AONT를 활용한 효율적인 K-분할 키 분배 기법

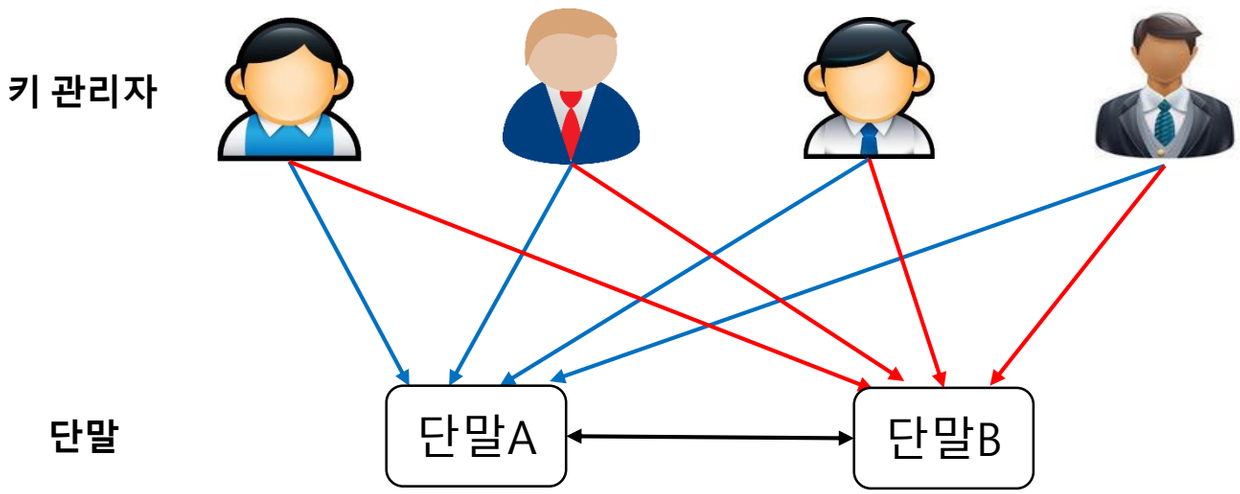
박다빈, 송민규, 송홍엽

연세대학교

2016년도 한국통신학회 동계종합학술발표회

1. 기법 개요

- **사물인터넷 극저성능 기기의 단대단 암호화 통신을 위한 효율적인 키 분배 기법[1]**
  - **공개키 기반 암호는 복잡한 수학 연산 기반으로 암호화·복호화 수행되므로, 보다 연산이 빠르고 쉬운 대칭키 기반 암호 사용**
  - **K-명의 키 관리자를 두어 키 관리자의 신뢰 문제 해결**
  - **대부분의 연산은 단말 대신 키 관리자가 하도록 함**

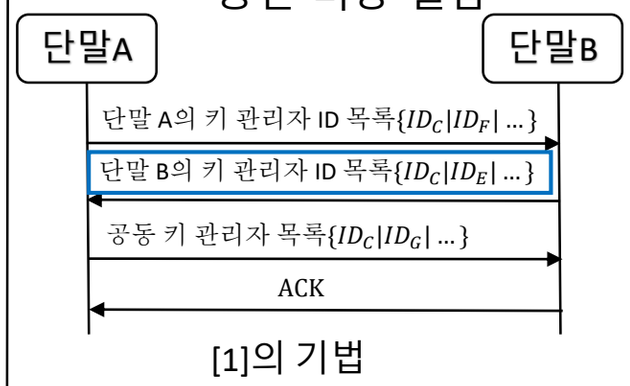


- **키 분배를 위한 단말과 K-명의 키 관리자와의 통신 과정에서 동일한 보안성 유지하면서 통신비용을 줄이기 위한 방법으로 AONT 비밀분산 기법 활용**

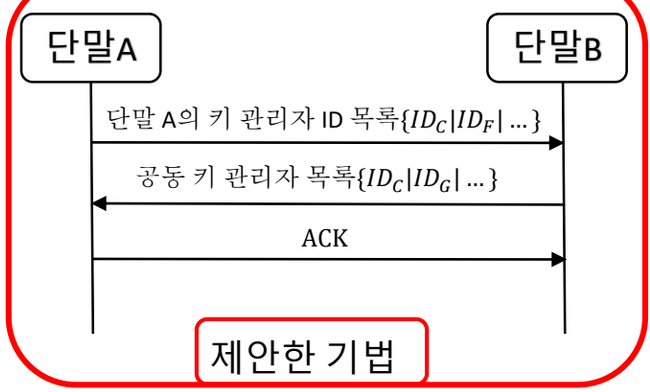
3. 키 합의 과정

a. 키 관리자 목록 교환 및 공동 관리자 집합 합의

- 하나의 단말만 자신의 키 관리자 목록 전송
- 통신 비용 절감



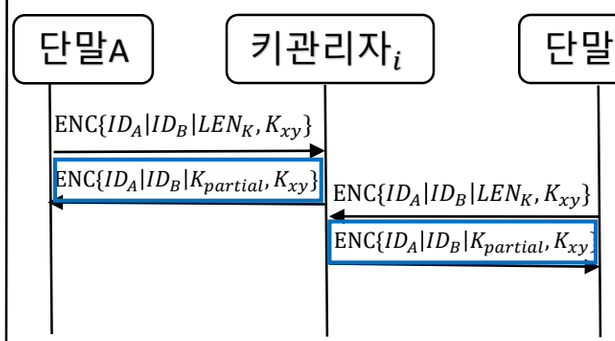
[1]의 기법



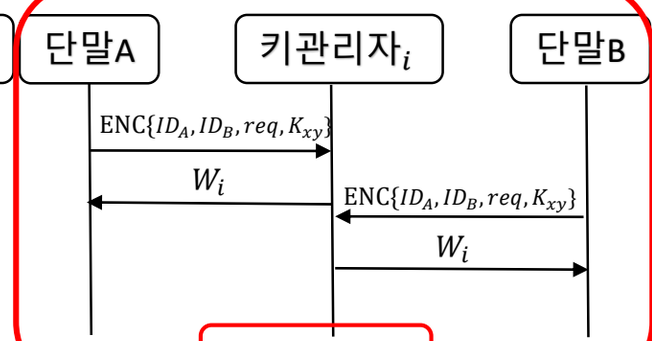
제안한 기법

b. 부분키(분산정보) 요청 및 부분키(분산정보) 전송

- 암호화 없이 분산정보 전송하여 통신비용 감소



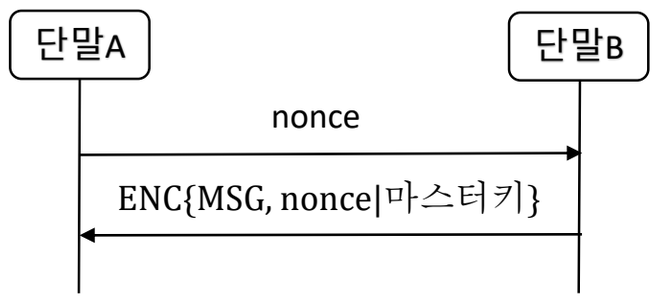
[1]의 기법



제안한 기법

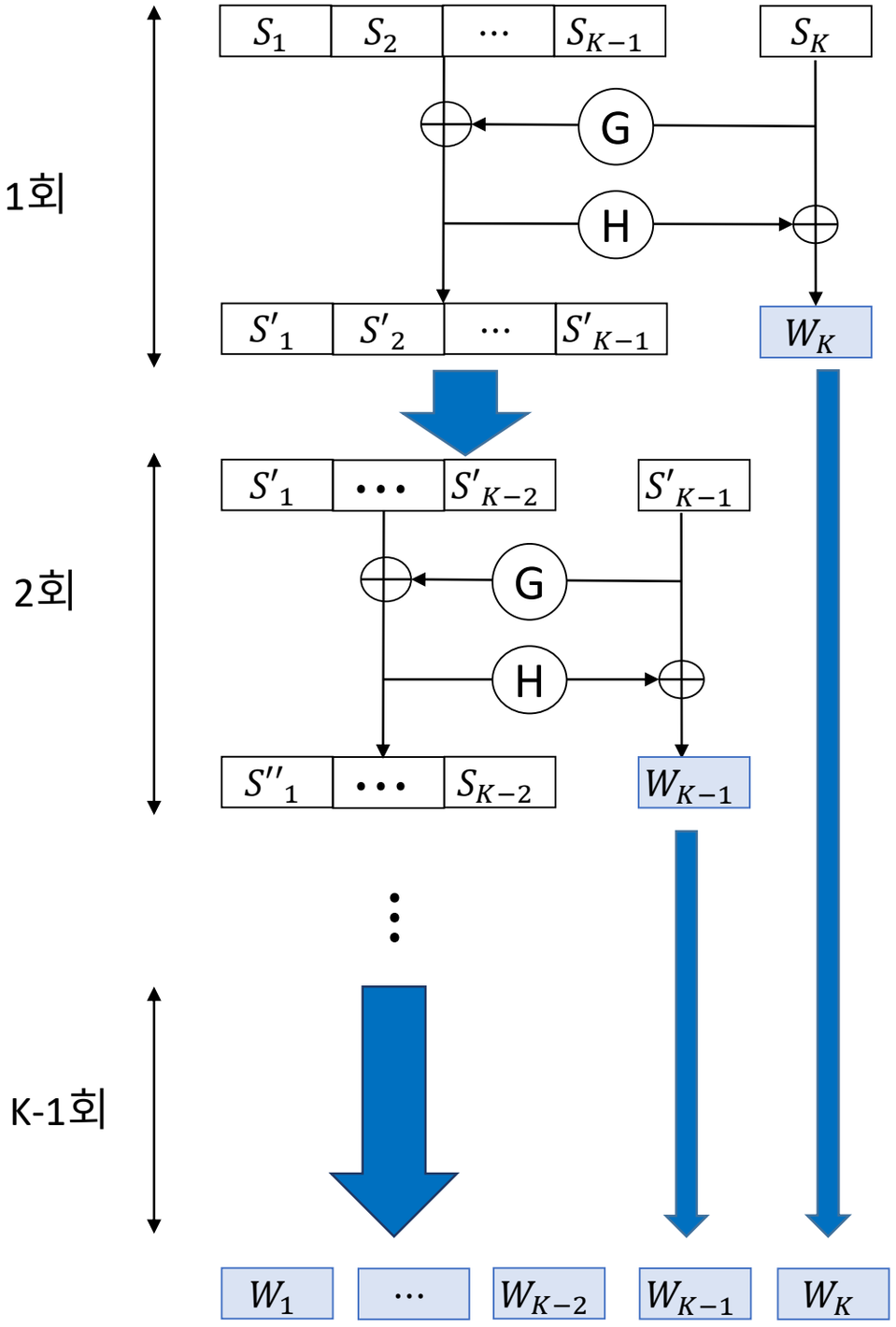
c. 단말간 세션키 생성

- [1]과 동일



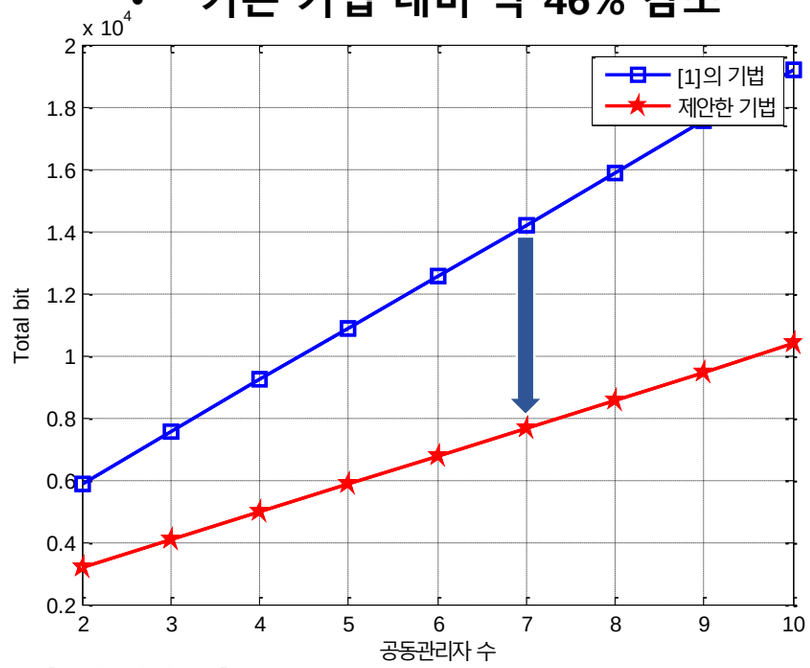
2. OAEP 기반 AONT 비밀 분산[2][3]

- 모든 분산정보 있어야만 원본 복원 가능
- 분산된 정보 합이 원본 크기와 같음



4. 성능 비교

- ID: IPv6(128bit), A, B의 키 관리자 수: 10으로 가정
- 공동 관리자 수 변화에 따른 송수신 bit 변화
- 공동 관리자 증가할 수록 통신비용 절감 효과 증가
  - 공동관리자: 7의 경우
    - 기존 기법 대비 약 46% 감소



- **향후 연구 주제**
  - 많은 양의 분산정보를 효율적으로 관리하기 위한 방법 연구
  - 단말 뿐 아니라 키 관리자의 연산 복잡도 및 통신비용 등의 부담을 줄이기 위한 연구
  - 여러 단말간의 암호화 통신을 위한 키 합의 과정 연구
- **참고문헌**

[1] 정도영, 정병호, "사물인터넷 저성능 기기의 단대단 보안을 위한 K-분할 키생성 기법," 한국통신학회 2015년도 추계종합학술발표회, 서울대학교, Nov. 2015.

[2] 송유진, 박광용, "대용량 e-비즈니스 데이터 분산 보안관리 모델", e-비즈니스연구, 제11권 제1호, pp.325-342, 2010.

[3] R. L. Rivest, "All-or-nothing encryption and the package transform," Fast Software Encryption FSE '97, Lecture Notes in Computer Science, Vol.1267, pp.210-218, 1997.

[4] 박지예, 신새미, 강남희, "사물인터넷 환경에서 경량화 장치 간 상호 인증 및 세션키 합의 기술," 한국통신학회 논문지, Vol.38, No9B, pp.707-714, Sep. 2013.