네트워크중심전(NCW)에서 WSN 정보누락의 위험도 및 방지 방안

An information security of wireless sensor network for NCW(Network Centric Warfare)

이명종, 김세헌
산업 및 시스템공학과, 대전시 유성구 구성동 373-1 KAIST

Abstract

현대 및 미래전은 네트워크가 중심이 된 전쟁, 즉 NCW(Network Centric Warfare)가 수행될 것이며 대항국에 비해 신속하고 다량의 정보 획득이 보장되어야 한다. 이런 NCW을 효과적으로 수행하기 위해 대규모의 센서 노드를 손쉽게 배치하여 정보를 획득할 수 있는 통신 네트워크인 WSN(Wireless Sensor Network)이 널리 사용될 것이다. 하지만 WSN은 정보누락, 경로변경, 도청 등 많은 악의적인 공격 위험성에 노출되어 있다. 따라서 위험에 대한 대처 방안이 마련되지 않는다면 우군을 공격하는 경우가 발생할 수 있고, 지휘결심의 혼선을 초래하게 될 것이다. 이 논문에서는 현대전에서 Military WSN망에서 가장 위협이 되는 공격유형이 무엇인지를 조사하고, 가장 위험성이 높은 정보 누락을 해결할 수 있는 알고리즘을 제시하고자 한다.

1. 개요

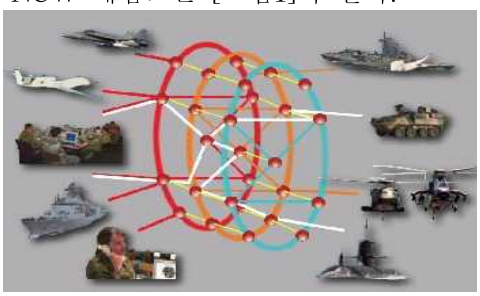
최근 인터넷등 IT기반이 발전을 기반으로 우리 일상생활은 많은 변화를 가져왔다. 일반 생활에서는 인터넷의 급속한 발전을 통해 통신, 정보 수집, 멀티미디어, 화상회의 등 열거할 수 없을 정도로 생활의 방식이 많이 변화되어 왔으며, 'Know-How'보다는 'Know-Where'가 더 중요하다고 이야기 할 정도로 신속하고 정확한 정보를 얼마나 많이 획득하고 있는가가 그 사람의 능력을 대변해 주고 있다고 한다. 이런 IT기반의 발전은 일반사회 뿐만아니라 군사분야에도 적용되어 사용되고 있는데, 그 대표적인 부분이 현대 및 장차전의 중심이 될 NCW(Net work Centric Warfare)일 것이다. 대항국에 비해 빠르게 정보를 획득할 수 있는 체계를 만들 수 있느냐가 전쟁의 승패를 좌우할 수 있다는 것이다. 이런 전쟁의 정보를 효과적이고 안전하게 획득할 수 있게끔 제시되고 있던 것이 Wireless Sensor Network이다. 이런 WSN은 적은비용, 저출력, 작은크기의 장비를 사용하며, 특히 통신 infrastructure가 구성되어 있지 않은 곳에서 ad-hoc wireless network를 이용하여 정보를 획득할 수 있게 된 것이다. 사실 이런 WSN은 전쟁지역 감시와 같은 군사부분 적용이 동기부여가 되어 개발[1]되었지만, 환경감시, Health-care, home-automation 등 많은 사회부분에 적용이 되기 시작하고 있다. 이렇듯 사회 전반에 사용되기 시작하면서, 악의적인 생각을 가진 사용자들로 인해 정보누락, 정보변경 등 많은 공격이 생겨나는 등 위험성도 증대되고 있다.

이 논문에서는 WSN에서 일어나고 있는 공격유형인 정보누락, 경로변경, 도청, data 변조에 대해 군 내부망의 특성에 따른 위험성을 AHP 기법의 중요도 평가 방법을 통해 조사하고, 가장 위험성이 큰 정보누락에 대응할 수 있는 절차를 제시하고자 한다.

2. Related work

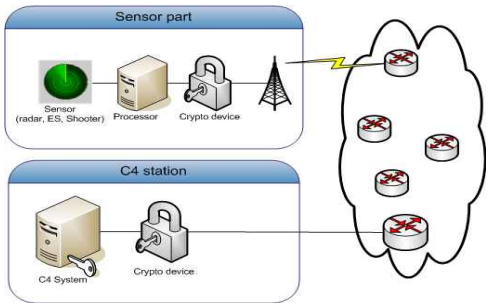
2.1. NCW 및 군 네트워크 특성

과거의 전쟁은 자신이 획득한 정보만을 바탕으로 전쟁을 수행했다면, 현대전은 다른 사람의 정보를 네트웍을 통해 전송받아, 비록 내가 보고 있지 못하는 표적이라 하더라도 유효한 표적에 대해 공격을 할 수 있는 시대가 되었다.[2] 이렇게 네트웍을 통해 전쟁을 수행하는 것이 NCW라고 할 수 있으며, NCW 개념도는 [그림1]과 같다.



[그림1] NCW 개념도

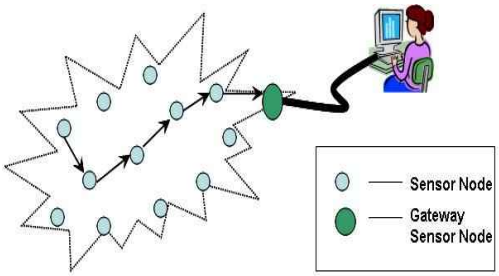
또한, 각각의 Sensor 들은 더 작은 Sensor들을 이용하여 정보를 획득할 수 있을 것이다. 이런 군 네트워크망에서 일반 상용망과 가장 큰 차이점은 [그림2]에서 보는 바와 같이 각각의 센서는 자체의 암호장비를 통해 정보를 암호화 하여 송신하고 복호화하여 관련 내용을 파악한다는 것이다. 그 이유는 관련정보의 중요성과 신뢰성을 향상시키기 위해서 이다. NCW에서도 정보의 신속성보다는 신뢰성이 뒷받침된 정확한 정보가 필요하다.



[그림2] 군 네트워크 시스템 구성도

2.2. Wireless Sensor Network

WSN은 다른 지역에 있는 온도, 소리, 진동, 압력이나 오염물질과 같은 물리적이거나 환경적인 상태를 협력 모니터를 위해 센서를 사용하는 독립적으로 공간에 분포되어 있는 장치로 구성된 무선네트워크이다.[3][4] 게다가 하나 또는 그 이상의 센서노드는 일반적으로 무선통신장치를 가지고 있으며, 작은 제어기, 적은 에너지를 사용하기 때문에 작은 센서를 만들 수 있다. 또한 WSN은 배터리, 계산능력, 메모리용량 및 짧은 통신거리로 인해 Sensor network는 [그림3]에서 보는 바와 같이 각각의 센서가 multi-hop routing algorithm(여러 노드는 데이터를 Base station 으로 전송)을 사용하는 wireless ad-hoc network 로 구성되어 있다.



[그림 3] Multi-hop WSN Architecture

WSN의 이런 구조를 통해 지휘소에 있는 지휘관은 전방 전투에 직접 참여하지 않아도, 전방 병사의 소형 카메라를 통해 획득된 정보를 여러단계의 협력 전송을 통해 보고가 되면, 이런 보고를 바탕으로 지휘관은 적절한 조치를 신속하게 내릴 수 있게 될 것이다.

이렇듯 유용하게 사용될 수 있는 Wireless ad hoc network인 WSN은 Sinkhole, Wormhole과 같은 경로 변경, 해당 정보를 삭제시키는 정보누락, 내부 정보를 변경하여 data의 무결성을 회손시키는 data 변조 공격 및 단순히 내용을 취하는 도청 등과 같은 공격 등에 노출되어 있으며, 이외에도 알려지지 않은 많은 공격에 위협을 받게 될 것이다. 이에 대응하가 위하여 IDS(Intrusion Detection System)등과 같은 대응책이 연구되고 있다.

2.3. AHP 기법

AHP는 계층적 구조를 가지는 문제에서 주관적인 평가 내용을 재정리하여 좀 더 객관적이고 체계적인 결과를 얻기 위한 방법으로, 의사결정자가 두 개씩 짝을 지어 상대적인 비교를 하는 경우에 좀 더 의미있는 결론을 많이 제공할 수 있다는 점에 착안하여 쌍대비교법(Pairwise Comparison)을 통해 의사결정자로부터 얻은 정보를 기초로 하여 가장 바람직한 결론을 도출하는 것이다.[5] 이 쌍대비교법은 서술적 표현의 9점 척도 스케일[표1]을 이용하여 평가하여 상대적인 중요도를 평가. 종합화 과정 및 일관성비율(CR:Consistency Ratio)을 통한 일관성 검증으로 각 기준의 중요도를 평가하게 된다.

서술적 표현	점수
훨씬 더 중요하다	9
	8
매우중요하다	7
	6
상당히 중요하다	5
	4
좀더 중요하다	3
	2
같다	1

[표1] 쌍대비교를 위한 9점 척도 스케일

3. NCW내 WSN망 공격위험 중요도 조사 결과

3.1. 일반사항

NCW상황하에서 WSN망에서 일어날 수 있는 공격위험 중요도를 평가하기 위하여 [표2]와 같은 군내 네트워크 관련부서 인원을 대상으로 조사하였으며, 총 125명으로 대상으로 실시하여 97명이 설문에 응답(응답률 77.6%)하였다.

응답자	125명 질의 97명 응답(응답률 77.6%)				
조사대상	경력 / 대상	1년미만	2~5년	5년이상	계
	일반인	1	7	2	10
	위관이하	5	24	51	80
	영관이상		1	6	7
	계	6	32	59	**97**

[표2] 표본집단

3.2. 조사결과

AHP 9점척도 스케일을 통해 정보누락, 정보도청, 경로변경, 도청의 공격을 대상으로 각각의 설문응답자의 쌍대비교 및 중요도합을 1로 규격화 한 종합화(Synthesization) 결과 일관성비율(CR=CI(일관성지수)/RI)이 10% 이하인 응답자(그림 4 : 표본 A 분석) 만을 대상으로 중요도를 평균한 결과는 [표3]과 같다. 이때 사용된 RI(Random Index)는[5]에 의해 [표4]를 적용하였다.

1. 쌍대 비교

	정보누락	data변조	경로변경	도청
정보누락	1.00	3.00	5.00	9.00
data 변조	0.33	1.00	4.00	8.00
경로변경	0.20	0.25	1.00	3.00
도청	0.11	0.13	0.33	1.00
	1.64	4.38	10.33	21.00

2. 종합화 과정

	정보누락	data변조	경로변경	도청	평균중요도
정보누락	0.61	0.69	0.48	0.43	0.55
data 변조	0.20	0.23	0.39	0.38	0.30
경로변경	0.12	0.06	0.10	0.14	0.10
도청	0.07	0.03	0.03	0.05	0.04
					1.00

3. 일관성 검증

3.1. 일관성 계산 1차

	정보누락	data변조	경로변경	도청	합	결과
정보누락	0.55	0.90	0.52	0.40	2.37	4.30
data 변조	0.18	0.30	0.42	0.35	1.25	4.18
경로변경	0.11	0.07	0.10	0.13	0.42	4.03
도청	0.06	0.04	0.03	0.04	0.18	4.04

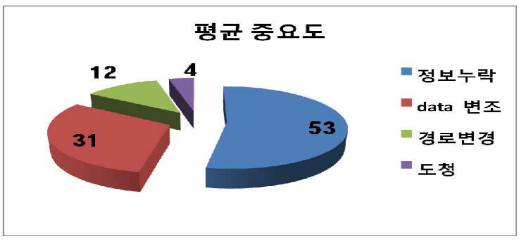
3.2. 일관성 지수(CI)=(λ-n)/(n-1) 0.05

λ= 4.14

3.3. 일관성 비율 0.05 RI(일관성 비율)=0.9

4. 결과 : 모순 5%로 사용 가능한 데이터

[그림4] 표본A 응답 분석 결과



[표3] 중요도 평가 결과[84명 자료 사용]

비교대상	3	4	5	6	7	8
RI	0.58	4	1.12	1.24	1.32	1.41

[표4] 일관성 검정을 위한 RI(Random Index)

[표3]에서 보는 바와 같이 군 네트워크 전문가 층에서는 WSN에서 일어날 수 있는 공격 중 NCW 작전 수행에 가장 위험한 공격을 중간 연결노드에 의해 수행되는 정보 누락으로 보고 있었으며, 이에 대한 대응책 개발이 필요하다고 응답했다.

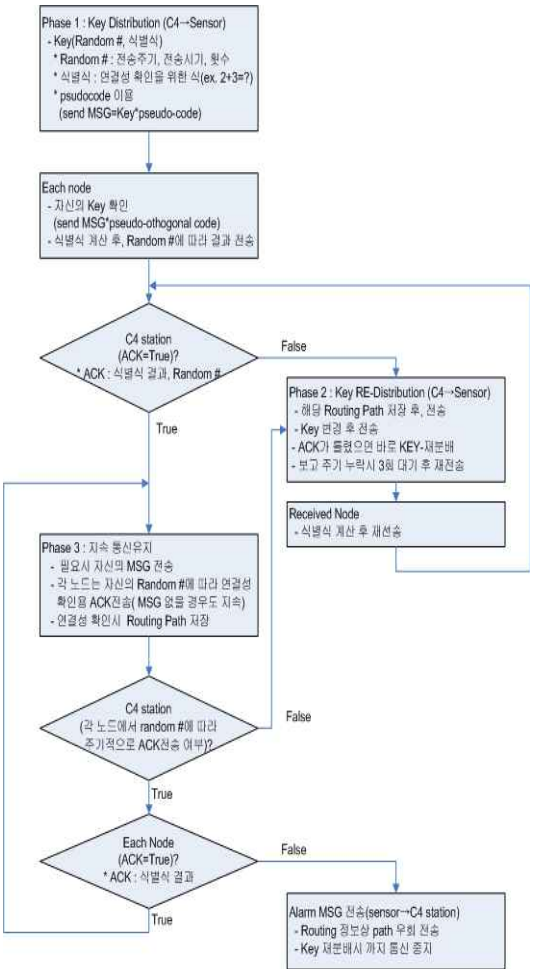
4. 정보누락 대응 절차

4.1. 기본개념

NCW와 같은 군 통신망은 각각의 Sensor에서 획득된 정보는 우선 지휘부인 C4(Command, Control, Communication, Computer) station으로 정보를 보내게 되며, C4 Station은 각각의 정보를 판단하여 지시를 하는 체계로 가지고 있다. 이러한 특성을 위해 각각의 Sensor는 중심제어부와 지속적인 교신을 실시하고 있다. 또한 군 Sensor는 사전 배치전 암호장비를 배치 받게 되며, Sensor에 필요한 Pseudo-random code를 생성할 수 있게 된다. 따라서 각 Sensor와 C4 Station만이 알고 있는 Pseudo-Othogonal code를 이용하여 Key 분배가 가능할 수 있기 때문에 주기적으로 암호화된 식별식을 Sensor와 주고받음으로써 중간단계의 악의적인 정보누락 여부 및 data 변조 가능성을 파악할 수 있다는데 착안하여 4.2.와 같은 알고리즘을 제안하였다.

4.2. 정보누락 대응 절차

군 통신망의 핵심부인 C4 station에서는 각 Sensor와 교신을 설정하기 위해 각 노드에 Key 분배를 하게 되는데 이때 포함되는 메시지는 Random #(상태신호 전송주기, 전송최초시간, 전송횟수) 및 식별식(연결성 확인용)을 C4 Station과 각 Sensor만이 알고 있는 Pseudo-code를 통해 변조하여 전송하게 되며, 각노는 자신의 Key를 확인하여 C4에서 지시한 규칙(Random #)에 따라 식별식을 전송하게 되며, C4 station에서는 결과의 정확성 및 해당 Sensor에서 보고가 정확하게 들어오는 가를 파악하게 하는 등 Key 분배를 통해 지정된 시기에 규칙적으로 보고가 행해지는 지를 판별하는 알고리즘 이며, 상세한 절차는 [그림5]에서 보는 바와 같다.



[그림5] 정보누락 대응 절차

5. 결론 및 향후과제

Wireless Sensor Network는 일반사회 뿐만 아니라 군 통신 등 특수분야에도 많은 영향을 미치고 있다. 그리고, 각 통신기반에 따른 정보의 위협의 정도도 틀릴 것이다. 앞서 살펴본 바와 같이 대량의 정보가 필요한 NCW에서 쉽게 수집 노드를 배치할 수 있는 WSN은 널리 사용될 예정이다. 본 논문에서는 현재 군 통신에서 가장 위협을 느끼는 부분이 어떤 것인지를 알아보았으며, 그중에서 가장 위협이 되는 정보누락에 대해 간단한 주기적 정보교환을 통해 쉽게 정보누락 여부를 확인할 수 있는 방안을 제시하였다. 앞으로의 연구에서는 본 대응방안의 실효성을 검증하고, 또한 정보누락 뿐만아니라 기타 위험 분야에 대한 연구를 진행해 나갈 것이다.

참고문헌

[1] Zhijun li and Guang Gong, "Survey on Seucrity in Wireless Sensor" in Journal of KIISC, VOL. 18 NO. 6(B), December 2008

[2] US Department of Defense(Washington D.C.), "The Implementation of Network-Centric Warfare", 2005

[3] Romer, Kay and Friedemann Mattern, "The Design Space of Wireless Sensor Networks", in IEEE Wireless Communications 11(6) 54-61, December 2004

[4] Thomas Haenselmann, "Sensornetworks", 2006

[5] 김세헌, “현대경영과학”, 제2판, 2008