韓國 컴퓨터情報學會 2007하계학술발표논문집&학회지
第15卷 第1號, 2007. 6.

센서네트워크 환경에서 다중 경로를 이용한 웜홀 검출

김 인 태*, 한 승 진*, 이 정 현**

Wormhole Detection using Multipath in sensor network

Intae Kim*, Seungjin Han*, Junghyun Lee**

요 약

센서 네트워크 라우팅에 대한 공격은 무선이라는 네트워크 환경 때문에 애드혹과 유사하게 이루어 지고 있다. 하지만 이를 대처하는 보안 매커니즘은 노드가 보다 제한된 자원을 가지므로 그대로 적용할 수 없어 새로운 연구가 필요하게 되었다. 본 논문에서는 웜홀 이라는 라우팅 공격에 대하여 다중 경로를 이용하여 공격을 회피하고 검출하는 방법에 대하여 제안한다. 다중 경로 환경에서 주경로와 대체 경로간 홉당 지연시간을 비교하여 웜홀 경로를 회피, 검출하고 검출 오차를 줄이기 위하여 블랙리스트를 방법을 사용한다. Ns-2 시뮬레이션 환경에서 제안한 방법을 이용한 웜홀 검출 메커니즘을 시뮬레이션하고 웜홀과 정상 노드의 검출율을 비교하여 성능을 측정하였다.

▸ Keyword : 보안(Security), 웜홀(Wormhole), 다중경로(Multiple path)

Ⅰ. 서 론

센서 네트워크는 낮은 비용으로 사용할 수 있다는 점 때문에 다양한 분야에서 활용되고 있다. 가정에서의 가전제품 제어뿐만 아니라 재난예방을 위해 광범위한 영역에 대한 위험요소 감시와 제어와 같은 긴급 상황을 알리는 역할로 센서네트워크의 사용이 증가함에 따라 성능향상을 위한 연구와 더불어 보안에 대한 중요성이 커지고 있다. 센서 노드의 제한된 자원과 무선이라는 네트워크 환경 때문에 기존에 사용하던 보안 메커니즘을 그대로 적용할 수 없다.

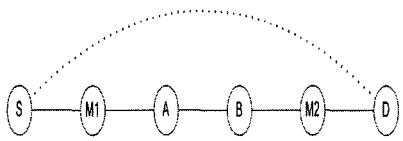
이는 센서네트워크이라는 환경에서 보다 적합한 보안 메커니즘에 위한 다양한 연구활동을 불러 일으켰으며 안전한 라우팅을 위한 연구가 이중 한 분야라고 할 수 있다. 무선 네트워크 라우팅에 대한 공격으로는 하나의 노드가 여러 식별자를 갖고 다중 노드임을 가장하는 Sybil[12] 공격과 악의적인 두 노드가 공모하여 라우팅 경로를 조작하는 경우, 데이터들이 악의적인 노드를 지나가도록 하는 웜홀[1] 공격 등이 있다. [13]에서는 이러한 다양한 공격유형과 이를 극복하기 위한 대처방안에 대하여 기술해 놓았다.

• 제1저자 : 김인태
* 인하대학교 컴퓨터정보공학과, **경인 여자 대학교

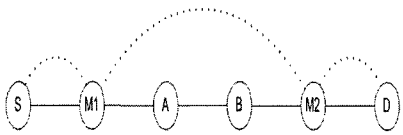
본 논문에서는 다중경로 라우팅 환경에서 노드에 별도의 하드웨어에 대한 부담 없이 DPH_{diff} (Delay Per Hop between Multipath)와 블랙리스트를 이용하여 효율적인 웜홀 공격에 대한 검출방법을 제안한다. DPH_{diff} 는 [8]에서 제안한 DPH (Delay per Hop)과 유사하지만 단일 경로 라우팅이 아닌 다중 경로 라우팅 환경에서 적용할 수 있는 웜홀 검출 요소로써 주 경로와 대체 경로간 DPH차이를 나타낸다. 본 논문에서는 Ns-2 시뮬레이션 환경[16]에서 DPH_{diff} 을 이용한 웜홀 검출 메커니즘을 시뮬레이션하고 웜홀과 정상 노드의 검출율을 비교하여 성능을 측정하였다.

2. 기존 연구

웜홀 공격은 최단 경로를 이용하여 데이터를 전달하는 센서네트워크나 애드혹 라우팅 알고리즘 특성을 악용하여 악의적인 노드를 정상적인 노드들 사이에 배치시켜 실제 경로보다 짧게 인식하게 하고 데이터들이 자신을 거쳐 가도록 하는 공격방법이다[1]. 웜홀의 공격 유형은 그림1과 같이 두 가지 유형으로 나누어진다. 그림 1-a) 같이 악의적인 노드가 데이터를 단순하게 전달하여 자신이 경로 정보에 드러나지 않게 하는 유형이 있으며 그림 1-b) 같이 여러 악의적인 노드가 공모하여 속이는 것으로 자신이 경로 정보에 드러나는 유형이 있다[2][8]. 무선 네트워크 환경에서 웜홀 검출에 대한 연구는 초창기 정확한 시간 동기화[4][5]나 방향성 안테나를 이용한 방법[3]으로 웜홀 검출을 시도하였으나 별도 하드웨어에 대한 부담으로 최근들어 간단하게 검출할 수 있는 방법들에 대한 연구가 시도되고 있다. 특히 센서네트워크 환경에서는 센서노드의 특성상 별도의 하드웨어 없이 웜홀을 검출하는 연구가 필수적이라고 볼 수 있다. 이러한 연구 중에는 이웃노드간 거리를 계산하여 노드들의 배치를 시각적으로 나타내고 이를 이용하는 연구[6]가 있었으며 통계적인 방법을 이용한 웜홀 검출 연구 등이 있었다[7].



a)



b)

〈그림 1〉 웜홀 유형

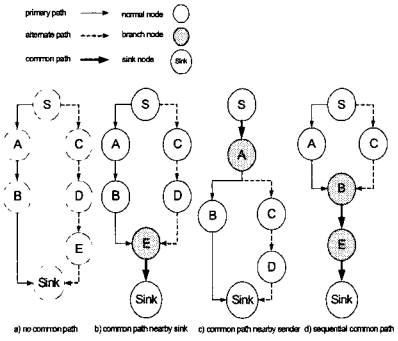
본 논문에서는 [8]에서 사용한 DPH값을 다중경로에 이용하여 다중 경로환경에서의 웜홀 검출 방법을 제안한다.

[10]에서 다중 경로 라우팅 방식이 단일 경로 라우팅 보다 좀더 신뢰성 있고 좋은 성능을 제공함을 보여주고 있으며 이를 바탕으로 최근 들어 다중 경로에 관한 여러 연구가 이루어지고 있다. 무선 애드혹에서 사용한 다중 경로 방식들은 송신자 중심 방식으로 경로당 하나의 라우팅 메시지를 생성하고 각 송신자와 수신자의 쌍에서의 다중 경로를 찾는데 목적을 두었다. 그러나 이러한 방식은 오버헤드도 많고 센서네트워크에 적절한 일대다 방식이 고려되지 않았으며 이에 대한 개선사항으로 H-SPREAD 방식이 제안되었고[9] 본 논문에서는 이를 활용한다.

본 논문은 [14]와 같은 안전한 다중 경로 라우팅 프로토콜에 관한 연구가 아니라 다중 경로 라우팅의 특징을 이용하여 효과적인 웜홀 검출 방법을 제안하는 것으로 다른 다중 경로 라우팅 프로토콜에도 적용가능 할 것으로 본다.

3. 웜홀 검출

H-SPREAD에서는 1단계에서 SPREAD[15]와 같이 TinyOs beacon 프로토콜[17]과 같은 방법으로 베이스스테이션에서 주기적으로 라우팅 갱신 메시지를 브로드캐스트 하고 처음 전송 받은 노드는 전송노드를 자신의 부모노드로 마크하고 이미 부모노드를 가지고 있다면 같은 부모를 가지고 있는지에 따라서 형제 또는 사촌으로 마크하고 다시 브로드캐스트 한다. 이렇게 마크된 정보를 이용하여 사촌 노드를 경유하는 새로운 대체 경로를 생성한다. 추가로 더 많은 다중 경로를 얻기 위해 부모와 형제노드가 가지고 있는 대체 경로들을 요청하여 더 많은 다중 경로를 생성한다. 본 연구에서는 H-SPREAD와 유사하게 다중 경로를 구성하고 다음과 같은 방법으로 주 경로와 대체 경로를 구성한다. 주 경로는 송신노드와 싱크노드간 경로 중 가장 짧은 홉 수를 가지고 있는 경로를 선택하며 대체 경로는 주 경로와의 공통 가지 개수에 따라 선택한다.



〈그림 2〉 대체 경로 선택 우선순위

그림 2는 대체 경로를 선택하는 우선순위를 설명하기 위한 경로들에 대한 예를 보여주고 있다. 가장 우선순위가 높은 대체 경로는 2-a) 같이 주 경로와 공통 가지 노드를 가지지 않는 경우이며 이는 주 경로와 대체 경로간 DHP 값의 차이를 극대화하기 위함이다. 3-b), c), d)와 같이 공통된 가지 노드를 가지는 경우 연속된 공통 가지의 개수에 따라 우선순위가 결정되며 3-d)인 경우 3-b), c)와 다르게 연속된 공통 가지를 가지고 있으므로 3-b), c)보다 낮은 우선순위를 갖게 된다. 3-b), c)는 공통 가지가 존재하는 위치에 따라 우선순위의 차이를 보여주기 위한 그림이다. 3-b)는 싱크노드 근처에 공통 가지가 존재하는 경우이며 3-c)는 데이터를 전송하는 센서노드 근처에 공통 가지가 존재하는 경우이다. 이런 경우 우선순위는 싱크노드와 거리가 먼 공통 노드를 가지고 있는 대체 경로가 더 높다. 이는 센서 네트워크에서의 웜홀을 포함한 많은 라우팅 공격 유형들이 싱크노드 근처에서 경로 정보를 획득하려는 행동을 취하기 때문에 이를 배제하기 위함 이다.

DPH는 [8]에서 웜홀 검출을 위해 계산된 홉당 지연시간을 말하며 식(1)에 나타나 있다. 는 대상노드 i와 싱크노드간 홉 수를 나타내며 는 싱크노드에서 전송한 시간을 나타내며 은 왕복하여 받은 시간을 나타낸다.

$$DPH = \frac{RTT}{2h_i} = \frac{t_r - t_s}{2h_i} \quad \cdots\cdots (1)$$

우리는 전송 노드가 자신의 전송 시간을 메시지에 붙여 전송하게 하였으며 싱크노드에서는 수신 시간과 차이를 계산하여 홉당 전송시간을 계산한다. 이는 식 (2)에 나타나 있다.

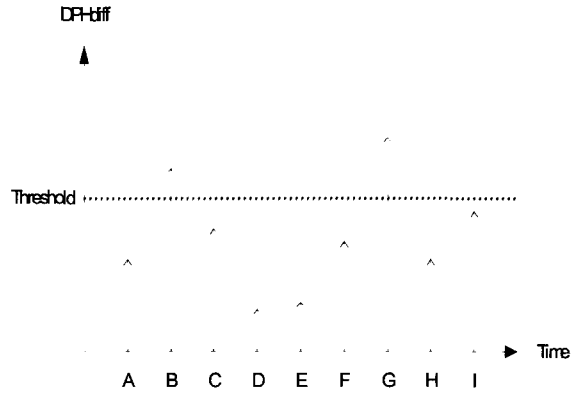
$$DPH = \frac{t_r - t_s}{hopcount} \quad \cdots\cdots (2)$$

일반노드에서 데이터 전송할 때 주 경로와 대체 경로로 동시에 전송하며 데이터를 수신한 싱크노드와 연결되어 있는 베이스 스테이션에서는 주 경로의 DPH값 DPH1 와 대체 경로의 DPH값 DPH2의 차이 DPH_{diff} 계산하여 각 노도의 DPH_{diff} 값 (3)을 관리하며 한계 값을 설정할 때 사용하기 위하여 저장한다.

$$DPH_{diff} = |DPH_1 - DPH_2| \quad \cdots\cdots (3)$$

각 노드의 DPH_{diff}의 분포를 구하여 각 노드의 DPH_{diff} 값을 비교하여 한계 값을 넘어가면 해당 경로에 웜홀이 있을 것으로 추정한다. 웜홀은 악의적인 두 노드간 경로를 터널링하여 최단거리인 것처럼 보이게 하므로 웜홀이 포함되어 있는 경로는 큰 DPH값을 갖게 되고 웜홀을 가지고 있지 않은 경로와의 DPH차이가 커지게 되므로 DPH_{diff} 값을 비교하여 웜홀 검출을 할 수 있다.

그림 3은 웜홀 노드가 포함되어 있는 경로와 그렇지 않은 경우의 DPH_{diff} 의 예를 보여주고 있다. 노드 B, I와 같이 DPH_{diff}가 한계 값을 넘어 가면 해당 노드와 싱크노드 사이에 웜홀이 있을 것으로 추정할 수 있다.



〈그림 3〉 웜홀 경로 검출

한계 값을 구하는 식은 식(4)에 나타나 있다.

$$DPH_{max} = MAX(DPH_{diff}(NormalNode))_{1..x} \quad \cdots\cdots (4)$$

$$T = DPH_{\max} + DPH_{\max} * \frac{y}{100}$$

이전에 전송한 x 개수 DPH_{diff} 중 최대값에 y%만큼의 한계 값을 가진다.

[8]에서는 웜홀 노드를 검출하기 위하여 웜홀이 있을 것으로 의심되는 경로에 있는 각 노드에 대해서 DPH를 비교하여 인접한 노드간 DPH값의 차이가 한계 값을 넘어가는 경우 웜홀노드로 간주하여 높은 검출율을 보였다. 그러나 실제 환경에서 [8]에서의 검출 방법은 웜홀 노드로 의심되는 노드가 순간적으로 네트워크 또는 노드의 문제로 다른 노드에 비해 DPH값이 크게 증가되는 경우 정상 노드를 웜홀 노드로 잘못 판단하는 경우가 발생하게 된다.

본 논문에서는 웜홀 경로로 의심되는 경로에 대하여 웜홀 노드를 바로 검출하여 제외하지 않으며 우선 해당 경로를 1단계 블랙 리스트에 넣고 다른 대체 경로를 선택한다. 1단계 블랙리스트에 포함된 경로들은 다중 경로에서 제외시킨다. 단, 본 논문에서는 악의적인 노드를 고립시키는 구체적인 방법에 대하여 제안하지 않는다. 1 단계 블랙리스트가 일정 개수만큼 쌓여 있으면 2단계 블랙리스트에 포함 시킬 경로를 축출한다. 1단계 블랙리스트에 포함되어 있는 경로를 분석하여 의심되는 노드의 쌍을 2단계 블랙리스트에 포함시켜 그 노드의 쌍을 포함하고 있는 경로들은 다중 경로에서 제외시킨다. 또한 1단계 블랙리스트도 갱신하는데 다음 두 경우에 리스트에서 삭제한다. 첫 번째는 해당 노드 쌍을 가지고 있는 경우이다. 이는 이미 2단계 블랙리스트에 포함되어 있으므로 더 이상 1단계로 해당 경로를 검출할 필요가 없기 때문이다. 두 번째는 첫 번째 경우에서 삭제 되는 경로와 동일한 싱크노드와 전송노드 쌍을 가지고 있지만 2단계 블랙리스트 쌍을 가지고 있지 않는 경우이다. 이는 잘못된 웜홀 경로 검출을 복구하기 위함이다.

이렇게 함으로써 정상노드를 웜홀 노드로 잘못 검출하고 바로 노드를 경로에서 제거하여 발생하는 비용을 줄일 수 있다. 물론, 블랙리스트의 관리는 싱크노드에서 이루어지기 힘들며 싱크노드와 연결되어 있는 베이스스테이션에서 수행해야 하겠다.

4. 결론

본 논문은 웜홀을 검출하는 간단한 방법에 대하여 소개하였으며 기존 DPH를 이용한 웜홀검출과 다르게 멀티경로들간에 DPH차이인 DPH_{diff}값을 이용하고 블랙리스트를 관리하여 웜홀 검출을 시도하였다. 이를 통하여 실제 환경에서 일어 날수 있는 임의의 전송 지연 시간에 때문에 발생할 수 있는 검출 오류를 극복하고자 하였으며 다중경로의 장점을 활용하여 동작 중에 웜홀을 검출할 수 있게 됐다. 이를 ns-2 시뮬레이터를 이용하여 지연시간에 따른 검출율을 실험하여 기존 DPH를 이용하는 방법보다 더 좋은 검출율을 가지게 됨을 증명했다.

본 논문에서 제안한 알고리즘은 Multipath 라우팅을 이용하는 방법으로써 역으로는 Multipath 라우팅 환경에서의 웜홀 검출방법으로도 활용될 수 있을 것으로 본다. 향후 실 환경에서의 실험을 통해 나타날 수 있는 더 많은 웜홀 패턴에 대한 연구로 보다 정확한 웜홀 검출에 대한 연구가 필요할 것으로 보인다.

참고문헌

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University,Tech. Rep. TR01-384, June 2002.

[2] Weichao Wang,y, Bharat Bhargava, Yi Lu and Xiaoxin Wu, "Defending against wormhole attacks in mobile ad hoc networks", Wireless Communications & Mobile Computing, vol.6, pp. 483-503, 2006.

[3] Lingxuan Hu and David Evans, "Using Directional Antennas to Prevent Wormhole Attacks", In Proceedings of the 2004 Symposium on Network and Distributed Systems Security (NDSS 2004), February 2004.

[4] February 2004. Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the 22nd INFOCOM, pp. 1976-1986, 2003.

[5] S. Capkun, L. Buttyán, and J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks," in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN 03), pp.21-32, 2003.

[6] W. Wang and B. Bhargava. "Visualization of wormholes in sensor networks." Proceedings of the 2004 ACM workshop on Wireless security, pp. 51-60, New York, NY, USA, 2004. ACM Press.

[7] Levente Buttyan, Laszlo Dora, Istvan Vajda, "Statistical wormhole detection in sensor networks", Security and Privacy in Ad-hoc and Sensor Networks, Second European Workshop, July. 2005.

[8] Hon Sun Chiu, King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", Wireless Pervasive Computing, 2006 1st International Symposium on, Jan. 2006.

[9] Wenjing Lou and Younggoo Kwon, "H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks", Vehicular Technology, IEEE Transactions on, vol. 55, pp. 1320-1330, July 2006.

[10] P. Pham and S. Perreau, "Performance analysis of reactive shortest path and multi-path routing mechanism with load balance", Proc. of INFOCOM 2003, pp.251-259, 2003.

[11] Secure Node Misbehaviors in Mobile Ad Hoc Networks

[12] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[13] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Elsevier's adhoc Netw. J., Spec. Issue Sensor Netw. Appl. Protocols, vol. 1, no. 2.3, pp. 293.315, Sep. 2003.

[14] Rosa Mavropodi, Panayiotis Kotzanikolaou and Christos Douligeris, "SecMR - a secure multipath routing protocol for ad hoc networks", Ad Hoc Networks, vol. 5, pp. 87-99, Jan. 2007,

[15] W. Lou, W. Liu, and Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks," in Proc. IEEE INFOCOM, Hong Kong, China, pp. 2404-2413 Mar. 2004

[16] "The Network Simulator - ns-2," At: http://www.isi.edu/nsnam/ns/

[17] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," at the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.