한국컴퓨터정보학회 하계학술대회 논문집 제21권 제2호 (2013. 7)

센서 네트워크에서 선택적 전달 공격 방어를 위한 GPSR 프로토콜 적용

문수영°, 이민정*, 조대호*
°*성균관대학교 정보통신대학
e-mail:{moonmouse, Radiantsun, thcho}@skku.edu°*

Application of GPSR Protocol for Countering Selective Forwarding Attacks in Sensor Networks

Soo Young Moon°, Minjung Lee*, Tae Ho Cho*
°*College of Information and Communication Engineering, Sungkyunkwan University

● 요 약 ●

센서 네트워크는 주변의 환경 정보를 수집하여 사용자에게 제공함으로써 지능적인 처리를 가능하게 하는 시스템이다. 센서 네트워크를 구성하는 센서 노드들은 메모리, 연산 능력, 에너지 등 자원 측면에서 제약을 갖고 있으며 무선 통신을 사용하므로 센서 네트워크 환경에서는 각종 보안 위협이 발생할 수 있다. 선택적 전달 공격에서 네트워크 내의 훼손 노드는 자신을 지나는 이벤트 보고서 중 전체 또는 일부를 제거함으로써 중요한 이벤트 정보가 싱크 노드까지 도달하지 못하도록 한다. 선택적 전달 공격을 방어하기 위한 기존 라우팅 기법은 많은 에너지 소비를 유발한다는 단점이 존재한다. 본 논문에서는 지형 기반의 라우팅 프로토콜인 Greedy Perimeter Stateless Routing (GPSR) 프로토콜을 기반으로 선택적 전달 공격 발생 지점을 우회할 수 있는 방법을 제안한다. 제안 기법은 선택적 전달 공격이 발생하는 환경에서 에너지 효율적으로 소스 노드에서 기지 노드까지 이벤트 보고서를 신뢰성 있게 전달하는데 활용될 수 있다.

키워드: 센서 네트워크(sensor network), 선택적 전달(selective forwarding), GPSR

I. 서 론

센서 네트워크는 빛, 습도, 움직임 등 주변의 환경 변화를 감지하고 계산을 통해 감지된 데이터를 유용한 정보로 변환하여 사용자에게 제공할 수 있는 시스템이다 [1, 2]. 센서 네트워크는 크게 이벤트 정보를 감지, 전달하기 위한 다수의 경량 센서 노드들과 수집된 정보를 취합하여 사용자에게 제공하기 위한 하나 이상의 싱크 노드로 구성된다.

센서 네트워크는 센서 노드들의 에너지, 계산 능력, 메모리 등 자원 측면에서 제한되어 있고 무선 통신을 사용하므로 보안 관점에서 매우 취약하다. 특히, 선택적 전달 공격은 소스 노드에서 발생한 정상 이벤트 보고서가 사용자에게 전달되지 못하도록 하는 서비스 거부 공격 (Denial of Service)이다 [3]. 선택적 전달 공격에서는 공격자에 의해 훼손된 노드가 포함된 라우팅 경로를 통과하는 정상 이벤트 보고서 중 전체 또는 일부가 제거되어 싱크 노드까지 전달되지 못하게 된다. 선택적 전달 공격은 시스템의 가용성을 심각하게 저해하는 공격이므로 이에 대한 대응 방안이 필요하다.

본 논문에서는 기존 라우팅 프로토콜의 하나인 Greedy Perimeter Stateless Routing (GPSR) [4]의 경로 설정 방법을 적용하여 선택적 전달 공격에 대응하는 방법을 제안한다. GPSR에서 보고서 전달 경로 상의 각 노드는 이웃 노드의 위치 정보에 기반 하여 greedy algorithm에 따라 다음 노드를 선택한다. 또한 GPSR은 greedy algorithm이 적용될 수 없는 지역에서는 perimeter routing을 사용하여 해당 지역을 우회하는 기능을 제공한다. 제안 기법은 이벤트 보고서 전달 중 선택적 전달 공격이 탐지될 경우 해당 지역을 GPSR의 perimeter routing을 활용하여 우회하는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 제안 기법의 배경 이론에 해당하는 GPSR 프로토콜의 동작 과정을 설명한다. 3장에서는 제안 기법에서 GPSR을 활용하여 선택적 전달 기법에 대응하는 방안을 설명한다. 4장에서는 결론과 향후 연구방향을 제시한다.

II. 배경 이론

1. GPSR

Greedy Perimeter Stateless Routing (GPSR) [4]은 무선 네트워크 환경을 위한 라우팅 프로토콜이다. GPSR은 확장성이 좋고

빠르게 경로 탐색이 가능하며 구현이 용이하다는 장점이 있다.

GPSR에서는 각 노드가 '이웃 노드의 위치'와 '패킷의 최종 목적지'를 고려하여 패킷의 최적 경로를 결정한다. 각 노드는 greedy algorithm을 사용하여 현재 위치에서 최종 목적지에 가장 가까운 이웃 노드를 다음 노드로 선택하고 패킷을 전달한다. 또한 greedy algorithm이 적용될 수 없는 지역에서는 perimeter routing을 사용하여 해당 지역을 우회하는 경로를 구축하는 기능을 제공한다.

GPSR의 기본 가정사항은 다음과 같다.

- 모든 router 노드는 자신의 위치를 알고 있다.
- 노드 사이의 채널은 양방향이다.
- 노드들은 평면 상에 위치한다.
- 소스 노드는 목적 노드의 위치를 알 수 있으며, 패킷 내에 목적지 노드의 위치를 포함시켜 전달한다.

그림 1~3은 GPSR의 동작 과정을 보여 준다.

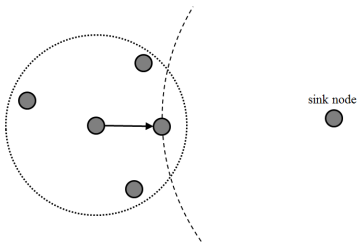

그림 1 Greedy forwarding

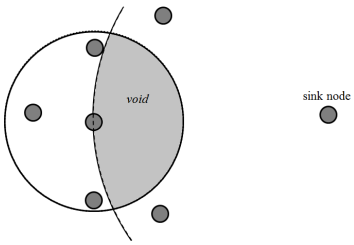

그림 2 hole problem

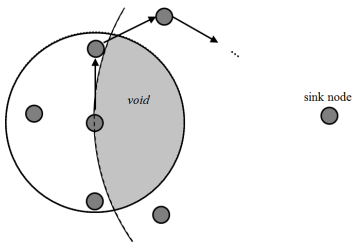

그림 3 perimeter routing (right-hand rule)

그림 1에 나타나 있듯이 GPSR에서 싱크 노드에게 이벤트 보고서를 전달하는 노드는 자신의 이웃 노드 중 싱크 노드에 가장 가까운 노드를 다음 노드로 선택하여 해당 이벤트 보고서를 전달한다. 이는 greedy routing이라 불리며 이웃 노드의 ID와 위치 정보만을 아는 상태에서 효율적으로 이벤트 보고서 전달 경로를 구축할 수 있다.

그러나 greedy routing 방식은 현재 노드가 자신의 모든 이웃 노드들보다 싱크 노드에 가까운 경우 다음 노드를 선택할 수 없다는 단점이 존재한다. 이를 'hole problem'이라 하며 그림 2에 나타나 있다. 따라서 GPSR에서는 greedy routing에 의해 다음 노드를 선택할 수 없을 경우, 오른손 규칙 (right-hand rule)에 의해 해당 지역을 우회하는 방법을 사용하며 이를 perimeter routing이라 하며 그림 3에 표현하였다.

right-hand rule에 의하면 각 노드는 자신과 이전 노드 사이의 연결을 기준으로 했을 때 반시계방향으로 첫 번째에 위치한 연결에 해당하는 이웃 노드에게 보고서를 전달한다. GPSR의 perimeter routing은 이벤트 보고서 전달 과정에서 greedy algorithm이 적용될 수 없는 지역이 존재하더라도 이를 우회하여 기지 노드까지 보고서를 전달할 수 있다.

2. 관련연구 (multipath routing, flooding)

센서 네트워크에서 발생 가능한 선택적 전달 공격에 대응하기 위한 기존 라우팅 기법들이 제안되었다 . [5]에 따르면 선택적 전달 공격에 대응할 수 있는 기존 라우팅 기법에는 다중 경로 라우팅 (multipath routing)과 플러딩 (flooding)의 두 가지 방법이 존재한다.

다중 경로 라우팅[6]은 소스 노드와 싱크 노드 사이에 둘 이상의 경로를 설정하고 한 경로가 실패했을 때 다른 경로를 사용하여 싱크 노드까지 이벤트 보고서를 전달할 수 있다. 그러나 다중 경로 라우팅은 경로의 수가 증가함에 따라 통신 오버헤드가 급격하게 증가한다는 문제점이 존재한다.

플러딩[7]은 각 노드가 수신한 메시지를 이웃 노드들에게 연속적으로 브로드캐스트(broadcast)하는 방식으로서 소스 노드에서 기지 노드까지 안전하게 이벤트 보고서를 전달하는데 사용될 수 있다. [PLM]에서는 전달 영역 제한을 통해 플러딩에서 발생하는 노드들의 에너지 소모를 줄이는 방법이 제안되었다. 그러나 플러딩은 다중 경로 라우팅과 비교하여 더 많은 통신 오버헤드를 유발한다. 그림 4, 5는 다중 경로 라우팅과 플러딩의 동작 과정을 보여준다.

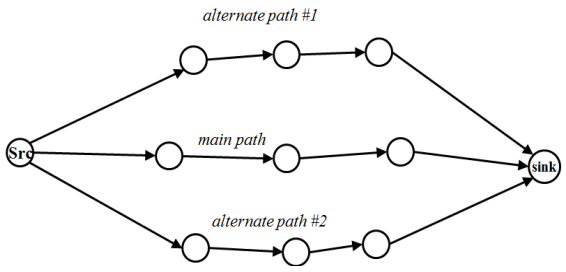

그림 4 다중 경로 라우팅 (multipath routing)

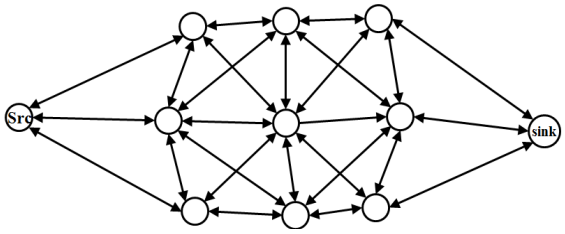

그림 5 플러딩 (flooding)

그림 4에서 볼 수 있듯이 다중 경로 라우팅에서는 소스 노드에서 싱크 노드까지의 최단 경로를 주 경로 (main path)로 설정하고 추가적으로 대체 경로 (alternate path)를 구축한다. 다중 경로 라우팅에서는 경로의 개수에 비례하여 통신 오버헤드가 증가한다. 그림 5에서 전달 영역에 속한 모든 노드는 이벤트 보고서를 수신한 후 자신의 이웃 노드들에게 수신된 보고서를 브로드캐스트한다. 이 과정에서 해당 영역 내의 노드 개수가 증가함에 따라 이에 비례하여 통신 오버헤드도 함께 증가한다.

III. 제안 프로토콜

선택적 전달 공격을 방어하기 위한 기존 기법 - 다중 경로 라우팅, 플러딩 (flooding) 등 - 은 소스 노드에서 기지 노드까지의 신뢰성 있는 데이터 전달을 제공하는 대신 많은 에너지 소비를 유발한다는 단점이 존재한다.

제안 기법은 이벤트 보고서 전달 과정에서 공격이 발생한 지점을 우회하는 경로를 선택하여 적은 에너지 소비로 소스 노드에서 기지 노드까지의 신뢰성 있는 데이터 전달 기능을 제공하는 것을 목표로 한다. 이를 위해서는 선택적 전달 공격 발생 시, 이에 대한 탐지 방법과 대응 방법이 모두 필요하다.

[8]에서는 다중 홉 ACK 메시지를 사용하여 선택적 전달 공격을 탐지하는 방법이 제안되었다. 따라서 제안 기법에서는 소스 노드에서 기지 노드로 데이터를 전달하는 과정에서 확률적으로 선택된 체크 노드 (check node)들에 의해 소스 노드 방향으로 ACK 메시지가 전달되며 ACK 메시지를 수신하지 못한 노드는 선택적 전달 공격이 발생했음을 탐지할 수 있다.

선택적 전달 공격이 탐지된 경우 이를 탐지한 노드는 GPSR에서 제안된 오른손 규칙에 기반 하여 공격 발생 지점을 우회하는 라우팅 경로를 구축한다.

그림 6~8은 제안 프로토콜의 동작 과정을 보여 준다.

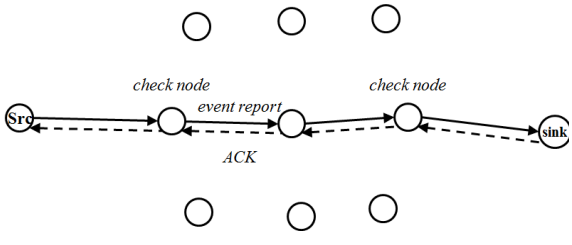

그림 6 이벤트 보고서 전달 및 다중 홉 ACK

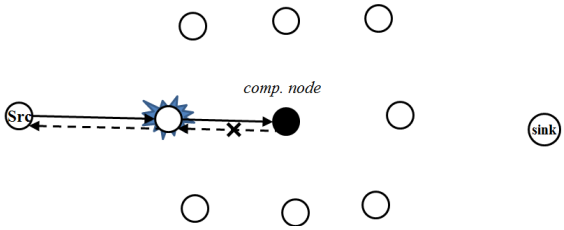

그림 7 선택적 전달 공격 탐지

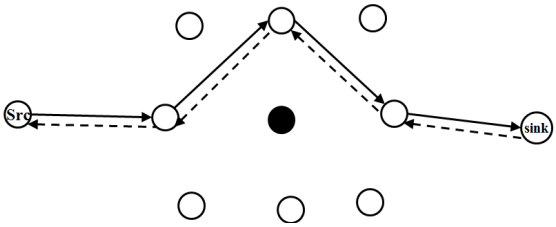

그림 8 Perimeter routing을 사용한 공격 발생 노드 우회 방법

그림 6에서 볼 수 있듯이 소스 노드에서 싱크 노드 방향으로 이벤트 보고서를 전달하는 과정에서 경로 상의 일부 노드가 확률적으로 체크 노드로 지정된다. 지정된 체크 노드는 수신된 이벤트 보고서에 대응하는 ACK 메시지를 소스 노드 방향으로 전달한다. ACK 메시지는 소스 노드 방향의 다음 체크 노드 또는 소스 노드까지 전달된다.

그림 7은 제안 프로토콜에서 선택적 전달 공격을 탐지하는 과정을 보여 준다. 그림 7에서 라우팅 경로 상에 훼손 노드가 존재하며 해당 훼손 노드는 수신된 이벤트 보고서를 다음 노드로 전달하지 않고 제거한다. 따라서 훼손 노드에게 이벤트 보고서를 보낸 체크 노드는 ACK 메시지를 수신하지 못하게 되므로 선택적 전달 공격을 탐지한다.

그림 8은 제안 프로토콜에서 선택적 전달 공격이 탐지된 경우 오른손 규칙에 따라 훼손 노드를 우회하는 과정을 보여 준다. 선택적 전달 공격을 탐지한 체크 노드는 오른손 규칙에 따라 훼손 노드가 위쪽에 위치한 노드에게 이벤트 보고서를 전달한다. 결과적으로 훼손 노드를 우회하는 라우팅 경로를 구축함으로써 싱크 노드까지 안전하게 이벤트 보고서를 전달할 수 있다.

IV. 결 론

센서 네트워크는 구성 요소인 센서 노드들의 자원 제약, 무선 통신 사용, 기반 시설의 부재 등으로 인하여 각종 보안 위협에 취약하다. 특히 선택적 전달 공격은 공격자에 의해 훼손된 노드가 라우팅 경로에 포함될 경우 자신을 지나는 이벤트 보고서 중 전체 또는 일부를 제거하는 공격으로 시스템 가용성에 치명적인 공격에 해당한다. 선택적 전달 공격에 대응 가능한 기존 라우팅 기법들은 신뢰성 있는 데이터 전달을 제공하는 반면 에너지 소모량 측면에서 비효율성이 존재하였다. 본 논문에서는 대표적인 라우팅 프로토콜의 하나인 GPSR 프로토콜을 적용하여 선택적 전달 공격 발

생 시 공격 발생 지점을 우회하는 경로를 구축할 수 있도록 하는 방법을 제안하였다. 향후 실험을 통해 제안 기법의 성능을 기존 기법의 성능과 비교 평가하고 개선하는 연구가 필요하다.

Acknowledgement

이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.(No. 2013R1A2A2A01013971)

참고문헌

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," Communications magazine, IEEE, vol.40, no.8, pp.102-114.

[2] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," Wireless Communications, IEEE, vol.11, no.6, pp.6-28.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc networks, vol.1, no.2, pp.293-315.

[4] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks,"Proceedings of the 6th annual international conference on Mobile computing and networking, pp.243-254.

[5] H. Y. Lee and T. H. Cho, "Fuzzy-based reliable data delivery for countering selective forwarding in sensor networks," in Ubiquitous Intelligence and ComputingAnonymous, pp.535-544, Springer, 2007.

[6] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," ACM SIGMOBILE Mobile Computing and Communications Review, vol.5, no.4, pp.11-25.

[7] S. H. Chi and T. H. Cho, "Fuzzy logic based propagation limiting method for message routing in wireless sensor networks," in Computational Science and Its Applications-ICCSA 2006, pp.58-67, Springer, 2006.

[8] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify suspect nodes in selective forwarding attacks," Journal of Parallel and Distributed Computing, vol.67, no.11, pp.1218-1230.