MQTT
경량의 메시지 프로토콜

20202430G7
김태현

- HTTP통신은 요청-응답으로 제한적 송수신
- MQTT는 특정채널에 일정 간격으로 계속송신
  - 구독만 하면 수신을 받을수 있음
- 연결 → 발행 → 구독 → 전달(메시지)

구독을 하면 수신받을 수 있다

보안위험! 데이터를 변조시킬수 있음

↳ 암호화를 하거나 수신을 제대로 하지 못하도록 해야함

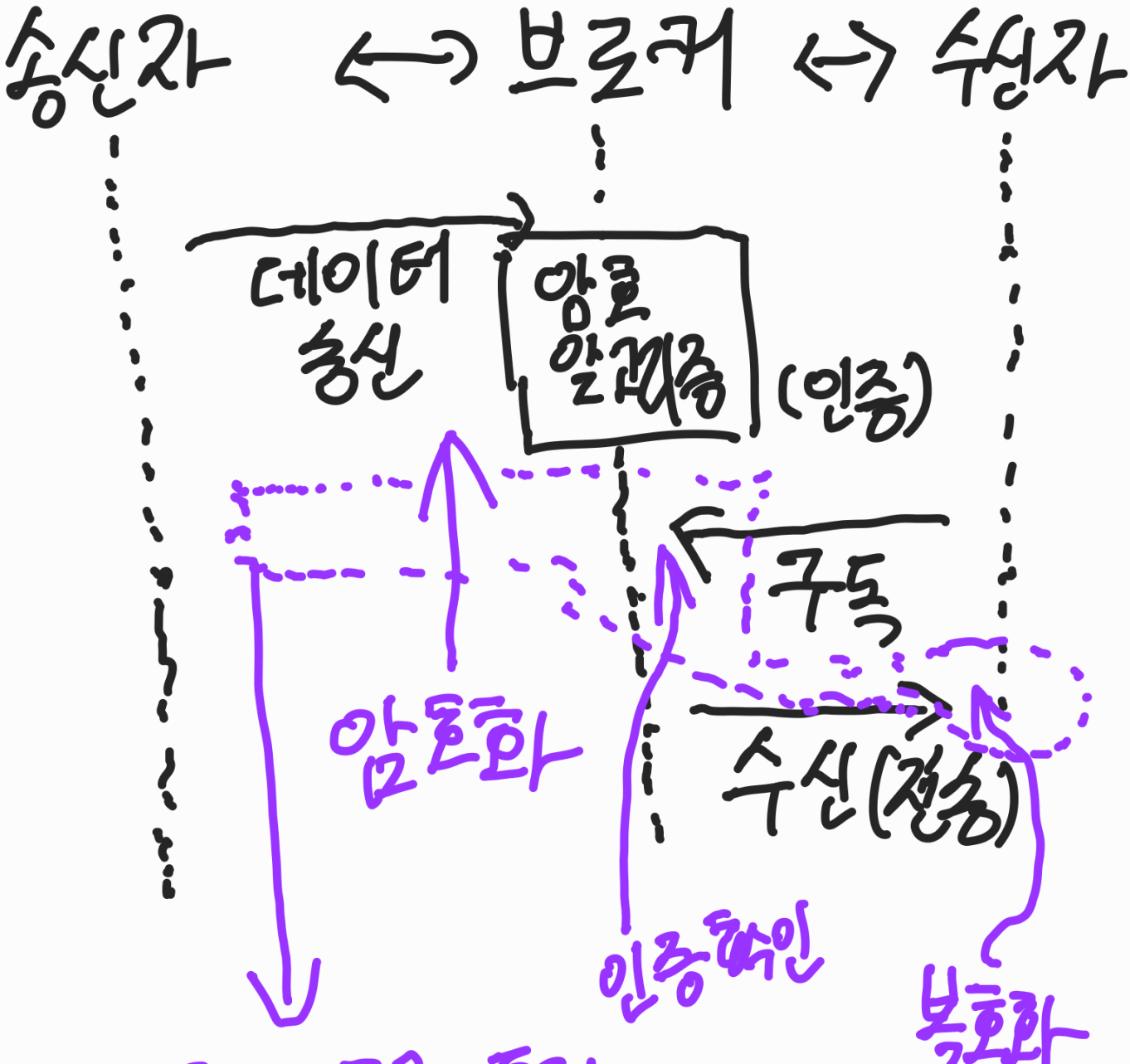
**혼돈신호

1. 데이터 암호화 : 크기↑ → 매우 민감반응(예측불가)
2. 보안 키 생성 및 교환 : 당사자 간 암호키 생성
3. 인증 : Client ↔ Broker 간의 연결 매커니즘 강화

혼돈 신호를 이용하면?

- 간단한 연산으로 구현 가능
  (리소스 자원 절약 → IoT에 적합)

- 복잡성 및 예측 불가능성
  ↳ 혼돈 시스템 특성으로 암호화 강도↑



혼돈신호를 통해
데이터의 위·변조, 감청 등 대응

이러한 프로토콜을 사용하면 효율성이 증가한다

- 도청공격 안전
- 스푸핑공격 안전
- 재전송공격 안전
- 서비스거부공격 안전
- 위치추적 보호

추후 조금 더 알아볼 필요 있음.

* 혼돈 신호를 이용한 IoT의 MQTT 보안 프로토콜 설계 (임거수, 2018) 참고