애드혹 네트워크 환경에서의 이동성을 고려한 비정상 노드의 효율적인 탐지 및 관리기법 연구

황동엽*, 김기형*, 유승화*
*아주대학교 일반대학원 컴퓨터공학과
*e-mail : bc8c@naver.com

A Study on the Efficient Method for Detection and Management of Unusual node in Mobile Ad-hoc Networks Environment

Dong-Yeop-Hwang*, Ki-Hyung Kim**, Seung-Wha-Yoo**
*Dept. of, Computer Science, Ajou University

요 약

본 논문은 비정상 노드의 이동성을 고려한 효율적인 탐지 및 관리 기법을 제안한다. 첫째로비정상 노드의 이동성을 고려하기 위하여 가중치 관리서버를 분산 배치하는 방법을 제안하고 둘째로 가중치를 부여하는 방안을 제안한다. 이러한 기법을 통하여 비정상노드의 이동을 탐지함과 동시에 효율적인 탐지성능을 보인다.

1. 서론

센서 네트워크 라우팅의 프로토콜은 매우 단순하므로 기존의 애드혹 네트워크에서의 다양한 공격들에 쉽게 당할 수 있다. 이러한 공격에 의하여 발생하는 문제를 해결하기 위하여 키 관리를 통한 보안 라우팅 기법에 대한 연구가 활발하기 진행되었다. [1-3]. 하지만 이러한 기법은 기존에 잘 알려지거나 명확하게 보안상의 문제가 되는 노드에 대한 대응 방법이다. 이러한 방법만을 가지고는 노드들간의 상호 협력을 기반으로 한 라우팅 프로토콜에서의 자원 제약 요소를 피하기 위하여 이기적인 행위를 하는 노드나 악의적인 목적을 가지고 데이터를 버리는 노드, 또는 네트워크의 와해를 목적으로 하는 비정상노드에 대한 대응방안이 될 수 없다. 따라서 이러한 비정상적인 노드들을 탐지하여 라우팅 경로에서 배제시키거나 불이익을 주는 방안들이 유용할 수 있다. 또한 노드의 이동성을 고려한 대응방안이 존재하지 않는다.

따라서 본 논문에서는 MS (Management Server)와 MN (Management Node)를 별도로 두어 노드의 네트워크간 이동시에도 비정상행위 노드에 대한 정보를 유지하는 방법을 제안한다. 또한 이기적인 노드와 허위신고노드의 비정상행위시 주어지는 가중치를 부여하는 방법에 차이를 두어 정상적인 노드는 빠르게 회복될 수 있는 방안을 제안한다.

본 논문은 제안기법을 효율적으로 설명하기 위하여 2 장에서는 비정상행위노드 탐지 및 관리 기법에 대한 기존의 연구에 대하여 설명하며, 3 장에서 효율적인 비정상행위노드 탐지 기법을 제안하며 4 장을 통하여 성능을 검증하고 5 장에서 결론을 맺는다.

2. 기존의 비정상노드 탐지 및 관리 기법

기 연구된 비정상노드 탐지 및 관리 기법은 NWMS(Node Weight Management Server.)를 두어 비정상행위에대한 신고메시지를 주고 받아 비정상행위에 대한 가중치를 부여하여 관리하는 방법이다. 이렇게 부여된 가중치를 통하여서 비정상행위를 하는 노드들을 네트워크로부터 배제한다.

비정상 노드를 탐지하기 위하여서 두가지 시나리오를 고려해야 한다. 첫째는 이기적인 노드가 패킷을 버리는 경우이고, 두번째는 허위신고노드가 거짓으로 신고를 하는 경우이다.

먼저 이기적인 노드의 탐지 기법은 다음과 같다. 전송노드(S-node)로부터 목적노드 (D-node)에게로 전송되는 데이터 패킷을 중계 노드인 B 노드가 의도적으로 버렸을경우 B 노드 이전 노드가 이를 판단하여 전송노드에게 이를 다시 알린다. 이때에 전송노드는 NWMS 로 B 노드를 신고함과 동시에 다중경로를 통하여 목적노드에게 데이터 패킷을 재전송하게 된다. 이때에 B 노드가 신고된 사실에 대한 정보를 함께 실어 보내는데, 데이터를 전송 받은 목적노드는 B 노드를통하여 이전에 데이터를 받은 기록이 있는지 여부를 판단하여 B 노드의 비정상행위 여부를 NWMS 에게 확인하여준다. NWMS 는 목적노드로부터의 확인을 받으면 B 노드의 비정상 가중치를 증가시킨다.

다음으로 이기적인 노드의 탐지 기법과 동일한 상황에서 B 노드가 라우팅 경로상의 다음 노드를 허위로 신고하는 경우의 탐지 기법이다. 라우팅 경로상의 B 노드의 다음 노드를 C 노드라 한다. 이기적인 노드의 탐지 기법에서 설명한 기법대로 C 에 대한 신고를

전송노드가 NWMS 에게 전달하게 되고 그와 동시에 목적노드로 재전송이 이루어진다. 재전송된 데이터를 받은 목적노드는 이전에 C 로부터 받은 동일한 데이터가 있음을 확인하면서 B 노드로부터의 신고가 허위임을 판단하게 된다. 목적노드는 이러한 사실을 NWMS 에게 알리고 NWMS 는 전송노드로부터 신고받은 C 노드가 아닌 허위사실을 알린 B 노드에 대한 비정상행위 가중치를 증가시킨다.

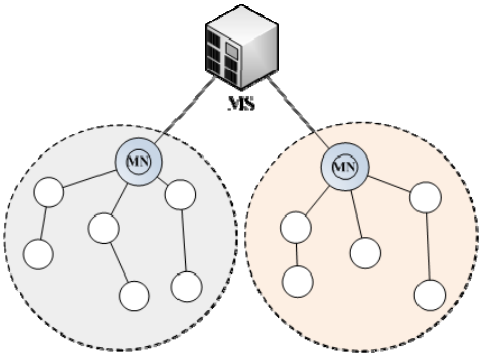
위의 과정을 통하여서 NWMS 에는 비정상행위를 보인 노드들에 대한 테이블이 생성되게 되고 각각의 가중치가 더해진다. 이 가중치가 미리 정해둔 임계치를 초과하게 되면 해당 노드를 네트워크로부터 고립시키게 된다. 하지만 이러한 기법에 몇가지 문제점이 있다. 먼저 비정상노드중 이기적노드와 허위신고노드의 구분이 없다. 이로 인하여 이기적 노드가 정상 노드로 전환될 가능성이 배제되어 잠재적인 데이터 처리량이 저하되고 패킷 손실이 생긴다. 또한 노드의 이동성을 전혀 고려하지 않아 비정상 노드가 새로운 네트워크로 이동할 경우 정상적 노드로 인지하여 피해를 입힐 수 있으며 가중치가 임계치에 도달하기전 이동을 반복하게 되면 지속적인 피해를 입히는 것도 가능하게 된다. 이러한 문제점을 해결하기 위하여 본 논문에서는 가중치를 분할하고 MS 와 MN 을 별도로 가지는 기법을 제안한다.

3. 비정상 노드의 탐지 및 관리 기법 제안

위의 2 장에서 기술한 NWMS 를 사용하는 기법의 문제점을 해결하기 위하여 본 논문에서는 두가지 기법을 제안하고자 한다. 첫째는 노드의 이동성을 고려하여 NWMS 를 분산하여 배치하는 기법이며, 두번째는 가중치를 부여하는 방법에 대하여 제안하고자 한다.

가) MS(Management Server)와 MN(Management Node)

기존의 기법은 NWMS 가 네트워크 내부에 위치하여 신고메시지를 처리하고 가중치도 함께 관리한다. 이는 가중치 관리 기능이 네트워크 내부에서만 접근이 가능하게 하기 때문에 주변의 다른 네트워크에는 영향을 줄 수가 없다. 이로 인하여 비정상행위를 하는 노드가 이동성을 가진다면 피해가 누적될 수 밖에 없다.



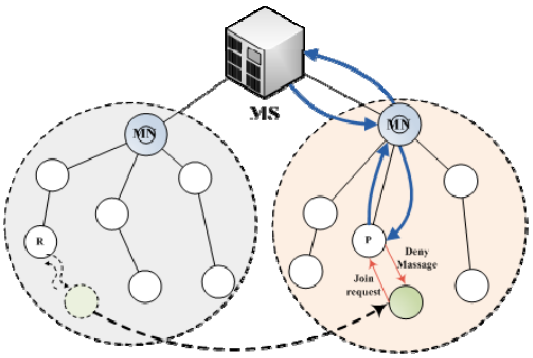
(그림 3) MS 와 MN 의 구성

이러한 문제점을 해결하기 위하여 위의 그림 3 과 같이 각각의 네트워크의 신고메시지와 가중치를 처리하는 MN 과 각각의 네트워크를 연결하고 가중치를 통합하여 관리해주는 MS 를 분산 배치하도록 한다. MS 와 MN 의 각각의 기능은 다음과 같다.

- MS : 자신에게 속한 MN 의 하위에 있는 모든 노드에 관련한 비정상 노드의 가중치 테이블을 관리한다. 이 정보들은 MN 이 특정 노드의 정보를 요청할때 제공한다.
- MN : 비정상 노드의 가중치 테이블을 관리하고 자신의 하위에 구성된 노드들에게 이러한 정보를 제공한다. 주기적으로 비정상 노드의 정보를 MS 에게 전달해 갱신하도록 한다.

나) MS 와 MN 의 이동노드 관리

위 그림 3 을 통하여 MN 을 통하여 하나의 네트워크의 비정상 노드가 관리되고 MS 를 통하여 MN 을 관리하고 가중치를 통합하여 관리 할 수 있는 토폴로지를 구성하였다. 이러한 네트워크의 구성을 기반으로 이동노드를 관리하기 위하여 몇 가지 규칙을 정하도록 한다.



(그림 4) 노드의 이동에 따른 동작

위의 그림 4 와 같이 이동한 노드가 주변의 P 노드에게 참여를 요청하였을때 MN 에 노드의 정보를 요청하게 되고 MN 은 자신의 테이블에 정보가 없으면 MS 에게 요청하여 정보를 제공한다. MS 와 MN 모두에게 노드의 정보가 없을 경우에는 완전히 새로운 노드로 간주하고 참여시킨다. 이러한 기법을 사용하면 다른 네트워크에서 피해를 주던 노드가 이동하였을 경우에도 이전에 축적되었던 가중치를 새 네트워크에 적용하여 관리 할 수 있게 된다.

다) 가중치 부여방법

일단 비정상 행위로 신고된 노드는 누적되어온 가중치에 의하여 네트워크로부터 고립시킬지 여부를 결정하게 된다. 하지만 이기적 노드와 허위신고 노드를 구분하여 관리하기 위하여 본 논문에서는 가중치 부여 방법에 관련하여 몇 가지 정책을 규정한다.

첫째로 정상행위에 대한 가중치와 비정상행위에 대한 가중치를 따로 두어 합산된 값이 임계치를 넘지 않는다 하여도 비정상행위에 대한 가중치가 일정 이상 부여되면 네트워크에서 고립시키도록 한다. 이를 통하여 두 행위의 비율을 맞추어 지속적으로 네트워크에 피해를 입히는 노드를 탐지할 수 있다.

둘째로 가중치의 합산을 가중평균방법을 적용하여 최근에 한 행위에 대한 가중치를 이전에 한 행위에 대한 가중치보다 높은 값을 부여하도록 한다. 또한 이기적 행위에 의하여 신고된 경우와 허위신고 행위로 신고된 경우의 가중치를 다르게 설정하여 차별화된 정책으로 비정상노드를 관리하도록 한다.

<표 1> 가중치 부여 도표

	이기적행위가중치(X_1)	허위신고행위가중치(X_2)
비정상행위 가중치 (X)	+5	+10
정상행위 가중치 (Y)	+1	

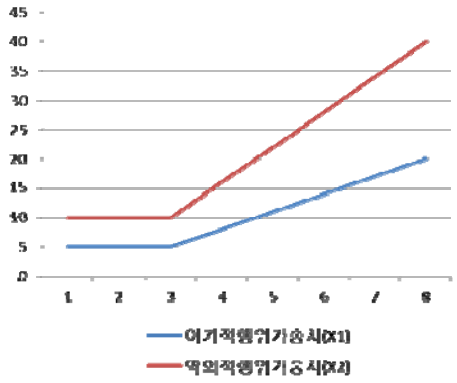
위의 표 1 과 같이 각각의 비정상행위에 대한 가중치를 차등 분배 하였고, 정상행위에 대한 가중치는 동일하게 설정 하였다.

$$x = \frac{W_1 \sum_{k=1}^{n-2} \overline{x_k} + W_2 \overline{x_{n-1}} + W_3 \overline{x_n}}{W_1 + W_2 + W_3}$$

$$= \frac{0.4 \sum_{k=1}^{n-2} \overline{x_k} + 0.7 \overline{x_{n-1}} + 1 \overline{x_n}}{2.1}$$

$$Y = \sum_1^n 1$$

위의 수식과 같이 비정상행위 가중치와 정상행위 가중치의 합을 가중평균을 이용하여 구하며 두 가중치의 증가는 다음 그래프와 같은 양상을 보인다.



(그림 5) 비정상행위 가중치와 정상행위 가중치

라) 이기적노드 가중치의 임계값 설정

임계치를 설정하기 위해서는 이기적인 행동과 정상적인 행동을 반복적으로 수행하여 두 가중치의 차이인 X-Y 의 값의 증가량이 적은 최악의 경우를 고려한다.

$$X - Y = \frac{2n + 4.5}{2.1} - n$$

위의 수식과 같이 두 가중치의 차를 계산 할 수 있으며 이 차이를 통하여 이기적노드를 7 번 이내에 탐지 할 수 있게 하는 임계치를 찾아낸다. 다음 그래프를 통하여 10 의 정절한 임계치를 찾아 낼 수 있다.

마) 허위신고노드 가중치의 임계값 설정

허위신고노드도 이기적노드의 경우와 동일하게 허위신고 행위와 정상적인 행위를 반복적으로 수행한느 최악의 경우를 가정하여 임계치의 도출을 하도록 한다.

$$X - Y = \frac{4n + 9}{2.1} - n$$

위의 수식과 같이 허위신고를 계속하였을 경우의 두 가중치의 차를 분석 할 수 있고, 허위신고행위의 경우 5 번 이내에 탐지해 내는 것을 기준으로 17 의 적절한 임계치를 찾아 낼 수 있다.

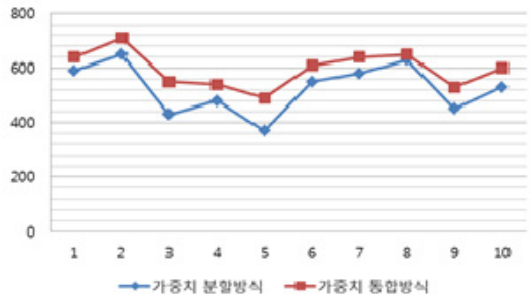
4. 평균 탐지시간 측정 및 분석

이 장에서는 본 논문에서 제안하는 방법에 대한 모의 실험을 통하여 그 결과를 토대로 성능을 비교 분석 해보고자 한다. 실험을 위하여 간단한 가중치 부여 알고리즘을 C 로 구현 하였으며 실험 환경은 다음과 같다.

<표 2> 실험 환경

환경변수	설정값
실험 시간	100 sec
행위발생주기	100 ms
노드의 수	10

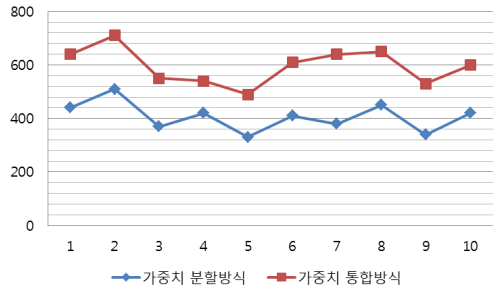
위와 같은 환경에서 각각의 노드는 비정상 행위와 정상 행위를 행위발생주기마다 랜덤하게 발생시키며 비정상 노드로 탐지될 때 마다 초기화 되는 것으로 가정하여 탐지에 소요되는 평균적인 시간을 측정하여 성능을 분석하였다.



(그림 8) 이기적노드의 평균 탐지 시간

위의 그림 8 은 10 개의 노드가 각각 이기적 노드로 탐지되기까지 소요된 평균 시간을 나타내고 있다. 실

험 결과 분석의 용이함을 위하여 기존의 비정상 행위 가중치와 정상 행위 가중치를 합하여 판단하는 기법을 가중치 통합방식이라 하고 본 논문에서 제안하는 방식을 가중치 분할방식이라 하도록 한다. 그래프를 볼 때 행위발생 주기가 100ms 인 것을 고려하면 평균적인 탐지시간이 7 번 이내인 것을 확인 할 수 있다. 또한 본 논문의 기법을 사용하였을 경우 50ms 이상 빠른 속도로 이기적 노드를 탐지 할 수 있음을 보이고 있다.



(그림 9) 이기적노드의 평균 탐지 시간

위의 그림 9 에서는 허위신고 행위에 대한 평균 탐지시간을 보이고 있다. 이 역시 행위발생 주기를 고려한다면 제안한 기법이 5 번 이내에 허위신고노드를 탐지해 내는 것을 볼 수 있다. 본 논문에서 제안한 기법이 역시 가중치 통합방식보다 빠른 시간에 허위신고노드를 탐지 하고 있으며 이기적노드 탐지보다 더욱 좋은 효율을 보인다. 이는 이기적노드의 정상노드로의 전환될 가능성을 고려하여 허위신고 행위에 더 큰 가중치를 부여 했기 때문이다.

위의 실험을 통하여 이기적 노드의 경우 50ms 이상, 허위신고노드의 경우 100ms 이상의 탐지 속토의 향상을 보였다. 실제의 환경에서는 비정상행위의 발생주기가 더욱 길기 때문에 두 기법간의 탐지시간의 격차가 클 것으로 기대된다.

5. 결론 및 향후 계획

본 논문에서는 기존의 비정상노드를 탐지하고 관리하는 기법을 개선하여 모바일 환경에 적용하고 탐지 성능을 향상 시키는 방안을 제안 하였다. 첫째로 MS 와 MN 으로 가중치를 관리하는 서버를 분산 배치하여 네트워크간 노드의 이동성을 보장 하였다. 둘째로 비정상행위에 대한 가중치 부여방법을 새롭게 제안함으로 비정상노드 탐지 성능을 높였다. 이러한 기법은 모의실험을 통하여서 탐지시간의 효율성을 분석 하였고, 또한 이기적인 노드의 정상노드로 전환되는 잠재적 가능성을 고려 했기 때문에 네트워크 전체의 측면에서 좀더 효율적으로 자원을 사용할 수 있을 것으로 기대 된다.

본 논문의 발전을 위하여 기존의 기법과 제안하는 기법을 사용하였을 때에 비정상노드에 의하여 손실된 패킷의 양을 측정하고, 일정 확률로 비정상노드가 발생하는 환경에서 기존의 방법과 비교하여 동일한 시간내에 얼마나 많은 양의 데이터 처리량을 보이는지를 비교하는 실험을 수행 할 계획이다. 이러한 실험을 통하여 본논문의 제안된 기법의 효율성에 대한 성능을 검증 및 분석을 기대 할 수 있다.

참고문헌

[1] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing Pairwise Keys for Secure Communication in Ad hoc Networks: A Probabilistic Approach," Proceedings of the 11th IEEE Conference on Network Protocols(ICNP'03), pp. 326-335, Nov.2003.

[2] M.G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," In Proceeding of the 2002 ACM workshop on wireless security, pp. 1-10, Sep. 2002.

[3] N. Asokan and P. Ginzboorg, "Key agreement in ad hoc networks," Computer Communication, pp. 1627-1637, Nov. 2000.

[4] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, pp.24-30, Nov. 1999.

[5] C.K. Toh, Ad Hoc Mobile Wireless Networks: Protocol and Systems, Prentice Hall PRT, Dec. 2001.

[6] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proceeding of the 6th International Conference on Mobile Computing and Networking, pp. 255-265, Aug. 2000.

[7] S. Buchegger and J.L. Boudec, "Performance analysis of the CONFIDANT Protocol," Proceeding of the 3rd ACM International Symposium on Mobile ad hoc networking & computing, pp. 226-236, June 2002.

[8] C.K. Toh, C. Lee, and N.A. Ramos, "Next-Generation Tactical Ad Hoc Mobile Wireless Networks," Technology Review Journal, pp. 103-113, Apr. 2002.

[9] J. Brand and G. Hartwig, "Management of tacticalad hoc networks with C2 data models," Military Communication Conference 2001 IEEE, pp. 915-922, Aug. 2001.

[10] C.E. Perkins, E.M. Royer, and S.R. Das, "Ad hoc on-demand distance Vector(AODV) routing," IETF Internet draft, MANET working group, Jan.2002.

[11] Yunho Lee, Soojin Lee, " An Efficient Detection and Management Technique of Misbehavior nodes in Ad-hoc Networks ", Korea institute of information Security & Cryptology, 2009, 10.