Sensor node network security

O O O

팀 원
O O O
O O O
O O O

지도교수	O O O
조 교	O O O

Contents

1. 연구 주제

센서 네트워크 보안을 향상시킬 새 키 관리 기술을 개발/구현한다. 센서 노드는 그 작은 크기로 인해 한정된 자원(연산속도, 배터리 등)을 가지고 있기에 정교한 알고리즘이 필요하며 그 알고리즘은 속도와 균형, 연결성 사이에서 적당한 균형을 맞추어야 한다. 이 키 관리 기술을 통해 전체 네트워크는 보안을 유지하며 악의적인 공격을 방어할 수 있다.

2. 연구의 필요성

센서 노드는 연산속도, 메모리, 배터리, 그리고 통신 전송속도 등에서 심한 제약을 가지고 있다. 따라서 일반 pc에서 사용되는 암호화 기법을 그대로 사용하기엔 무리가 따른다. 그러나 네트워크 보안을 유지하기 위해 센서 네트워크의 보안기법은 필수적이라 할 수 있겠다. 보안기법 중 키 관리 기술은 센서가 주고 받는 키를 적의 공격으로부터 방어하는 기술인데, 여러 보안기법 중 핵심적인 부분이라 할 수 있겠다. 이 키 관리 기술은 여러가지 알고리즘으로 구현할 수 있는데, 각 알고리즘은 속도와 균형, 연결성 사이에서 트레이드-오프를 가진다. 결론적으로 각 네트워크가 주로 사용되는 분야에 따라 이 세 가지 특성 중 몇 가지를 골라 특화된 키 관리 기술을 사용한다면 좀 더 효과적으로 네트워크를 악의적인 공격공격부터 보호할 수 있을 것이다.

3. 연구 내용

이번 중간발표1 까지 수행하였던 내용은 다음과 같다.

1. 기존 알고리즘 향상 / 새 알고리즘 구현 / 기존 알고리즘 의 세 가지 연구방향 중 '기존 알고리즘 향상' 으로 연구 주제를 좁힘.

2. 여러가지 기존 알고리즘을 분석.

3. 기존 알고리즘 중 'key infection' 기법에 초점을 맞추어 기존 알고리즘을 개선시키기로 결정.

4. 속도/보안성/연결성 세 가지 특성에 대해 각각 연구하기로 결정.

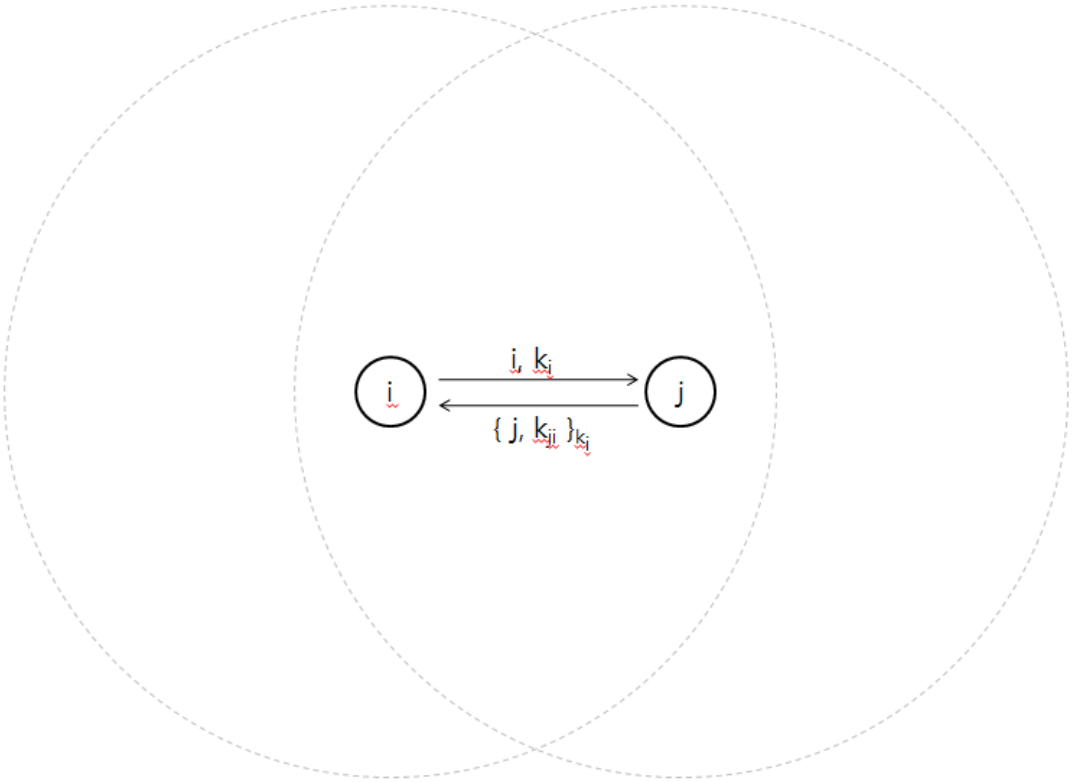
가장 먼저 연구 주제를 명확히 하였다. 연구 제안서에서 계획했던 세가지 연구방향을 모두 수행하기엔 시간적, 실력적으로 무리가 있다고 판단하였고, 조교님과 상의 끝에 '기존 알고리즘 향상' 이 가장 의미가 있으면서도 난이도가 아주 높지 않은 연구 주제라는 결과가 나와 그것에 초점을 맞추기로 하였다. 연구 주제를 명확히 한 다음엔 기존 알고리즘들을 분석하였다.

기법	설명
Network-wide Shared Key	모든 네트워크가 같은 키를 사용. 하나의 키만탈취되어도 전체 네트워크가 뚫리게 됨. 보안 가장 취약.
Random Key Pre-distribution	미리 배포된 랜덤한 키 중 몇 개를 골라서 사용. 미리 배포된 랜덤한 키가 유출되면 마찬가지로 보안 취약.
Random Pairwise Key	랜덤하게 배포된 키 중 쌍이 맞는 노드끼리 통신.

Key infection	통신하는 각 노드 고유의 키를 가지고 세션키를 만들어 통신. 각 노드의 키가 모두 탈취되어야 통신 감청 가능.

이렇게 분석을 마친 뒤 이 중 최근에 나왔고, 개선 여지가 많은 key infection 기법에 대해 연구하기로 최종결정 하였다.

 # Key infection 기법



다음 그림과 같이 i,j노드가 있다고 가정할 경우 ishem는 자신의 비밀키를 평문으로 주위 노드에게 전송하게 된다. 이 비밀키를 받은 노드 j는 이 키를 가지고 자신의 비밀키를 암호

화해서 다시 I 노드로 전송하게 된다. 이렇게 생성된 세션키를 가지고 통신을 하게 되는데, 이 통신을 감청하기 위해서는 i노드와 j노드의 비밀키를 모두 파악해야 하기에 감청이 쉽지 않다는 점이 장점이다.

알고리즘 개선의 방향

세 가지 알고리즘 개선 방향이 있다. 첫번째는 보안성 부분으로, 적대적 노드에 의해 탐지되어 감청되는 노드간 통신의 개수를 줄이는 것으로, 이를 높이려면 일반적으로 속도가 희생되게 된다. 두번째는 속도로, 노드가 배치되고 모든 노드간의 통신이 연결되어 네트워크가 구성되는 데에 걸리는 시간을 줄임으로써 성능을 향상시킬 수 있다. 일반적으로 보안성이 떨어지게 된다. 마지막으로 연결성이 있는데, 배치된 노드가 네트워크에 연결되는 확률을 높이고자 하는 방향이다. 이 세가지 방향을 연구함으로써 균형잡힌 발전을 이루고자 한다.

4. 현재 진행 상황

▶ 세부 연구주제 선정 완료.

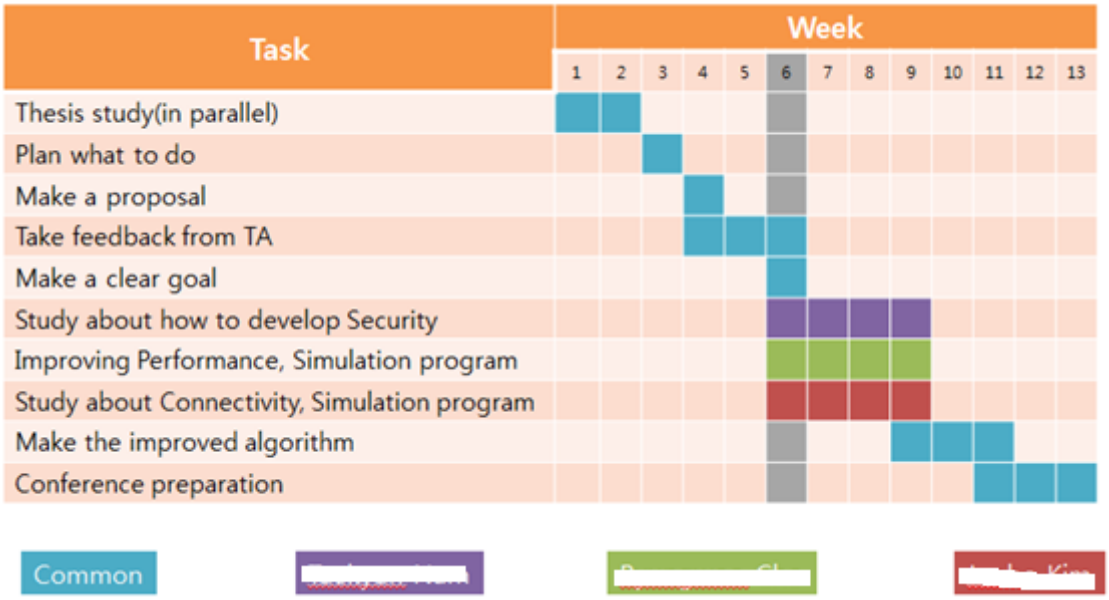
▶ 여러가지 키 관리 기술에 대한 분석 완료.

▶ 키 인펙션 기술에 대한 분석 완료.

▶ 조원당 알고리즘 개선 방향 확립.

▷ 각 담당한 분야에서 알고리즘 개선방향 연구 진행중.

5. 일정 및 역할 배분


Task
Week
1 2 3 4 5 6 7 8 9 10 11 12 13
Thesis study(in parallel)
Plan what to do
Make a proposal
Take feedback from TA
Make a clear goal
Study about how to develop Security
Improving Performance, Simulation program
Study about Connectivity, Simulation program
Make the improved algorithm
Conference preparation
Common