무선네트워크에서의 보안기술 분석

변 병 길, 이 기 영

인천대학교 정보통신공학과

The Analysis of Security in Wirless Sensor Netwroks

Byung kil-Byun* · Ki Young-Lee**

*University of Incheon

E-mail : bgbyun@stu.ac.kr

요 약

인터넷의 발달로 인하여 네트워크의 편익성을 느낀 세대가 무선네트워크의 실현을 재촉하고 있다. 그러나 무선네트워크에서의 보안은 모든 예상가능한 공격으로부터 시작되어야 하는데 특히 L1계층에서 L7계층까지 고려되어야 하겠다. 유선에 비하여 다양한 센서단말기와 보이지 않는 전파망을 이용한 침입등이 보안에 취약하다고 하겠다. 더욱이 무선네트워크는 센서네트워크라고 할만큼 밀접한 관계이므로 센서네트워크에도 적용이 되는 보안제안이 있어야 하겠다. 물리적계층, 네트워크계층,응용계층에서의 보안제안을 알아보고 향후 무선네트워크의 보안 개발점을 논하고자 한다.

ABSTRACT

A generation to have felt convenience of a network by a development of Internet is pressing for realization of a wireless network. However, security of wireless network must begin with an attack to be good at all expectations. especially considred from L1 layer to L7 layer. Wireless Network weaker than wire because smuggle through various sensor terminal and invasion of radio waves netwwork. Wireless network recognizes a security proposal of physical, network, application layer, and is going to discuss a security development point of wiress network from now on.

키워드

Wireless Network, Sensor Network, security, mobile

I. 서 론

인터넷의 사용자 증가로 네트워크의 편익성을 경험한 세대는 서서히 그 중심축을 mobile로 옮겨가고 있다. 유선이 갖는 시간및 장소에 대한 한계, 단말기및 통신선로의 추가 개설에 따른 미관을 해치는 주위환경등이 무선에 대한 선호를 증가시키며, 각종 가전제품의 네트워크화가 디지털시대의 또다른 무선혁명이 일어나고 있다. 가장 선두주자인 이동통신의 경우는 휴대폰 음성위주의 서비스가 주가되고 데이터 전송률의 속도가 최대 2Mbps를 넘어가지 않을 것으로 예측되고 있다[1]. 세계적인 범용망으로 다양한 콘텐츠를 가진 인터넷을 지원하는 무선랜 서비스는 노트북과 PDA가 있으나 이또한 서비스 지역이 한정되어 있는 단점이 있다. 마크와이저는 유비쿼터스 논문을 통해 구텐베르그의 인쇄혁명에 버금가는 그 어떤 것이 앞으로 개발될것이라는 예측한바 있다.[2] 인쇄물의 재질이 단지 종이가 아니고 도기,섬유,플라스틱,철등 다양화 되었듯이 우리가 생각하는 휴대폰,노트북만이 정보제공의 센서라는 개념은 TV, 냉장고등 가

전제품에 심어지면서 서서히 깨져가고 있다. mobile에서 휴대전화의 경우는 작은화면 고비용이, 노트북의 경우는 밧데리및 지역한계성등이 무선환경의 범용화를 저해하는 이때에 센서 네트워크및 홈네트워크의 개발은 눈 여겨 볼만하다. 지금은 단지 한가지의 단순한 기능만 하는 센서및 홈네트워킹의 기능등이 이러한 이동전화와 노트북과도 연동이 되어 활용되어 질것이다. 유선 인터넷에서 표준이된 TCP/IP와 같이 무선 인터넷에서도 프로토콜의 표준이 이루어져 보안에 대한 대책이 수립되어야 한다고 본다. 본 고에서는 L1에서 L7 계층에서 일어날수 있는 공격의 유형에 대하여 살펴보고 III장에서는 센서네트워크에서 일반적으로 쓰이는 센서의 종류및 특징을 알아보고 IV장에서는 실제적으로 진행되고 있는 보안사례를 알아보고 이동성에 따른 무선네트워크의 효율적인 보안정책을 제시한다.

II. 모바일에서의 공격유형

2.1. 공격 가능성의 다양화

많은 연구가 이루어지고 있는 무선 네트워크의 보안연구는 유선망에서 우려되는 데이터의 위조나 변조, 그리고 사용자의 인증 자체가 위조되지 않았음을 보증하는 암호학적 접근의 키분배 및 관리, 인증, 보안등에 중점이 되어 있다. 이는 암호학적 접근이 보안의 패러다임으로 인식하는데에 기인한다. 그러나 각각의 무선 노드들은 고정된 라우터나 호스트, 무선 기지국등이 없으므로 각 이동노드들끼리 데이터를 전달하여야 할뿐만 아니라 이동 노드들이 라우터의 기능을 수행해야 하는등 유선보다 더 많은 역할이 요구되어지고 있다. 더욱이 센서노드인 경우는 일반적으로 특정지역에 무작위로 뿌려지는 일회성인 경우를 감안할 때 ad hoc network보다도 보안이 더욱 취약하다는 특성을 갖는다.

유선에서는 line의 최종지점인 L7에서 packet의 L4에서의 보안관리가 주를 이루었으나 무선에서는 L1에서 L7까지 보안관리가 고려되어야 한다.

아래에 무선네트워크의 환경 예를 소개한다. 그림 1에서와 같이 유선에서의 경우는 firewall을 설치 최종Line의 길목에서 침입자의 공격을 차단할수 있으나 만약 침입자가 물리적 공간으로 이동하여 화장실이나 기타안보이는 공간에서 무선 액세스포인트를 이용하여 내부망을 뚫고 접근하여 홈네트워크나 서버,PC,인터넷전화등을 교란시킬수 있는 L1계층에서의 공격에 대한 보안에는 취약하다

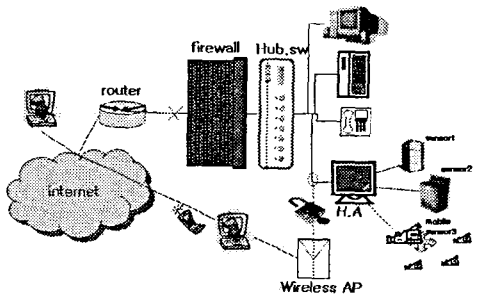

그림 1 무선네트워크 배치도

.2.2 각계층에서의 공격

1)L1,L2에서의 공격

주파수가 link layer인 주파수의 jam으로 인한 충돌,혼잡,간섭등이 있고 알려진 source node의 물리계층인 MAC layer공격이 있다.

2)L3에서의 공격

- 공격이 없는 상황에서도 무선이 갖는 seamless가 하나의 무선네트워크의 공격이라 할수 있다.
- sinkholes나 selective holes와 같이 어떤 메시지나 정해진 byte등은 돌려 보내고 그림과 같이 거짓된 정보를 참 정보로 인식하여 이를 받아들이도록 하는 공격이 그 예이다.

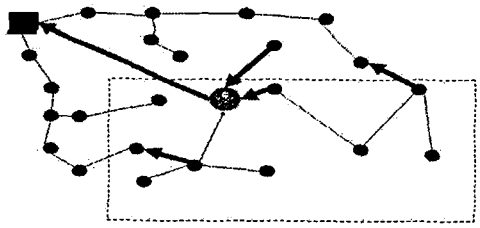

그림 2 sinkhole attack

- sybil attack의 경우는 x=3, y=2의 좌표를 갖는 A node가 A1(2,3), A2(1,2)의 위치에 허상으로 존재케 하여 B node가 C node와 통신을 중간에 가로막아 방해함으로서 geographical한 routing에 치명적 피해를 입힌다.
- 또 다른 wsn routing의 공격은 wormholes로서 실제로는 존재하지 않는 전혀 다른 토폴로지를 마치 노드연결이 있는 것처럼 인식하게 공격하여 엿듣기 공격이나 selective forwarding과 같이 활용되기도 한다.
- Hello floods공격으로 멀리있는 공격자가 강한 강도의 신호로 Hello packet을 보냄으로 마치 이웃에 있는 노드로 착각하여 응답을 하도록 하지만 실은 공허한 수고로 만드는 것으로 이는 고전적인 신호방해공격과 같이 통신 채널을 혼란시킨다.[3]

4)L4에서의 공격

침입으로서 lure, spoofing, sybil 거짓으로 퍼뜨려놓고 선택하게 한다. 그림에서와 같이 침입자

는 mobile node의 홈어드레스의 주소를 구하게 된다. 침입자는 이동시 가능한 care-of-Address모든 할당주소를 binding update시키고 마치 자신이 MN인것 처럼 traffic을 훔쳐 통신하게 된다.

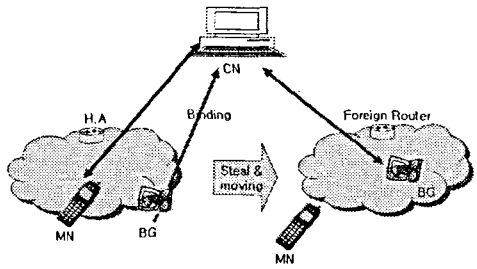

그림 3 spoofing attack of Bad Guys

5)L4-L7에서의 공격

응용계층에서의 보안은 Data confidentiality, Data integrity, Authentication, Access control, Non-repudiation, Availability등을 파괴하는 공격을 막는 것으로 유선네트워크에서 많이 개발되어 왔으나 무선인 만큼 최대한 전력소비를 줄이는 보안인증의 연구가 필요하다.

III. 센서 네트워크

센서란 인간의 눈,코,귀와 같이 보고, 듣고, 냄새맡고, 느낄수 있는 감각기관에 해당되는 기기로서 입력값을 판단하여 전자신호로 각종 기계기구를 제어할수 있다. 이러한 센서는 실세계와 컴퓨터및 네트워크를 연결시켜 주는 중요한 역할을 하고 있다. 향후 유비쿼터스 환경에서는 벽,가구,천정등 모든 사물이 센서화되어 사용될수 있다고 하겠다.

3.1 센서의 분류

센서원리에 따른 분류로는 광학적(optical): 적외선 센서, 열선 센서, 연기 센서가 있고 전자적(electirc): 자석 센서, 셔터 센서등이 있다. 장력 센서, 충격감지센서,유리센서는 역학적 센서이다. Thermal sensor로는 Thermocouple,Thermistor, Pyrometer등이 있으며 Chemical sensor로는 연기센서, 가스 센서등이 있다. [4]

환경 변화를 감지하여 발생되는 신호의 처리 방법에 따라 능동형과 수동형으로 나눌수 있다. 능동형은 RF발신가, 적외선 발신기,셔터 감지기, 초음파(ultrasonic)가 있고 수동형은 GPS(global positioning systems), 음향감지기, 장력 감지기, 충격 감지기, 열선감지기, X-vison과 같이 외부에서 보낸 신호및 정보를 입력 받아 처리한다.

송신방법에 따라 유선센서와 무선센서로 구분하고 일반적으로 유선 센서는 출력이 Relay(무전압 접점) 또는 아날로그로 발생되어 센서와 컨트롤러 사이를 유선으로 연결하는 방식이며 무선은 센서 발생 출력을 무선으로 컨트롤러에 송신하는 형태이다.

3.2 센서 네트워크 보안취약 사항

앞장에서 무선네트워크에서의 각 계층간의 공격유형에 적용되며 이에 추가하여 데이터 링크층에서는 센서 노드들이 좁은 영역에 조밀하게 분포되고, 대량의 노드들이 산재하므로 collsion, overhearing(자기와는 상관없는 데이터를 수신하여 전력 낭비), control packet overhead(과도한 컨트롤 패킷), idle listeng(데이터를 수신하지 않으면서도 신호를 계속 감지)등의 문제가 있고 네트워크 계층에서는 센서노드간의 통신이 아닌 베이스 노드와의 broadcasting방식으로서 데이터가 중심(data centric)이 되는 문제점과 주위의 노드들이 alive한 상태인지 파악할 수 없는 베터리 소모 효율성의 개선요구가 필요하다. 어플리케이션층에서는 각 노드들의 Authentication, Recognition, Reconfiguration의 보안문제가 있다. 현재 이루어지고 있는 대부분의 센서 네트워크 보안기술연구는 키분배및 관리 인증 보안을 위한 네트워크 구조, 라우팅등 다양한 보안요소들이 결합된 형태로 이루어졌다. 아래 표에서는 각 계층간 서비스 공격에 대한 방어책을 나타냈다.

표 1 센서네트워크의 공격및 방어책

계층	서비스 거부공격	방어책
물리	jamming	대역확산, priority messages, lower duty cycle, region mapping, mode chaange
	간섭(tampering)	Tamper-proofing, hiding
데이터링크	충돌(collision)	Error-correcting code
	소진(exhaustion)	Rate limitation
	불공평성(unfairness)	Small frames
네트워크 & 라우팅	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black holes	Authorization, monitoring, redundancy
Transport	Flooding	Client puzzles
	Desynchronization	Authentication

IV. 보안 제안

데이터 링크층에서의 문제해결을 위해 Self-Organizing Medium Access Control(이하 SMAC)이 제안되었다.[5] SMAC에서는 노드가 주기적으로 슬립모드와 리스닝모드사이를 반복한다. 실제로 데이터를 전송할 때만 깨어나서 전송을 하고 나머지는 슬립상태에서 전력소모를 최소화한다. 이 방법은 비활성시 수신과 충돌, 오버히어링 등에 대한 문제는 해결하나, 노드들의 동기화가 이루어져야 한다는 단점이 있다.

네트워크층에서의 Worrmhole에 대한 공격의 방어를 위해 packet leash메카니즘이 제안되었는데 [6] geographical leashes와 temporal leashes로 구분된다. geographical leashes는 각각의 노드들은 자기주소를 갖고 있고 패킷을 보내는 시간, 패킷을 받는시간 보내는 패킷, 받는 패킷과의 연산이

receiver와 sender의 거리보정계수보다 클때에 허락하는 gps적인 방법이다.

트랜스포트층에서의 강력한 hello flood공격은 위 gps적인 방법으로 ack를 통해 방지할수 있다. 아직 UDP를 통해 무차별적으로 발송되는 문자메시지 공격에 대하여는 향후 무선에서 고려하여야 할 Quality of Service제어에 대한 연구가 필요하다.

application층에서는 유선기반을 응용한 무선기반의 PKI가 연구되고 있다.

일부 노드의 노출이 근접 이웃 노드까지 노출시키는 위협을 최소화하기 위한 leap이라는 키관리 프로트콜을 제안Leap은 각 센서 노드을 위한 네가지 형식의 키에 대한 설정 구조와 노드 간 인증프로토콜을 Sencun Zhu, Sanjeev Setia와 Sushil Jajodia는 제시하였다[7]

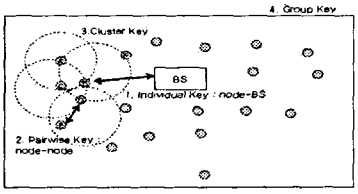

그림 4 4개의 키 in leap Protocol

Leap은 BS와의 인증뿐 아니라 단방향 키 체인을 기반으로 한 노드 간 인증 프로토콜도 제공하는데 우선 모든 노드가 단방향 키체인을 생성하여 체인의 commitment값을 각 이웃과의 pairwise key로 암호화하여 전송한 다음, 나중에 메시지를 보낼때 다음 인증키 값을 같이 보내면 이웃이 처음에 받은 commitment값과 비교함으로써 인증을 수행한다. Leap의 가장 큰 장점은 제안하는 키관리 메카니즘을 통해 in-network프로세싱이 가능함과 동시에 이웃 노드가 보안 위협에 노출된 경우라도 노드의 보안을 유지할수 있다는 점이다.

V. 결론

본 고에서는 무선 네트워크에서의 보안기술은 향후 다가올 모든 사물에 심어지는 센서노드간의 전달, 이동및 공유 라우팅을 비롯한 복합기술이므로 유선 네트워크에 비하여 다양한 계층에서의 보안접근이 고려되어야 하나 주로 보안기능및 전송이 유선네트워크에 기반한 관점이 주를 이루고 그외에는 체계적인 연구가 부족한 상태이다. 본고에서는 무선 네트워크이기에 발생할수 있는 L1층에서 L7층까지 예측되는 공격과 그에 대한 보안기술등에 대해서 알아 보았다. 이제는 인터넷을 키워드로 유무선 통합서비스시대가 도래된 만큼 보안의 패러다임을 개방형 네트워크에 맞추어야 하고 그러기 위해서는 보다 많은 보안취약점들을 해결하여야 한다. 무선네트워크는 선세네트워크라고해도 좋을 만큼 밀접한 관계를 갖고 있으므로 다양한 종류의 단말기와 Ad-hoc형태를 포함한 여러 가지 토폴로지로 네트워크가 형성될 것이다. 본론에서 언급한 공격외에 더 다양한 공격모델이 도출될것이다. 무선네트워크의 보안 취약성. 예상 가능한 보안 위협에 대한 대응책과 보다 강화된 보안 기술로의 개발과 표준화가 필요한 시점이라 할것이다.

참고문헌

[1] 김충남 저, 차세대 무선인터넷 서비스, 29, 전자신문사, 2003

[2] M. Weiser, "Hot topic:Ubiquitous Computing", IEEE computer 72, octobert 1993

[3] Chris karl of and David Wagner, "Secure Routing in Wireless Sensor Networks : Attacks and Countermeassure" First IEE international Workshop on sensor Network protocol and Applications, May 2003.

[4] 안창훈외2인 공저, 시큐리티 시스템 개론, (주)인포더, 54-55 , 2005

[5]Katayoun Sohrabi외3인,Protocols for self-Organization of a wireless Sensor Network, IEEE Personal Communication, 18 October 2000

[6]Yih-Chun Hu외2인, Packet Leashes : A Defense against Wormhole Attacks in Wireless Networks , 1978 2003 IEEE

[7]Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP : Efficient Security Mechanisms for LargeScale Distributed Sensor Networks," Proc. of the 10th ACM Conference on Computer and Communication Security(CCS), 2003