무선 센서 네트워크를 위한 물리계층 보안 기술연구

임상훈, 전형석, 최진호*, 하정석
한국과학기술원, *광주과학기술원

요 약

본고에서는 센서 네트워크의 분산 검출 분야에서 최근 활발히 연구되고 있는 물리계층 보안기술들을 소개하고자 한다. 복잡한 연산과정을 요구하는 기존 암호학 기반의 보안 시스템은 배터리용량과 연산 능력이 제한된 센서 네트워크에서 많은 유지보수 비용을 유발할 수 밖에 없다. 본고에서 소개할 물리계층 보안기술들은 기존의 통신 모뎀 기술을 보안 강화의 목적으로 재활용하는 기술이다. 따라서, 복잡한 연산이나 추가적인 하드웨어를 필요로 하지 않기 때문에 자원이 제한된 센서 네트워크에 매우 적합하다. 본고에서는 센서네트워크에서 제안된 대표적인 물리계층 보안기술인 확률적 암호화 (stochastic encryption) 기법과 채널 인지 암호화 (channel aware encryption) 기법을 소개한다. 제안된 물리계층 암호화 기술을 두 가지 무선 채널 모형 PAC (parallel access channel)과 MAC (multiple access channel)에서 간략화된 모델로 재해석하여 센서 네트워크를 위한 보안 기술로서 적합성 여부를 평가하도록 하겠다.

Ⅰ. 서 론

본고에서는 무선 센서 네트워크가 분산 검출 (distributed detection)을 수행할 때 통신 물리계층에서 적용 가능한 보안 연구들을 소개하고자 한다.

분산 검출 시스템은 다수의 센서가 네트워크를 구성하여 목표물 (target)의 변화를 감지하고 이 정보를 융합 센터 (fusion center, FC)에 전달하여 대상의 최종 상태를 검출하는 기술이다. 분산 검출 시스템의 주요 응용 분야는 기온/습도 등의 기상 관측부터 화재/지진 등의 재난 탐지, 환경 오염 감시, 전시 적군의 공격 및 화학 물질 감지 등 다양하다[1].

분산 검출 시스템에서 센서들이 감지한 정보는 데이터 프라이버시 보호를 위해 보안 기술을 적용해 융합센터로 전송한다. 하지만 무선 센서 네트워크의 통신 환경은 기본적으로 보안에 취약한 구조를 가지고 있다. 첫째, 센서들이 융합센터에 정보를 전송하는 채널은 도청이 용이한 무선채널이다. 따라서 누구나 센서의 전송 정보 무선채널로부터 취득할 수 있으며 악의적인 목적으로 취득정보를 해독/임의가공/공유할 수 있다는 문제가 있다. 둘째, 분산 검출 시스템에서 센서들은 물리적으로 접근이 어려운 곳에 배치되며 센서의 배터리 교체가 어렵기 때문에 복잡도가 높아 전력소모량이 많은 강력한 암호 시스템을 사용하기 어렵다. 따라서 센서 네트워크에서는 연산 복잡도가 높은 비대칭 (asymmetric) 암호 키 기술 보다는 경량암호화 시스템에 적합한 대칭 (symmetric) 암호 키 기술을 주로 사용하고 있다. 하지만 대칭 암호 키 기술은 암호 키의 분실 및 훼손에 대비하여 주기적인 암호 키의 갱신이 필요하기 때문에 키 관리/분배를 위한 메커니즘을 필요로 하며, 이로인한 센서들의 추가적인 에너지사용은 배터리 수명을 단축시키는 주된 원인이 되고 있다.

물리계층 보안 기술은 이러한 센서 네트워크의 보안 취약성을 보완해줄 수 있는 기술로 최근 정보이론에 기반을 둔 물리계층 보안 기술이 많은 관심을 받고 있다. 물리계층 보안 기술의 가장 큰 장점은 기존의 물리계층 통신 기술들을 보안의 목적으로 재활용하기 때문에 구현에 있어서 추가비용이 적다는 점과 보안 키의 사전 분배 없이 기존 암호학 시스템에서 제공하는 보안 수준보다 높은 완벽 보안 (perfect security)을[1] 제공한다는 점이다. 정보이론 기반의 물리 계층 보안 기술은 Aaron D. Wyner에 의해서 처음 제안되었다[3]. 최근에는 무선 채널의 무작위성[4], 인공 잡음 (artificial noise)[6] 등을 이용한 물리계층 보안 기술들이 소개되었으며, 실제 구현에 관한 연구[5]도 활발히 진행 중에 있다.

분산 검출을 위한 무선 센서 네트워크에서도 검출 정보의 기밀성을 보장하는 물리 계층 보안 기술들이 소개되었다[7-11]. 본고에서는 최근 소개된 무선 센서 네트워크에 적용 가능한 물리계층 보안 기술인 확률적 암호화 기법 (stochastic

1 완벽보안이란 공격자가 암호 시스템을 공격할 시 어떠한 기술이나 자원을 이용하더라도 정보 취득이 불가능한 상황을 의미한다. 즉, 정보이론적으로 계산한 정보량이 제로인 상태를 의미한다 [2].

encryption) [7][8]과 무선 채널의 무작위성을 이용한 채널 인지 암호화 기법 (channel aware encryption) [10][11]을 소개하고자 한다. 두 기술 모두 적 융합센터 (enemy fusion center, EFC)가 센서들의 전송 정보를 도청한다는 가정아래 센서들이 각자의 검출 정보를 아군 융합 센터 (ally fusion center, AFC)에 전송한다. 본고에서 소개할 암호화 기술은 물리계층의 자원 및 기술을 이용하여AFC는 센서의 전송 정보로부터 목표물의 상태를 정확히 검출하면서, EFC는 목표물의 최종 상태를 검출할 수 없도록 하는 기술이다. 본고에서는 센서 네트워크의 대표적인 두 가지 무선 채널 모형인 PAC (parallel access channel)과 MAC (multiple access channel)을 고려하여 제안된 물리계층 암호화 기술을 새롭게 해석하고 비교/분석한다.

Ⅱ. 분산 검출을 위한 무선 센서 네트워크의 시스템 모델

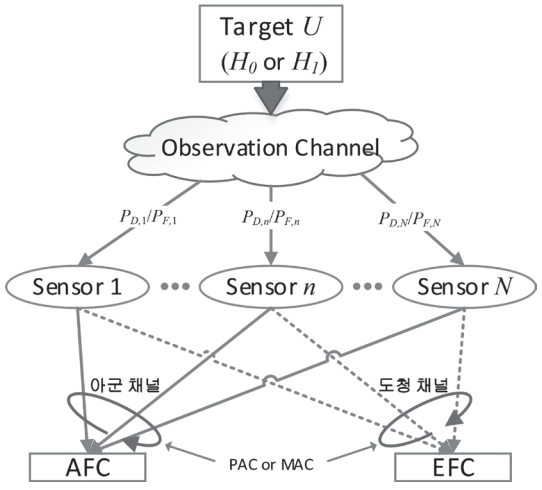


그림 1. 분산 검출을 위한 무선 센서네트워크 시스템 모델

1. 시스템 모형

본고에서는 〈그림 1〉에서와 같이 검출 대상인 목표물이 두 가지 상태를 가지는 이진 (binary) 분산 검출 시스템을 가정하도록 한다. 목표물의 상태는 랜덤 변수 U로 나타낸다[2]. $U=0$ (혹은 H_0로 표기) 은 영 가설 (null hypothesis)을 의미하고 $U=1$ (혹은 H_1로 표기)은 대체 가설 (alternative hypothesis) 을 의미한다.

목표물을 검출 하려는 센서 네트워크는 다수의 센서들과 AFC로 구성되어있다. 본고에서는 목표물 주변에 N개의 센서가 배치되어있는 상황을 가정한다. 센서들은 목표물의 상태를 검출하여 지역 결정 값 (local decision)을 도출하고 이를 AFC로 전송한다. 본고에서는 분산 검출 시 사용하는 한정된 주파수 대역폭을 고려하여 각 센서들은 이진신호로 지역 결정 값을 양자화한다고 가정한다. AFC는 센서들로부터 수집한 지역 결정 값을 바탕으로 목표물의 상태에 대한 최종 결정을 내린다.

본고에서는 N개의 센서와 융합 센터가 이루는 채널에 대해서 두 가지 채널 모형인 PAC과 MAC을 고려한다. PAC 모형에서는 N개의 센서들이 서로 독립적인 채널을 통해서 AFC 로 지역 결정 값들을 전송한다. MAC 은 N개의 센서들이 하나의 채널을 공유하여 융합 센터에 지역 결정 값들을 동시에 전송하는 모형이다. PAC모형은 각 센서가 독립적인 채널을 할당 받아야 하기 때문에 분산검출에 필요한 주파수 자원이 센서 수에 비례하여 늘어나며, 주파수 효율 측면에서는 MAC에 비해 비효율적이다. 하지만 개별 센서들의 지역 결정 값들을 융합센터에 정확히 전달할 수 있는 장점이 있다.

2. 분산 검출 환경에서의 완벽 보안

물리계층 보안은 기본적으로 Shannon이 정의한 정보의 모호도 (equivocation)를 보안의 척도로 사용한다[2]. EFC가 센서들로부터 수신한 신호를 r^E 라고 정의하고, 목표 대상의 상태를 u라고 정의하면 다음의 조건을 만족할 때 Shannon의 완벽 보안이 보장된다[2]:

$$I\left(R^E;U\right)=0 \text{ or } H\left(U\mid R^E\right)=H\left(U\right) \quad (1)$$

수식 (1)의 등호는 다음의 조건을 만족할 때 성립한다.

$$f\left(R^E\mid U\right)=f\left(R^E\right)=\sum_u f\left(R^E\mid U=u\right)f\left(U=u\right)$$

여기서 $f\left(R^E\right)$와 $f\left(R^E\mid U\right)$는 각각 R^E의 PDF (probability density function)와 주어진 U에 대한 R^E의 conditional PDF 이다. 수식 (1)에서 정의한 완벽보안은 EFC가 어떠한 기술을 사용하더라도 실질적으로 취득할 수 있는 정보량이 제로임을 보장한다. 따라서 도청자의 계산 능력의 한계를 가정하고 있는 기존 암호학 시스템의 연산 복잡도 기반 보안 (computational security) 요구사항 보다 더 강력한 보안을 보장한다. 다음 절에서는 완벽 보안을 보장하는 물리계층 암호화 기술들을 PAC과 MAC 모형에 따라 소개하도록 하겠다.

2 본고에서의 대문자 표기는 랜덤 변수를 의미한다.

3 $I\left(R^E;U\right)$는 U와 R^E사이의 상호정보량 (mutual information)을 $H\left(U\mid R^E\right)$은 주어진 R^E에 대해 U의 조건부 엔트로피 (conditional entropy)를 의미한다.

Ⅲ. PAC 환경에서 보안 분산 검출 연구

본 절에서는 PAC 모형에서 물리 계층의 특성을 이용한 보안 전송 방법에 대한 두 가지 연구 결과를 소개하도록 하겠다. 첫 번째는 센서 검출 정보의 확률적 암호화 기법이고, 두 번째는 무선 채널의 무작위한 특성을 이용한 채널 인지 암호화 기법이다. 확률적 암호화 기법은 센서와 AFC만이 알고 있는 확률 값을 기반으로 센서가 지역 결정 값을 암호화 하는 기술이고, 채널 인지 암호화 기법은 센서와 AFC사이의 채널의 특성을 활용하여 지역 결정 값을 암호화하는 기술이다.

1. 센서 검출 정보의 확률적 암호화 (stochastic encryption) 기법

확률적 암호화 기법은 분산 추정을 위한 무선 센서 네트워크에서 센서가 추정한 정보를 EFC로부터 보호하기 위해 처음 제안되었다[9]. 그 후 Nadendla 에 의해 분산 검출 환경으로 적용 분야가 확장되었다[7].

1.1 시스템 모형 및 최적 지역 결정 값 융합 규칙

임의의 n번째 센서의 지역 결정 (local decision) 값을 u_n ($u_n \in \{0,1\}$)이라고 정의한다. 각 센서의 지역 결정 값에 대한 목표물 검출 성능은 오경보 확률인 $P_{F,n}$과 검출 확률 $P_{D,n}$로 표현되며 각 확률 값은 다음과 같다.

$$P_{F,n} = \Pr(U_n = 1 | U = 0 \text{ or } H_0);$$
$$P_{D,n} = \Pr(U_n = 1 | U = 1 \text{ or } H_1).$$

PAC 모형에서는 각 센서들이 서로 독립적인 채널을 통해서 AFC로 지역 결정 값을 전송한다. 이 때, AFC가 n번째 센서로부터 수신한 정보를 r_n^A이라고 정의한다. AFC의 일반적인 수신 신호 모형에서는 채널 페이딩 (fading)과 잡음에 의한 영향을 고려하지만 확률적 암호화 기법에서는 분석의 용이성을 위해 무잡음 (noiseless) 채널을 가정한다. 따라서 AFC는 각 센서의 지역 검출 값을 오류 없이 수신한다($r_n^A = u_n$, $n = 1,2,...,N$). AFC가 수신한 신호 $\{r_n^A\}_{n=1}^N$를 바탕으로 최대 우도 검출 (maximum likelihood detection)을 수행하면 최적 융합 규칙 (optimal fusion rule)은 다음과 같다.

$$U_0 = \begin{cases} 1, \text{ if } \sum_{n=1}^{N} r_n^A \geq \kappa^A; \\ 0, \text{ if } \sum_{n=1}^{N} r_n^A < \kappa^A, \end{cases} \quad (2)$$

여기서 κ^A는 AFC에서 최종 결정을 내리기 위한 임계 값으로 $0 < \kappa^A < N$범위의 값을 갖는다.

각 센서들은 독립적으로 목표물의 상태를 검출한다. 각 센서의 검출 성능이 동일하다고 가정하면 모든 n에 대하여 $P_{F,n} = P_F$, $P_{D,n} = P_D$이고, AFC의 검출 성능은 다음이 정리된다.

$$Q_F^A = \sum_{i=\lceil \kappa^A \rceil}^{N} \binom{N}{i} P_F^i (1-P_F)^{N-i};$$
$$Q_D^A = \sum_{i=\lceil \kappa^A \rceil}^{N} \binom{N}{i} P_D^i (1-P_D)^{N-i}.$$

여기서 AFC의 오경보 확률은 Q_F^A이고 검출확률은 Q_D^A이다.

EFC가 AFC와 같은 방법으로 무잡음 채널을 통해 지역 결정 값을 수신하면, EFC에서 수신한 신호, $\{r_n^E\}_{n=1}^N$는 모든 n ($n = 1,2,...,N$)에 대하여 $r_n^E = u_n$이 성립한다. 이때 EFC는 수식 (2)과 동일한 방법으로 최적 융합 규칙을 얻을 수 있다.

1.2 확률적 암호화 기법 및 보안 성능 최적화

확률적 암호화 기법에서는 각 센서들이 주어진 확률 값 p_1과 p_2에 따라 지역 결정 값을 임의로 변경하여 AFC에 전송한다 ($p_1, p_2 > 0$). 센서의 지역 결정 값이 0인 경우 p_1의 확률로 지역 결정 값을 1로 변경하고, 센서의 지역 결정 값이 1인 경우 p_2의 확률로 지역 결정 값을 0로 변경한다. 따라서 AFC에서 수신한 임의의 n번째 센서의 지역 결정 값은 다음과 같이 표현된다.

$$\Pr(R_n^A = 1 | U_n = 0) = p_1;$$
$$\Pr(R_n^A = 0 | U_n = 1) = p_2.$$

확률적 암호화 기법이 보안을 제공함에 있어 가장 중요한 가정은 p_1과 p_2가 오직 센서들과 AFC에만 알려진 정보라는 것이다[7]. AFC는 p_1과 p_2를 조절하여 EFC의 오 경보 확률 Q_F^E와 검출 확률 Q_D^E를 일정 수준 이상으로 높이면서 동시에 AFC의 검출 성능 열화를 최소화하는 방향으로 최적화한다. 성능 열화의 척도로서 융합된 정보의 오류 확률 P_e^j를 다음과 같이 정의한다.

$$P_e^j = q_0 Q_F^j + (1-q_0)(1-Q_D^j)$$

여기서 $j \in \{A, E\}$이고 q_0는 오 경보 확률 Q_F^j과 검출 실패 확률 $1-Q_D^j$에 대한 무게 요소 (weighting factor) 값 이며, $0 \leq q_0 \leq 1$ 의 범위를 갖는다.

[8]에서는 AFC에서의 보안 성능 최적화 문제를 다음과 같이

공식화 하였다.

$$\begin{aligned}&\arg\min_{p_1,p_2,\kappa^A} P_e^A\left(p_1,p_2,\kappa^A\right)\\&\text{subject to } P_e^E\left(p_1,p_2,\kappa^E\right)\geq\alpha,\\&\qquad 0\leq p_1,p_2\leq 1,\\&\qquad 1\leq\kappa^A\leq N.\end{aligned}$$

여기서 α는 EFC의 오류 확률에 대한 최소 요구치 이다. 주어진 최적화 문제는 p_1, p_2 값을 조절하여 EFC의 오류 확률을 α 이상으로 보장하면서 AFC의 융합 정보 신뢰도를 가장 높이는 방향으로 최적화 한다. p_1, p_2, κ^A값을 닫힌 해 (closed form solution) 형태로 찾기는 힘들기 때문에 전체 검색 (exhaustive search) 방법을 이용해서 값을 찾을 수 있다.

EFC에서는 p_1, p_2의 존재를 모르기 때문에 융합 임계 값 κ^E를 찾기 위한 최적화 문제를 다음과 같이 공식화 할 것이다.

$$\begin{aligned}&\arg\min_{k^E} P_e^E\left(p_1=0,p_2=0,\kappa^E\right)\\&\text{subject to}\quad 1\leq\kappa^E\leq N.\end{aligned}$$

최적화된 임계 값을 κ^{E*}로 정의하고 AFC는 $p_1=p_1^*$, $p_2=p_2^*$로 암호화 기법의 확률 값을 최적화 했다고 가정하자. 이때 EFC가 κ^{E*}를 사용하여 센서로부터 수신한 정보를 융합하면 EFC의 실제 오류 확률은 $P_e^E\left(p_1^*,p_2^*,\kappa^{E*}\right)$으로 EFC가 기대한 오류 확률 $P_e^E\left(p_1=0,p_2=0,\kappa^{E*}\right)$보다 크거나 같은 값을 가지게 된다. 따라서 AFC는 최소한 주어진 α 이상으로 EFC의 검출 성능 오류 확률 값을 증가 시킬 수 있다.

확률적 암호화 기법은 다음과 같은 단점을 가지고 있다. 첫째, EFC가 p_1, p_2값을 모르는 상황을 가정하기 때문에 p_1, p_2는 보안 전송을 위해 사전에 할당된 암호 키로 해석될 수 있다. 따라서, 제안된 보안 전송 기법을 이용하더라도 센서에 보안 키를 분배 해야 하는 문제가 여전히 남아있다. 둘째, 또한 보안의 척도가 융합된 정보의 오류 확률이기 때문에 제안된 기술로는 정보이론의 완벽 보안을 보장할 수 없다.

2. 센서 검출 정보의 채널 인지 암호화 기법

채널 인지를 통한 보안 전송 기법은 물리 계층에서 무선 채널의 무작위한 특성을 이용하여 지역 결정 값을 암호화 하는 방식이다[10]. 채널 인지를 통한 보안 전송 기법이 기존 방식과 차별화되는 점은 무선 채널의 특성이 보안 전송을 위한 보안키 역할을 하기 때문에 사전에 별도로 보안 키를 분배 할 필요가 없으며, 정보이론에 기반한 완벽 보안을 제공한다는 것이다.

2.1 시스템 모형 및 보안을 위한 지역 결정 값 전송 규칙

채널 인지를 통한 보안 전송 기법은 시분할 이중 (Time division duplex) 통신 환경에서 동작한다. 따라서, 각 센서는 하향 링크 (downlink)를 통해 AFC로부터 파일럿신호를 수신하여 센서와 AFC의 무선채널 이득 값을 추정한다. 각 센서는 추정된 채널 이득의 크기를 기준으로 서로 분리된 두 개의 그룹 G_1, G_2 중 한 그룹에 속하게 된다. 그룹 G_1에 속하는 센서들은 그룹 G_2에 속하는 센서들보다 더 강한 채널 이득을 갖도록 그룹을 나누며 그룹을 결정하는 채널 이득의 크기에 대한 경계 값들은 각 센서들에 미리 저장되어있다고 가정한다. 따라서, 채널 이득의 통계적인 분포를 고려하면 각 그룹에 속하는 평균 센서 수를 조절 할 수 있는 임계 값을 결정할 수 있다.

각 센서로부터 AFC로의 채널 $\left\{h_n^A\right\}_{n=1}^N$ 은 서로 독립적이고 동일한 분포를 갖는다고 가정한다. 또한, 각 센서로부터 EFC로의 채널 $\left\{h_n^E\right\}_{n=1}^N$도 서로 독립적이고 동일한 분포를 갖는다고 가정한다. AFC와 EFC는 충분한 거리 (주파수의 반 파장 이상)를 두고 위치하여 $\left\{h_n^A\right\}_{n=1}^N$ 와 $\left\{h_n^E\right\}_{n=1}^N$는 서로 독립적인 상황이고, 채널 상관시간 (coherent time) 동안에는 채널 이득 값이 일정한 블록 페이딩 환경을 따른다고 가정한다.

채널 인지 암호화 기법은 센서가 AFC로부터 파일럿을 수신하고, 자신의 지역 검출 값을 AFC에 전송하는 일련의 과정이 상관시간 이내에 이루어진다. [10]에서 제시된 보안 전송 방식의 핵심 아이디어는 다음과 같다. 그룹 G_1에 속하는 센서들은 올바른 지역 결정 값을 송신하고, 그룹 G_2에 속하는 센서들은 EFC의 정보 융합을 방해하는 목적으로 지역 결정 값의 반대 값을 송신한다. n번째 센서의 지역 결정 값 $u_n(u_n\in\{0,1\})$을 암호화한 값을 $s_n(s_n\in\{-1,1\})$ 이라고 정의하면, s_n은 n번째 센서가 속한 그룹에 따라서 다음 연산을 통해서 얻는다.

$$s_n=\begin{cases}2u_n-1 & \text{if } n\text{th sensor in } G_1\\ 2(1-u_n)-1 & \text{if } n\text{th sensor in } G_2\end{cases}$$

2.2 AFC 와 EFC 단에서 지역 결정 값 융합 규칙

AFC가 n번째 센서로부터 수신한 정보 r_n^A은 다음과 같이 표현된다.

$$r_n^A=h_n^A s_n+z_n^A$$

여기서 z_n^A은 잡음을 의미한다. EFC가 n번째 센서로부터 수신한 정보 r_n^E는 다음과 같다.

$$r_n^E=h_n^E s_n+z_n^E$$

편의상 AFC와 EFC가 수신한 신호들을 벡터 형태인 $\mathbf{r}^A=\left[r_1^A\ldots r_N^A\right]^T$와 $\mathbf{r}^E=\left[r_1^E\ldots r_N^E\right]^T$로 표기 한다. 각 센서들은 s_n을 전송하기에 앞서 파일럿 신호를 전송한다고 가정한다.

파일럿 신호를 통해 AFC와 EFC는 각각 $\{h_n^A\}_{n=1}^N$와 $\{h_n^E\}_{n=1}^N$를 추정할 수 있지만, h_n^A와 h_n^E가 서로 독립이기 때문에 EFC에서 $\{h_n^A\}_{n=1}^N$의 추정은 불가능하다. 따라서 $\{h_n^A\}_{n=1}^N$는 AFC와 센서만이 공유하고 있는 보안 키로 확률적 암호화 기법과는 달리 AFC와 센서가 사전에 저장하지 않고 실시간으로 무선 채널을 통해 획득한다.

AFC는 각 센서로부터 지역 결정 값을 수신할 때 채널 이득 값을 추정하여 각 센서가 속한 그룹을 추정한다. 만일 센서가 그룹 G_2에 속할 경우 수신된 신호는 채널 인지 암호화 방법에 따라 변경되기 이전 값으로 다시 복원한다. 따라서, AFC에서의 최적 융합 규칙은 보안을 고려하지 않은 상황에서의 최적 융합 규칙인 수식 (3)과 동일하게 된다[12][13].

$$\frac{f\left(R^A \mid H_1\right)}{f\left(R^A \mid H_0\right)} = \sum_{n=1}^{N}\left[\frac{\Sigma_{u_n} f\left(R_n^A \mid U_n=u_n\right)\Pr(U_n=u_n \mid H_1)}{\Sigma_{u_n} f\left(R_n^A \mid U_n=u_n\right)\Pr(U_n=u_n \mid H_0)}\right] = \sum_{n=1}^{N}\left[\frac{f\left(R_n^A \mid U_n=1\right)P_D + f\left(R_n^A \mid U_n=0\right)(1-P_D)}{f\left(R_n^A \mid U_n=1\right)P_F + f\left(R_n^A \mid U_n=0\right)(1-P_F)}\right]. \quad (3)$$

수식 (3)의 융합 규칙은 센서 수 N이 증가함에 따라 오류 확률이 점근적으로 0에 접근하는 것을 보장한다[11][12].

한편, EFC는 $\{h_n^A\}_{n=1}^N$를 모르는 상황에서 U를 검출해야 한다. EFC에게는 최상의 시나리오를 가정하여 EFC는 무 잡음 채널을 통해서 센서의 전송 신호를 수신한다고 가정하겠다. 따라서 $r_n^E = h_n^E s_n$이고 EFC에서의 최적 융합 규칙은 다음과 같이 유도된다.

$$\begin{aligned}\frac{f\left(R^E \mid H_1\right)}{f\left(R^E \mid H_0\right)} &= \sum_{n=1}^{N}\frac{\Pr\left(S_n \mid H_1\right)}{\Pr\left(S_n \mid H_0\right)} \\ &= \frac{\sum_{u_n}\int f\left(S_n, h_n^A, U_n=u_n \mid H_1\right)dh_n^A}{\sum_{u_n}\int f\left(S_n, h_n^A, U_n=u_n \mid H_0\right)dh_n^A} \\ &= \frac{\sum_{u_n}\Pr\left(U_n=u_n \mid H_1\right)\int f\left(S_n, h_n^A \mid U_n=u_n, H_1\right)dh_n^A}{\sum_{u_n}\Pr\left(U_n=u_n \mid H_0\right)\int f\left(S_n, h_n^A \mid U_n=u_n, H_0\right)dh_n^A} \\ &\overset{(a)}{=} \frac{\sum_{u_n}\Pr\left(u_n \mid H_1\right)\int \Pr\left(s_n \mid h_n^A, u_n\right) f\left(h_n^A\right)dh_n^A}{\sum_{u_n}\Pr\left(u_n \mid H_0\right)\int \Pr\left(s_n \mid h_n^A, u_n\right) f\left(h_n^A\right)dh_n^A}\end{aligned} \quad (4)$$

여기서 (a)는 U, u_n, h_n^A, s_n이 $U \to \{u_n, h_n^A\} \to \{s_n\}$과 같이 Markov chain을 형성하기 때문이다. n번째 센서가 그룹 G_i $(i \in \{1,2\})$에 속할 확률을 λ_i라고 정의하자. n번째 센서가 그룹 G_i에 속하는 경우 $\Pr\left(S_n \mid h_n^A, U_n\right)=1$이기 때문에 수식 (4)에서 $\int \Pr\left(S_n \mid h_n^A, U_n\right) f\left(h_n^A\right)dh_n^A = \lambda_i$이다. 따라서 수식 (4)의 $\Pr\left(S_n \mid H_k\right)$는 다음과 같이 간략화할 수 있다.

$$\Pr\left(S_n \mid H_k\right) = \begin{cases}\lambda_1 \Pr\left(U_n=1 \mid H_k\right) + \lambda_2 \Pr\left(U_n=0 \mid H_k\right) & \text{if } S_n=1; \\ \lambda_1 \Pr\left(U_n=0 \mid H_k\right) + \lambda_2 \Pr\left(U_n=1 \mid H_k\right) & \text{if } S_n=-1.\end{cases}$$

만일 $\lambda_1 = \lambda_2$이면, $\Pr\left(S_n \mid H_1\right) = \Pr\left(S_n \mid H_0\right)$이 성립하므로 두 가설 상황에 대해서 센서로부터 수신한 정보의 확률 분포도는 완벽히 동일하게 된다. 따라서, EFC 는 목표물 상태에 대한 통계적 추론을 전혀 할 수 없게 된다. 채널 인지 암호화 기법의 가장 큰 장점은 채널 이득 값을 추정하여 지역 결정 값을 변경시키는 단순한 방법만으로도 완벽보안을 제공할 수 있다는 것이다.

Ⅳ. MAC 환경에서 보안 분산 검출 연구

본 절에서는 채널 인지 암호화 기법을 MAC (multiple access channel) 환경에 적용하는 방법을 소개하도록 하겠다. PAC 환경과는 다르게 MAC 환경에서는 하나의 채널을 모든 센서들이 공유한다. AFC는 하나의 채널을 통해서 센서들의 지역 결정 값들을 동시에 수신하기 때문에 PAC환경에서와 같이 파일럿 송수신을 통해 개별 센서의 채널 이득을 추정할 수 없다. [11]에서는 이러한 문제를 다중 사용자 다이버시티 (multi-user diversity)를 이용하여 극복하였다.

제안된 방식은 PAC 모형과 같은 방법으로 각 센서는 AFC 가 송신하는 파일럿을 통해서 채널 이득을 추정하고, 그 크기에 따라 그룹 G_1 또는 그룹 G_2에 속할지 결정한다. 여기서 그룹 G_1에 속하는 센서들은 그룹 G_2에 속하는 센서들보다 더 강한 채널 이득을 갖도록 그룹을 설정한다. PAC 모형과 마찬가지로 그룹 G_1에 속하는 센서들은 지역 결정 값을 그대로 송신하고, 그룹 G_2에 속하는 센서들은 지역 결정 값의 반대 값을 송신한다. 즉, 지역 결정 값이 0이면 1을, 지역 결정 값이 1이면 0을 송신한다. 그룹 G_i에 속하는 센서의 수를 N_i라고 정의하자 $(N_1 + N_2 \le N)$. 그룹 G_i에 속하는 n번째 센서의 지역 결정 값을 $u_{i,n}$으로 표기하고 채널 인지 암호화된 값을 $s_{i,n}$으로 표기한다. 그룹 G_i에 속하는 n번째 센서와 AFC사이의 채널이득은 $h_{i,n}^A$으로 표기하고 그룹 G_i에 속하는 n번째 센서와 EFC사이의 채널이득은 $h_{i,n}^E$으로 표기하겠다. AFC에서의 수신 신호 모형은 다음과 같다.

$$r^A = \sum_{n_1=1}^{N_1} h_{1,n_1}^A s_{1,n_1} + \sum_{n_2=1}^{N_2} h_{2,n_2}^A s_{2,n_2} + z^A,$$

여기서 z^A는 AFC에서의 잡음을 의미한다. EFC에서의 수신 신호 모형은 다음과 같다.

$$r^E = \sum_{n_1=1}^{N_1} h_{1,n_1}^E s_{1,n_1} + \sum_{n_2=1}^{N_2} h_{2,n_2}^E s_{2,n_2} + z^E,$$

여기서 z^E는 EFC에서의 잡음을 의미한다. 각 채널과 채널 인지 암호화된 값을 벡터 형태로 표기하면 다음과 같다.

$$\mathbf{h}_i^A = \left[h_{i,1}^A \ \cdots \ h_{i,N_i}^A \right]^{\mathrm{T}}, \mathbf{h}_i^E = \left[h_{i,1}^E \ \cdots \ h_{i,N_i}^E \right]^{\mathrm{T}};$$
$$\mathbf{s}_i = \left[s_{i,1} \ \cdots \ s_{i,N_i} \right]^{\mathrm{T}}.$$

AFC와 EFC의 수신 신호 모형을 다시 정리하면 다음과 같다.

$$r^A = \left(\mathbf{h}_1^A\right)^T \mathbf{s}_1 + \left(\mathbf{h}_2^A\right)^T \mathbf{s}_2 + z^A;$$
$$r^E = \left(\mathbf{h}_1^E\right)^T \mathbf{s}_1 + \left(\mathbf{h}_2^E\right)^T \mathbf{s}_2 + z^E.$$

1. 다중 사용자 다이버시티 (multi-user diversity)를 이용한 AFC에서의 분산 검출

MAC에서의 채널 인지 암호화 기법은 PAC에서와 같이 채널 이득 $\mathbf{h}_1^A$, $\mathbf{h}_2^A$을 보안키로 사용한다. 하지만 MAC의 특성상 모든 센서들이 하나의 채널로 지역 결정 값을 동시에 전송하기 때문에 AFC에서는 각 센서의 채널 이득 값을 추정할 수가 없다. 따라서 그룹 G_2에 속하는 센서들이 보내는 지역 결정 값을 다시 복원할 수 없으므로 $\mathbf{s}_2$ 신호는 AFC가 목표물의 상태를 검출하는데 있어서 간섭신호로 작용한다.

[11]에서는 이를 극복하고자 다중 사용자 다이버시티 효과를 이용하는 채널 인지 암호화 기법을 제안하였다. 수신신호의 간략화를 위해, AFC가 각 그룹으로부터 수신한 신호를 $y_i^A = \left(\mathbf{h}_i^A\right)^T \mathbf{s}_i$ 로 표기하자. AFC의 수신 신호는 다음과 같이 정리된다.

$$r^A = y_1^A + y_2^A + z^A.$$

여기서 그룹 G_2를 결정하는 채널 이득의 임계 값을 임의로 조정함으로써 간섭 신호 y_2^A의 영향을 줄일 수 있다. 각 그룹을 결정하는 채널 이득의 임계 값을 τ_1 과 τ_2 로 표기하고, 각 그룹을 다음의 규칙에 따라 나누도록 하자:

$$\mathbf{h}_{1,n_1}^A \geq \tau_1, \ \text{for } n_1 = \{1, \cdots, N_1\},$$
$$\mathbf{h}_{2,n_2}^A \leq \tau_2, \ \text{for } n_2 = \{1, \cdots, N_2\}.$$

만약 τ_2를 매우 작은 값으로 설정하면 AFC의 수신 신호는 다음과 같이 근사화된다.

$$r^A \approx y_1^A + z^A.$$

따라서 AFC에서는 G_1 그룹에서 전송된 지역 결정 값을 바탕으로 목표물의 상태를 추정할 수 있게 된다. PAC모형에서는 AFC가 독립적인 채널을 통해 지역 결정 값을 수신 했기 때문에 G_1 그룹과 G_2 그룹의 센서들이 전송하는 모든 지역 결정 값들을 구분하고 이들을 목표물 검출에 활용할 수 있었다. 하지만 MAC모형에서는 AFC가 두 그룹의 신호를 분리해낼 수 없기 때문에, 그룹 G_2를 결정하는 임계 값 τ_2를 낮춰 G_1 그룹의 지역 결정 값으로 목표물의 최종 상태를 검출해낸다. 이때 다중 사용자 다이버시티는 임계 값 τ_2을 임의의 매우 작은 값으로 설정(동시에 τ_1을 임의의 매우 큰 값으로 설정)하더라도 센서의 수 N이 충분하다면 각 그룹에 적어도 한 개 이상의 센서가 존재함을 보장한다. 따라서 임계 값 τ_2를 0으로 접근 시키면, AFC는 수신 신호를 다음의 융합 규칙을 이용해 최종 목표물의 상태를 검출할 수 있다:

$$\lim_{\tau_2 \to 0} \frac{f\left(R^A \mid H_1\right)}{f\left(R^A \mid H_0\right)},$$

위 수식은 MAC모형에서 N_1개의 활성화된 센서가 보안을 고려하지 않았을 시의 융합 규칙과 동일하다[15]. 또한 다중 사용자 다이버시티를 이용하면, 임의의 센서 수 N에 대해 임계 값 τ_1을 적절한 높은 값으로 설정하여 AFC의 검출 오류 확률을 낮출 수 있다.

2. 적 융합 센터에 대한 완벽 보안

본 절에서는 EFC의 목표물에 대한 검출 성능을 분석하기 위해 EFC에게 최상의 시나리오를 가정한다. 즉, EFC는 무 잡음 채널을 통해서 센서들로부터 전송 신호를 수신한다고 가정한다. 따라서 EFC의 수신신호는 다음과 같이 표현된다.

$$r^E = \left(\mathbf{h}_1^E\right)^T \mathbf{s}_1 + \left(\mathbf{h}_2^E\right)^T \mathbf{s}_2$$

수신 신호 r^E에 대해 목표물 상태에 대한 완벽 보안을 보장하기 위해서는 다음의 조건을 만족해야 한다[2].

$$I\left(R^E; U\right) = 0 \text{ or } f\left(R^E \mid H_0\right) = f\left(R^E \mid H_1\right) \qquad (5)$$

[16]에서는 완벽 보안이 보장되는 조건 식 (5)를 유도하기 위해 우선적으로 다음의 사실들을 가정 하였다.

가정 1: 각 그룹에 속하는 센서의 수가 같다. ($N_1 = N_2$)

가정 2: $\mathbf{h}_1^E$와 $\mathbf{h}_2^E$가 서로 독립이고 동일한 통계적 분포를 따른다

가정 3: 센서들의 지역 결정 값들은 조건부 독립이다.

Theorem 1 [16]: 앞서 정의한 가정 1,2,3의 상황에서, 만약 $P_F = 1 - P_D$이고 EFC가 $\mathbf{h}_1^E$와 $\mathbf{h}_2^E$ 추정할 수 없다면, 채널 인지 암호화 기법은 완벽 보안을 보장한다.

증명: EFC가 각 그룹으로부터 수신한 신호를 $y_i^E = \left(\mathbf{h}_i^E\right)^T \mathbf{s}_i$로 표기하면 AFC의 수신 신호는 다음과 같이 정리된다.

$$r^E = y_1^E + y_2^E.$$

가정 1,2,3 에서 만약 $P_F = 1 - P_D$이면 그룹 G_2에 속하는 센서들은 지역 결정 값 0은 1로 지역 결정 값 1은 0으로 전송하므로 다음 조건이 성립된다.

$$f\left(Y_1^E \mid H_0\right) = f\left(Y_2^E \mid H_1\right) \text{ and } f\left(Y_1^E \mid H_1\right) = f\left(Y_2^E \mid H_0\right)$$

따라서 가설 H_0일 때의 전송신호 Y_1^E, Y_2^E의 결합확률밀도 함수는 다음과 같이 유도된다.

$$\begin{aligned} f\left(Y_1^E, Y_2^E \mid H_0\right) &= f\left(Y_1^E \mid H_0\right) f\left(Y_2^E \mid H_0\right) \\ &= f\left(Y_2^E \mid H_1\right) f\left(Y_1^E \mid H_1\right) \\ &= f\left(Y_1^E, Y_2^E \mid H_1\right) \end{aligned}$$

따라서 가설 H_0에 대한 수신신호 r^E의 확률밀도 함수는 다음과 같이 H_1에 대한 수신신호 r^E의 확률밀도 함수와 같음을 증명할 수 있으므로 완벽 보안이 보장됨을 확인할 수 있다.

$$\begin{aligned} f\left(R^E \mid H_0\right) &= \iint_{y_1^E + y_2^E \le r^E} f\left(Y_1^E = y_1^E, Y_2^E = y_2^E \mid H_0\right) dy_1^E y_2^E \\ &= f\left(R^E \mid H_1\right) \end{aligned}$$

Theorem 1은 각 그룹의 신호가 EFC에 통계적으로 동일한 강도로 전달되면 채널 인지 암호화 기법이 완벽 보안을 보장할 수 있음을 보여준다. 따라서, 가정 1을 다음과 같이 완화 하더라도 각 그룹의 신호가 EFC에 통계적으로 동일한 강도로 전달되기 때문에 완벽 보안을 보장할 수 있다.

가정 4: N_1과 N_2가 서로 독립이고 동일한 분포를 따른다.

Theorem 2 [16]: 가정 2,3,4의 상황에서 만약 $P_F = 1 - P_D$이고 EFC가 $\mathbf{h}_1^E$와 $\mathbf{h}_2^E$를 추정할 수 없다면, 채널 인지 암호화 기법은 완벽 보안을 보장한다

증명: [16] 참조

가정 4는 임계 값 τ_1과 τ_2를 적절히 조절하여 각 그룹에 속하는 평균 센서 수를 동일($\lambda_1 = \lambda_2$)하게 만들면 만족할 수 있다. 이러한 조건이 만족되면 EFC가 오류 없이 센서의 전송 정보를 수신하더라도 완벽 보안을 보장할 수 있다.

채널 인지 암호화 기법의 핵심은 각 그룹의 센서로부터 EFC로의 채널이 서로 독립이고 통계적으로 동일한 분포를 따라야 한다는 것이다. MAC모형에서의 채널 인지 암호화 기법은 PAC 모형과는 달리 활성화된 각 센서의 암호화된 지역결정 값을 복원 하려 하지 않고 두 그룹의 융합된 전송정보가 EFC에게는 동일한 강도로, AFC에게는 그룹 G_1의 융합 정보가 G_2의 융합정보보다 강하게 전달되도록 하는 것이 특징이다. MAC 모형에서는 다중 사용자 다이버시티를 이용하여 AFC가 그룹 G_2로부터 수신하는 간섭의 영향을 극복하였다.

V. 결 론

본고에서는 무선 센서 네트워크가 분산검출을 수행 시 EFC의 도청을 방지할 수 있는 물리계층 보안 기술들을 살펴보았다. 살펴본 물리계층 보안 기술들은 무선 채널의 무작위성과 같은 물리계층의 자원을 적절히 활용하면 단순한 연산과정만으로도 강력한 보안을 제공할 수 있음을 보여준다. 따라서 물리 계층 보안 기술은 자원 활용이 제한된 무선 센서네트워크와 같은 환경에서 많은 에너지 소모가 필요한 기존 암호학 기술을 보완/대체할 수 있는 보안 기술로 활용될 수 있다.

Acknowledgement

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012R1A1B3002684)

참 고 문 헌

[1] P. K. Varshney, Distributed Detection and Data Fusion, New York:Springer-Verlag, 1997.

[2] C. Shannon, "Communication Theory of Secrecy Systems," Bell Syst. Tech. J. vol. 28, pp. 656-715 Oct. 1949.

[3] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[4] R. Ahlswede and I. Csiszar, "Common randomness in

information theory and cryptography – Part I: Secret sharing," IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121 – 1132, July 1993.

[5] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.–J. Kwak, "LDPC codes for the Gaussian wiretap channel," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 532 – 540, Sept. 2011.

[6] S. Goel and R. Negi,"Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun, vol. 7, no. 6, pp. 2180 – 2189, June 2008.

[7] V. Nadendla, Secure Distributed Detection in Wireless Sensor Networks via Encryption of Sensor Decision, MS Thesis, Louisiana State University and Agricultural and Mechanical College, 2009.

[8] R. Soosahabi and M. Naraghi–Pour, "Scalable phy–layer security for distributed detection in wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol. PP, no. 99, p. 1, 2012.

[9] T. C. Aysal, K. E. Barner, "Sensor Data Cryptography in Wireless Sensor Networks," IEEE Trans. Inf. Forensics Security, vol.3, no.2, pp.273 – 289, June 2008.

[10] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol.8, no.4, pp. 619 – 625, Apr. 2013.

[11] H. Jeon, D. Hwang, J. Choi, H. Lee, and J. Ha, "Secure type–based multiple access," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 763 – 774, Sept. 2011.

[12] B. Chen, L. Tong, and P. K. Varshney, "Channel–aware distributed detection in wireless sensor networks," IEEE Signal Process. Mag., vol. 23, no. 4, pp. 16 – 26, July 2006.

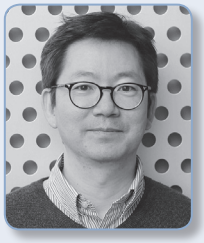
[13] R. Niu, B. Chen, and P. K. Varshney, "Fusion of decisions transmitted over Rayleigh fading channels in wireless sensor networks," IEEE Trans. Signal Process., vol. 54, no. 3, pp. 1018 – 1027, Mar. 2006.

[14] D. Tse and P. Viswanath, Fundamentals of Wireless Communication. Cambridge: Cambridge University Press, 2005.

[15] C. R. Berger, M. Guerriero, S. Zhou, and P. Willett, "PAC vs. MAC for decentralized detection using noncoherent modulation," IEEE Trans. Signal Process., vol. 57, no. 9, pp. 3562 – 3575, Sept. 2009.

[16] J. Choi, H. Jeon, and J, Ha, "Physical Layer Security for Wireless Sensor Networks," IEEE PIMRC 2013, London, Sept. 2013.

약 력

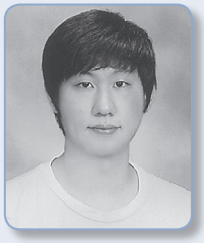


하 정 석

1992년 경북대학교 전자공학과 학사
1994년 포항공과대학교 전자전기 석사
2003년 Georgia Tech 박사
2004년~2010년 한국정보통신대학교 조교수
2010년~현재 한국과학기술원 부교수
관심분야: 통신, 채널부호, 물리계층 보안

전 형 석

2004년 동국대학교 공학사
2005년 한국과학기술원 공학석사
2010년 한국과학기술원 공학박사
2010년~2011년 한국과학기술원 연수연구원
2010년~2011년 Georgia Technology Institute 방문 연구원
2011년~현재 Georgia Technology Institute Postdoc
관심분야: 무선통신 신호처리, 정보이론, 물리계층 보안



임 상 훈

2009년 숭실대학교 전자 및 전자공학부 공학사
2011년 한국과학기술원 전기 및 전자 공학과 공학석사
2011년~현재 한국과학기술원 전기 및 전자 공학과 박사과정
관심분야: 무선통신 신호처리, 정보이론, 물리계층 보안

최 진 호

1989년 서강대학교 공학사
1991년 한국과학기술원 공학석사
1994년 한국과학기술원 공학박사
2006년~2013년 영국 Swansea University 교수 (Chair of Wireless Communications)
2013년~현재 광주과학기술원 교수
관심분야: MIMO, 협력 통신, 신호처리, 물리계층 보안