Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.6, Dec. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.6.1165

클러스터 기반 WSN에서 비정상적인 클러스터 헤드 선출 공격에 대한 통계적 탐지 기법*

김 수 민,[1†] 조 영 호[2‡]
[1,2]국방대학교 (대학원생, 교수)

A Statistical Detection Method to Detect Abnormal Cluster Head Election Attacks in Clustered Wireless Sensor Networks*

Sumin Kim,[1†] Youngho Cho[2‡]
[1,2]Korea National Defense University (Graduate student, Professor)

요 약

무선 센서 네트워크(Wireless Sensor Network: WSN)에서 센서들을 클러스터(Cluster) 단위로 그룹화하고 각 클러스터에서 통신 중계 역할을 하는 클러스터 헤드(Cluster Head: CH)를 선출하는 클러스터링 알고리즘이 에너지 보존과 중계 효율을 위해 제안되어 왔다. 한편, 오염된 노드(Compromised Node), 즉 내부공격자를 통해 CH 선출과정에 개입하여 네트워크 운영에 치명적인 영향을 미치는 공격기법들이 등장하였으나, 암호키 기반 대응방식과 같은 기존 대응방법은 내부공격자 방어에 한계가 있었다. 따라서, 본 연구에서는 클러스터링 알고리즘의 CH 선출 통계를 바탕으로 비정상적인 CH 선출 공격을 탐지하는 통계적 탐지기법을 제안한다. 대표적인 클러스터링 알고리즘인 LEACH와 HEED가 운영되는 환경에서 오염노드에 의한 비정상적인 CH 선출 공격을 설계하고, 제안기법의 공격탐지여부에 대한 실험을 통해 제안기법의 효과성을 확인하였다.

ABSTRACT

In WSNs, a clustering algorithm groups sensor nodes on a unit called cluster and periodically selects a cluster head (CH) that acts as a communication relay on behalf of nodes in each cluster for the purpose of energy conservation and relay efficiency. Meanwhile, attack techniques also have emerged to intervene in the CH election process through compromised nodes (inside attackers) and have a fatal impact on network operation. However, existing countermeasures such as encryption key-based methods against outside attackers have a limitation to defend against such inside attackers. Therefore, we propose a statistical detection method that detects abnormal CH election behaviors occurs in a WSN cluster. We design two attack methods (Selfish and Greedy attacks) and our proposed defense method in WSNs with two clustering algorithms and conduct experiments to validate our proposed defense method works well against those attacks.

Keywords: WSN Security, Abnormal Cluster Head Election, Greedy Attack, Selfish Attack

Received(09. 21. 2022), Modified(1st: 11. 14. 2022, 2nd: 11. 17. 2022), Accepted(11. 18. 2022)

* 본 논문은 2022년 정보보호학회 하계학술대회에 발표한 '클러스터링 WSN에서 비정상적인 클러스터 헤더 선출에 대한 통계적 탐지기법'을 확장한 논문임을 밝힌다.

† 주저자, shclass93@gmail.com
‡ 교신저자, youngho@kndu.ac.kr(Corresponding author)

I. 서 론

WSN(Wireless Sensor Network)은 무선 센서들로 이루어진 네트워크를 의미한다. 이 센서들은 필요한 공간에 배치되어 수집한 데이터를 기지국(Base Station)으로 전달한다. 일반적으로 센서들은 값싼 소형 무선장비이고 외부 전원 없이 배터리로 구동되기 때문에 에너지 효율성이 매우 중요하다[1].

수집한 데이터를 에너지 효율적으로 전송하기 위해, 센서들은 기지국으로 데이터를 직접 전송하지 않고 인근 센서(노드)의 중계통신을 통해 데이터를 전송한다. 나아가 센서들을 여러 개의 클러스터로 그룹화하고 각 클러스터에서 CH를 선출하여 센서들로부터 수신한 데이터를 통합, 압축하여 기지국으로 전송함으로써 WSN의 에너지 효율을 개선하는 클러스터링 알고리즘이 제시되어 왔다[2, 3].

한편, 클러스터 기반의 WSN에서 CH의 중요성으로 인해 CH는 공격자에게 매우 매력적인 표적이 되었다. 즉, 공격자는 클러스터링 WSN의 CH 선출 과정에 개입함으로써 네트워크에 치명적인 영향을 줄 수 있다[4]. 예를 들어, 공격자는 오염노드를 CH로 반복 선출시켜 CH에 부여된 권한으로 클러스터 데이터들을 삭제 또는 변조하거나, CH로 지속 선출되지 않게하여 네트워크의 운영을 방해할 수 있다.

이러한 공격들에 대응하기 위한 연구들[5, 6]이 제안되어 왔으나 본 연구에서 확인한 바로는 메시지 암호화를 통해 공격자가 CH 선출 절차를 확인하지 못하게 하는 암호키 기반 기법은 암호키 유출 및 내부자 공격에 취약하다. 또한 노드간 신뢰도를 평가하고 이를 CH 선출 변수로 반영하는 신뢰 및 평판 기법은 평가 조작에 취약할 수 있다. 그리고 이런 기법들은 노드의 리소스(에너지, 계산능력, 저장공간)을 필요로 하기 때문에 제한된 리소스를 효율적으로 사용해야 하는 WSN 환경에 불리하다.

따라서 본 연구에서는 기존 연구들과 다른 방향으로 공격자에 의한 비정상적인 CH 선출 공격을 탐지하기 위한 기법을 제안한다. 제안기법은 정상적인 환경에서 사전 확인한 CH 선출 통계와 실제 환경에서 구해진 CH 선출 통계를 비교한 결과가 임계치를 벗어났을 때, 비정상적인 CH 선출이 발생한 것으로 간주한다.

이후 논문의 구성은 다음과 같다. 2장에서는 배경지식과 관련연구를 설명하고, 3장에서는 제안기법의 아이디어와 동작방식을 소개한다. 4장에서 실험을 통해 제안기법의 유효성을 검증하고 성능을 평가한다. 끝으로 5장에서는 결론을 맺는다.

II. 배경지식 및 관련 연구

2.1 CH 선출 방법과 공격

클러스터링 알고리즘은 WSN의 클러스터화와 주기적인 CH 선출을 담당한다. 기존 연구의 개선, 다양한 조건에서의 최적화 등을 이유로 수많은 클러스터링 알고리즘들이 현재까지 제안되고 있으며, 이들은 CH 결정에 관여하는 변수들에 따라 Table 1.과 같이 분류할 수 있다[2, 3].

이러한 클러스터링 알고리즘들은 일반적으로 CH를 선출할 시기가 되면 Fig.1.과 같은 선출 절차를 거친다:

① 변수 생성 단계에서, 노드들은 어떤 노드가 CH에 가장 적합한지 결정하기 위한 변수를 생성한다.
② 선출 순위값 계산 단계에서, 노드들은 변수를 사전에 정의된 공식에 투입하여 CH 선출 순위값을 계산한다.
③ CH 선출 단계에서, 각 노드는 계산한 CH 선출 순위값을 같은 클러스터에 속한 노드끼리 비교하여 가장 적합한 노드를 해당 주기의 CH로 선출한다.

Table 1. Clustering Algorithms Classified by CH Determination Parameters

Criteria	Clustering Algorithms
Random number	LEACH, TEEN, EEHC
Range	Adaptive algorithm, WSNCABC
Residual energy	LEACH-C, APTEEN, HEED, Bayesian algorithm
Multiple variables	EECS, MRPUC, S-WEB, EEUC, Fuzzy Logic algorithms

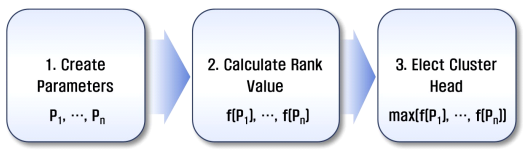

Fig. 1. CH Election Procedure

한편, 공격자는 변수 생성 단계 또는 공식화 단계에서 오염노드의 기준값 또는 선출 순위값을 변조하여 CH 선출에 개입할 수 있다. [4]의 연구에서는 이러한 공격을 유형화하여, 오염노드를 CH로 반복 선출하는 것을 탐욕 공격(Greedy Attack), CH로의 선출을 의도적으로 기피하는 것을 이기적 공격(Selfish Attack)이라고 설명하였다.

2.1.1 LEACH(Low-Energy Adaptive Clustering Hierarchy)

LEACH[7]는 초창기에 제안된 클러스터링 알고리즘으로, CH 선출 주기가 도래하면 각 노드는 랜덤값을 생성하고 사전 정의된 임계값보다 랜덤값이 낮은 노드는 CH로 선출된다. 또한, CH로 선출된 노드는 클러스터 내 나머지 노드들이 선출되기 전까지 재선출되지 않는다. 따라서, LEACH의 CH 선출은 균등분포를 따르게 되어 CH 선출을 공정하게 한다는 장점이 있으나, 선출에 노드의 지리적 위치를 고려하지 않기 때문에 노드별 에너지 보존 효율이 균등하지 않다는 제한사항이 있다.

2.1.2 HEED(Hybrid, Energy-Efficient, Distributed clustering)

HEED[8]는 LEACH와 같은 기존 클러스터링 알고리즘의 단점을 개선한 기법이다. HEED는 CH 선출을 위한 1차 변수로 노드의 잔여 에너지를 사용하고, 만약 노드의 1차 변수가 동일할 경우 2차 변수인 노드의 통신 비용이 가장 낮은 노드가 CH로 선출된다. 통신 비용이란 어떤 노드가 CH가 되었을 때 클러스터의 일반노드들이 CH와 통신하는데 필요한 에너지 소모량을 종합한 것이다.

2.2 기존연구

WSN의 공격 노드에 대한 방어 연구로 암호키 기반 기법과 신뢰 평판 기법이 있다[5, 6, 9, 10]. SecLEACH[9]와 같은 암호키 기반 기법들은 센서가 소유한 암호키로 메시지를 암호화하여 외부 공격자를 방어하는 기법이고, 신뢰 평판 기법은 인접 센서 간 신뢰 수준을 주기적으로 평가한 후 신뢰할 수 없는 노드를 네트워크에서 배제하는 방어기법이다.

또한, 비정상적인 CH 선출 공격에 대한 대응연구들도 이러한 기법의 응용으로 제시되었다. 암호키 기반 기법의 응용으로 Buttyan 등[5]은 CH 선출 과정에서 교환되는 메세지를 암호화하여 공격자가 CH 선출 절차 및 결과를 확인하지 못하게 하는 비공개(private) 클러스터링 기법을 제안하였다. 그러나 이 기법은 내부 오염노드에 의한 공격에 취약할 뿐 아니라 오염노드는 자신을 CH로 선언할 수도 있다.

신뢰 평판 기법의 응용으로 Saidi 등[6]은 CH 선출 변수중 노드의 신뢰값에 높은 가중치를 두어 CH를 선출하는 기법을 제안하였으나 다수 오염노드들이 협력한 평가 조작에 취약하다. 예를 들어, 공격자는 오염노드끼리 신뢰 수준을 높게 평가하거나(false-praise attack), 정상노드는 낮게 평가하는 공격(bad-mouth attack)을 시도하여 오염노드가 CH로 선출될 가능성을 높일 수 있다[10].

III. 제안기법

3.1 아이디어

2.1에서 설명한 것과 같이, 모든 클러스터링 알고리즘들은 서로 다른 변수와 선출 공식에 따라 주기적으로 CH를 재선출하므로, 알고리즘 분석과 시뮬레이션을 통해 CH 선출 경향과 선출 통계를 확인할 수 있다. 따라서, 예상되는 CH 선출 통계와 실제 WSN 운영 과정에서 수집된 선출 통계가 특정 임계치 이상으로 차이가 난다면 비정상적인 CH 선출이 일어난 것으로 판단할 수 있다.

예를 들어, 5개의 노드가 클러스터를 구성하고 있는 WSN이 정상적인 환경에서 Fig.2.의 좌측 그래프와 같은 CH 선출 통계를 보였다고 가정하자.

이때 특정 라운드부터 5번 노드에 탐욕 공격이 발생했다면 통계는 Fig.2.의 우측 상단의 그래프처럼

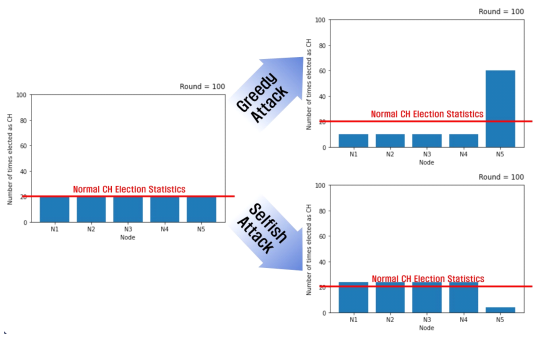

Fig. 2. Abnormal CH Election due to Attacks

변할 것이고, 이기적 공격이 발생했다면 우측 하단의 그래프처럼 변할 것이다. 그리고 정상적인 선출 통계를 뜻하는 붉은 선상을 기점으로 선출 통계가 이격된 정도를 보고 공격 여부를 판단할 수 있다.

3.2 제안기법 설계

제안기법은 비정상 CH 선출 공격인 탐욕 공격과 이기적 공격을 탐지하는 것을 목적으로 하며, Fig.3.과 같이 4단계로 동작한다.

① 안정된 CH 선출률 확인 및 임계값 설정

노드 i의 CH 선출률($R_{CH(i)}$)을 (식 1)이라 할때, 충분히 많은 선출 라운드를 수행하여 안정된 노드별 R_{CH}를 구하고 이를 $R_{CH}{}^{S}$이라 한다.

$$R_{CH(i)} = CH \text{ 선출횟수} \ / \ \text{라운드 수} \qquad (1)$$

임계값(T)은 $R_{CH}{}^{S}$와 실제 환경에서 구해진 R_{CH}의 차이를 바탕으로 비정상적인 CH 선출 여부를 판단하기 위한 기준값이다.

② CH 선출 및 결과 기록

기지국은 매 라운드마다 선출된 CH를 확인하여 각 노드의 R_{CH}을 계산한다. 그리고 n번째 라운드마다 계산한 R_{CH}를 $R_{CH}{}^{r(n)}$ 이라 한다.

③ CH 선출률과 임계값 비교

기지국은 n번째 라운드마다 (식 2)와 같은 조건식을 통해 비정상적인 CH 선출 여부를 판단한다.

$$\left| R_{CH}^{r(n)} - R_{CH}{}^{S} \right| > T \qquad (2)$$

만약 어떤 노드 i에 대해 조건식이 참이면 해당 노드의 실제 환경에서의 CH 선출률이 임계값을 벗어난 것을 의미하므로, 비정상적인 CH 선출이 발생한 것으로 간주할 수 있다.

④ 비정상적인 CH 선출 탐지

③의 조건식이 참일때 제안기법은 비정상적인 CH 선출 공격이 발생한 노드를 관리자가 알 수 있도록 탐지결과를 알려준다.

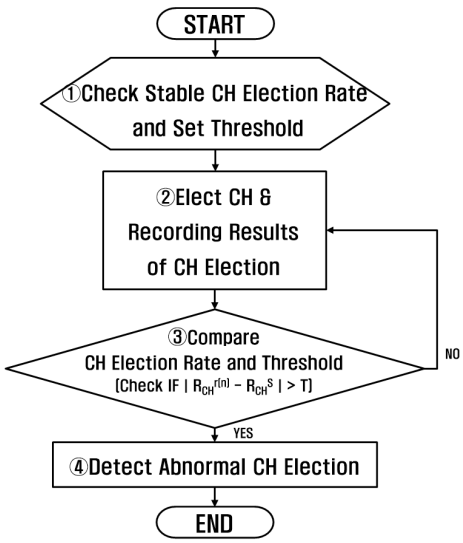

Fig. 3. Flowchart of the proposed method

IV. 실험결과

4.1 실험목적 및 방법

실험목적은 다양한 클러스터링 알고리즘이 운용되는 환경에서 비정상적인 CH 선출 공격이 수행될 경우 제안기법이 해당 공격을 탐지할 수 있음을 보이고 탐지결과를 분석하는 것이다.

실험환경과 방법은 다음과 같다. 먼저, 10개의 노드가 단일 클러스터를 구성하는 WSN을 모델링하고, 이중 하나를 오염노드로 선정한다. 노드 배치가 달라져도 공격 탐지가 가능한지 확인하기 위해 노드들은 매 실험마다 클러스터 내에서 랜덤 배치한다.

그리고 제안기법이 다양한 클러스터링 알고리즘에서 유효함을 증명하기 위해 LEACH, HEED를 고려하여 CH 선출 알고리즘을 Python으로 구현하였다. LEACH와 HEED는 CH 선출에 서로 다른 변수를 사용하며, 다른 연구에서도 자주 인용되는 보편적인 알고리즘으로써 본 연구에서도 참고하였다.

각 알고리즘에서 탐욕 공격, 이기적 공격 케이스는 다음과 같이 구현하였다. LEACH에서 오염노드가 탐욕 공격 수행시 CH 선출 변수는 난수가 아닌 0인 고정값을 갖게 되고, 이기적 공격이 발생하게 되면 1인 고정값을 갖는다. HEED에서 오염노드가 탐욕 공격 수행시 노드의 잔여 에너지는 초기 에너지 값으로 고정되며, 이기적 공격 수행시 잔여 에너지는 소진된 것처럼 알고리즘을 속이도록 설계하였다.

일정한 선출 통계를 기반으로 공격을 탐지하는 제안기법 특성상, 임계값 설정에 따라 선출 통계가 안정적이지 않은 초기 라운드에서는 정상적인 CH 선출도 공격으로 오탐할 수 있다. 또한 많은 라운드가

Table 2. Average of attack detection round in case of abnormal CH election attack

Clustering algorithm	Attack case	Threshold (T)	Round of starting attack				
			100	500	1000	1500	2000
LEACH	Greedy attack	0.015	101.07	508.12	1016.17	1525.11	2033.10
		0.010	101.04	505.12	1011.11	1516.07	2022.09
		0.005	failure	502.09	1005.10	1508.10	2011.12
	Selfish attack	0.015	116.56	587.56	1176.16	1763.80	2351.90
		0.010	110.80	554.90	1110.80	1665.79	2222.23
		0.005	failure	526.34	1052.00	1578.00	2104.57
HEED	Greedy attack	0.015	101.12	507.92	1016.38	1525.00	2033.36
		0.010	100.65	505.08	1010.86	1516.34	2021.83
		0.005	failure	502.33	1005.11	1507.98	2010.73
	Selfish attack	0.015	118.16	588.38	1182.21	1775.88	2387.10
		0.010	111.07	558.68	1116.84	1671.74	2233.09
		0.005	failure	526.90	1055.76	1582.07	2108.58

지나 선출 통계가 안정화된 환경에서는 탐욕 및 이기적 공격으로도 R_{CH}가 크게 변하지 않아 탐지가 늦어질 수 있다. 본 연구에서는 이러한 초기 라운드에서의 오탐문제와 임계값 변화에 따른 탐지속도 변화를 확인하기 위해 임계값을 0.005, 0.010, 0.015로 다양하게 설정하였다.

3장에서 밝힌 바와 같이 R_{CH}^{S}는 충분히 많은 수의 라운드가 필요하므로, 실험에서는 1000 라운드 시점의 R_{CH}를 R_{CH}^{S}로 설정하였다. 그리고 해당 라운드 전·후로 하여 탐지가 정상적으로 이루어지는지를 확인하기 위해 공격 시작 라운드는 100, 500, 1000, 1500, 2000번째 라운드로 설정하였다.

끝으로 탐지성능의 일관성 확인을 위해 100회 실험을 통해 공격 탐지 라운드의 평균값을 측정한다.

4.2 평가 및 분석

탐지 라운드의 평균값은 Table 2.와 같으며 실험 분석 결과는 다음과 같다.

첫째, 제안기법은 두 가지 클러스터링 알고리즘에서 탐욕 공격과 이기적 공격을 모두 탐지하였다. Table 2. 빨간색 테두리 내 값은 LEACH에서 100번째 라운드부터 탐욕 공격이 발생하였을 때(임계값 = 0.015) 평균 101.07번째 라운드에 공격을 탐지했다는 의미이다. 즉, 공격 발생 시점으로부터 약 1라운드 뒤 공격을 탐지한 것이다.

둘째, 예상했던 바와 같이 임계값을 작게 설정할수록 전반적인 공격 탐지는 빨라졌으나, 너무 작게 설정할 경우 초기 라운드에서의 정상적인 CH 선출을 공격으로 오탐하는 경우가 있었다. Table 2. 파란색 테두리안 failure는 100번의 실험에서 모든 정상적인 CH 선출을 공격으로 오탐한 것을 의미한다.

셋째, 임계값이 동일하게 설정되었을 때, 전체적으로 탐욕 공격보다 이기적 공격의 탐지가 늦은 경향이 있었다. 이는 특정 노드가 CH 선출을 반복할 경우의 R_{CH} 변화량보다 CH 선출을 기피할 경우의 R_{CH} 변화량이 더 작기 때문으로 판단되며, 따라서 이기적 공격에 대한 탐지속도를 향상시키기 위해선 임계값을 더 작게 설정할 필요가 있다.

V. 결 론

본 연구는 비정상 CH 선출 공격인 탐욕 및 이기적 공격을 탐지하는 통계적 기법을 제안하였으며, 실험을 통해 제안기법의 유효성과 탐지성능을 보였다.

제안기법은 안정된 CH 선출 통계와 실제 통계의 차가 임계치를 넘어설 경우 공격을 탐지하므로, 암호키 기반 방식과 같은 기존 방어기법과 함께 상호 보완적으로 사용할 수 있다. 예를 들어 암호키 기반 기법으로 외부 공격자를 방어하고, 제안기법으로 내부 공격자의 비정상적인 CH 선출을 방어할 수 있다.

향후 연구계획으로, 제안기법은 탐지를 기지국에서 수행하므로 공격방어를 위해 센서의 추가적인 리소스를 소모하지 않으므로, 제안기법의 에너지 효율 실험을 통한 효과 검증을 수행할 예정이다.

References

[1] T. Rault, A. Bouabdallah and Y. Challal, "Energy efficiency in wireless sensor networks: A top-down survey", Comput.

Netw., vol. 67, pp. 104-122, Jul. 2014.
[2] M. M. Zanjireh and H. Larijani, "A survey on centralised and distributed clustering routing algorithms for WSNs", Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring), pp. 1-6, May. 2015.
[3] O. Boyinbode, H. Le, A. Mbogho, M. Takizawa and R. Poliah, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Proc. 13th Int. Conf. Netw.-Based Inf. Syst., pp. 358-364, Sep. 2010.
[4] H. Rifà-Pous and J. Herrera-Joancomartí, "A fair and secure cluster formation process for ad hoc networks," Wireless Personal Communications, vol. 56, no. 3, pp. 625-636, Feb. 2011.
[5] L. Buttyan and T. Holczer, "Private cluster head election in wireless sensor networks", Proc. IEEE 6th Int. Conf. Mobile Adhoc Sensor Syst., pp. 1048-1053, Oct. 2009.
[6] A. Saidi, K. Benahmed and N. Seddiki, "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks," Ad Hoc Networks, Vol. 106, pp. 102215, Sep. 2020.
[7] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci., pp. 10-20, Jan. 2000.
[8] O. Younis and S. Fahmy, "HEED: A hybrid energy-efficient distributed clustering approach for ad hoc sensor networks", IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366-379, Oct. 2004.
[9] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab and A. A. F. Loureiro, "SecLEACH－A random key distribution solution for securing clustered sensor networks", Proc. 5th IEEE Int. Symp. Netw. Comput. Appl., pp. 145-154, Jul. 2006.
[10] T. Suh and Y. Cho, "An enhanced trust mechanism with consensus-based false information filtering algorithm against bad-mouthing attacks and false-praise attacks in WSNs," Electronics, vol. 8, no. 11, pp. 1359-1375, Nov. 2019.

〈저자소개〉

김 수 민 (Sumin Kim) 정회원
2016년: 해군사관학교 해양학과 (이학사)
2016년~현재: 대한민국 해군 대위
2021년~현재: 국방대학교 국방관리대학원 사이버전협동전공 석사과정
〈관심분야〉 무선네트워크, 사이버보안, 정보보호

조 영 호(Youngho Cho) 종신회원
1998년: 공군사관학교 산업공학과 (공학사)
2006년: 연세대학교 컴퓨터산업시스템공학 (공학석사)
2013년: University of Maryland, College Park, Electronical and Computer Engineering 전공 (공학박사)
2017년~현재: 국방대학교 국방관리대학원 컴퓨터공학/사이버전협동전공 부교수
〈관심분야〉 네트워크 보안, 스테가노그래피 봇넷, 신뢰 메커니즘, 블록체인, AI 보안 등