무선 센서 네트워크 라우팅 보안 강화 기법의 설계

김우진○ 길아라
숭실대학교 컴퓨터학과
jin21110@hanmail.net, ara@ssu.ac.kr

A design of the wireless sensor network routing improved security method

Woojin Kim○, Ara Khil
School of Computing, Soongsil University

요 약 본 논문에서 제안하는 라우팅 기법은 분산된 센서 네트워크 상의 시작 노드에서 목적지 노드까지 데이터를 전송 할 때, 유효 데이터를 암호화 하고 그것을 분할하여 서로 다른 경로를 통해 전송함으로써 스니핑 공격에 암호화된 부분 데이터만 노출하여 정보 유출의 가능성을 감소한다. 스니핑 공격에 의한 정보 유출 가능성 감소의 정도는 시뮬레이션을 이용하여 전체 데이터를 단일 경로로 전송하는 경우와 비교한 실험 결과를 통하여 나타내 보이며, 해당 경로의 선택을 위한 알고리즘은 이론의 증명을 통해 나타내 보인다.
키워드 : 센서 네트워크, 정보 보호, 데이터 분할, 분산 라우팅, 스니핑

As a part of preparing the sniffing attack, this routing method presented in this thesis decreases the risk rates of the leaking of information through separating valid data and transmitting by a multi-path. then data is transmitted from start node to destination node on distributed sensor network. The level of reduction in leaking of information by the sniffing attack is proved by experimental result thich compare the case described above with the case of transmitting whole data with the single path by simulation, and the algorithm for choosing the routing path is showed by proof of the theorem.
Key words : sensor network, information protection, split data, distributed routing, sniffing

1. 서론

유비쿼터스 센서 네트워크(이하 USN)는 다수의 센서 노드로 구성된 무선 네트워크로써 다양한 위치에 설치된 센서 노드들로부터 사람과 사물 및 환경 정보를 인식한 후, 인식한 정보를 통합및 가공하여 언제, 어디서나, 안전하고 자유롭게 이용할 수 있게 하는 정보서비스 인프라를 뜻한다[1]. 즉, USN은 필요한 모든 곳에 센서 노드를 부착하고 이를 통해 주변의 여러 환경정보를 탐지해, 이를 실시간으로 네트워크에 연결해 정보를 관리한다[1,2].

USN을 통하여 전송하고자 하는 정보는 특정 지역의 정보를 담고 있기 때문에 그것을 대체할 수 있는 정보가 없다는 특성이 있다. 따라서 해당 정보에 대한 신뢰성을 확보하는 것이 중요하다. 하지만 센서 노드는 제한된 자원과 한정된 전력량을 가지고 그것을 재보급 할 수 없다. 이렇게 제한된 전력은 빈번한 네트워크의 진입과 탈퇴를 발생 시켜 잦은 위상의 변화를 가져온다[2]. 이는 기존의 네트워크처럼 모든 노드가 충분히 원할히 동작하고 충분한 자원을 활용할 수 있는 상황에서 제안된 각종 보안 기법을 적용하기 어렵다는 문제점을 야기한다[3]. 다양한 공격 기법에 노출된 환경과 기존의 보안 기법을 적용하기 어렵다는 점을 고려하여 USN은 기존의 보안 요구사항인 Confidentiality, Authentication, Integrity, Freshness 뿐만 아니라 USN의 요구사항인 Avaliability,, Secure Handoff 등을 만족 시킬 수 있는 보안 기법이 필요하다[4]. 해당 요구사항을 기준으로 USN에서 필요로 하는 보안 기능은 암호 알고리즘와, 키 관리 및 보안 인증 프로토콜, 라우팅 보안 기법, 보안 데이터 집합 관리 기법으로 압축한다[5]. 현재 이루어지고 있는 대부분의 USN 보안 기술은 키 분배 및 관리, 인증, 보안을 위한 네트워크 구조, 라우팅 등 다양한 보안요소가 결합된 형태를 취한다[6].

기존의 USN 보안 기법에 대한 연구는 암·복호화와 인증에 치우쳐 있다. 따라서 키가 노출되었을 때 모든 데이터를 노출할 가능성이 크다[7,8]. 이에 따라 보안을 위한 라우팅 구조에 대한 연구를 진행한다. 기존의 라우팅 기법이 키를 보호하고 그것에 따라 클러스터링을 구성하는 기법을 적용하였다면 본 연구 에서는 라우팅 계층에서의 패킷 보호기법을 기존의 논리적인 보호와 함께 물리적으로 보호할 수 있는 기법을

제안한다. 제안하고자 하는 기법의 성능은 수식과 시뮬레이션을 통한 공격가능 범위의 측정을 통해 나타내 보인다. 이를 위한 알고리즘은 사선식을 활용하여 방향성을 판단하여 적절한 라우팅 노드를 선택하는 알고리즘을 제시한다.

2. 관련 연구

센서 네트워크에서는 무선통신이라는 특성으로 인하여 도청이 용이하다. 이를 방지하기 위하여 센서 노드간에 주고받는 데이터에 대하여 암호화를 사용하여 기밀성을 보장한다. 이를 위해 IEEE 802.15.4표준규격[9]에서는 AES암호[7]를 사용하여 기밀성을 보장하도록 하고 있다. 따라서 AES의 암호 알고리즘은 하드웨어 블록으로 제공하고 있다. 사용자는 이를 통해서 통신 데이터에 대한 최소한의 기밀성을 보장할 수 있다. 하지만 AES암호화 알고리즘은 센서 노드가 분산되어 있다는 특성으로 인하여 키 분배 기법이 필요한 문제점을 가지고 있다. 키 분배 기법은 다양한 제안이 이루어지고 있으나 표준 규격으로 정해진 것이 없으며 각각이 장단점을 가지고 있다. 또한 센서 네트워크는 그 특성과 목적 때문에 물리적인 공격에 노출되기 쉬운 환경에 각 노드가 존재한다[10].

센서 네트워크의 물리적인 공격으로는 간단한 방법으로 물리적인 손상이나 절취 등이 가능하다. 그리고 방사되는 전자파 정보와 같은 부채널 정보를 사용하여 키 값 등의 정보를 알아내는 방법[11]이 있다. 이 기법으로는 SPA(simple power analysis attack)[12]와 DPA(differential power analysis attack)[13], EM(electromagnetic attack)[14] 공격 등이 있다. 이를 방지하기 위하여 side channel resistant인 공개키 암호 알고리즘을 적용하는 연구 등을 진행하고 있다. 타원 곡선 암호 알고리즘의 scalar multiplication 단계에서 SPA/DPA reasistant 한 인코딩 기법에 대한 연구가 이에 해당한다. 하지만 위의 기법은 비대칭 암호화기법이기 때문에 암호화에 소비되는 에너지가 매우 크다. 또한 위 기법은 키를 완전히 보호할 수 없는 기법은 아니므로 보안 키의 노출로 인한 도청 등의 공격에 대해 방어기제가 될 수 없으며 키가 공개된 이후에 해당 키를 이용한 2차적인 공격을 방어 할 수 없다. 대표적인 2차 공격방법으로는 Bogus routing information, Selective forwarding, HELLO Floods, Wormholes, Sybil attack, Acknowledgement spoofing 등[15]이 있으며 다른 기법은 이 기법 중 하나 이상을 변경 및 조합하여 사용하는 형태이다. 이를 방어하기 위해 SPIN[16], TinySec[17] 등의 보안 프로토콜이 제시되었다. 하지만 이는 네트워크의 도청 등에 의한 패킷 손실과 정보 유출에 대한 것은 암호화로만 처리함으로 특수한 상황 즉 물리적인 공격 등에 의해 키가 노출되었을 경우 그 공격에 대처할 수 있는 방법이 없다.

제안하고자 하는 기법의 목적은 노드간의 통신 시 스누핑을 통한 데이터의 유출 및 키 공개를 방지하는 것이다. 이를 위해 전송하고자 하는 데이터를 분산하여 두 개 이상의 서로 다른 경로를 통해 전달한다. 하나의 암호화 된 데이터를 두 개 이상의 패킷으로 분할하여 전송함으로서 해당 데이터를 모두 탈취하지 않는 이상 데이터를 확인할 수 없으며 해당 데이터에 대한 2차적인 공격을 방지한다. 분할된 데이터는 데이터의 보호효과를 극대화하기 위해 가상의 경로를 설정한다. 가상 경로는 상호간의 간섭을 최소화 하며 네트워크의 부하를 줄이기 위해 최대한 효율적인 경로를 상정한다. 이후 실제 라우팅을 수행할 시는 기 상정한 라우팅 경로와 오차가 가장 적은 라우팅 경로를 설정해야 데이터의 보호효과 및 에너지 소비에 대한 오버헤드를 줄일 수 있다. 이로 인하여 네트워크의 보안성과 생존성을 확충한다. 이러한 요구조건을 만족하는 라우팅 경로의 선정 기법을 제안한다.

3. 네트워크 구성 및 동작 알고리즘 설계

3.1 네트워크 구성을 위한 가정 및 정의

본 논문에서 제안하는 시스템은 다음과 같은 가정을 기반으로 한다.

가정 1. 노드는 싱크 노드와 센서 노드로 구분한다. 하나의 싱크노드와 수많은 센서 노드로 네트워크가 구성된다.

가정 2. 전체 센서 노드들은 자신의 위치를 알고 있다. 다중경로 보안 라우팅 프로토콜은 각 센서 노드와 싱크 노드가 GPS(Golbal Positioning System)나 사용자에게 위치 정보를 입력받아 자신의 위치를 알고 있다. 노드가 자신의 위치 정보를 알고 있으면 효율적으로 주변 노드를 찾을 수 있고[18], 토폴로지 구성 후 센서 노드에 의해 요구되는 질의 정보에 대해 생성되는 데이터의 위치를 파악한다.

가정 3. 싱크 노드는 전체 센서 노드들의 위치정보를 가지고 있다. 싱크 노드는 많은 에너지와 메모리 공간을 가지고 있어서 전체 센서 노드들의 위치정보를 네트워크가 구성될 때 전달 받는다. 위치정보는 데이터베이스 형태로 싱크 노드에 저장되고, 센서 노드의 위치를 판단할 때 사용된다.

가정 4. 모든 노드는 자신의 이웃노드를 알고 있다. 즉 자신과 한 홉으로 통신할 수 있는 노드의 좌표와 노드 번호를 통신으로 이미 알고 있으며 해당 이웃노드를 하나의 집합으로 분류하여 사용한다. 전체 네트워크의 노드 분포는 랜덤한 위치에 랜덤한 개수로 분포한다.

가정 5. 공격자 노드의 수신범위는 센서 노드와 동일하다. 센서 네트워크를 공격하는 공격 노드는 네트워크를 구성하는 노드와 동일한 수신 거리를 가지며, 공격자는 네트워크를 이루는 노드들 중에 일부를 포획하거나 새로운 노드를 침투시킨다.

가정 6. 공격자는 암호화된 데이터를 쉽게 풀 수 있다. 공격자는 포획된 노드를 통해 암호키를 얻거나 Cache Timing Attack[19]과 같은 기술을 이용하며 키를 찾아내고, 이를 통

해 암호화된 패킷을 복호화 할 수 있다.

본 논문의 기법을 제안하기 위한 정의는 다음과 같다.

def. Let n_i be sensor nodes in sensor network, where ni = (xi, yi) : a set N = {n0,n1,…nn}, and Let s, e where s, e ∈ N

def. Let F_{ni} be a set : n_i's neighbor, a set of nodes n_i can send message directly
F_{ni} = {n_j | n_i' neighbor}, F_{ni} ⊂ N

def. Let count be number of path, S, E be sets:
S = {s_i = n_i | n_i ∈ F_s, i < count},
E = {e_i = n_i | n_i ∈ F_e, i < count}

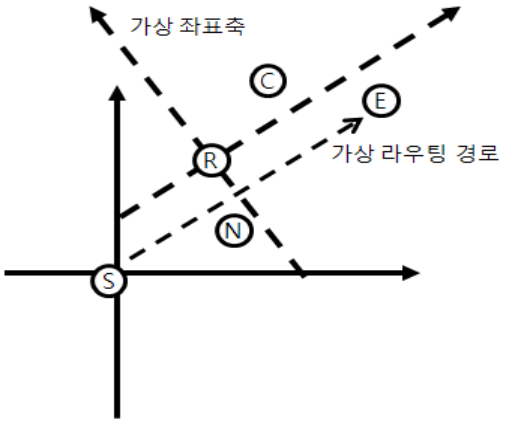
3.2 라우팅 노드 선정 알고리즘

라우팅 노드에서의 후보군 선정 과정은 다음과 같다.

1. 패킷 수신
2. 이웃노드군 중 후보군 선정
3. 후보군 중 다음 라우팅 패킷 전달 노드 선정

1에서 data를 수신한 노드는 해당 data의 header를 확인하고 방향을 설정한다. 그리고 방향에 따른 좌표축의 변환을 수행한 후 이웃 노드 중 후보군을 선정하여 해당 후보군 중 가장 경로에 일치하는 노드를 선정하는 방식이다. 위의 전체 알고리즘은 세부적으로 후보군의 선정과정과 후보군 중 라우팅 노드의 선정 과정으로 나눌 수 있다.

후보군 선정과정은 현재 라우팅 경로의 진행 방향에 역행하는 노드를 후보군에서 제거하여 경로 상의 무한 루프 등의 비정상적인 라우팅 경로를 취하는 것을 방지하기 위한 기법이다. 우선 이웃 노드 군을 자신의 좌표를 기준으로 평행이동한 값으로 재배치한다. 그리고 패킷의 header에 포함되어 있는 start와 end 노드 사이의 각에 대한 sin, cos 값을 가지고 해당 방향을 판단한 후 해당 방향으로 각각의 이웃 노드군을 회전이동 하여 1사분면과 4사분면 두 영역에 있는 노드를 후보군으로 선정한다. 이를 통해 경로의 진행 방향에 역행하는 노드가 후보에서 배제되어 올바른 진행방향에서의 라우팅 노드를 선정할 수 있다. 후보군 선정 기법의 세부적인 과정은 라우팅을 위한 후보군 선정 기법은 [그림 1]과 같이 이루어진다.



[그림 1] 후보군 선정을 위한 좌표축 변환

현재의 라우팅 노드가 패킷 전달이 가능한 후보군을 선정하기 위해 가상의 라우팅 경로와 x축이 평행하고 자신의 주소를 원점으로 하는 가상의 좌표축을 선정하고 자신의 이웃군 노드를 가상의 좌표축에 따른 새로운 좌표로 변환한다. 이때 각각의 노드는 자신의 이웃노드를 모두 알고 있다는 가정을 한다. end 노드까지 메시지를 전송하기 위해 유효한 방향에 있는 노드를 찾기 위해 좌표축 변환을 마친 이웃군 중 x좌표가 양인 노드가 [그림 1]에서의 c로 표현한 메시지를 전송하기 위한 유효한 후보이다. 해당 후보노드를 집합으로 묶은 것이 집합 C 이다.

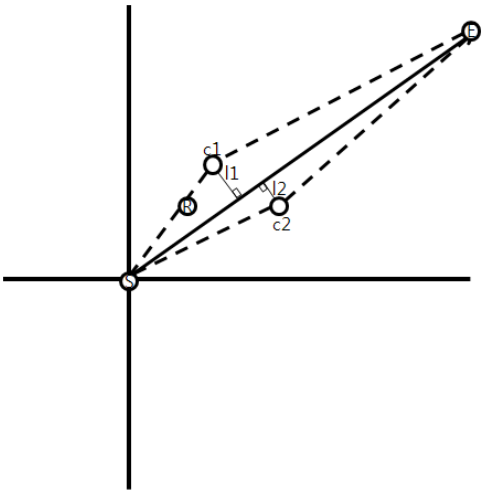
이를 선정하는 전체의 후보군 선정에 사용하는 식은 (1)과 같다.

$$C_{\ni} = \{n_j | where\, n_j \in F_{\ni}, \cos\theta_i * (x_{nj} - x_{\ni}) + \sin\theta_i * (y_{nj} - y_{\ni})\} \quad (1)$$

이 식은 좌표축의 평행이동과 회전이동을 모두 수행한다. 그리고 회전 변환에 의한 연산은 삼각함수의 연산에 의한 오버헤드가 크고 하나의 사분면만을 방향으로 선택할 때 최선의 선택을 할 수 없으므로 X축에 대한 연산만으로 해당 후보군을 선정한다.

두 번째로 라우팅 노드의 선정과정은 다음과 같다.

데이터를 전송하고자 하는 노드가 해당 데이터를 분할하여 전송할 때 자신이 전송할 노드의 좌표를 알고 있으므로 전송하고자 하는 노드는 송신 노드의 좌표와 수신 노드의 좌표를 패킷에 입력하여 전송한다. 라우터 역할을 수행하는 노드들은 [그림 2]과 같이 송신 노드와 수신 노드의 좌표를 기반으로 가상의 직선을 산정한다. 가상의 직선과 자신의 이웃노드간의 거리가 가장 짧은 노드를 다음 노드로 선정하는 것이다. 즉 [그림 2]와 같이 노드 R이 다음 라우팅 노드를 선정하고자 할 때 해당 이웃 노드가 c1과 c2가 존재한다고 가정하자. 그리고 c1과 c2의 위치와 가상의 라우팅 경로 사이의 거리를 l1, l2라 하자. 이때 R은 l1과 l2의 길이를 비교하여 가장 짧은 길이를 가지고 있는 노드를 다음 라우팅 노드로 선정한다.



[그림 2] routing 노드 선택 과정

여기서 각각의 노드와 가상 라우팅 경로 사이의 거리를 비교하여 최적의 라우팅 노드를 선정하기 위해 하나의 thm을 제안한다.

thm. 사선식으로 선택한 min 값을 가지는 node는 전체 오차에서 최소오차를 가지는 값이다.

이에 대한 증명은 4장에서 한다.

이것은 두 점의 x, y 좌표를 알고 있다면 가능하다. 이것은 사선식을 사용하여 각 후보노드와 start, end 노드가 만드는 삼각형의 넓이를 구하고 해당 삼각형의 넓이가 가장 작은 삼각형을 가지는 점이 선택된다. 사선식은 세 점을 알 때 삼각형의 넓이를 구하는 공식이다. 본 논문에서는 삼각형의 넓이를 구하는 것이 중요한 것이 아니므로 이 중 불필요한 부분을 제외하고 비교 하고자 하는 대상만을 선택한다면 아래의 (2)와 같은 식을 도출할 수 있다.

$$\begin{vmatrix} x_1 & x_2 \cdots & x_{n-1} & x_n \\ y_1 & y_2 \cdots & y_{n-1} & y_n \end{vmatrix} = \left| \begin{matrix} (x_1y_2 + x_2y_3 + \cdots + x_{n-1}y_n + x_ny_1) \\ -(x_2y_1 + x_3y_2 + \cdots + x_ny_{n-1} + x_1y_n) \end{matrix} \right|$$

$$x_1y_2 + x_2y_3 + x_3y_1 - x_2y_1 - x_3y_2 - x_1y_3 \qquad (2)$$

이 중 start point (x_1, y_1)와, end point (x_2, y_2)는 미리 알고 있고 각각의 노드는 자신의 주변 노드의 좌표를 알고 있다고 가정하였으므로 해당 넓이의 비교가 가능하다.

즉 후보노드 (x_3, y_3)를 변화해가며 가장 작은 값을 찾아 그 노드로 전송하는 것이다.

전체적으로 다음 노드를 선택하는 알고리즘은 아래 수식과 같다.

$t = set\,of\,candidate$

$n_k = selected \neq xt\,node$

$$n_k = \min(x_1y_2 + x_2y_t + x_ty_1 - x_2y_1 - x_ty_2 - x_1y_t) \qquad (3)$$

위에서 언급한 정의와 (1), (2), (3)의 수식을 바탕으로 한 전체적인 후보노드 선정 알고리즘은 다음과 같다.

thm. Let $\sin\Theta_i$ = $\sin\Theta$ between s_i, e_i where i < count,
$\cos\Theta_i$ = $\cos\Theta$ between s_i, e_i where i < count
,and let R_i = {node set of path between s_i, e_i}
,then C_{ni} = {n_j|where $n_j \in F_{ni}$, $\cos\Theta_i*(x_{nj}-x_{ni})+\sin\Theta_i*(y_{nj}-y_{ni}) > 0$}
so, next node r_{ij} = n_j, where
n_j = $\min(x_s*(y_{ei}-y_{nj}) + x_{ei}(y_{nj}-y_{si}) + x_{nj}(y_{si}-y_{ei}))$, $n_j \in C_{ni}$

전체의 알고리즘에서 제시한 기법을 적용하기 위해 start node는 start node와 end node 사이의 sin값과 cos값 그리고 end node의 좌표 등의 정보가 필요하다. 하지만 이 값은 라우팅 노드에 영향을 받지 않는 정보이고 해당 연산에 소비하는 오버헤드가 크므로 이를 매번 라우팅을 수행하는 노드에서 연산을 수행하는 것은 비효율적이다. 따라서 해당하는 값을 start node에서 미리 연산하여 전달할 필요가 있다. 이에 따라 해당 정보를 추가하여 구성한 헤더를 포함한 메시지 패킷의 형태는 [그림 3]으로 제시할 수 있다.

2byte	2byte	2byte	4byte	4byte	2byte	4byte	4byte	12byte
MSG No	Start Id	End Id	Start addr	End addr	Current Id	Sinθ	Cosθ	Data

[그림 3] 메시지 포맷

4. 성능 분석

본 기법의 적용 시 사용가능성을 확인하기 위하여 수학적인 증명 및 해당 기법을 적용하여 시뮬레이션을 수행하였다.

1. 증명

본 기법에서 제안한 이론의 증명은 다음과 같다.

thm. 사선식으로 선택한 min 값을 가지는 node는 전체 오차에서 최소오차를 가지는 값이다.

proof>

let s, e, s = (x_0, y_0), e = (x_n, y_n)

then we can make linear equation y = ax + b,

where $y_0 = ax_0 + b$ (1)

$y_n = ax_n + b$

then, $a = (y_0-y_n)/(x_0-x_n)$, $b = y_0 - ax_0$

and we select A for route s to e for read route.

then by least square method, standard error is

$\Phi(a, b) = \Sigma(ax_k + b - y_k)^2$ (where k = 1,…n-1)

and at point A

$(ax_\alpha + b - y_\alpha)^2 - ax_\alpha+b)^2 - 2((ax_\alpha + b)y_\alpha) + y\alpha^2\beta$ (2)

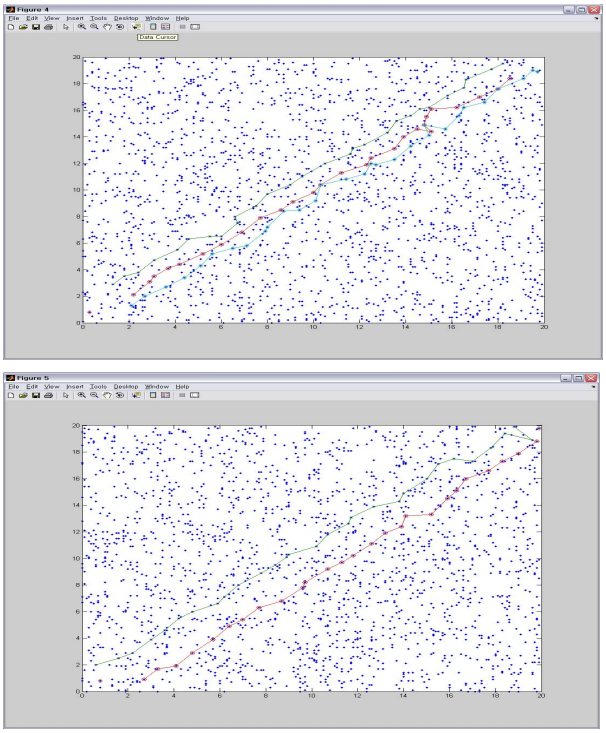
…

$= (x_\alpha y_0 + x_0y_n + x_ny_\alpha - x_\alpha y_n - x_ny_0 - x_0y_\alpha)^2 / (x_0 - x_n)^2$ (3)

s와 e를 start node와 end node라고 설정 하였을 때 여기서 가상의 직선을 만들 수 있고 그 직선의 방정식을 1과 같다 하자 이 때 s와 e사이의 공간에 실제의 경로를 설정할 수 있다. 이 경로는 최소 자승법에 의해 각각의 노드 전달 당 error를 산출할 수 있고 해당 산출 기법은 2와 같다. 그때 산출 기법을 변형하면 3과 같은 식이 나온다. 3은 사선식으로 산정한 현재 노드에서 최선의 노드를 선택하는 공식과 동일하다. 본 증명을 통해 각각의 노드에서 제안하고자 하는 알고리즘을 적용하여 최선의 노드를 탐색 시 전체 경로에서도 최선의 노드가 선정된다는 것을 확신할 수 있다.

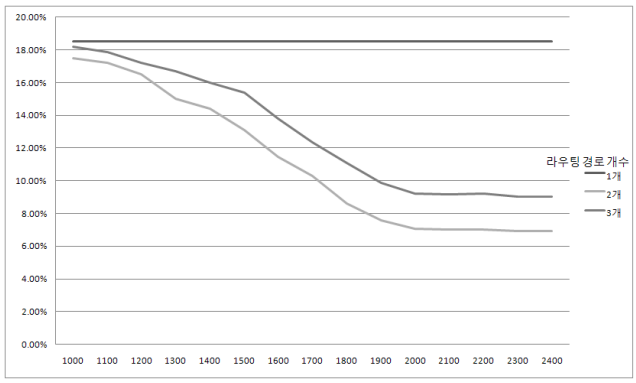
2 시뮬레이션 결과

본 기법의 정확한 성능분석을 위하여 시뮬레이션을 통해 20m*20m의 400m^{2}의 영역에 네트워크 영역을 설정하고 2000개의 노드를 랜덤한 위치에 조밀하게 구성된 네트워크 상의 노드를 바탕으로 실험한다. 각 노드의 통신 가능 범위는 1m로 설정하였다. 테스트를 위하여 start node의 좌표를 (0,0) end node를(19,19)로 선정하고 각각의 영역에서 패킷의 라우팅 경로의 개수를 조정하여 해당 라우팅 선정경로와 송신 노드와 수신 노드를 랜덤한 위치로 선정하였을 때 공격 가능 범위를 측정하였다 라우팅 경로를 3개와 2개로 구분한 경로선정 그래프는 [그림 4]와 같다. [그림 4]에서의 각 점은 각각의 노드를 나타낸다. [그림 4]는 20m*20m의 랜덤한 노드 배치 상에서 해당 라우팅 경로 설정을 보여준다. 라우팅 경로의 선정은 노드가 밀집되어 있는 네트워크 구조를 가질 때 원할히 이루어지며 해당 경로의 선정은 산정한 가상의 경로를 최대한 유지하는 것을 확인할 수 있다.



[그림 4] 라우팅 경로 구성도

또한 해당 영역에서의 밀집도에 따른 경로 중복도를 확인하기 위하여 [그림 5]와 같이 해당 네트워크 영역에 배치하는 노드의 개수를 변화시켜 공격가능 영역의 범위를 측정하였다.



[그림 5] 노드 밀집도에 따른 공격가능 영역 변화

본 기법을 적용하였을 때 우선 1개의 라우팅 경로만을 가지고 있을 경우 해당 라우팅 시 공격 가능 영역의 범위는 달라지지 않는 것을 알 수 있었으며 평균 18% 정도의 공격가능 영역을 내포한다. 다중 경로로 분할한 경우 반경 400m^2 를 기준으로 1400개의 노드를 배치하였을 때는 1개의 경로를 사용하는 경우와 거의 차이가 없지만 약 2000개 정도의 충분하게 다양한 경로를 사용할 수 있는 경우에는 각각 약 7%와 9%정도로 공격가능 영역이 감소하는 것을 확인하였다. 그리고 노드가 충분히 밀집한 이후에는 노드 밀집도가 높아질 경우에도 공격가능 영역이 크게 감소하지는 않는 것을 확인하였다. 그리고 각각의 영역별 공격가능성과 라우팅시의 오버헤드는 3개의 영역으로 구분 했을 때 해당 라우팅의 소비패킷은 약 200~250개이며 3개의 패킷 전체가 노출되는 정도는 약 9%정도의 공격 노출 범위를 보인다. 반면에 2개의 영역으로 구분하였을 경우는 전체 라우팅 소비패킷도 160~220개 정도로 감소하며 약 7%정도의 공격 노출 범위를 가져 3개의 다중경로 선정보다 2개의 경로선정이 더 유리한 것으로 나타난다.

5. 결론

USN은 다수의 센서 노드로 구성된 무선 네트워크로서 그 연구의 필요성과 응용분야가 확대되는 분야이다. 무선 센서 네트워크는 그 특성상 제한적인 자원이 할당되므로 다른 네트워크 환경보다 보안기법을 적용하기 힘들다. 특히 USN의 스니핑 공격 방지를 위한 암호화 기법의 경우 물리적인 공격을 통해 해당 키를 알아내어 2차적인 공격으로서 적용이 매우 쉽다.

본 논문에서 제안하는 기법은 공격자가 암호화 키를 입수하여 해당 키를 통해 데이터를 복호화 할 수 있다 하더라도 유효할 데이터를 확보할 수 없도록 패킷을 암호화 한 후 해당 패킷을 분할하여 다중경로를 통해 전송한다. 해당 경로에서의 패킷 탈취 가능성을 최소화 하기 위하여 해당 경로의 중복을 막고 원할한 전송을 유지하는 기법을 제안한다. 이를 통해 단

일 경로로 전송하는 라우팅 기법에 비해 약 10%~ 12%정도의 패킷 공격가능 범위를 줄일 수 있다. 다만 중복된 경로를 통해 전송함으로서 라우팅 패킷의 개수가 늘어 해당 데이터의 전송 시 소비하는 에너지의 양이 증가하지만 이는 네트워크 구성과 유지를 위해서 소비되는 패킷의 양과 합쳐 전체의 네트워크 소비 패킷에서 비교했을 때 매우 작은 양의 증가폭을 가져온다. 또한 보호하고자 하는 데이터의 크기가 커져도 전달하는데 필요한 오버헤드는 동일하여 데이터의 크기가 커질수록 더욱 효율적이다.

다만 네트워크의 노드 밀집도가 감소할 때 라우팅 경로를 유지하기 위하여 경로의 중첩이 발생 할 수 있고 경로의 중첩이 많을 수록 스니핑 공격에 의한 방어기제로서의 역할수행이 힘들어지므로 노드 밀집도가 감소한 상황에서의 경로 분산처리와 공격에 의한 특정 데이터의 유실시 해당 데이터를 복구하는 연구가 향후 연구과제로 남아있다.

references

[1] Mark Weiser, “Hot Topic: Ubiquitous Computing”, IEEE Computer, October 1993.

[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci., "Wireless sensor network: a survey.", Computer Networks, April 2002.

[3] H. Cam, S. Ozdemir, D. Muthuavinashiappan, and P. Nair, "Energy-efficient security protocol for wireless sensor networks", IEEE VTC Fall 2003 Conference, Orlando, October 2003.

[4] “유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향연구”,한국정보화진흥원 December 2004.

[5] Tieyan Li,"Security Map of Sensor Network", Institute for Infocomm Research, March 2005.

[6] “센서 네트워크 보안 연구 동향”, 전자통신동향분석 제20권 제1호, February 2005.

[7] J.Deamen and V.Rijmen, "AES proposal: Rijndael Block Cipher", NIST Document ver.2, Mar 1999.

[8] R. Baldwin, R. Rivest “The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms”, RFC 2040, October 1996.

[9] IEEE Std. 802.15.4-2003.

[10] 김호원, 이석준, 오경희, "센서네트워크 보안 기술 개발 동향", 한국정보보호학회, 정보보호학회지, 제18권 제2호 April 2008.

[11] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," in Proceedings of ESORICS ''98, Springer-Verlag, September 1998.

[14] S. Mangard, "A Simple Power-Analysis (SPA) attack on implementations of the AES key expansion", ICISC 2002, LNCS 2587, Springer-Verlag, 2002.

[13] P. Kocher, J. Jaffe, and B. Jun, “"Differential power analysis,"" in Advances in Cryptology: Proceedings of CRYPTO''99, M. Wiener, Ed., 1999, vol. 1666 of LNCS, pp. 388 - -397, Springer-Verlag.

[14] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic analysis: Concrete results,” in Proceedings of 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES), C¸ . K. Koc¸, D. Naccache, and C. Paar, Eds., 2001, vol. 2162 of LNCS, pp. 255 - -265, Springer-Verlag.

[15] Chris Karlof and David Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, to appear First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[16] A. Perrig and R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom), 2001.

[17] Chris Karlof, Naveen Sastry, David Wagner, “TinySec : A Link Layer Security Architecture for Wireless Sensor Networks”, Sensys 2004.

[18] B. Karp and H. T. Kung, "GPSR: Greedy perimeter Stateless Routing for Wireless Networks." Proceedings of ACM/IEEE MobiCom 2000, August 2000.

[19] Courtois, N.T. and Pieprzyk, J. “Cryptanalysis of block ciphers with overdefined systems of equations.” In: Zheng, Y. (ed.) Advances in Cryptology – ASIACRYPT 2002 8th International Conference on the Theory Application of Cryptology and Information Security Queenstown, New Zealand, December 1 - 5, 2002 Proceedings. Lecture Notes in Computer Science (2501). Springer Verlag, Berlin/ Heidelberg, Germany.