**무선 센서 네트워크에서 허위 보고서 삽입 공격 탐지를 위한 DEFS에 trajectory활용 방법**

**(A Method for Detecting False Report Injection Attack using Trajectory for Dynamic En-Route Filtering in WSN-based IoT)**

**성균관대학교 대학원**

**전자전기컴퓨터공학과**

**안 가 현**

**< 목차 >**

**1. 서론**

**2. 관련 연구**

**2.1 허위 데이터 및 허위 보고서 삽입 공격**

**2.2 Dynamic En-route Filtering Scheme (DEFS)**

**2.3 Trajectory 설명**

**2.4 BM-DEVS 설명**

**3. 제안 기법**

**4. 향후 연구**

**5. 참고문헌**

**6. 요약**

**7. 진행현황 제시**

**1. 서론**

   무선 센서 네트워크(Wireless Sensor Networks; WSNs)는 센서 노드와 기지국(Base Station: BS)으로 구성되어 있고, 군사, 교통, 건강, 산업 등 주로 무인 환경에서 사용된다. WSNs에서 센서 노드는 저전력, 저용량으로 에너지가 제한적이며 각각의 센서 노드들은 센서 필드에서 발생한 이벤트 데이터를 감지 및 수집하여 기지국으로 이벤트 데이터를 전달한다. 데이터를 전달하는 과정에서 센서 노드들은 주로 무인 환경 즉, 개방적인 환경에 존재하기 때문에 외부의 공격자로부터 쉽게 손상 및 훼손될 수 있다. 공격자들은 손상된 센서 노드를 통해 허위 데이터 및 허위 보고서를 센서 네트워크에 삽입하여 기지국으로 하여금 허위 보고서가 전달되도록 공격한다. 이러한 네트워크 공격은 보고서가 전달되는 과정에서 에너지가 제한적인 센서 노드의 자원 고갈로 이어질 수 있으며, 허위 보고서가 기지국에 도착하였을 때 기지국에서 잘못된 행위를 유발할 수 있다.

위와 같은 공격에 대응하기 위해 Yu와 Guan는 DEFS (Dynamic En-Route Filtering Scheme; 이하 DEFS)를 제안하였다. DEFS는 키 사전 배포 단계, 키 보급 단계, 보고서 전달 단계, 총 3단계로 구성된다. 이 기법에서는 센서 필드에 센서 노드가 배포된 후에 각각 최소 n개의 노드를 포함하는 여러 클러스터가 센서 네트워크에 형성된다고 가정한다. 형성된 클러스터에는 무작위로 선택된 한 개의 클러스터 헤드 노드(Cluster Head node; 이하 CH)를 선택한다. 이벤트가 발생하였을 때 주위에 이벤트를 감지한 센서 노드는 자신이 속한 클러스터의 헤드 노드에게 이벤트 내용과 auth-key를 전달한다. 클러스터 내의 모든 센서 노드에게 이벤트 내용과 auth-key를 전달받은 CH는 auth-key를 수집한K(n) 메시지와 이벤트 정보와 메시지 인증 코드(Message Authentication Code; 이하 MAC)을 수집한 센싱 보고서 R메시지를 생성하여 다음 노드로 전달한다. 포워딩 노드에서는 전달받은 R 메시지를 다음 포워딩 노드에게 바로 전달합니다. 이후 K(t)메시지에 존재하는 auth-key의 진위 여부를 확인하고, 확인된 키를 이용하여 R메시지의 MAC을 확인하여 보고서의 무결성과 유효성을 검증하고, R메시지가 무결하지 않다면 다음 노드에게 Fail이라는 메시지를 전송하고, 무결하다면 OK 메시지를 전송하도록 합니다. 위와 같은 과정을 반복 실행하여 BS까지 메시지가 전달될 수 있도록 합니다.

본 논문에서는 허위 데이터 및 허위 보고서 삽입 공격이 발생하였을 때 공격을 탐지하는 기법인 DEFS에서 공격이 발생하지 않고 보고서가 정상적으로 전달되는 과정을 standard trajectory로 정하고, 공격이 발생하였을 때 보고서가 비정상적으로 전달되는 과정을 공격 trajectory로 정한다. 이후 standard trajectory와 공격 trajectory를 timing diagram으로 표현한 후에 비교하여 차이점을 찾아낸다. 찾은 trajectory를 활용하여 공격 탐지율을 향상시킴으로써 보안성 향상을 기대한다.

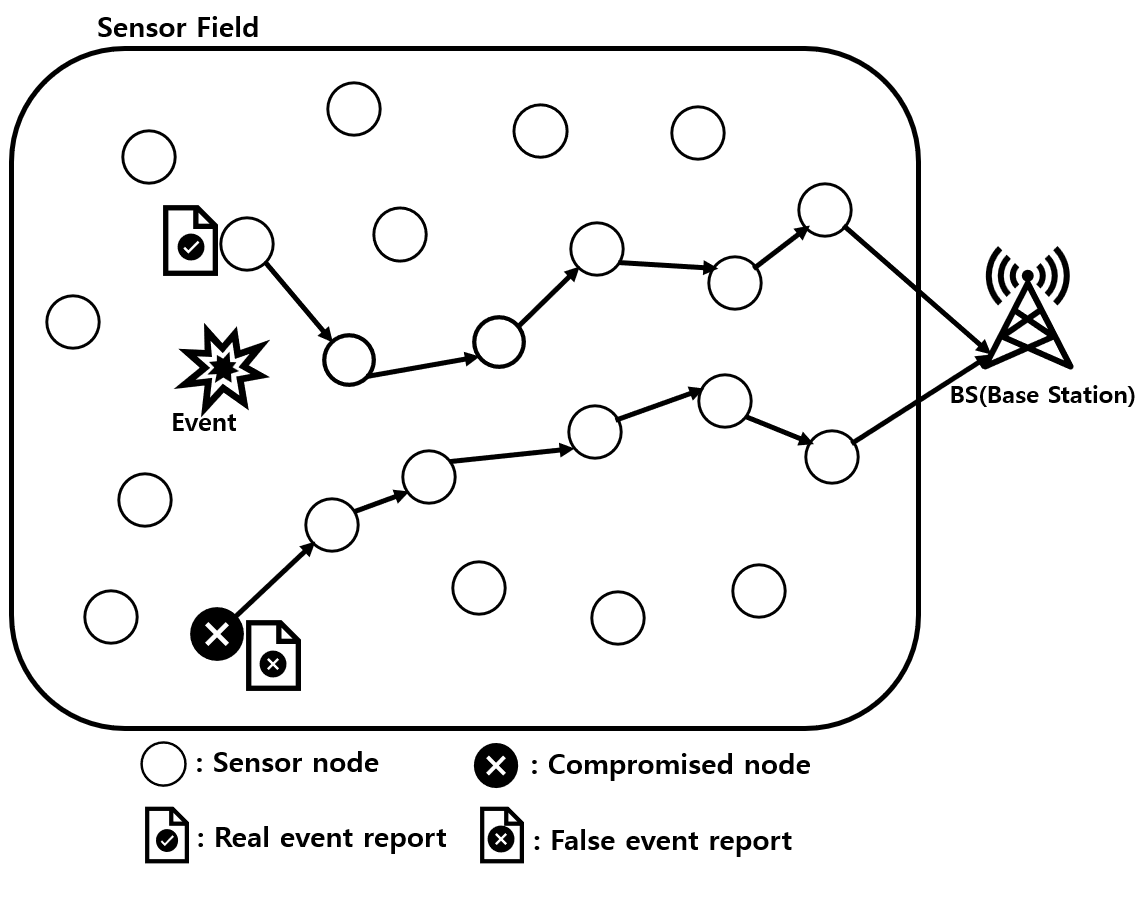
본 논문의 구성은 다음과 같다. 2장에서는 DEFS와 허위 데이터 및 허위 보고서 삽입 공격 그리고 trajectory에 관해 설명한다. 3장에서는 제안 기법에 대해 설명한다. 4장에서는 향후 연구에 관해 서술한다.

**주제어:** 무선 센서 네트워크, 사물인터넷, 허위 데이터 및 허위 보고서 삽입 공격, DEFS, Trajectory

**2. 관련연구**

허위 데이터 및 허위 보고서 삽입 공격이 발생하기 위해 공격자는 센서 노드를 손상시킨다. 본 논문에서는 손상된 센서 노드를 탐지하기 위해 DEFS기법에 trajectory를 활용할 수 있도록 하는 기법을 제안한다.

**2.1 허위 데이터 및 허위 보고서 삽입 공격**



[그림 ]. 허위 데이터 및 허위 보고서 삽입 공격

[그림 1] 은 WSNs에서 허위 데이터 및 허위 보고서 삽입 공격을 나타낸 것이다. [그림 1]에서와 같이 센서 필드에 존재하는 정상 센서 노드의 경우 이벤트가 발생하였을 때 발생한 이벤트에 대한 보고서를 생성하여 보고서를 기지국으로 전달한다. 하지만 허위 데이터 및 허위 보고서 삽입 공격의 경우 센서 필드에 존재하는 정상 센서 노드가 외부 공격자에 의해 손상되고, 공격자는 손상된 노드를 통해 발생하지 않은 이벤트에 대한 보고서를 생성하고 보고서를 기지국으로 전달하게 된다. 이러한 공격을 통해 공격자는 기지국에서 잘못된 행동이 발생하도록 하거나, 보고서를 기지국으로 전달하는 과정에서 포워딩 노드들의 에너지를 고갈시킬 수 있다. 이러한 공격을 탐지하기 위해 Yu와 Guan는 DEFS (Dynamic En-Route Filtering Scheme; 이하 DEFS)를 제안하였다.

**2.2 Dynamic En-Route Filtering Scheme (DEFS)**

Yu와 Guan는 무선 센서 네트워크에서 발생할 수 있는 허위 데이터 및 허위 보고서 삽입 공격을 탐지하기 위해 동적 경로 필터링 기법인 DEFS를 제안하였다. 이 기법에서 센서 네트워크는 클러스터를 기반으로 클러스터 헤드 노드와 센서 노드로 구성되어 있다. 이 기법은 각 노드가 갖고 있는 시드 키를 해시 함수를 사용하여 고유한 인증 키로 생성하고, 각 노드는 시드 키 외에도 비밀 키를 갖고 있으며, 이 두가지 키를 이용하여 보고서를 생성하고 검증하게 된다. 이 기법은 키 사전 배포 단계, 키 보급 단계, 보고서 전달 단계 총 3단계로 구성되어 있으며 자세한 내용은 아래에서 설명한다.

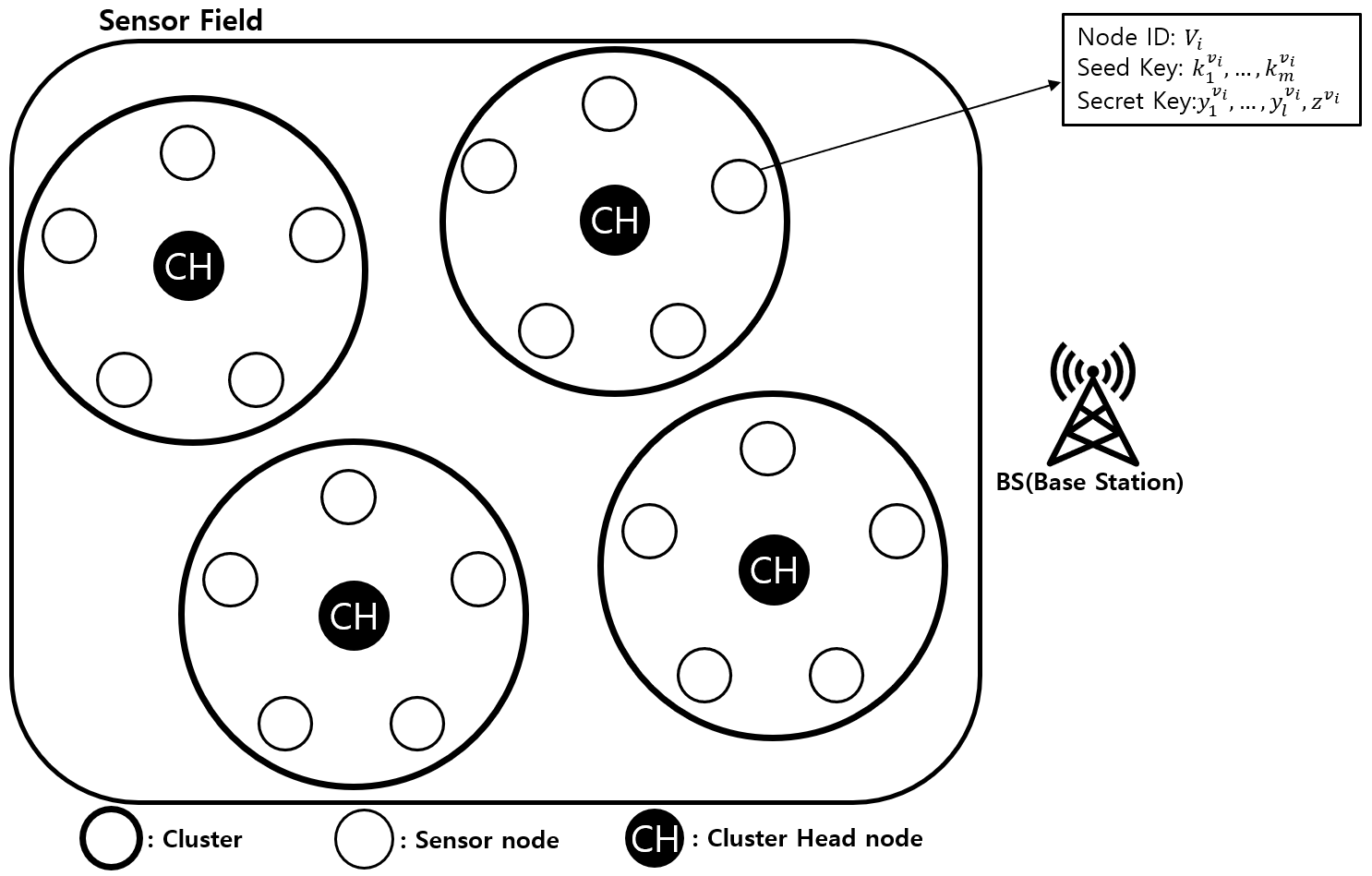
1) 키 사전 배포 단계(Key pre-distribution phase): 이 단계는 총 2개의 과정으로 구성되어 있으며, 네트워크에서 한 번만 수행한다. [그림 2]는 이 단계의 센서 네트워크를 나타낸다.

1. 각 노드에는 고유한 시드 키가 존재한다. 노드는 시드 키를 해쉬 함수를 사용하여 고유한 auth-key(인증 키)를 생성한다. 해쉬 함수를 통해 인증 키를 생성하는 과정은 (1)과 같다.

텍스트이(가) 표시된 사진

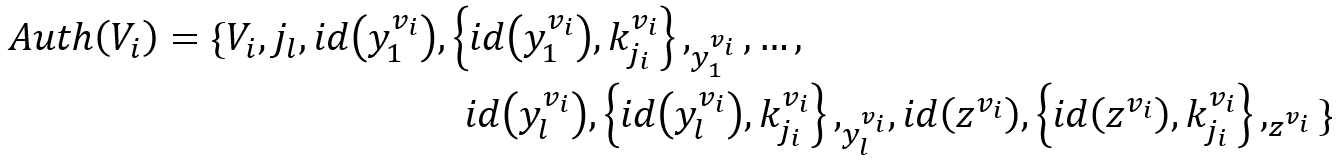
자동 생성된 설명(1)

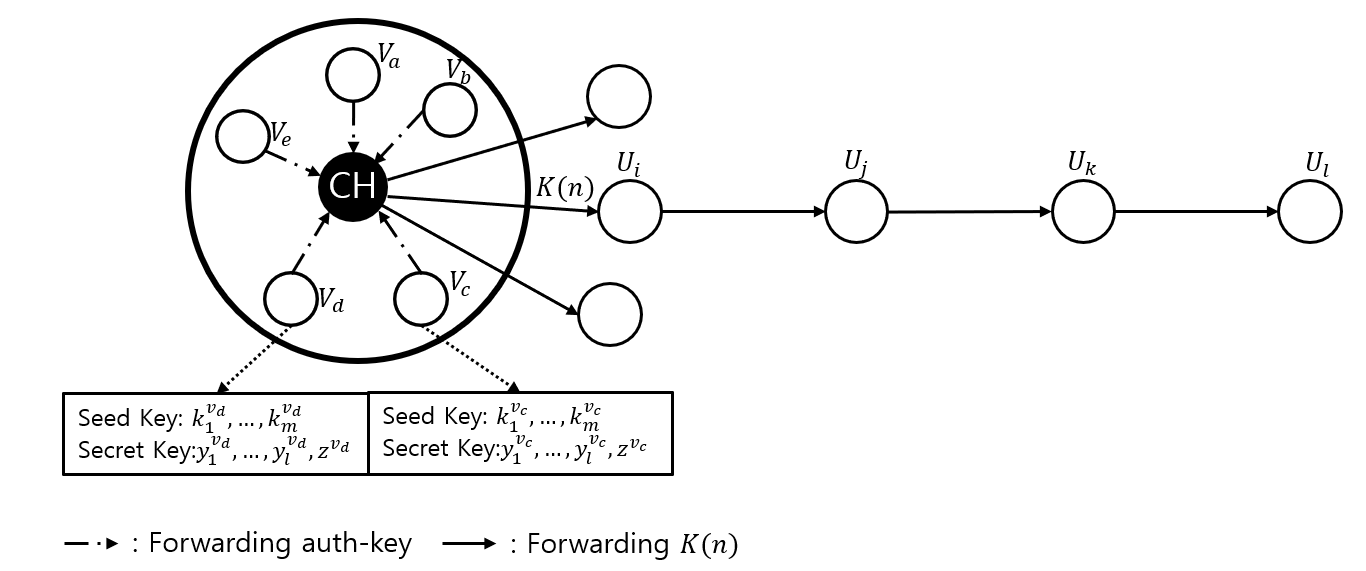
1. 시드 키 외에도 각 노드에는 개의 비밀 키가 존재한다. 크기가 v인 y-global key pool에서 개의 y-key가 무작위로 선택되고, w 크기의 z-global key pool에서 1개의 z-key가 무작위로 선택된다.



[그림 2]. 키 사전 배포 단계

2) 키 보급 단계(Key dissemination phase): 이 단계는 총 4개의 과정으로 구성되어 있다. [그림 3]은 이 단계를 보여준다.

1. 각 센서 노드는 현재 갖고 있는 인증키와 비밀키를 포함하는 Auth-Message를 생성한다. Auth-Message의 내용은 (2)와 같다.  
   (2)  
   (2)에서 는 현재 인증 키의 index를 의미하며 인 경우 첫번째 전파를, 는 y-key pool 내에 의 index를, 는 키를 이용한 암호화 연산을 의미한다.
2. CH노드는 클러스터 내의 모든 센서 노드에게 Auth-Message를 수집하고, 이 메시지들을 집계하여 K(n)메시지를 생성한다. K(n) 메시지는 (3)과 같다.  
   (3)  
   (3)에서 은 클러스터 내 센서 노드의 ID를 의미한다.
3. CH 노드는 인접 노드에서 개 이상의 포워딩 노드를 선택하고 K(n)을 전달한다. 그 이유는 한정된 자원으로 구성된 센서 노드가 수명을 다 하였을 때 K(n)을 다시 전파하지 않고 개의 노드 중 하나를 선택하여 전달할 수 있도록 하기 위해서이다.
4. 포워딩 노드가 K(n) 메시지를 수신하면 아래와 같은 검증 작업을 수행한다.
5. K(n)에 최소 t개의 고유한 z-key index가 존재하는지 확인한다.
6. 공유 키가 존재하는지 확인하기 위해 K(n)의 비밀 키 인덱스를 확인한다.  
   비밀 키가 존재한다면 해당 키를 사용하여 해당 인증 키를 복호화 하여 인증 키를 메모리에 저장한다.  
   인증 키와 함께 암호화된 인덱스를 확인하여 키가 올바른 것인지 확인한다.
7. K(n)은 BS에 도달할 필요 없이 hmax(최대 홉 수)만큼 전파되었다면 K(n)메시지를 삭제한다.



[그림 3]. 키 보급 단계

3) 보고서 전달 단계: 센서 노드는 반복적으로 새로운 인증 키를 선택하고 현재 인증 키로 이벤트 센싱 보고서를 생성한다. 새로운 인증 키를 선택하는 횟수는 센서 노드가 배포되기 전에 미리 결정되어 있다. 센서 노드의 이벤트 센싱 보고서 내용은 (4)와 같다. 이 단계는 총 5개의 과정으로 구성되어 있으며, [그림 4]는 이 단계를 보여준다.

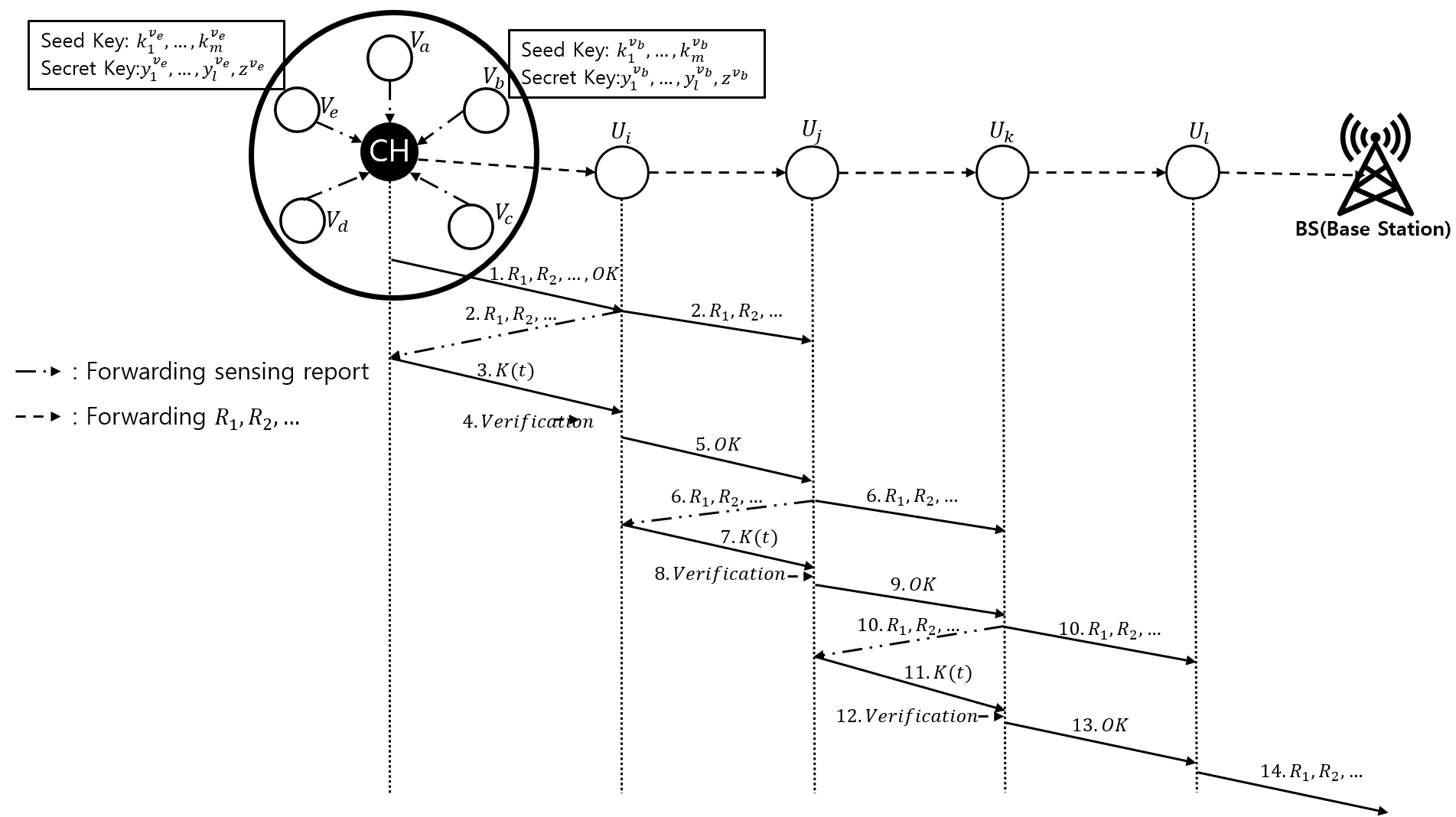
텍스트이(가) 표시된 사진

자동 생성된 설명(4)

E는 이벤트 정보, 는 센서 노드 ID, 는 의 현재 인증 키 인덱스, 는 키 를 사용하여 E에 대해 생성된 MAC을 의미한다.

1. 클러스터 내에 모든 센서 노드는 자신이 생성한 센싱 보고서를 CH노드에게 노드에게 전달하고, CH노드는 전달받은 보고서를 수집 및 집계하여 와 같은 여러 집계 보고서를 생성한다. 집계 보고서의 내용은 (5)와 같다.  
   텍스트, 시계이(가) 표시된 사진

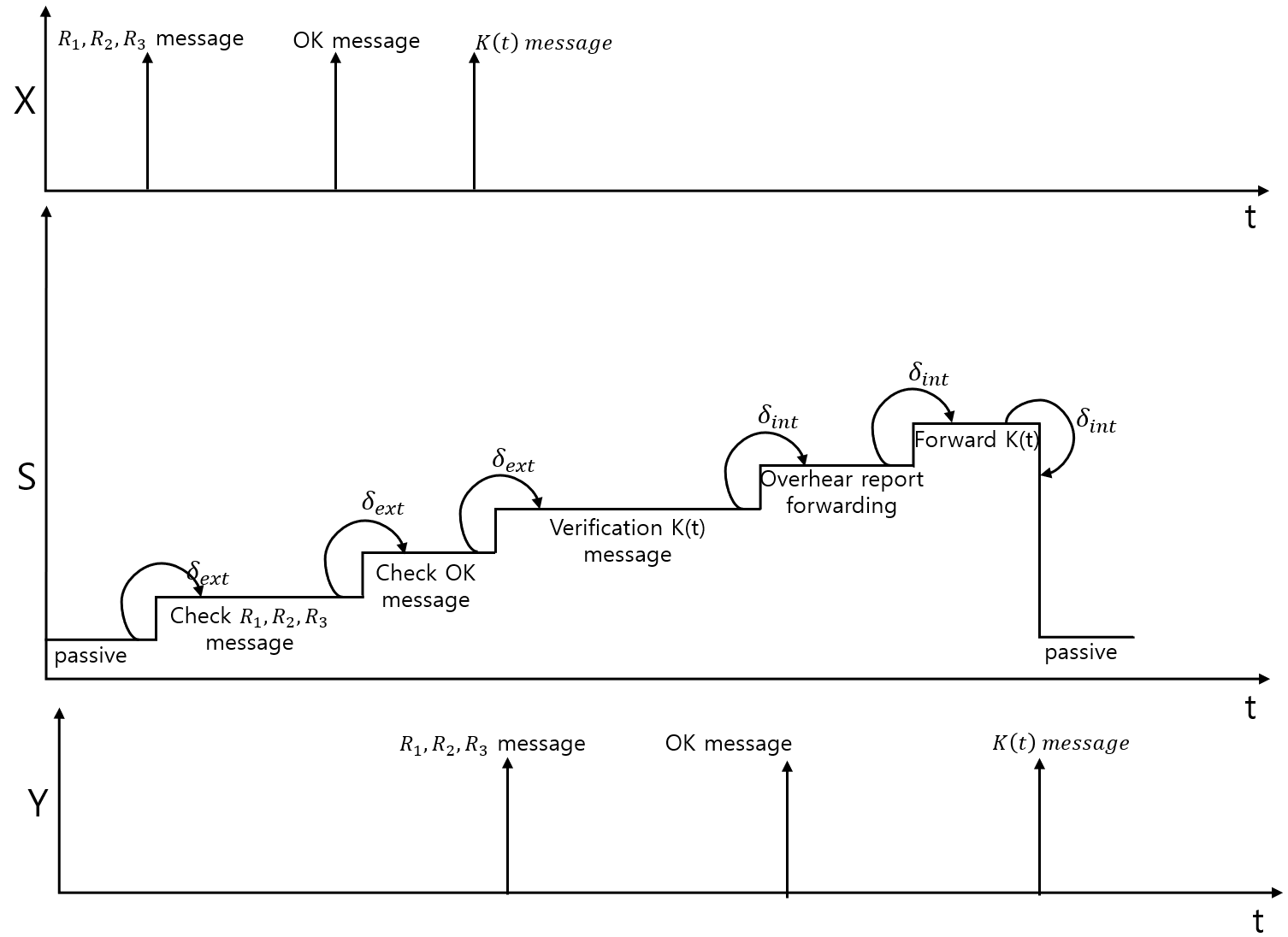
   자동 생성된 설명(5)  
   는 z-key가 다른 t개의 센서 노드를 의미한다.
2. CH노드는 R메시지와 OK를 다음 포워딩 노드인 [그림 4]의 노드로 전달하고, 노드는 다음 포워딩 노드인 노드로 R 메시지를 전달한다.
3. CH노드는 노드가 노드에게 R 메시지를 전달하는 것을 엿듣고 K(t) 메시지를 노드에게 전달한다. K(t)메시지는 이전 키 보급 단계의 K(n)메시지와 형식은 같지만, t개의 z-key가 존재하는 Auth-Message로 구성된 메시지를 의미한다.



[그림 4]. 보고서 전달 단계

1. 노드는 전달받은 K(t)메시지의 내용을 검증한다. 검증 방법은 아래와 같다.
   1. K(t) 메시지의 형식이 올바른 지 확인하고, t개의 z-key를 포함하고 있는지를 확인한다.
   2. 는 K(t)의 유효성을 확인하기 위해 에 존재하는 인증 키를 특정 횟수만큼 해싱하여 K(t)메시지에 존재하는 인증 키를 생성할 수 있는지 확인한다
   3. II에서 확인한 인증 키를 통해 MAC을 확인한다.
2. 메시지의 내용이 유효한 경우 노드에게 OK 메시지를 전달한다.

**2.3 Trajectory**



[그림 5]. DEFS에서 포워딩 노드의 보고서 전달 단계 과정

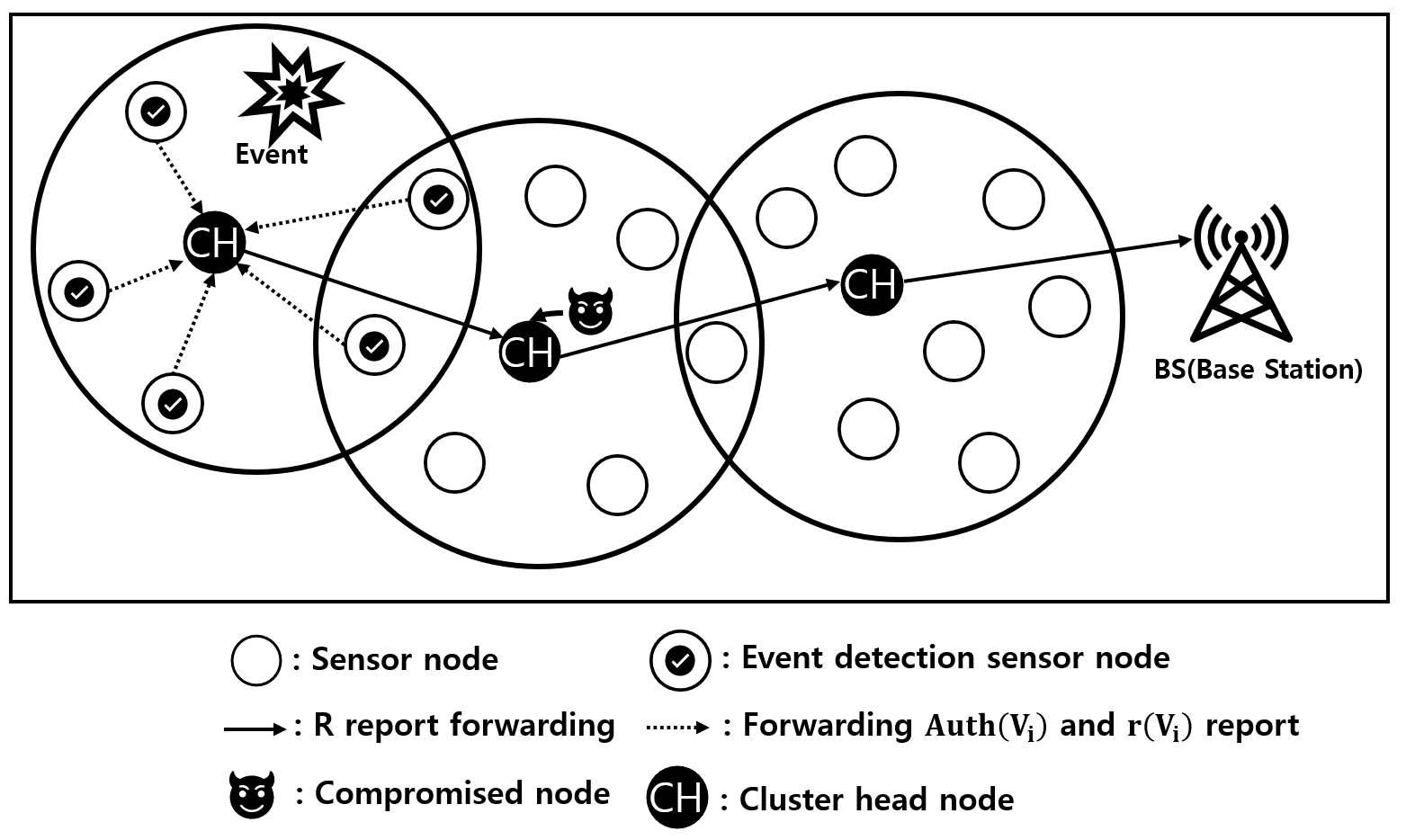
[그림 5]는 DEFS에서 포워딩 노드에 보고서가 수신되었을 때 보고서가 전달되는 과정을 시간에 따라 나타낸 timing diagram으로 X는 input timing diagram, S는 state timing diagram, Y는 output timing diagram을 나타내고 있다.

X diagram을 통해 보고서가 포워딩 노드에 수신되었다는 것을 알 수 있다. 보고서가 수신되면서 S diagram에서 passive 상태였던 포워딩 노드는 [그림 5]와 같이 시간에 따라 차례대로 상태 변화가 일어나는 것을 알 수 있다. 또한 상태 변화가 발생함에 따라 출력이 발생하는 것을 Y diagram을 통해 알 수 있다.

Trajectory는 시간에 따라 어떤 문제나 사건 또는 [그림 5]의 S diagram과 같이 상태 변화를 말하며, 본 논문에서는 Trajectory에 축적된 정보 혹은 데이터를 이용하여 허위 데이터 및 허위 보고서 삽입 공격을 탐지할 수 있도록 한다.

**3. 제안 기법**

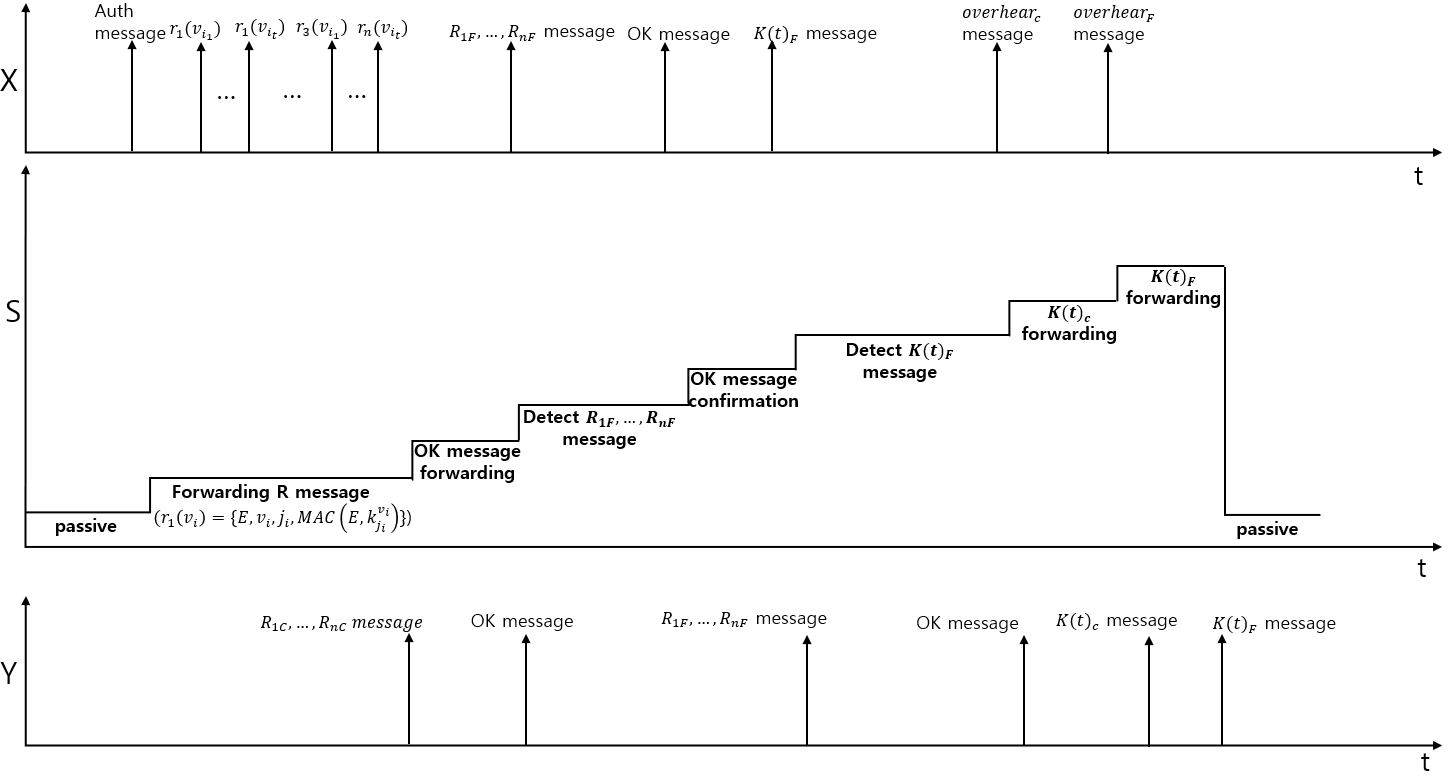
이 장에서는 허위 데이터 및 허위 보고서 삽입 공격을 탐지하는 DEFS 기법에 Trajectory를 활용하여 공격률 향상을 통해 보안성을 향상시킬 수 있도록 하는 제안 기법에 대해 설명한다.



[그림 6]. 허위 데이터 및 허위 보고서 삽입 공격 발생

DEFS 기법에서는 CH노드에서 허위 데이터 및 허위 보고서 삽입 공격이 발생할 수 있다. 이때 CH노드가 CH의 역할을 하는 경우, 보고서를 전달하는 포워딩 노드 역할을 하는 경우, CH의 역할과 포워딩 노드 역할을 동시에 하는 경우로 나눌 수 있다.

[그림 7]은 DEFS 기법에서 허위 데이터 및 허위 보고서 삽입 공격이 발생하지 않고, 정상적으로 보고서가 생성 및 전달되는 과정을 timing diagram으로 나타낸 것이다.



[그림 7]. DEFS 기법의 정상 동작 timing diagram

**4. 향후 연구**

제안 기법의 trajectory를 [그림 6]과 같은 timing diagram으로 표현한다. 이러한 timing diagram을 rule로 표현하고, 실험을 통해 rule을 실행하여 공격 탐지율을 향상시킬 수 있도록 연구를 진행하고자 한다. 또한 기지국에서 여과되지 못한 보고서 IoT 기기에서 처리하는 방법에 관한 연구도 진행하고자 한다.

**5. 참고문헌**

[1] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1.2-3 (2003): 293-315.

[2] Akyildiz, Ian F., et al. "A survey on sensor networks." *IEEE Communications magazine* 40.8 (2002): 102-114.

[3] Kumar, Alok, and Alwyn Roshan Pais. "En-route filtering techniques in wireless sensor networks: a survey." Wireless Personal Communications 96.1 (2017): 697-739.

[4] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[5] Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." Journal of Network and Computer Applications 88 (2017): 10-28.

[6] Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on selected areas in communications 23.4 (2005): 839-850.

[7] Yi, Chuanjun. "En-Route Message Authentication Scheme for Filtering False Data in WSNs." Security and Communication Networks 2021 (2021).

[8] Jeba, S., and B. Paramasivan. "False data injection attack and its countermeasures in wireless sensor networks." European Journal of Scientific Research 82.2 (2012): 248-257.

[9] Wang, Jianxin, et al. "Defending collaborative false data injection attacks in wireless sensor networks." Information Sciences 254 (2014): 39-53.

[10] Yang, Hao, et al. "Toward resilient security in wireless sensor networks." Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. 2005.

[11] Cho, Tae Ho. "Simulation Methodology-Based Context-Aware Architecture Design for Behavior Monitoring of Systems." Symmetry 12.9 (2020): 1568.

**6. 요약**

사물 인터넷은 다양한 IoT 기기가 무선 센서 네트워크를 통해 이벤트 데이터를 수집하고, 수집된 데이터를 인터넷 환경에서 서로 공유할 수 있도록 하는 기술이다. 무선 센서 네트워크는 다수의 센서 노드와 기지국으로 구성되어 있으며, 센서 노드는 저전력, 저용량으로 에너지가 제한적이다. 또한 주로 무인 환경, 개방적인 환경에서 사용되기 때문에 외부의 공격자로부터 쉽게 손상 및 훼손될 수 있고, 그로 인해 다양한 공격이 발생할 수 있다. 그 중 허위 데이터 및 허위 보고서 삽입 공격은 네트워크에서 센서 노드가 기지국으로 보고서를 전달하는 과정에서 허위 보고서가 전달되도록 하는 공격으로, 에너지가 제한적인 센서 노드의 자원 고갈로 인해 보고서가 전달되지 못하거나, 허위 보고서가 기지국에 도착하였을 때 잘못된 행위를 유발할 수 있다. 이러한 공격을 탐지하기 위해 Ye와 Luo는 SEF를 제안하였다. 하지만 이 기법의 경우 보고서의 내용 중 MAC의 위조 여부만 확인할 수 있고 이벤트 발생 내용에 관련된 위조 여부는 확인할 수 없다. 따라서 공격이 발생하지 않은 경우 SEF의 동작 과정과, 공격이 발생하였을 때 SEF의 동작 과정을 비교하여 공격 탐지가 가능한 추가적인 데이터를 발견하여 공격의 탐지율을 높일 수 있을 것이다. 본 논문에서는 허위 데이터 및 허위 보고서 삽입 공격의 탐지율을 높여 보안성을 향상시키기 위해 SEF에 Trajectory를 활용할 수 있도록 제안한다.

**7. 진행현황**

위 내용과 같이 사물 인터넷과 무선 센서 네트워크에 관련된 기본적인 내용을 Survey를 통해 진행하였고, 그와 관련된 공격 및 방어 기법들에 대한 기본적인 내용들 또한 Survey를 통해 진행하였습니다. 이후 통계적 여과 기법에 대한 연구를 진행하였고, 이 기법에서 사용하고 있는 MAC 이외의 문제점을 해결하여 공격 탐지율을 높이고, 그로 인한 보안성 향상을 위해 연구를 진행 중에 있습니다. 현재 Trajectory를 찾는 연구를 진행 중이며, 이후 발견한 Trajectory를 timing diagram으로 표현하고, timing diagram을 rule로 표현하여 실험을 통해 결과를 도출할 예정입니다.