센서 네트워크 보안을 위한 SWAD-KNH 기법 설계

정은희* · 이병관**

A Design of SWAD-KNH Scheme for Sensor Network Security

Eun-hee Jeong* · Byung-kwan Lee**

이 논문은 중소기업청에서 지원하는 2012년 산학연공동기술개발사업(No.C0035768)의
연구수행으로 인한 결과물임을 밝힙니다.

요 약

본 논문에서는 클러스터 단위로 센서 노드의 키와 그룹키를 생성한 후 분배하는 KGDC(Key Generation and Distribution based on Cluster) 모듈과 이 키를 이용하여 시빌 공격과 웜홀 공격을 탐지할 수 있는 SWAD(Sybil & Wormhole Attack Detection) 모듈로 구성되는 SWAD-KNH(Sybil & Wormhole Attack Detection using Key, Neighbor list and Hop count) 기법을 제안한다. KGDC 모듈은 ECDH 알고리즘, 해시함수, 키 체인 기법을 이용하여 그룹키와 센서 노드의 키들을 생성하고 안전하게 배포한다. SWAD 모듈은 2단계 키 확인절차를 수행함으로써 시빌 공격 탐지를 강화시키고, 근원지와 목적지 노드의 공동이웃노드들의 수와 홉 카운트를 이용하여 웜홀 공격을 탐지한다. 그 결과 SWAD-KNH 기법은 시빌 공격 탐지율은 91.2%, 평균 FPR(False Positive Rate)은 3.82%이고, 그리고 웜홀 공격 탐지율은 90%, 평균 FPR(False Positive Rate)은 4.64%으로 평가되므로 시빌과 웜홀 공격 탐지율 및 시빌과 웜홀 공격 탐지의 신뢰성을 향상시켰다.

ABSTRACT

This paper proposes an SWAD-KNH(Sybil & Wormhole Attack Detection using Key, Neighbor list and Hop count) technique which consists of an SWAD(Sybil & Wormhole Attack Detection) module detecting an Worm attack and a KGDC(Key Generation and Distribution based on Cluster) module generating and an sense node key and a Group key by the cluster and distributing them. The KGDC module generates a group key and an sense node key by using an ECDH algorithm, a hash function, and a key-chain technique and distributes them safely. An SWAD module strengthens the detection of an Sybil attack by accomplishing 2-step key acknowledgement procedure and detects a Wormhole attack by using the number of the common neighbor nodes and hop counts of an source and destination node. As the result of the SWAD-KNH technique shows an Sybil attack detection rate is 91.2% and its average FPR 3.82%, a Wormhole attack detection rate is 90% and its average FPR 4.64%, Sybil and wormhole attack detection rate and its reliability are improved.

키워드

센서 네트워크, 시빌 공격, 웜홀 공격, 그룹키, 이웃리스트, 홉 카운트

Key word

Sensor Network, Sybil Attack, Wormhole Attack, Group key, Neighbor list, Hop count

* 정희원 : 강원대학교(제1저자)

** 정희원 : 관동대학교(교신저자, bkleee@kd.ac.kr)

접수일자 : 2013. 05. 01

심사완료일자 : 2013. 05. 24

I. 서 론

센서 네트워크에서는 상호간 통신을 위해 무선매체를 사용하고, 센서 노드는 물리적 한계를 가지므로 기존의 유무선 기술보다 보안에 더욱 취약하다. 특히, 센서 네트워크에서는 센서 노드들과 베이스 스테이션이 무선으로 통신을 하기 때문에 공격에 쉽게 노출되는데, 그 중에서 가장 대표적인 것이 시빌(Sybil) 공격과 웜홀(Wormhole) 공격이다. 시빌 공격은 네트워크에서 공격 노드가 다량의 거짓 노드를 생성하여 베이스 스테이션에 거짓 데이터를 전송함으로써 베이스 스테이션이 엉뚱한 판단을 하도록 하는 것이고, 웜홀 공격은 공격자가 센서 네트워크의 경로 상에서 자신만의 터널을 만들어 그 경로로 정보를 전송하도록 하여 베이스 스테이션으로 가는 경로를 변조시키거나 정보를 가로채는 것이다.

본 논문에서는 그룹키 기반 키 분배기법을 보완하여 클러스터 단위로 센서 노드 키를 생성하고, ECDH 알고리즘을 이용하여 그룹키를 분배한다. 그리고 이 키들로 센서 노드를 인증하여 시빌 공격을 탐지하고, 공동이웃 노드와 홉 카운트를 이용하여 웜홀 공격을 탐지할 수 있는 SWAD-KNH(Sybil & Wormhole Attack Detection using Keys, Neighbor list and Hop count) 기법을 제안하여 센서 네트워크의 보안을 강화시키고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구를 소개하고, 3장에서는 본 논문에서 제안한 SWAD-KNH 기법을 기술한다. 4장에서는 SWAD-KNH 기법에 대한 실험결과를 설명하고, 이를 통해 SWAD-KNH 기법의 우수성을 입증하고, 5장에서 결론을 맺는다.

II. 관련연구

센서 노드의 하드웨어적인 제약으로 인해 기존 무선 네트워크 보안 기법 적용이 어려워 메시지 무결성, 기밀성 및 노드 인증 등의 보안 요소 구현을 위해 경량화된 키 분배 및 인증 기법 연구가 진행되고 있다[1].

사전 키 기반 분배 기법인 클러스터 기반 그룹키는 센서 노드들끼리 그룹을 형성하고, 그룹 안에서 그룹키를 사용하는 기법을 말한다. 그룹키의 기본 구조는 베이스 스테이션과 클러스터 마다 중간에 Aggregator를 두고, 다음과 같은 절차에 따라 그룹키를 센서 노드에 배포한

다[2, 3, 4, 5].

- 그룹을 선언하고, 베이스 스테이션이 모든 센서 그룹의 정보와 각 그룹의 Aggregator에 대한 정보를 모든 센서 노드들에게 브로드캐스트 한다.
- 베이스 스테이션은 베이스 스테이션과 Aggregator 사이의 비밀키로 암호화하여 각 그룹의 Aggregator에게 그룹키를 유니캐스트 한다. 그리고 베이스 스테이션과 Aggregator 사이의 공유키로 생성한 MAC값을 같이 보내다.
- 각 그룹의 Aggregator는 자신이 속한 그룹안의 모든 센서 노드들에게 그룹 분별 아이디, 그룹키, 그리고 MAC값을 전달한다.
- 센서노드는 Aggregator로부터 받은 MAC값을 확인한다.

그룹 키 관리 기법에서는 공유키 탐색을 위해 센서 노드들이 주고받는 메시지의 양이 감소하고, 각 그룹키는 자신만의 그룹영역을 담당하므로 해당 그룹의 센서 노드가 이동하더라도 그 영향이 그룹 내로 한정되는 장점이 있다. 하지만, 그룹키 관리 기법은 임의의 센서 노드에 관한 개별 인증을 할 수 없고 단지 그룹에 대해서 멤버 여부의 인증만 가능하다. 그리고 그룹키를 안전하게 전송하기 위해서는 미리 비밀키를 갖고 있어야 한다. 만약 비밀키를 가지고 있지 않으면 센서 노드가 네트워크에 들어왔을 때 안전하게 그룹키를 받을 수 없다. 또한 그룹키가 알려지면 전체적으로 시스템 보안에 영향을 끼치게 되는 단점이 있다[2, 4].

센서 네트워크 환경에 적합한 보안 솔루션을 제공하는 알고리즘으로는 UC Berkeley에서 제안한 SPINS(Security Protocol for Sensor Network)가 있다[6]. SPINS는 베이스 스테이션과 센서 노드간에 미리 공유된 마스터키를 이용하여 필요한 대칭키를 생성하며, 데이터의 무결성, 기밀성 및 인증기능을 제공하는 SNEP(Sensor Network Encryption Protocol)와 브로드캐스트 인증 기능을 제공하는 μ TESLA(micro Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol)로 구성된다. μ TESLA는 단방향 해시 함수를 이용한 키 체인의 생성과 키 체인을 이용한 구간별 MAC(Message Authentication Code) 생성 및 지연된 키 공개 방식을 사용한다. μ TESLA는 해시체인을 이용하여 효과적으로 데이터인증을 제공할 수 있고 수신 노드들의 입장에서 중간에 패킷 분실이 발생하더라도 다음 패킷을 통해 이전 패킷들을

검증할 수 있는 장점을 갖는다. 그러나 모든 노드들이 시간 동기화가 되어 있어야하고 실제 네트워크 전송 지연이 있을 수 있으므로 이를 위한 키 노출지연시간의 설정 및 패킷의 저장을 위한 공간이 추가로 필요하다는 단점을 갖는다[6,7,8,9,10].

LEAP은 센서 네트워크상에서 인증과 기밀성을 보장하며 메시지 타입에 따라 개인 키, 쌍대 키, 클러스터 키, 그룹키를 선택적으로 사용한다. 복수개의 키를 이용하기 때문에 하나의 키로는 할 수 없는 여러 가지 형태의 보안 메시지를 전송할 수 있으며 키 생성 과정이 초기 한번만 이루어지기 때문에 에너지 측면에서도 효율적이다. 그러나 이동노드를 위한 핸드오프 과정과 키 갱신을 지원하지 않으며 초기 사용한 마스터 키를 키 갱신 작업 없이 지속적으로 사용하기 때문에 공격자가 키 전달과정에서 초기 마스터 키 정보를 획득할 경우 통신에 사용하고 있는 모든 키들을 생성할 수 있다[6,9,11].

본 논문에서는 베이스 스테이션과 센서 노드 사이에 Aggregator 역할을 하는 코어 노드를 위치시킨다. 하지만 기존의 클러스터 기반 그룹키처럼 베이스 스테이션이 전달하는 그룹키를 센서 노드에게 전달하는 것이 아니라 Aggregator인 코어노드는 직접 센서 노드의 키와 코어 노드가 속한 그룹의 그룹키를 ECDH 알고리즘을 이용하여 생성하도록 설계한다.

III. SWAD-KNH 기법 설계

본 논문에서는 센서 네트워크에서 안전하게 키를 배포하고 키와 이웃노드리스트, 홉 카운트를 이용하여 시빌 공격과 웜홀 공격을 탐지하는 SWAD-KNH (Sybil & Wormhole Attack Detection using Keys, Neighbor list, and Hop count) 기법을 설계한다.

제안하는 SWAD-KNH 기법은 클러스터 단위로 센서 노드의 키와 그룹키를 생성한 후 분배하는 KGDC(Key Generation and Distribution based on Cluster) 모듈과 이 키와 이웃노드리스트, 홉 카운트를 이용하여 시빌 공격과 웜홀 공격을 탐지할 수 있는 SWAD(Sybil & Wormhole Attack Detection) 모듈로 구성된다.

각 모듈은 다음과 같은 가정 하에 설계한다.

첫째, 베이스 스테이션은 인증기관으로부터 인증서를 부여받은 신뢰할 수 있는 서버역할을 담당한다.

둘째, 베이스 스테이션, 코어노드들은 각각 타원곡선암호(Elliptic Curve Cryptography)의 공개키와 비밀키를 보유하고 있다.

셋째, 센서 노드들은 마스터키를 보유하고 있다.

본 논문에서 사용하는 약어는 표 1에서 설명하고 있다.

표 1. 약어 설명
Table. 1 the description of abbreviation

약어	설명
BKey	베이스 스테이션과 코어노드들 사이의 그룹키
GKey	코어노드와 센서노드들사이의 그룹키
GPKey	그룹 공개키
SK	센서 노드 키(Sensor node Key)
SKey	비밀키
PKey	공개키
MK	Master Key
ID	센서 노드 식별자(Identifier)
NL	이웃 노드 리스트(Neighbor List)
CNL	공동이웃노드리스트(Co-Neighbor List)
nonce	랜덤한 수
H	해시함수
Hn	nonce를 해시함수로 해시한 결과 값
E	암호화(encrypt)
D	복호화(decrypt)
Edata	암호화된 데이터
Hdata	해시 함수로 해시한 결과 값
$\oplus$	XOR 연산 기호
$\parallel$	연접(concatenation) 기호
mod	modular 연산 기호

그림 1은 SWAD-KNH 기법의 구성과 전체적인 흐름을 설명한 것이다.

BKey, GKey : Group Key, SK : Sensor node Key
NL : Neighbor List, CNL : Co-Neighbor List

그림 1. SWAD-KNH 기법의 흐름도
Fig. 1 the flowchart of SWAD-KNH scheme

3.1. KGDC 모듈 설계

본 논문에서는 베이스 스테이션과 코어 노드 사이에는 ECDH 알고리즘을 이용하여 그룹키를 생성하고, 코어 노드는 키 체인 기법, 해시함수, XOR 연산으로 센서 노드의 키와 클러스터 단위의 그룹키를 생성한 후 센서 노드에게 분배하는 KGDC(Key Generation and Distribution based on Cluster) 모듈을 설계한다[12].

3.1.1. 베이스 스테이션 그룹키 생성

그림 2는 베이스 스테이션과 코어 노드의 그룹키 설정 방법을 설명한 것이며, 단계별 절차는 다음과 같다.

[1 단계] 코어 노드들은 자신의 공개키와 랜덤하게 생성한 수(*nonce*)를 베이스 스테이션에 전달한다.

$$PKey_{cl} = SKey_{cl} \times P \mod n$$

[2 단계] 베이스 스테이션은 전달받은 코어노드들의 공개키와 자신의 비밀키를 곱셈 연산하여 그룹키인 BKey를 생성한다.

$$BKey = SKey_B \times PKey_{cl} \times PKey_{c2} \mod n$$

[3 단계] 베이스 스테이션은 코어노드로부터 전달받은 공개키, 랜덤한 수(*nonce*), BKey를 연결하여 해시함수로 해시한다.

$$\text{코어노드}(C1): Hn1 = H(\text{nonce1} \parallel PKey_{cl} \parallel BKey)$$

$$\text{코어노드}(C2): Hn2 = H(\text{nonce2} \parallel PKey_{c2} \parallel BKey)$$

[4 단계] 베이스 스테이션은 자신의 공개키와 전달할 코어노드의 공개키를 제외한 코어노드의 공개키들을 곱셈 연산한 키 값(*GPKey*), 해시한 값, 그리고 베이스 스테이션의 인증서를 전달한다.

$$\text{코어노드}(C1): GPKey_{cl} = PKey_B \times PKey_{c2} \mod n$$

$$\text{코어노드}(C2): GPKey_{c2} = PKey_B \times PKey_{cl} \mod n$$

그림 2. 그룹키 생성 흐름도
Fig. 2 the flowchart of group key generation

[5 단계] 코어 노드는 베이스 스테이션으로부터 전달받은 다른 코어노드의 공개키들을 곱셈 연산한 키 값 (*GPKey*), 그리고 자신의 비밀키(*SKey*)로 곱셈 연산하여 그룹키인 BKey를 생성한다.

$$\text{코어노드}(C1): BKey = SKey_{cl} \times GPKey_{cl} \mod n$$

$$\text{코어노드}(C2): BKey = SKey_{c2} \times GPKey_{c2} \mod n$$

[6 단계] 코어 노드는 베이스 스테이션에 전달했던 랜덤한 수(*nonce*), 코어노드의 공개키(*PKey*), 그리고 그룹키(*BKey*)를 연결하여 해시함수로 해시한다.

$$Hn = H(\text{nonce1} \parallel PKey_{cl} \parallel BKey)$$

[7 단계] 코어노드는 베이스 스테이션으로부터 전달받은 해시값(*Hn1*)과 코어노드가 계산한 해시값(*Hn*)을 비교하여 같으면 그룹키 BKey가 정확하게 생성된 것으로 판단한다.

따라서 베이스 스테이션과 코어노드들은 같은 그룹키인 BKey를 획득한다.

3.1.2. 센서 노드의 키 생성 및 분배

클러스터 헤더 노드인 코어 노드는 자식노드인 센서 노드들에게 센서 노드의 키와 그룹키를 안전하게 배포한다. 그리고 이 키를 이용하여 센서 노드의 신분을 확인함으로써 시빌 공격을 탐지하고, 그룹키로 센싱된 정보를 암호화하여 전달함으로써 데이터의 위조 및 변조를 방지할 뿐만 아니라 워홀 공격을 탐지하고자 한다.

그림 3은 클러스터 헤더인 코어 노드가 센서 노드의 키와 그룹키를 생성하여 센서 노드들에게 키를 분배하는 과정을 설명한 것이며, 단계별 절차는 다음과 같다.

그림 3. 키 생성 및 분배 흐름도

Fig. 3 the flowchart of key generation and distribution

[1 단계] 코어 노드는 Seed값을 선정하여 해시함수로 해시하여 키 값에 필요한 초기값을 생성한다.

$$SK_1 = H(Seed)$$

[2 단계] 센서 노드는 센서 노드의 Master Key(MK_{S1})와 센서 노드의 ID(S_1)를 해시한 값(H_{S1})과 nonce를 코어 노드에 전달한다.

$$H_{S1} = H(S_1 || MK_{S1})$$

[3 단계] 코어노드는 센서 노드의 키 값(SK_1)과 센서 노드로부터 전달받은 해시 값을 XOR 연산으로 센서 노드의 키 값을 간단하게 암호화하여 센서 노드에 전달한다.

$$SK_{S1} = SK_1 \oplus H_{S1}$$

[4 단계] 코어노드는 센서 노드로부터 전달받은 해시 값

($H_{S1}, H_{S2}, \dots$)들을 모두 연결하여 해시한 후, 코어 노드의 비밀키(SK_{C1})로 XOR 연산을 하여 코어 노드가 관리하는 클러스터의 그룹키($GKey_{C1}$)를 생성하여 센서 노드에 전달한다.

$$GKey_{C1} = SK_{C1} \oplus H(H_{S1} || H_{S2} || \dots)$$

[5 단계] 센서 노드는 코어노드로부터 전달받은 키 값을 센서 노드의 Master key와 ID를 연결하여 해시한 값으로 XOR 연산을 하여 코어 노드가 전달한 키 값들을 복구한다.

$$SK_1 = SK_{S1} \oplus H_{S1}$$

[6 단계] 센서 노드는 코어 노드로부터 전달받은 키 값인 그룹키($GKey_{C1}$), 센서노드의 키(SK_1), 그리고 nonce를 XOR 연산한 결과를 코어 노드에 전달한다.

$$N_{S1} = Gkey_{C1} \oplus SK_1 \oplus nonce$$

[7 단계] 코어 노드는 센서 노드로부터 전달받은 nonce, 배포한 센서 노드의 키 값, 그룹키를 XOR 연산한 결과(N_c)와 센서 노드로부터 전달받은 N_{S1} 와 비교한다. 그 결과가 참이면 키 값이 정확하게 전달된 것으로 판단한다.

$$N_c = GKey_{C1} \oplus SK_1 \oplus nonce$$

즉, 코어 노드는 자식노드인 센서 노드에 그룹키가 안전하게 배포되었다고 판단한다.

3.2. SWAD 설계

3.2.1 시빌 공격 탐지

본 논문에서는 베이스 스테이션과 코어노드, 코어노드와 센서노드 사이에는 각각 그룹키가 배포되어 있다. 특히, 코어 노드는 키 체인 기법으로 자식노드인 센서 노드의 키를 생성하고, 이때 생성된 키들에 대한 Key pool을 생성한다. 코어노드는 센서 노드들의 키, 그룹키를 이용하여 그림 4에서 설명하고 있는 절차에 따라 시빌 공격을 탐지하도록 설계한다.

[1 단계] 센서 노드는 그룹키($GKey_{C1}$)로 센싱된 정보(Data)를 암호화한 값($Edata$)과 해시한 값($Hdata$)을 코어 노드에 전달하는데, 이때 암호화된 전달되는 데이터는 센서노드의 키(SK_1)를 포함한 데이터이고, 해시한 값은 데이터 무결성을 검증할 때 사용한다.

$$Edata = E(Data || SK_1, GKey_{C1})$$

$$Hdata = H(Data \parallel SK_1)$$

[2 단계] 코어노드는 센서 노드로부터 전달받은 데이터를 그룹키로 복호화한다.

$$Data \parallel SK_1 = D(Edata, GKey_{cl})$$

[3 단계] 코어노드는 전달받은 메시지 해시 값($Hdata$)과 코어노드가 해시한 값을 비교하여 데이터의 무결성을 검증한다. 두 해시 값이 일치하지 않으면 메시지가 위조되었거나 그룹키($GKey_{cl}$)로 암호화되지 않은 것으로 판단한다.

[4 단계] 그룹키가 확인되면, 코어노드는 복호화된 데이터에서 센서노드의 키(SK_1)를 추출하여 코어노드의 Key Pool에 센서 노드의 키가 존재하는지를 확인한다.

[5 단계] 이때 센서 노드의 키(SK_1)가 Key Pool에 존재하지 않으면 시빌 공격을 판단한다.

그림 4. 시빌 공격 탐지 흐름도
Fig. 4 The detection flowchart of Sybil attack

3.2.2. 웜홀 공격 탐지

본 논문에서는 센서노드가 센싱한 정보가 반드시 코어 노드에서 집계되어 데이터가 전달되므로 코어노드가 1차적으로 웜홀 공격을 탐지하도록 설계한다. 그림 5는 본 논문에서 제안하는 웜홀 공격을 탐지하는 절차를 설명하고 있으며, 웜홀 노드를 탐지하는 단계별 절차는 다음과 같다.

[1 단계] 모든 센서 노드들은 이웃노드목록을 생성한다. 즉, 근원지 노드는 근원지 노드의 이웃노드목록인 NL_S (Neighbor List)를 생성하고, 목적지 노드는 목적지 노드의 이웃노드목록인 NL_C 를 생성한다.

[2 단계] 근원지 노드는 경로 요청 메시지를 목적지 노드에 전달한다. 본 논문에서는 코어 노드가 데이터를 집계하는 Aggregator 이므로 목적지 노드는 코어 노드라 할 수 있다.

[3 단계] 코어 노드는 코어 노드의 이웃노드리스트인 NL_C 를 RREP에 포함시켜 근원지 노드에게 유니캐스트 한다.

[4 단계] 근원지 노드는 자신의 이웃노드목록 NL_S 과 전달받은 목적지 노드의 이웃노드목록 NL_C 를 비교하여 중복되는 공동이웃노드목록(CNL_{sc})을 추출한다.

[5 단계] 이때, 공동이웃노드의 수가 홉 카운트보다 크다면 웜홀 노드가 경로에 존재한다고 판단한다.

[6 단계] 경로에 웜홀 노드가 존재하는 것으로 판단되면, 경로내의 각 노드와 목적지 노드 사이의 홉 카운트를 비교하여 웜홀 노드를 검출한다.

[7 단계] 모든 노드들에게 웜홀 노드를 공지하여 라우팅 테이블에서 해당 노드를 삭제하도록 한다.

그림 5. 웜홀 공격 탐지 흐름도
Fig. 5 the detection flowchart of Wormhole attack

IV. 분 석

4.1. 보안 분석

본 논문에서는 베이스 스테이션과 코어 노드, 코어노드와 센서 노드 사이에 각각의 그룹키를 생성하도록 설

계하였다.

베이스 스테이션과 코어 노드는 ECDH 알고리즘을 이용하여 각자의 공개키를 교환하고, 자신의 비밀키로 곱셈 연산하여 그룹키를 생성하므로 공개키와 그룹키가 노출된다고 하더라도 베이스 스테이션과 코어 노드의 비밀키를 추적할 수 없다.

코어 노드와 센서 노드는 해시함수를 이용하여 그룹키를 생성하였고, 코어노드는 키 체인 기법으로 자식노드인 센서 노드의 키가 생성하고, 이때 생성된 키들에 대한 Key pool을 생성하도록 설계하였다. 즉, SWAD-KNH 기법은 이 Key pool을 이용하여 센서 노드의 키와 그룹키를 이용하여 센서 노드들이 해당 그룹의 구성원인지를 2단계에 걸쳐서 확인함으로써 시빌 공격을 탐지할 수 있을 뿐만 아니라, 그룹키로 메시지를 암호화하여 전송하여 악의적인 공격자에 의한 메시지 위·변조 공격으로부터 안전한 통신을 지원 할 수 있다.

4.2. 탐지율 평가

본 논문에서 제안한 시빌 공격과 웜홀 노드 탐지 기법의 평가는 Intel(R) Core(TM) i5-2467M CPU @ 1.60GHz, RAM 4GB 환경에서 NS-2 Simulator 버전 2.35[13,14]을 이용하였다. 표 2는 시뮬레이션 파라미터를 설명한 것이다.

표 2. 시뮬레이션 파라미터
Table. 2 the parameters of simulation

파라미터	값
시뮬레이터	NS-2 version 2.35
시뮬레이션 시간	100sec
시뮬레이션 영역	1000 × 1000m
센서 노드의 총 수	50
베이스 스테이션 수	1
코어 노드 수	5
악의적인 노드	5
라우팅 프로토콜	AODV
트래픽 유형	UDP-CBR
패킷 크기	512bytes
전송 범위	250m

실험에서는 메시지를 전달받은 코어 노드가 센서 노드의 키와 그룹키를 다르다면 시빌 공격으로 판단하고 전달받은 데이터를 버리도록 하였다. 그리고 근원지 노드에서 목적지 노드로 경로를 선정할 때, 웜홀 노드가 포함되어 있다고 판단되면 데이터를 버리도록 하였다.

그림 6은 공격이 없을 경우와 시빌 공격과 웜홀 공격이 존재할 경우의 실험결과를 설명한 것으로 악의적인 노드의 수가 증가할수록 패킷 전송 비율(Packet Delivery Rate)이 감소하는 것을 알 수 있다.

PDR(Packet Delivery Rate)는 목적지에 도착한 패킷의 수를 전송 패킷의 수로 나누는 방식으로 식(1)과 같이 계산하였다. 공격이 없는 경우의 평균 PDR이 92.6%, 시빌 공격이 있는 경우의 PDR은 81%, 웜홀 공격이 있는 경우의 PDR은 75.8%이다. 웜홀 공격이 있는 경우의 패킷 도착 비율이 더 낮은 것으로 나타났다.

$$PDR(\%) = \frac{\text{목적지에 도착한 패킷의 수}}{\text{근원지에서 전송한 패킷의 수}} \times 100 \quad (1)$$

그림 6. 패킷 도착 비율
Fig. 6 Packet Delivery Rate

그림 7은 시빌 공격과 웜홀 공격의 탐지율(Attack Detection Rate)과 FPR(False Positive Rate)를 설명하고 있다. 두 공격에 대한 탐지율 계산은 식(2)를 이용하였고, FPR은 식(3)을 이용하였다.

$$ADR(\%) = \frac{\text{공격으로 탐지된 수}}{\text{총 공격 수}} \times 100 \quad (2)$$

$$FPR(\%) = \frac{\text{False Positive로 탐지된 수}}{\text{총 실험 수}} \times 100 \quad (3)$$

실험결과, 본 논문에서 제안한 SWAD-KNH 기법의 시빌공격 평균 ADR은 91.2%, 웜홀 공격 평균 ADR은 90%이고, 시빌공격 평균 FPR은 3.82%, 웜홀 공격 평균 FPR은 4.64%이다. 즉, SWAD-KNH기법의 평균 ADR은 90.6%이고, 평균 FPR은 4.23%으로 센서 네트워크의 신뢰성을 향상시켰다고 볼 수 있다.

(a)

(b)

그림 7. 공격 탐지율과 FPR
(a) 공격 탐지율(ADR) (b) FPR

Fig. 7 Attack Detection Rate and FPR
(a) Attack Detection Rate(ADR) (b) FPR

V. 결 론

본 논문에서는 클러스터 단위로 센서 노드의 키와 그룹키를 생성한 후 분배하는 KGDC(Key Generation and Distribution based Cluster) 모듈과 센서노드 키, 그룹키, 이웃노드리스트, 그리고 홉 카운트를 이용하여 시빌 공격과 웜홀 공격을 탐지할 수 있는 SWAD(Sybil & Wormhole Attack Detection) 모듈로 구성되는 SWAD-

KNH(Sybil & Wormhole Attack Detection using Keys, Neighbor list, and Hop count) 기법을 설계하였다.

KGDC 모듈은 ECDH 알고리즘을 이용하여 베이스 스테이션과 코어 노드 사이의 그룹키를 생성하고, 해시 함수를 이용하여 코어노드와 센서노드 사이의 그룹키를 생성할 뿐만 아니라, 코어노드는 해시 키 체인 기법으로 센서 노드의 키들을 생성하고 안전하게 배포하도록 설계하였다.

SWAD 모듈은 2단계 키 확인절차를 수행함으로써 시빌 공격 탐지를 강화시켰으며, 근원지 노드와 목적지 노드의 이웃노드리스트를 생성하고, 두 노드의 이웃노드들의 수가 홉 카운트보다 크다면, 웜홀 노드가 존재하는 것으로 판단하여 웜홀 노드를 탐지하도록 설계하였다.

그 결과 SWAD-KNH 기법은 시빌 공격 평균 ADR과 웜홀 공격 평균 ADR이 각각 91.2%와 90%이고, 평균 FPR이 각각 3.82%, 4.64%으로 평가되므로 Sybil과 Wormhole 공격 탐지율 및 Sybil과 Wormhole 공격 탐지의 신뢰성을 향상시켰다고 볼 수 있다.

참고문헌

- [1] 나상호, 허의남, “센서 네트워크를 위한 안전한 노드 식별자 기반 위임 인증 프로토콜,” Information Network Review, vol.23, no.3, 2009. 12.
- [2] 한국인터넷진흥원, “USN 환경에서의 키관리 기술 적용 모델 개발,” KISA-WP-2009-0043, 2009.09.
- [3] 광진, 오수현, “분산 센서 네트워크용 키 분배 프로토콜 연구 동향,” 정보통신연구진흥원 주간기술동향, 제1307호, pp.1-9, 2007
- [4] 나채준, 채기준, 정교일, “센서 네트워크 보안 연구 동향,” ETRI 전자통신동향분석, 제20권, 제1호, 2005
- [5] 이채원, 허준, 홍충선, “WSN환경에서 논리적 그룹형성과 키 분배 방법,” 정보과학회논문지 : 정보통신 제 34권, 제4호, pp.296-304, 2007
- [6] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar, “SPINS : Security Protocols for Sensor Network,” In Proceedings of Seventh Annual International Conference on Mobile Computing and Networks, Rome, Italy, July 2001.

- [7] 이경화, “계층적 센서 네트워크 환경에서 이동노드를 위한 Trust Center 기반 키 관리기법,” 숭실대학교 대학원, 박사학위논문, 2010.12.
- [8] 문형석, 이성창, “무선 센서 네트워크에서의 효율적인 Broadcast Authentication 방안,” 전자공학회논문지, 제43권 TC편 제6호, pp.683-689, 2006.
- [9] 김완주, 남길현, 이수진, “무선 센서 및 액터 네트워크를 위한 효율적인 키 관리 프로토콜,” 정보과학회논문지 컴퓨터의 실제 및 레터, 제13권, 제7호, pp.540-544, 2007.
- [10] Adrian Perrig, R. Canetti, Briscoe, J. D. Tyger and D. Song, “TELSA : Multicast source authentication transform,” IRTF draft, draft-irtf-smug-telsa-00.txt, November, 2000.
- [11] S. Zhu, S. Setia and S. Jajodia, “LEAP : Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” CCS’03, pp.62-72, 2003.08
- [12] 정은희, 이병관, “USN 환경에서 ECDH 알고리즘을 이용한 KDPC(Key Distribution Protocol based on Cluster) 설계,” 한국정보통신학회 종합학술대회논문집, 제17권 제1호, pp.856-858, 2013.
- [13] The Network Simulator NS-2, <http://www.isi.edu/nsnam/ns/>
- [14] Nam: Network Animator, <http://www.isi.edu/nsnam/nam>

이병관(Byung-kwan Lee)

1979년 부산대학교 기계공학과
공학학사

1986년 중앙대학교 전자계산공학과
공학석사

1990년 중앙대학교 전자계산공학과 공학박사

1988년~현재 관동대학교 공과대학 컴퓨터학과 교수

※관심분야: 네트워크 보안

저자소개

정은희(Eun-hee Jeong)

1991년 강릉대학교 통계학과
이학사

1999년 관동대학교 전자계산공학과
공학석사

2003년 관동대학교 전자계산공학과 공학박사

2003년~현재 강원대학교 인문사회과학대학
지역경제학과 부교수

※관심분야: 네트워크 보안, 전자상거래 보안