2013년도 공동학술대회 논문집 pp. 195~197

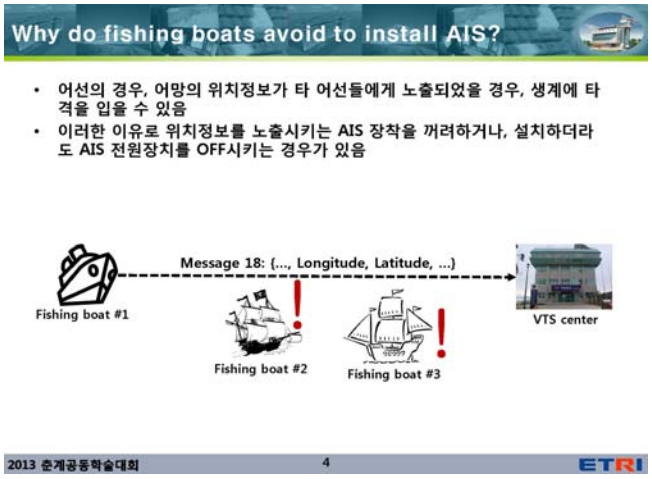
신뢰성 있는 해상정보교환을 위한 안전한 AIS 통신 프로토콜

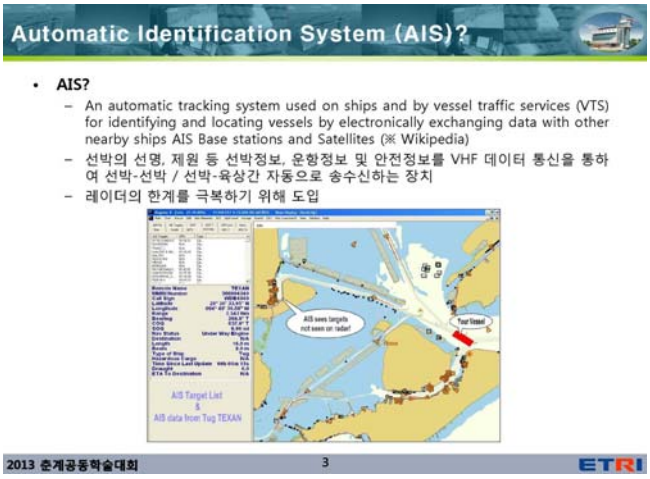
† 조관태 · 이병길*†

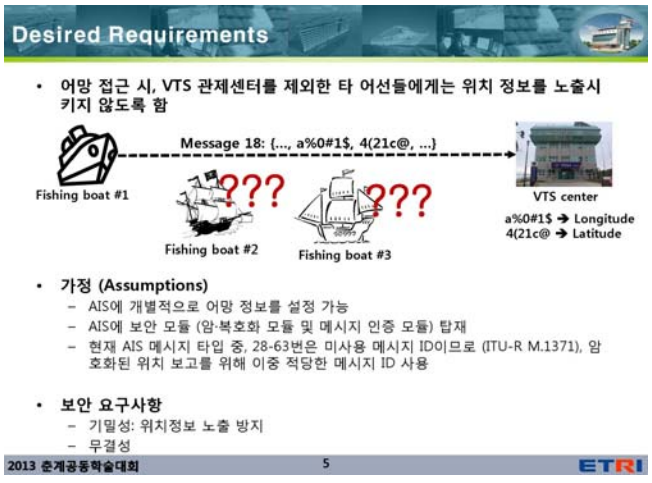
† 한국전자통신연구원

요 약 : 선박자동식별장치(AIS)는 선박의 선명, 제원 등 선박 정보, 운항정보 등을 선박과 선박 간, 선박과 관제센터 간 자동 송수신하는 장치다. 현재 국내에서는 전국 통합망 구축 사업 완료를 통해 AIS와 시스템이 본격적으로 운용되고 있다. 이러한 AIS 정보는 선박 대 선박 간의 충돌회피, 연안국이 불분명한 선박 및 그 화물에 대한 정보 획득, 선박 대 육상간의 통항관제를 위하여 사용된다. 하지만, 어선들은 생계와 관련된 어망의 위치가 노출되기 때문에, AIS 사용을 꺼려한다. 본 논문에서는 어선들의 위치가 노출되지 않도록 위치 정보를 암호화하고 인증하는 신뢰성 있는 AIS 통신 프로토콜을 제안한다.

핵심용어 : VTS, 선박자동식별장치, 보안, 메시지 인증, 객체 인증







조관태(주저자), kwantaecho@etri.re.kr, 042)860-1356

* 이병길(교신저자), bglee@etri.re.kr, 042)860-1689

Necessity of Data Security

- IALA Guideline No. 1086 on The Global Sharing of Maritime Data & Information, Edition 1, Jun. 2012

> 4.3.2 Data Security and Confidentiality
>
> Users are concerned with issues of data security and confidentiality and in particular any commercial sensitivity of data as it relates to release of information that may compromise investors or introduce a competitive advantage / disadvantage.
>
> Other information that requires protection includes location sensitive information, such as location of fishing grounds, or personal identification information. Personal data includes identity data relating to vessels as well as individuals.
>
> In many cases confidentiality is already protected by legislation but this is not universal throughout the maritime domain. The requirement to protect access to data may go beyond the limits of primary legislation. Confidentiality needs, at least, to be protected by appropriate levels of access rights to data exercised through physical security, encryption and password protection.

- IALA Guidelines on the Universal Automatic Identification System (AIS) Vol. 1, Part II – Technical Issues Edition 1.1, Dec. 2002

> *14.2 Security*
>
> The network should provide adequate protection against unauthorized use of the information and the network. A concept of user rights and authorization can be established to ensure that unauthorized users do not have the ability to change or obtain information to which they are not entitled. Likewise unauthorized transmission of data over the network should be prevented.

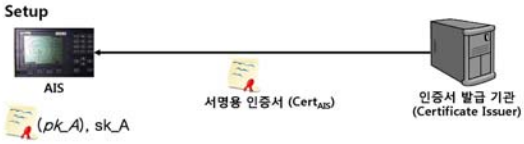
AIS Products supporting Security Service

Underlying Problem

- 이산대수 문제 (DLP, Discrete Logarithm Problem)
  - 유한순환군 G=<g>와 어떤 y∈G가 주어졌을 때, $y=g^x$인 x, $1 \le x < |G|$를 찾는 것은 계산적으로 매우 어려움

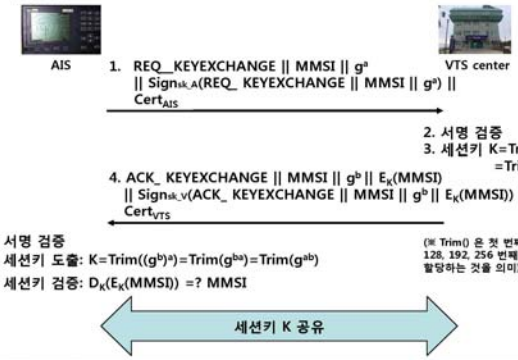
Proposed Solution (1/3)

- Setup



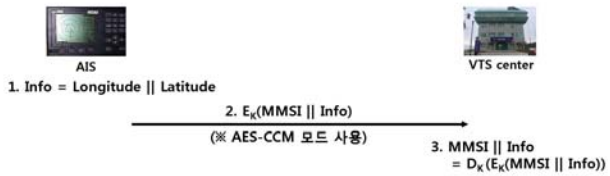
Proposed Solution (2/3)

- 출항 전



Proposed Solution (3/3)

- 출항 후, 어망 진입 시 보안 모듈 사용하여 주기적으로 위치 보고



Message Format

- 기존 메시지 구조를 변경하여 1 slot으로, 암호화된 위치정보 보고 가능

Message 18: Standard Class B equipment position report (ITU-R M.1371-3)

Parameter	Length (bits)
Message ID	6
...	...
Longitude	28
Latitude	27
...	...

Total: 168 bits

128 bits

Total: 241 bits < 256 bits (per 1 slot)
=168-28-27+128

(※ 총 128bits 내에서 위·경도 이외에 프라이버시를 위해서 필요하다고 생각되는 파라미터 추가 가능)

Conclusion

- 어망의 위치 정보를 암호화함으로써 타 선박에게 노출되지 않음
- 어망의 위치 정보 노출로 인하여 AIS 설치를 꺼리는 어선들에게 AIS 설치 독려 가능
- 1 Slot으로 AIS 메시지 전송이 가능함으로써, 암호화로 인한 통신 비용 증가 없음