital signature of Route Plan, ID of publisher) as recorded values to Block-Chain.
- The stakeholder that receives Route Plan verify contents of Route Plan with that of distributed ledger. First, it compares identity of publisher and ID of Route Plan between Route Plan and distributed ledger. Then the publisher verify whether Route Plan is forged or not by using digital signature for its contents. If the Route Plan is verified successfully, then the stakeholder accept the Route Plan.

V. CONCLUSION

The Route Plan and its exchange become more important. E-Navigation was proposed by IMO and Autonomous vessel is researched very rapidly. To provide E-Navigation MSP with safety, such as collision prediction and most effective safe voyage, reliable Route Plan is essential. On the other hand, the autonomous vessel will be depend on Route Plan when it decides its movement. Due to the amount of information for generating optimum Route Plan, the generation or modification of Route Plan are expected to perform by the control center on Shore, not autonomous vessel itself. Thus trust of Route Plan itself and the publisher of Route Plan will be disputed. In this paper, we suggest novel method to avoid threat, such as forgery, repudiation, avoidance of responsibilities. Moreover, our proposed scheme also provide novel method to avoid limitation of legacy PKI and auditing system which expected to related with Route Plan.

Acknowledgment (HEADING 5)

This research was financially supported by the Ministry of Trade, Industry and Energy(MOTIE) and Korea Institute for Advancement of Technology(KIAT) through the International Cooperative R&D program.

References

[1] IEC 61174, “Maritime navigation and radiocommunicatino equimenet and systems – Electronic chart display and information system (ECDIS) – Operational and performance reqruiements, methods of testing required test results, 2015, IEC.

[2] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile, RFC 5280, May 2008

[3] L. Axon, “Privacy-awareness in Blockchain-based PKI,” 2015. [Online]. Available: http://goo.gl/3Nv2oK

[4] C. Fromknecth, D. Velicanu, and S. Yakoubov, “CertCoin: A NameCoin Based Decentralized Authentication System,” 2014. [Oline]. Available: https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf