애드-혹 무선 네트워크에서 보안을 고려한 생존정보 전달 프로토콜

김형진*, 조영종*, 강경란*
*아주대학교 컴퓨터공학과
e-mail : gilsiun@ajou.ac.kr

A Secure Liveness Information Dissemination Protocol for Wireless Ad-hoc Networks

Hyung-Jin Kim*, Young-Jong Cho*, Kyung-ran Kang*
*Dept. of Computer Engineering, Ajou University

요 약

애드-혹 무선 네트워크를 구성하고 유지하기 위해서는 네트워크 내에 생존하고 있는 노드에 대한 정보가 공유되어야 한다. 본 논문에서는 영공간(null-space)을 활용하여 효율적이면서 보안을 유지할 수 있는 생존정보 전달 프로토콜을 제안한다. 이론적인 분석에서 제안하는 프로토콜은 생존 정보를 누적함으로써 전송횟수를 최소한으로 줄일 수 있고 도청과 오염 공격에 대해 강건함을 확인하였다.

1. 서론

무선 센서 네트워크 혹은 전장 네트워크 등의 애드-혹 네트워크에서는 실제적인 데이터 통신에 앞서 통신하고자 하는 노드가 현재 정상적으로 기능하고 있는지를 파악할 필요가 있다. 주기적으로 혹은 필요할 시 노드들의 생존정보를 수집함으로써 현재 어떠한 노드들이 작동하고 있는지를 한 번에 파악할 수 있으며, 이미 기능하지 않고 있는 노드와의 통신 시도를 차단할 수 있다.

이러한 생존정보를 전달하는 방식으로는 개별 전송 방식과 인덱스-마킹 방식이 있다. 개별 전송 방식은 생존정보 전송을 요구 받은 모든 노드들이 각자의 ID 를 담은 ACK 메시지를 중간의 다른 노드들을 통해 최초의 정보요구자에게 전달하는 방식이다. 이 방식은 네트워크 상의 노드의 수만큼 메시지가 발생하기 때문에 전송 횟수의 측면에서 비효율적이다. 인덱스-마킹 방식은 각 노드들이 자신의 인덱스와 엿들은 정보로부터 얻은 노드들의 ID 를 마킹하여 주변으로 전달하는 방식으로 개별 전송 방식의 단점인 전송 횟수를 줄일 수 있다. 하지만 인덱스-마킹 방식 또한 도청과 오염 공격에 매우 취약할 수 있다는 단점이 존재하기 때문에 보안이 요구되는 네트워크에서는 사용되기 어렵다.

본 논문에서 제안하는 영공간(null-space)을 활용한 생존정보 전달 방식은 인덱스-마킹 방식과 동일한 전송 횟수에 생존정보를 전달할 수 있으며 도청과 오염 공격 모두에 뛰어난 저항성을 가지고 있다. 서로 통신하는 노드들 간에 미리 알고 있는 ID 테이블이 없고 ID 의 길이가 적당히 길다면, 악의의 공격자가 생존정보 메시지를 도청한다 하더라도 정보를 해독해낼 수 없으며, 유효한 오염 메시지를 생성할 확률도 지극히 낮다.

2. 제안 기법

2.1 부분 공간과 영공간

n 개의 노드가 애드-혹 네트워크를 구성하고 있다고 가정한다. 각 노드의 ID 는 유한체 $\mathbb{F}_q$로부터 선택된 $d(d > n)$ 개의 element 로 이루어져 있으며 ID 벡터 간 서로 일차독립인 고유의 ID 벡터를 가진 것으로 생각할 수 있다. 노드 i 의 ID 벡터를 x_i로 두었을 때, X 는 i 번 째 열이 x_i인 $d \times n$ 행렬이라고 표기한다. 이 때 Π_X는 기저벡터 $\{x_1, x_2, \dots, x_n\}$로 이루어진 부분공간을 나타내며 $\Pi_X^{\perp}$는 X 의 영공간을 나타낸다[2]. 행렬 X 의 영공간 $\Pi_X^{\perp}$은 $zX = 0$ 을 만족하는 모든 벡터 z 로 이루어진 공간을 의미한다. $m \times n\ (m > n)$ 행렬 A 가 주어질 때 다음과 같은 식을 만족한다.

$$\mathrm{rank(A)} + \mathrm{nullity(A)} = \mathrm{m} \qquad (1)$$

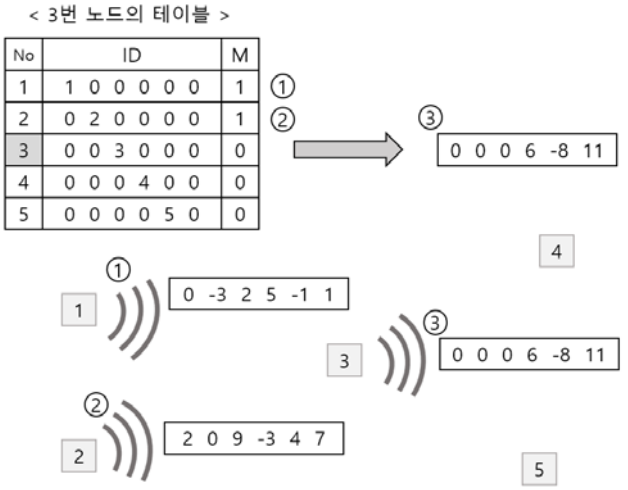
X 행렬에서 rank(X) 는 n 이며 nullity(X) 는 $d - n$ 이 될 것이다. 따라서 행렬 X 의 영공간은 $d - n$ 차원이다[1].

2.2 전달 방식

노드가 생존정보를 주변에 전파할 때 자신이 현재까지 축적한 생존정보를 이용하여 임의의 영공간 벡

터를 계산해낸 후 이를 전송한다. 이 영공간 벡터는 자신과 주변 노드들이 가진 생존 정보, 즉 정상적으로 작동하고 있는 노드들의 ID 벡터를 행렬 X 로 나타냈을 때 $\Pi_X^{\perp}$ 의 벡터 중 임의의 하나를 선택한 벡터이다. 이를 위한 기본 가정으로 각 노드에서 영공간을 계산해내기 위해 다른 모든 노드의 ID 벡터 정보를 테이블의 형태로 소유하고 있어야 한다.

각 노드는 주변의 다른 노드들이 전송하는 생존정보 메시지를 수신할 때마다 ID 벡터 테이블에서 아직 생존이 확인되지 않은 각 노드 번호의 열 벡터와 내적을 수행하여 0 이 나오는지를 확인함으로써 다른 노드들의 생존정보를 갱신한다.



(그림 1) n = 5, d = 6 일 때 생존정보 전달 과정

그림 1 은 생존정보 전달 과정 중간에서 노드 3 이 자신이 가지고 있는 생존정보를 생성한 후 전송하는 모습을 나타낸 것이다. 노드 3 은 자신의 전송 타이밍이 아닐 때에는 노드 1 과 노드 2 가 전송하는 생존정보를 엿들으면서 자신의 ID 벡터 테이블의 정보를 갱신한다. 노드 3 이 노드 1 로부터 [0 -3 2 5 -1 1] 를 수신하면 테이블의 각 ID 벡터와 내적을 수행한다. 이 벡터는 노드 1 의 ID 벡터와만 내적값이 0 이 되므로 노드 1 이 전파하는 생존정보 메시지로부터 노드 1 이 생존해 있음을 알 수 있다. 이와 같은 방식으로 노드 2 가 전파하는 메시지도 수신하여 같은 작업을 수행한다. 노드 3 의 생존정보 전송 시, 지금까지 축적한 ID 벡터 테이블의 정보를 토대로 임의의 영공간 벡터를 생성한 후 이 ID 벡터를 전송한다.

3. 분석

3.1 전송횟수

인덱스-마킹 방식과 영공간 활용 방식의 전송횟수는 동일하다. n 개의 노드로 이루어진 네트워크에서, 최악의 경우인 노드들이 일렬로 위치한 경우라 하더라도 $O(n)$ 의 횟수 내에 생존 정보 전송을 완료할 수 있다. 그러나 개별 전송은 최악의 경우 $O(n^2)$ 의 전송횟수가 필요하다.

3.2 도청과 오염 공격

인덱스-마킹 방식의 경우 도청자가 생존정보 메시지의 구조를 알고 있다면 손쉽게 다른 노드들의 생존정보를 파악할 수 있을 뿐만 아니라 마킹 정보를 조작하여 전송함으로써 생존정보의 오염을 초래할 수 있다. 하지만 영공간 활용 방식의 경우 도청자가 ID 벡터 테이블을 알고 있지 않다면 생존정보 메시지를 도청하더라도 노드들의 생존 정보를 알아낼 수 없다. 영공간 활용 방식에서 오가는 생존정보 메시지는 전체 노드 ID 벡터가 이루는 벡터 공간 중에서 일부 차원, 즉 생존이 확인된 노드들의 ID 벡터가 이루는 영공간에서 임의로 선택된 하나의 벡터이기 때문에 아무리 많은 생존 정보 메시지를 도청한다 하더라도 이를 통해 생존 정보를 유추해낼 수 없다.

생존정보 조작을 통한 오염 공격의 경우 두 방식 모두 실제로 동작하지 않는 노드들도 정상적으로 동작하고 있는 것처럼 조작을 시도한다. 그 반대의 경우(정상적으로 동작하지만 실제로 동작하지 않는 것처럼 조작)는 공격자 노드가 아닌 정상 노드가 조작을 시도하는 번호의 노드로부터 생존정보 메시지를 수신하였을 경우 공격자 노드가 성공적으로 오염 메시지를 생성하여 전송하였다 하더라도 최종적으로 생존 정보를 취합하면 정상적으로 생존정보를 알 수 있으므로, 노드들이 희박하게 분포한 환경이 아니라면 공격이 성공할 수 없다.

동작하고 있지 않은 노드 중 하나라도 정상적으로 동작 중인 것처럼 조작된 메시지를 생성해낼 수 있는 확률은 다음과 같다[3].

$$1-\left(1-\frac{q^n}{q^{d-n}}\right)^n = 1-\left(1-\frac{1}{q^d}\right)^n \quad , \qquad (2)$$

여기서, d 는 ID 벡터의 길이, q 는 유한체의 크기, 를 의미한다. 따라서 ID 벡터의 길이와 유한체의 크기가 충분히 크다면, 메시지를 임의로 만들어내는 오염 공격이 성공할 확률은 0 에 가까워진다.

4. 결론

본 논문에서는 애드-혹 네트워크에서 노드들 간의 생존정보를 교환할 때 영공간을 활용하여 효율적이면서 보안을 유지할 수 있는 프로토콜을 제안하였다. 이에 대한 이론적 분석을 바탕으로, 향후 실험을 통해 제안한 영공간 활용 방식을 기존의 개별 전송 방식이나 인덱스-마킹 방식과 비교하여 전송횟수와 보안적 측면에서 비교할 예정이다.

참고문헌

[1] D. Poole, Linear Algebra: *A Modern Introduction*, 2nd Ed., Thomson Brooks, 2006.

[2] D. Koutsonikolas, C. Wang, Y. C. Hu, “Efficient Network-Coding-Based Opportunistic Routing Through Cumulative Coded Acknowledgments,” IEEE/ACM Transaction on Networking, vol.19, no.5, Oct. 2011.

[3] E. Kehdi, B. Li, “Null Keys: Limiting Malicious Attacks Via Null Space Properties of Network Coding,” in Proc. IEEE INFOCOM, 2009.