# 네트워크 중심전을 위한 센서간의 상호인증기법

양호경* · 차현종* · 신효영** · 유황빈***

## 요 약

정보기술의 발전에 따라 전쟁의 양상이 무기체계 위주 재래식 전쟁에서 네트워크를 기반으로 한 네트워크중심전(NCW)로 바뀌어 가고 있다. NCW(네트워크중심전)는 컴퓨터의 자료 처리 능력과 네트워크로 연결된 통신 기술의 능력을 활용하여 정보의 공유를 보장함으로써 성공적, 효과적인 작전 수행을 위해서 작전참여 구성원들의 공조활동방식의 상호교류를 통해서 군사력의 효율성을 향상 한다는 개념으로, 우리 군에서도 정보통신 기술발전과 더불어서 각각의 개체들과의 상호 연결을 통해서 원활한 전장자원 정보를 공유하여 효과적인 전쟁을 하기 위한 방법들을 연구하고 있다.

본 논문에서는 센서 네트워크를 사전에 클러스터링 해 주고 클러스터 그룹에 CH(Cluster Header) 두어 네트워크를 구성하게 된다. 배치 이전에 BS(Base Station)와 센서 노드 사이에 인증서[9]를 제공하고 클러스터링 후 BS와 센서 노드간에 인증을 거치게 된다. 여기에 클러스터 헤더 간의 인증 기술을 추가시켜 센서노드의 파괴나 교체에 능동적으로 대응할 있다. 또한 두 번의 인증과정을 거치기 때문에 더 높은 보안성을 제공 할 수 있다.

# Mutual Authenticate Protocol among Sensor for Network Centric Warfare

Ho-Kyung Yang* · Hyun-Jong Cha* · Hyo-Young Shin** · Hwnag-Bin Ryou***

## ABSTRACT

As the network composed of numerous sensor nodes, sensor network conducts the function of sensing the surrounding information by sensor and of the sensed information. Our military has also developed ICT(Information and Communication Technology) along with the methods for effective war by sharing smooth information of battlefield resources through network with each object.

In this paper, a sensor network is clustered in advance and a cluster header (CH) is elected for clusters. Before deployment, a certificate is provided between the BS and the sensor nodes, and after clustering, authentication is done between the BS and the sensor nodes. Moreover, inter-CH authentication technique is used to allow active response to destruction or replacement of sensor nodes. Also, because authentication is done twice, higher level of security can be provided.

**Key words : Senser, Authenticate, NCW**

접수일(2012년 11월 30일), 수정일(1차: 2012년 12월 10일), 게재확정일(2012년 12월 11일)

* 광운대학교 방위사업학과
** 경북대학 컴퓨터정보과
*** 광운대학교 컴퓨터소프트웨어학과

# 1. 서 론

정보통신 기술의 발전에 따라 미래 전장 수행개념은 비접적, 비선형, 원거리 전투, 네트워크 중심 전쟁, 병렬, 동시・ 통합작전 그리고 효과 중심의 신속 기동전 형태로 변화하고 있다. 전쟁의 양상도 무기체계 위주의 재래식 전쟁에서 각 무기체계 및 관련 시스템이 서로 연결되어 있는 네트워크 중심전(NCW : Network Centric Warfare)의 개념으로 변하고 있다. 군에서는 임무의 특수성으로 인해 독자적인 전용 지휘통신망을 발전시키고 있었다. 새로운 정보기술의 발전은 21세기 변화된 형태의 전쟁을 수행하기 위해 군 정보통신분야의 적용이 필수적이며 이를 통해 전술적인 감시나 추적 또한 전장정보의 실시간 수집 등의 효과를 공유하여 조직화됨으로써 전투력 발휘효과를 극대화 시켜 효율적인 전쟁을 치르기 위해서 노력 하고 있다. 그러나 이러한 네트워크 발전과 같이 보안적인 위협도 늘어나고 있는 실정이다. 네트워크가 확장됨에 따라 공격할 수 있는 루트도 증가하게 되고 이동하는 데이터의 양도 증가함에 따라 유출되면 위험한 데이터의 양도 증가하게 된다. 단순한 데이터 유출을 위한 침입이 아닌 사이버전 양상의 네트워크상의 전쟁이 일어날 가능성도 날로 증가하고 있는 실정이다. 특히 군과 같은 정보와 데이터가 중요한 집단에서는 사소한 정보 유출도 큰 위험으로 나타날 수 있기 때문에 다른 네트워크 환경보다 보안을 중요시해야 한다.

미래 전장 수행개념은 비접적, 비선형, 원거리 전투, 네트워크 중심 전쟁, 병렬, 동시・ 통합작전 그리고 효과 중심의 신속 기동전 형태로 변화하고 있다. 이런 세계적인 발전방향에 부합하고 북한은 물론 다양한 미래의 위협에 능동적으로 대비하기 위하여 우리군도 장거리 정밀타격과 지 ・ 해 ・ 공 입체 고속능력을 향상시키고 생존성을 보장하기 위한 방향으로 전력구조를 발전시키고 있다. 이러한 혁신적인 발전과 더불어 군의 전쟁수행 환경도 빠르고 다양하게 변화하고 있다. 새로운 정보기술의 발전은 21세기 변화된 형태의 전쟁을 수행하기 위해 군 정보통신분야의 적용이 필수적이며 이를 통해 전술적인 감시나 추적 또한 전장정보의 실시간 수집 등의 효과를 공유하기 위하여 노력하고 있다. 이러한 NCW 환경에서의 중요한 하나의 부분으로 센서네트워크가 중요시 되고 있다.

센서 네트워크는 일반적으로 특정 지역의 많은 센서들이 무작위로 뿌려져서 대상에 대해 감지하고 감지된 데이터를 중앙의 BS로 전송하는 구조를 갖는다. 각 센서 노드가 다른 노드의 데이터를 중계해주는 기능을 한다는 점에서 기존의 모바일 Ad-hoc 네트워크의 한 특수한 형태로 인식하는 경우도 있지만 센서 노드는 일회성을 갖는 경우가 많아 가격도 매우 저렴하고 크기도 작아야 하며 작은 기억 공간, 제한된 계산 능력 등을 특성으로 하므로 사실상 Ad-hoc 네트워크 보안 제약 사항이 많다[1]. 센서 네트워크는 수많은 노드들이 감지된 정보를 BS에게 보내야 하므로 중복된 데이터도 많고 BS이 각각의 데이터를 일일이 취합하기에 어려움이 많을 뿐 아니라 불필요한 트래픽의 증가로 이를 중계해야하는 노드들에게 부담이 되어 수명을 줄이는 결과를 가져올 수 있으므로 중간에 Aggregator(또는 Gateway)를 두는 계층적 기반의 형태가 대부분이다. 센서 네트워크는 센서 노드들이 좁은 영역에 조밀하게 분포되고, Broadcast방식의 통신 방식을 사용하는 등의 특징을 가진다. 하나의 센서 노드가 통신하는 노드의 수가 하나가 아닌 다대다 통신인 그물망 통신(Mesh)으로 이루어지는 센서 네트워크에서는 노드들의 상호 인증과, 제한된 센서 자원을 이용하여 인증과 암호화에 사용될 암호 키 관리의 문제가 주요 이슈중에 하나이다[2]. 센서 네트워크는 네트워크가 갖는 기본적인 특성으로 인해 일반 네트워크보다 훨씬 보안에 취약하다는 특성을 갖는다. 특히 군과같은 보안이 중요한 집단에서는 이와같은 센서간의 상호인증과 보안이 더욱 중요하게 여겨지게 된다.

본 논문에서는 센서 네트워크를 사전에 클러스터링 해 주고 클러스터 그룹에 CH(Cluster Header) 두어 네트워크를 구성하게 된다. 배치 이전에 BS(Base Station)와 센서 노드 사이에 인증서[9]를 제공하고 클러스터링 후 BS와 센서 노드간에 인증을 거치게 된다. 여기에 클러스터 헤더 간의 인증 기술을 추가시켜 센서노드의 파괴나 교체에 능동적으로 대응할 있다. 또한 두 번의 인증과정을 거치기 때문에 더 높은 보안성을 제공 할 수 있다.

# 2. 관련연구

### 2.1 NCW (Network Centric Warfare)

정보화시대에 들어서면서 미국은 군사혁신을 통하여 정보기술을 비롯한 현 시대의 기술적 성과를 군사부문에 반영하고자 노력하였는데, 그 산물 중의 하나가 네트워크 중심전이다. 현대의 발전된 컴퓨터 기술 및 네트워크가 군대에 도입되어 지휘통제통신체계의 혁신이 일어날 수 있었고, 이를 통하여 모든 부대와 각 개인들을 네트워크로 연결한다는 개념이 가능하게 되었기 때문이다. 무기체계적인 면에서도 정밀타격능력의 발전으로 인하여 이제는 표적의 위치나 형태를 식별하기만 하면 즉각적인 제압이 가능하고, 부대의 기동성이 증대되어 물리적 공간과 시간의 제한사항이 축소되고 있다. 따라서 네트워크 중심전은 이러한 현대 군대의 발전성과를 통합할 수 있는 하나의 개념으로서 제시되었다[2].

### 2.2 TICN(Taciocal Information and Communication Network)

TICN은 네트워크 중심전에서 정보의 원활한 소통을 위해 센서체계, 지휘통제체계, 타격체계에게 고속 대용량의 정보통신로를 제공하는 것을 목적으로 하는 체계이다. TICN의 부체계로서는 기간망 전송체계, 기간망 교환접속체계, 망제어체계, 전투무선망체계, 전술이동통신체계로 구분된다. 이중 전술이동통신체계는 지휘소 및 주변지역, 원격지원의 전술용 다기능 단말기 가입자에게 음성, 데이터 및 멀티미디어 서비스를 통해 이동통신 수단을 지원해주는 것을 목표로 한다[3].


(그림 1) TICN 체계 개념도

### 2.3 LECH-CE

LEACH-C와 같은 중앙 집중형 기법에서 매 라운드마다 모든 노드들이 자신의 현재 남아있는 에너지 레벨을 BS에게 전송해야 한다는 문제점을 해결하기 위해 클러스터 헤드와 일반노드의 에너지 소비량을 예측하는 기법을 제안하였다. 각각의 에너지 소비량을 예측하여 클러스터 헤드였던 노드는 클러스터 헤드의 소비량 만큼 가지고 있는 에너지를 차감하고 일반 노드는 일반 노드의 소비량 만큼 가지고 있던 에너지를 차감하여 다음 라운드의 클러스터링을 위한 정보로써 이용될 수 있도록 하였다. 기존 LEACH-C에 비해 좀 더 네트워크의 생존 시간을 늘릴 수 있었고 총 사용된 에너지의 양도 줄일 수 있었다[4][5].

### 2.4 μTESLA

μTESLA는 TESLA방식을 센서 네트워크에 적용 가능하도록 응용한 것으로 인증키 생성이나 브로드캐스팅 생성 방식은 TESLA와 유사하다. 이 방식은 key를 알고 있는 센서 노드에 의해 해석이 가능하도록 하는 대칭키 기반의 인증 방식을 제공한다. BS에서 키 체인을 생성하여 유지 시켜주고 해시 체인을 이용하여 효과적으로 데이터 인증을 제공할 수 있다. 중간에 패킷의 분실이 발생하더라도 다음 패킷을 통해 이전 패킷들을 검증 할 수 있다. 이 방식은 두 노드 사이에 공유하여야 하는 비밀키의 노출을 최대한 늦춤으로써 비대칭 암호키 방식을 사용한 듯한 효과를 누릴 수 있다. 하지만 인증하여야 하는 노드 수가 많아질 경우에는 지연 시간이 길어지는 단점을 가지고 있다. 전송하려는 데이터의 무결성이나 인증을 할 때 많이 사용되는 방식이다[6][7].

## 3. 제안기법

본 기법의 전체적인 동작방법은 다음과 같이 구성되어 있다.

가. 센서 노드들을 배치하기 이전에 BS과 센서 노드들에게 인증서와 인증서 리스트를 포함시켜서 배치

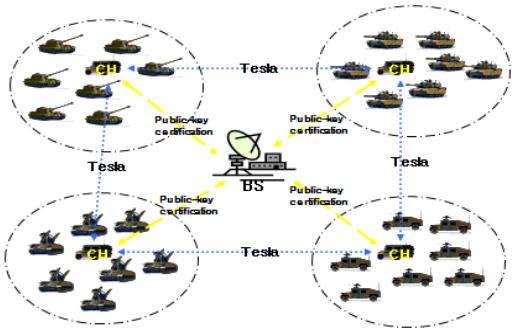
나. ECSE[8] 방식을 사용하여 CH를 선출하고 네트워

크를 구성

다. CH로 선출된 센서 노드는 BS에게 보고를 하고 BS에서는 key값을 생성해서 CH에게 배포

라. BS에서 생성해준 key값과 인증서 리스트를 가지고 μTESLA 방식으로 주변의 CH끼리 인증

마. 인증 과정이 끝나고 인증이 성공되면 서로의 CH가 속해있는 그룹을 인증




(그림 2) 네트워크 구성도

(그림 2)과 같이 전체적인 센서 네트워크의 구조가 구성되어 있다. 전체적인 동작 단계를 살펴보면 우선 센서 노드들을 배치해 주기 이전에 인증서와 인증서 리스트를 포함 시킨다. BS에서는 이 인증서 리스트를 기반으로 초기에 센서 노드들을 인증시켜준다[7].

ECSE Protocol 기법을 사용하여 CH를 선출하고 네트워크를 구성하여 준다. CH가 선출된 이후에는 BS과 센서 노드사이에 직접적으로 인증은 하지 않고 CH를 거쳐서 인증을 한다. CH가 선출되면 BS와 통신을 하여 이것을 보고하게 되고 BS은 인증서 리스트를 확인하여 올바른 CH인지를 인증한다. 정당한 CH로 판명이 되면 BS은 key값을 생성하여 보내주게 된다. BS과 CH의 인증과정은 한번으로 끝나는 것이 아니라 BS에서는 인증된 상태를 확인하기 위해 주기적으로 인증서를 발행시켜주고 CH는 자신이 가지고 있는 인증서리스트와 내용을 비교하여 BS에서 온 리스트가 맞는지 확인하게 된다. CH는 BS이 생성하여 보내준 key값을 가지고 자신의 주변의 CH와 TESLA 인증기법을 사용하여 인증을 하게 된다. 이 인증 기법을 사용하여 한 번으로 인증을 끝마치는 것이 아니라 주기적으로 인증을 하여 주변의 CH가 수명이 다하거나 외부의 공격을 받아 제대로 된 역할을 수행할 수 없을 때 BS에 이 정보를 보고를 하여 새로운 CH가 선출되게 할 수 있다. 또한 CH의 파괴로 인해 BS에게 전달할 수 없었던 센서 노드들도 자신이 속해 있는 CH에게 인증된 다른 CH에게 데이터를 전달하여 BS에게 정보를 전달 할 수 있다. 이 기법을 사용하게 되면 두 번의 인증단계를 거치기 때문에 보안성을 높일 수 있다. 다른 CH를 가지고 있는 그룹에 데이터를 전송할 때 CH 간의 인증이 되어 있으므로 안심하고 데이터를 전송 할 수 있다. 또한 CH가 다른 그룹을 인증할 때 BS을 따로 거치지 않기 때문에 전송에 의한 전력량 등의 자원의 낭비를 막을 수 있고 시간적인 효율성도 높일 수 있을 것이다[9].

## 4. 실험 및 성능 분석

본 장에서는 알고리즘 분석을 하고 이 모델을 제안된 방법에 적용하여 관련연구와 비교 분석한다.

### 4.1 실험환경

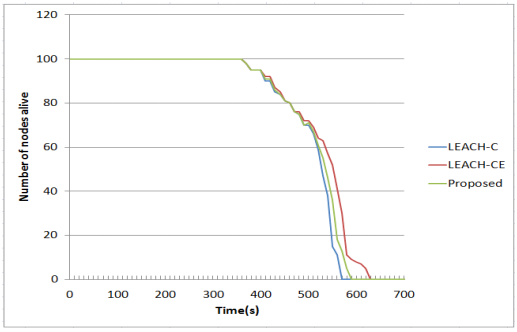
실험은 리눅스상에서 NS-2 네트워크 시뮬레이터를 사용하였고, LEACH-CE의 모듈은 MIT의 uAMP 프로젝트의 일환으로 개발된 LEACH-C의 소스를 다운 받아 구현된 것을 사용하였으며, 이를 수정하여 제안모델을 구현하였다.

<표 1> 실험환경

| 요소 | 정의 값 |
|---|---|
| 토폴로지 노드수 | 100 개 |
| 센서 필드의 면적 | 100m X 100m |
| 데이터 전송속도 | 1Mbps |
| 데이터 전송지연 | 1ps |
| 전파속도 | 3 X $10^{8}$m/s |
| 안테나 | 전방향 안테나(Omni antena) |
| 인터페이스 | 914MHz의 Lucent WaveLan DSSS(Direct-Sequence Spread-Spectrum |

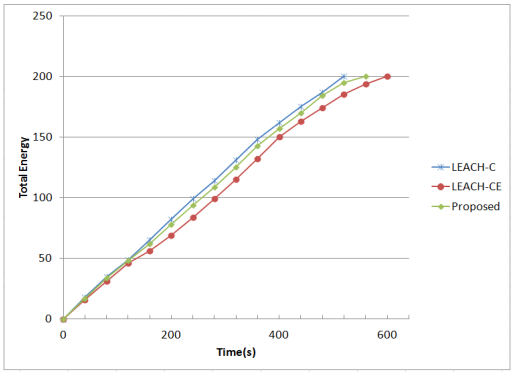
### 4.2 실험결과

실험에서 사용되는 네트워크 토폴로지는 동일한 면적에서 각각 50, 100, 150, 200개의 노드가 임의의 위치로 분포되어 고정되어있다고 가정한다. 또한, LEACH_CE에서 실험을 통해 얻어낸 최적의 예측주기인 8라운드 예측주기를 적용하였다. 센서네트워크의 네트워크 생존시간은 노드 중 처음으로 에너지 소모를 다하여 네트워크에서 사라지는 시간(FND:First Node Diest)과 마지막 노드의 사라지는 시간(LND:Last Node Diest)로 나뉜다.




(그림 3) 센서의 생존시간

(그림 3)은 시간에 따른 생존 노드의 수를 비교한 그래프이다. FND는 비슷하나 LND는 LEACH-CE보다는 다소 빨랐다. 이는 인증을 위한 처리 때문이라는 것을 알 수 있다.




(그림 4) 총 에너지량

## 5. 결 론

센서 네트워크에서는 노드들의 상호 인증과, 제한된 센서 자원을 이용하여 인증과 암호화에 사용될 암호 키 관리의 문제가 주요 이슈 중에 하나이다. 센서 네트워크는 네트워크가 갖는 기본적인 특성으로 인해 일반 네트워크보다 훨씬 보안에 취약하다는 특성을 갖는다. 특히 군과같은 보안이 중요한 집단에서는 이와같은 센서간의 상호인증과 보안이 더욱 중요하게 여겨지게 된다. 이 논문에서는 초기에 센서 노드들을 배치시키기 전에 BS(Base Station)과 센서 노드가 인증서와 인증서 리스트를 가지고 있다. CH를 선출하여 BS과 인증을 하고 이 인증이 완료되면 BS이 key값을 생성하여 CH에게 주게 된다. 이 key값을 가기고 다른 그룹에 CH와 TESLA인증기법을 가지고 인증을 하게 된다. 이 기법은 CH가 외부나 내부의 공격자로부터 공격을 당하여 파괴되었을 때 주기적으로 다른 CH와의 통신을 해주기 때문에 이것을 파악 할 수 있다. 또 자신의 CH와 통신이 안 될 경우 자신이 속한 그룹과 인증된 다른 그룹의 CH에게 전송을 해주어서 데이터를 전송하게 된다. 이 기법은 두 번의 인증을 거치기 때문에 전반적인 네트워크의 보안성을 높여줄 수 있다. 또 다른 CH을 인증을 할 때 BS을 거치는 과정이 없기 때문에 자원의 낭비를 막을 수 있고 시간적인 효율성도 높일 수 있다

## 참고문헌

[1] 나재훈, 채기준, 정교일, “센서 네트워크 보안 연구 동향”, 전자통신동향분석 제20권 제1호 통권91호, pp.112-122, 2005 .

[2] 배달형, 조용건 ,“NCW 컴퓨터네트워크작전(CNO)의 작전적 원리와 한국군의 발전방향”, 국방연구 제52권 제2호, 국방대학원안보문제연구소, pp.39-67, 2009.

[3] 고석주, “ 소부대 지휘자 통신체계 구현방안 연구”, 배재대학교 정보통신대학원, 2005.

[4] T. Murata and H. Ishibuchi, “Performance evaluation of genetic algorithms for flowshop schedul

ing problems", Proceedings of the 1st IEEE Conference Evolutionary Computation Vol. 2, pp.812-817, 1994.

[5] 주현규, 한인성, 김진묵, 유황빈, "중앙 집중형 계층적 라우팅 프로토콜에서의 예측을 통한 효율적인 클러스터 설정 기법", JCCI 2006, 2006.

[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. of the 7th ACM/IEEE International Conference on MobiCom, 2001.

[7] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," In Proc. of the 10th ACM CCS'03, 2003.

[8] Trong Thua Huynh, Choong Seon Hong, "Saving Energy using Intra-Cluster Routing in Wireless Sensor Networks", 한국정보처리학회 추계학술발표대회 논문집 제11권 제2호, 2004.

[9] 양호경, 차현종, 유황빈, 조용건, "군 작전 환경에서의 센서간의 상호인증기법", 정보보안 논문지 제9권제3호, pp.19-24, 2009.

## [저자소개]

**양 호 경 (Ho-Kyung Yang)**

2005년 광운대학교
컴퓨터소프트웨어학과 공학사
2007년 광운대학교
컴퓨터과학과 공학석사
2010년 광운대학교 방위사업학과
공학석사
2012년 광운대학교 방위사업학과
박사과정

email : porori2000@nate.com

**차 현 종 (Hyun-Jong Cha)**

2005년 광운대학교
컴퓨터소프트웨어학과 공학사
2008년 광운대학교 컴퓨터과학과
공학석사
2011년 광운대학교 방위사업학과
공학석사
2012년 광운대학교 방위사업학과
박사과정

email : chj826@kw.ac.kr

**신 효 영 (Hyo-Young Shin)**

1986년 광운대학교 전자계산학과
이학사
1988년 광운대학교 전자계산학과
이학석사
1998년 광운대학교 전자계산학과
이학박사
1988년~1993년 ㈜LG소프트 연구원
1994년~현재 경복대학교
컴퓨터정보과 부교수

email : hyshin@kyungbok.ac.kr

**유 황 빈 (Hwang-Bin Ryou)**

1968년 인하대학교 전자공학과 학사
1975년 연세대학교 전자공학과
공학석사
1984년 경희대학교 전자공학과
공학박사
1981년~현재 광운대학교
컴퓨터소프트웨어학과 교수

email : ryou@kw.ac.kr