Vol.6, No.7 pp.315~320 pISSN: 2287-5891 https://doi.org/10.3745/KTCCS.2017.6.7.315

Weighted Voting Game and Stochastic Learning Based Certificate Revocation for the Mobile Ad-hoc Network

Min Jung Kim† · Sung Wook Kim††

ABSTRACT

In this paper, I design a new scheme that is immune to malicious attack based on the weighted voting game. By using stochastic learning, the proposed scheme can revoke the certification of malicious node. Through the revocation process, the proposed scheme can effectively adapt the dynamic Mobile Ad hoc network situation. Simulation results clearly indicate that the developed scheme has better performance than other existing schemes under widely diverse network environments.

Keywords : Weighted Voting Game, Stochastic Learning, Mobile Ad Hoc Network, Intrusion Detection System

이동 애드 혹 네트워크 환경에서 가중투표게임과 확률러닝을 이용한 악의적인 노드의 인증서 폐지 기법

김 민 정† · 김 승 욱††

요 약

본 논문에서는 무선 네트워크 환경에서 악의적인 사용자의 인증서를 폐지하여 네트워크의 안정화를 지원하는 효율적인 기법을 제안한다. 제안된 기법은 무선장치 내의 침입탐지시스템을 기반으로 실시간으로 이웃노드의 악의적인 행동을 감지한다. 침입탐지시스템의 판단은 오차가 발생할 수 있으므로 오차를 보완하여 정확한 악의적인 노드의 인증서를 폐지하기위해 신뢰도기반의 가중투표게임과 확률러닝을 사용하여 정확성을 높일 수 있었다. 폐지과정을 통해 제안된 기법이 동적인 이동 애드혹 네트워크 환경에 효율적으로 적용되는 것을 알 수 있었으며 컴퓨터 시뮬레이션을 통해 기존에 제안된 다른 기법에 비해 악의적인 she의 인증서 폐지 성공률과 네트워크의 안정성 부분에서 좋은 성능을 보였다.

키워드 : 가중투표게임, 확률러닝, 이동 애드혹 네트워크, 침입탐지시스템

1. 서 론

이동 애드혹 네트워크(MANET: Mobile Ad-hoc Network)는 주로 전쟁이나 비행기, 선박, 임시 재해복구 현장과 같은 외부 인터넷과 고립되거나 통신시설을 이용 불가능한 환경에서 특정한 네트워크 인프라가 없는 무선 인터페이스를 가진 다수의 노드들에 의해 자율적으로 구성되는 네트워크를 의미한다. 이와 같은 네트워크는 고정된 인프라가 없어 네트워크의 노드들이 네트워크의 기능을 수행하기 위해 서로 의존하고 노드들의 자유로운 이동성에 따라 네트워크망이 동적으로 변하게 되어 그 형태를 예측할 수 없다. 이러한 환경은 각종 보안공격에 대해 취약점을 드러냈으며 노드를 관찰 또는 분석할 필요가 있고 노드간의 안전한 통신을 위해 보안에 위배되는 노드를 차단하여야 한다[1-3].

MANET에서 보안문제에 대한 해결책은 악의적인 노드의 인증서를 폐지하여 더 이상 통신에 참가할 수 없도록 하는 것이다. 이는 침입탐지시스템(IDS: Intrusion Detection System)을 사용하여 네트워크상황을 실시간 모니터링하고 정치학, 경제학, 사회학, 논리학 등 여러 방면에서 잘 알려진 가중투표 게임(WVG: Weighted Voting Game)을 활용하여 폐지시킬 수 있다[4-8].

본 논문에서는 MANET과 같은 수명이 짧은 네트워크 환경에서 악의적인 노드를 제거하고 노드간의 안전한 통신환경을 위해 새로운 투표 기반의 의사결정 메커니즘과 확률학습기술을 제안한다.

† 비 회 원 : 삼성SDS(주) 네트워크관리자
†† 종신회원 : 서강대학교 컴퓨터공학과 교수
Manuscript Received : January 9, 2017
First Revision : February 27, 2017
Accepted : May 2, 2017
* Corresponding Author : Sung Wook Kim(swkim01@sogang.ac.kr)

2. 관련 연구

MANET환경에서 안전한 통신을 제공하기 위한 필수적인 인증서 폐지 메커니즘은 다양한 방법으로 연구되어 왔지만 노드들의 투표에 의해 의사결정이 내려지는 투표 기반의 인증서 폐지 메커니즘이 가장 널리 알려진 방법이다.

2.1 RevoGame(Revocation Game) 프로토콜

RevoGame 프로토콜[6]은 수명이 짧은 네트워크에서의 폐지게임을 말하며 게임이론을 사용하여 노드들이 전략적으로 전략을 선택하고 이를 Tree로 나타내었으며 에너지와 비용 효율적인 방법을 제시하여 전체적인 네트워크의 수명을 높였다. 본 게임의 전략은 찬성, 기권, 자살 총 3가지가 있으며 전략에 따라 발생하는 에너지와 비용이 다르다. 전략은 순차적게임을 기반으로 게임을 하는 플레이어, 즉 노드가 순차적으로 전략을 선택한다. 노드의 폐지 방법은 투표에 참가하는 노드가 자살 전략을 선택한 경우 또는 총 투표수가 사전에 미리 정해진 목표 투표수를 만족했을 경우 고발된 노드의 인증서는 폐지가 된다. 게임의 진행이 순차적게임이고 찬성 및 자살전략은 에너지가 소모되고 그 만큼 사회적 비용이 발생하게 된다. 또한 악의적인 노드를 폐지하지 못하였을 경우 전체 네트워크가 공격의 피해로 인해 사회적 비용이 발생한다[6].

2.2 임계 값 기반의 인증서 폐지 방법

임계 값 기반의 인증서 폐지 방법[9, 10]은 CA없이 기존의 인증서 폐지보다 더 빠른 인증서 폐지를 제공한다. 각 노드들은 네트워크에 참가하기 위해 CA로부터 유효한 인증서를 획득한다. 그러나 인증서 폐지 절차에서는 CA의 도움없이 1홉내의 모든 노드들을 모니터링하고 이웃끼리 정보를 공유한다. 모니터링과 공유한 정보를 바탕으로 이웃노드의 잘못되거나 악의적인 행동을 파악하고 노드간의 투표를 통해 미리 정해진 임계 값을 만족하거나 초과하면 인증서를 폐지할 수 있다. 이 과정에서 인증서 발급을 제외한 모든 것을 CA를 대신해서 CH가 시행한다[9].

이 방법에서 거짓된 고발을 방지하기 위해서 특정 노드에 대한 고발횟수와 특정 노드에 의해 만들어지는 고발횟수에 대한 임계 값을 설정하고 제한하였다. 이와 같은 방법으로 CA없이 더 빠른 인증서 폐지를 제공하고 악의적인 노드에 의해 발생되는 거짓된 고발을 방지한다[10].

3. 제안된 기법

제안 알고리즘은 MANET시스템에서 이웃 노드들로부터 획득하는 정보와 각 노드에 가중치를 적용하여 빠르게 악의적인 노드를 폐지하는 투표 기반의 폐지게임을 소개한다. 이 게임 모델은 빠르게 변화하는 네트워크 환경에서 시스템 안전성을 유지하는 동안 의심스럽고 악의적인 행위를 하는 노드를 성공적으로 제거할 수 있다.

3.1 가중투표게임

MANET환경에서 악의적인 노드의 인증서를 폐지하기 위해서 가중 투표 게임(WCG: Weighted Voting Game)모델을 사용한다. 먼저 노드들을 제시한 방법으로 클러스터를 형성하고 WCG모델을 적용하여 클러스터내의 노드가 악의적인 노드인지 아닌지를 식별한다. WVG모델의 게임형태(G)는 플레이어들, 각 플레이어의 전략집합, 전략의 결과집합(예: 보수의 집합), 게임에서 이기기 위해 만족해야 하는 임계 값, 플레이어들의 투표가중치, 특성함수와 같이 6개의 파라미터로 표현될 수 있다. 게임 G 는 $G=\{N,\{S_i\}_{i\in N},\{P_i\}_{i\in N},\tau,\{\omega_i\}_{i\in N},\nu(\bullet)\}$와 같이 수학적으로 정의될 수 있다.

N은 플레이어들의 유한집합이다. 즉 클러스터내의 노드를 나타내며 S_i는 플레이어 i의 전략 집합이다. 전략으로는 찬성과 반대가 있다. P_i는 플레이어 i의 보수이며 τ는 클러스터내의 악의적인 노드를 게임에서 이기기 위해 만족해야 하는 임계값이다. ω_i는 플레이어 i의 투표가중치 또는 평판이라 할 수 있다. 그리고 $\nu(\bullet)$는 승자와 패자의 이익을 보여준다.

제안된 기법에서 모든 게임 플레이어는 투표절차에 활동적으로 참가하는 것을 가정한다. 게임에서 전략은 단지 두 가지이다. 찬성투표(AV)는 플레이어가 감지된 악의적인 노드에 대항하여 폐지를 찬성하는 전략이다. 반대투표(OV)는 플레이어가 보고된 고발에 대해 반대를 하는 것을 의미한다. 전통적으로 플레이어들은 개인적으로 합리적이고 그들의 선호에 따라 행동한다고 가정된다. 본 논문에서는 플레이어들은 가능한 최선의 결과를 보장하기 위해 노력하고 투표게임의 결과는 다른 플레이어들의 행동의 순차적 특성을 기반으로 한다.

가중된 투표게임의 과정을 수행하기 위해서 핵심문제점은 가중치와 할당량을 적응적으로 결정하는 것이다. 노드의 가중치는 신뢰성을 기반으로 계산하고 신뢰성이 높으면 높은 가중치를 얻을 것이다. 그러나 동적으로 변화하는 MANET 환경에서는 각 노드의 신뢰성에 대한 불확실성이 존재한다. 제안된 기법에서는 신뢰성은 신뢰도와 행동기록에 기반하여 얻어진다. 첫 번째로 신뢰도(Y)는 과거의 행동에서 찬성 또는 반대투표수에 의해서 평가된다. t 번 반복 후에 t 시간에서의 노드 i 의 신뢰도 값 $(Y_i(t))$은 α_t^i/β_t^i와 같이 얻어진다. α_t^i는 노드의 폐지가 성공적으로 완료되었을 때 AV전략의 개수이고 β_t^i는 AV와 OV전략의 총합에 해당한다. 두 번째로 노드 i 의 행동기록(B_h^i)은 노드 i 의 행동 적절성을 나타내기 위한 지수이다. 높은 값의 B_h^i는 더 적절하다고 감지된다. 본 논문에서 B_h^i는 Equation (1)과 같이 정의된다.

$$B_h^i = 1-\left(\frac{1}{A}\times\zeta_i\right)-\left(\frac{1}{A}\times\Psi_i\right),\ s.t., 0\le B_h^i\le 1 \qquad (1)$$

A는 클러스터에서 모든 노드의 고발수의 총합이다. ζ_i는 노드 i 가 다른 노드들로부터 받은 고발개수이고 Ψ_i는 노드

i 가 고발은 했지만 노드를 폐지하는 것을 실패한 횟수이다. Y_i와 B_h^i 값에 기반하여 ω_i값을 계산한다. MANET 시스템에 새로운 노드가 가입될 때 ω의 초기값은 0보다크고 처음엔 매우 빠르게 증가될 수 있어야 한다. 이것은 새로운 노드에게 시스템에 기여할 수 있도록 동기를 부여하는 것이다. 이러한 요구사항을 충족시키기 위해서 시간t에서 노드i의 가중치(ω_i)는 신뢰도와 함께 단조적으로 증가하는 함수와 같이 정의되며 Equation (2)와 같다.

$$\omega_i = \frac{1}{1+\left[g\times\exp\left(-\theta\times\left[\frac{Y_i(t)+B_h^i}{2}\right]\right)\right]} \tag{2}$$

g는 증가속도를 조절하기 위한 파라미터이다. 가중치의 결정과 함께 투표자가 가중 투표 게임에서 승리하기 위한 τ값을 결정하는 것을 목표로 한다. 그러나 τ값을 결정하는 것은 어려운 문제이다. 만약 τ값이 매우 클 경우 악의적인 노드는 폐지될 수 없고 시스템에 대한 공격을 성공적으로 유지할 수 있다. 반대로 τ값이 너무 작으면 잘못된 고발이 빈번히 발생될 수 있다. 고정된 τ값은 동적으로 변화하는 환경에서 효과적으로 적용될 수 없다. τ값을 결정하기 위해서, 동등한 단위시간으로 시간 축을 분할하고 τ값은 동적으로 변화되어야 하며 이를 위해 본 논문에서는 확률적 학습 기술을 사용한다. 확률적 학습이란 기존에 전략에 대한 확률이 존재하며 확률에 따라 전략을 선택하고 인지된 결과에 의해 확률을 갱신해나가는 학습 방법이다. 시간t에서 선택한 전략에 대해 인지된 결과가 만족되거나 높으면 시간t+1에서는 시간t에서 선택한 전략에 대한 확률 값이 증가한다. 그렇지 않다면 확률 값은 감소한다. 반복적으로 확률적 학습을 통해 학습을 하게 되면 시스템의 상태는 안정화된 상태로 수렴할 수 있다.

본 논문에서는 집합T는 $T=\{\tau^j\in[\tau_{low},\tau_{high}]\}$이며 최적의 τ값을 찾기 위해서 확률적 학습을 적용하였다. τ값에 의해서 게임의 승패가 결정이 되며 그에 따라 게임에 대한 보상이 결정된다. τ^j는 집합T에서 j번째 값 또는 원소를 나타낸다. τ_{low}와 τ_{high}는 각각 사전에 미리 정의된 최소값과 최대값이며 이는 반복되는 게임과정에서 학습에 의해 값이 동적으로 적용된다. 따라서 시간 $t+1$에서 τ^j의 선택될 확률을 학습하기 위해서 먼저 시간t에서 τ^j에 대한 인센티브를 구해야 한다. τ^j에 대한 인센티브는 Equation (3)과 같이 정의된다.

$$\jmath(\tau^j(t))=\frac{u(\tau^j(t))-R}{sup_{k\in T}|u(k)-R|} \tag{3}$$

$\jmath(\tau^j(t))$는 시간 t에서 τ^j에 대한 인센티브를 의미한다. $u(\tau^j(t))$는 보상함수로써 인지된 결과값에 해당이 되며 다음과 같이 나타낸다.

$$u(\tau^j(t))=\frac{1}{C^t} \text{ and } C^t=N_a^t\epsilon+N_\nu^t\theta \tag{4}$$

보상함수 $u(\tau^j(t))$는 시간t에서 발생하는 사회적 비용 C^t의 역인 $1/C^t$로 나타낼 수 있다. N_a^t는 시간t에서 악의적인 노드의 브로드캐스팅 횟수에 해당되며 ε는 브로드캐스팅의 단위비용에 해당된다. N_ν^t는 시간t에서 고발된 노드에 대한 투표수에 해당이 되며 θ는 투표비용에 해당된다. 이와 같이 사회적 비용 C^t는 악의적인 노드에 의해 발생하는 비용과 일반적인 노드의 투표비용의 합으로 계산된다.

Equation (3)에서 R은 클러스터헤더가 요구하는 네트워크시스템이 만족해야 하는 보상 값이라고 할 수 있다. 계산한 인센티브를 활용하여 시간 $t+1$에서의 각 τ^j에 대한 확률을 갱신할 수 있다. 갱신하는 방법은 다음과 같이 정의된다.

$$\begin{cases} P_{t+1}(\tau^j)=\begin{cases} P_t(\tau^j)+\mu\times\jmath(\tau^j(t))\times(1-P_t(\tau^j)) & \text{if } \jmath(\tau^j(t))\geq 0 \\ P_t(\tau^j)+\mu\times\jmath(\tau^j(t))\times P_t(\tau^j) & \text{if } \jmath(\tau^j(t))<0 \end{cases} \\ P_{t+1}(\tau^n)=P_t(\tau^n)/\sum_{l=1}^{M}P_t(\tau^l) \qquad s.t.\ M=|T| \text{ and } \tau^n,\tau^l\in T \end{cases} \tag{5}$$

μ는 러닝비율을 나타내며 $0<\mu<1$값을 가진다. τ값의 선택에 대한 확률 값을 구한다음 시간 $t+1$에서는 Equation (5)에 따라 τ값을 선택한다.

제안된 학습방법은 과거의 τ값과 인지된 결과를 학습하고 러닝비율 μ와 과거의 학습기록에 기반하여 동적으로 τ값을 설정한다. 반복적인 학습을 통해 네트워크는 안정화된 상태를 유지하고 적절하고 빠른 악의적인 노드의 인증서 폐지, 인증서 폐지 고발의 남용과 잘못된 고발에 대한 대처를 할 수 있다. 이와 같은 방법은 현재 급변하는 MANET환경에서의 인증서 폐지를 위한 적합한 해결책이 될 수 있다.

3.2 인증서 폐지 메커니즘의 과정

가중투표게임에 대한 접근 방법은 오직 이론적인 모델링과 수학적인 분석에 초점을 맞추고 고려한다. 그러므로 현실적인 구현문제는 아직 잘 개발되어 있지 않다. 본질적인 관점에서 제안된 알고리즘은 실제 MANET운영 중에 현실적인 구현에 초점을 두고 있다.

편의를 위해, 하나의 악의적인 노드의 폐지 시나리오를 고려한다. 하나의 악의적인 노드는 순차적으로 발생하고 폐지절차 또한 순차적으로 되풀이된다. 첫 번째로 이 알고리즘은 악의적인 노드의 존재를 감지하는 것에서 시작한다. 감지하는 순간 클러스터헤더는 클러스터에 해당되는 모든 노드에게 고발메시지를 브로드캐스팅한다. 개인적으로 각 노드는 고발된 노드가 악의적인 노드인지 아닌지를 결정하기 위해 투표에 참가한다. 클러스터내의 노드들로부터 받은 투표를 수집한 후에 클러스터헤더는 인증기관에 결과를 보고하고 인증기관이 보고된 결과를 검증한다. 만약 노드들의 가중치의 합Q이 할당량τ보다 크면 고발된 노드는 MANET 시스템으로부터 성공적으로 폐지가 된다. 예를 들어 노드j가 폐지된다면 폐지되기 위해 j가 받은 가중치의 합Q_j은 Equation (6)과 같이 얻어진다.

$$Q_j = \sum_{k=1}^{n} (\delta_{kj} \times \omega_k) \quad (6)$$

$$, s.t., \ \delta_{kj} = \begin{cases} 1, & \text{노드}k\text{가 노드}j\text{의 폐지과정에서} \\ & AV\text{전략을 선택한경우} \\ 0, & \text{노드}k\text{가 노드}j\text{의 폐지과정에서} \\ & OV\text{전략을 선택한경우} \end{cases}$$

τ와 Q_j값에 기반하여 노드j의 인증서 상태를 결정할 수 있다. 만약 $\tau \leq Q_j$이면 노드j의 인증서는 폐지된다. CA의 결정에 따라 클러스터헤더는 클러스터내의 모든 노드에게 폐지 메시지를 브로드캐스팅한다. 마지막으로 가중 다수결 투표그룹에 속하는 노드들의 가중치 ω가 수정된다. 그래서 각 노드의 신뢰도 또한 동적으로 조정된다.

전통적인 게임모델은 모든 플레이어들이 게임의 완전한 정보를 가지고 게임의 결과는 고정된다는 가정을 기반으로 디자인된다. 그러나 실제 MANET환경에 바로 적용될 수 없다. 이 문제를 다루기 위해서 본 논문의 폐지 알고리즘은 잘못된 고발을 회복하기 위해서 디자인되었다. 폐지 알고리즘에서 인증서 폐지와 복원 과정은 가중된 투표 게임 기반하여 같은 방법으로 수행된다. 노드의 폐지가 잘못 발생하였을 때, 잘못 고발된 노드는 인증서를 회복하기 위해 항소할 수 있다. 항소요청이 받아졌을 때 클러스터헤더는 이전의 폐지가 정확한지 아닌지 확인하기 위해 탄원 메시지를 다시 브로드캐스팅한다. 모든 노드로부터의 투표를 기반으로 CA는 의사결정을 한다. 만약 Q_j값이 현재τ값보다 크다면 노드는 성공적으로 회복된다. 마지막으로 클러스터헤더는 잘못된 고발을 폐지하기 위해서 모든 노드들에게 정정메시지를 브로드캐스팅한다.

보통 고전적인 비협력 게임이론은 플레이어들이 내쉬균형을 결정할 수 있다고 가정한다. 그러나 동적인 MANET환경에서 이 가정은 너무 엄격하다. 플레이어들은 제한된 합리성과 함께 불완전하고 부정확한 지식을 가지기 때문이다. 게다가 내쉬균형의 아이디어는 대부분 정적인 설정에서 개발되었다. 그러므로 이 해결책은 플레이어들의 동적인 전략 변화를 적응시킬 수 없다. 전통적인 방법과 대조적으로 제안된 알고리즘은 현실적인 MANET시스템을 위한 좀 더 복잡하고 현실적인 모델링을 허락한다.

4. 성능 평가

이 장에서는 본 논문에서 제안한 가중투표게임 기반의 인증서 폐지 기법의 성능을 시뮬레이션을 통해 기존에 존재하는 타 기법들과의 차이를 비교한다. 이를 통해 본 논문에서 제안하는 기법의 성능을 평가하고 성능평가를 위한 네트워크 환경은 다음과 같이 설정하였다.

Table 1은 성능평가를 위한 네트워크 환경 설정에 해당하고 Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5를 통해 제안된 알고리즘의 성능을 파악할 수 있다.

Fig. 1은 MANET과 같은 네트워크 환경 내에 존재하는 악의적인 노드의 비율에 변화를 주는 상황에서 제안된 기법, Revogame이라 불리는 게임이론기반의 폐지기법과 임계 값 기반의 폐지기법의 폐지 성공률을 보여준다. 실험결과, 제안된 기법이 다른 두 기법에 비해 상대적으로 좋은 성능을 보였다. 일반적으로 악의적인 노드가 네트워크의 절반에 가까울수록 폐지 성공률이 급격히 떨어진다. 그러나 제안된 기법의 경우 반복되는 러닝에 의해서 일반적인 노드의 가중치가 높아지고 그에 따라 네트워크는 전체적으로 안정화되고 쉽게 악의적인 노드를 폐지할 수 있었을 뿐만 아니라 악의적인 노드의 공격에 의한 일반적인 노드가 폐지되는 상황도 초래하지 않았다.

Table 1. Network Composition/Parameter for Simulation

구분	설정 값
최소 노드 수(N)	100
최대 노드 수(N)	200
악의적노드최소비율	10%
악의적노드최대비율	50%
실험 횟수	100회
폐지 투표 진행 주기	1초
네트워크 크기	250m×250m
가중치(ω) 초기 값	0.5
러닝비율(μ) 초기 값	0

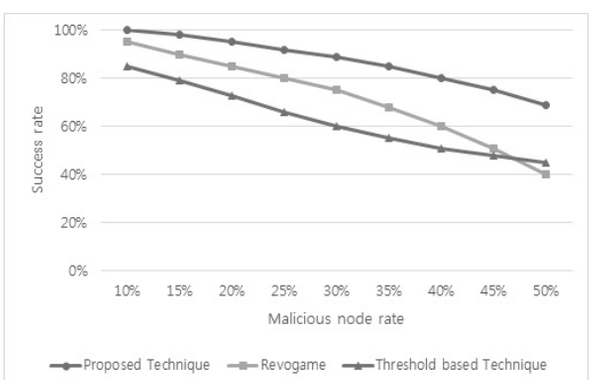

Fig. 1. Success Rate Against Malicious Node Rate

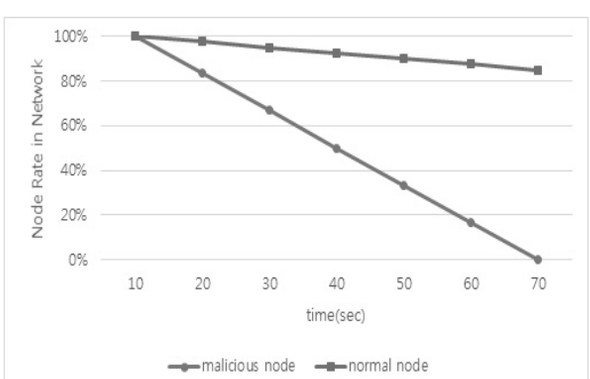

Fig. 2. Node Rate in Network Against Time(sec)

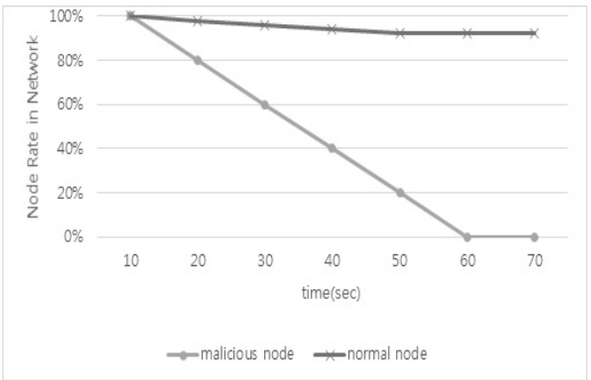

Fig. 3. Node Rate in Network Against Time(sec)

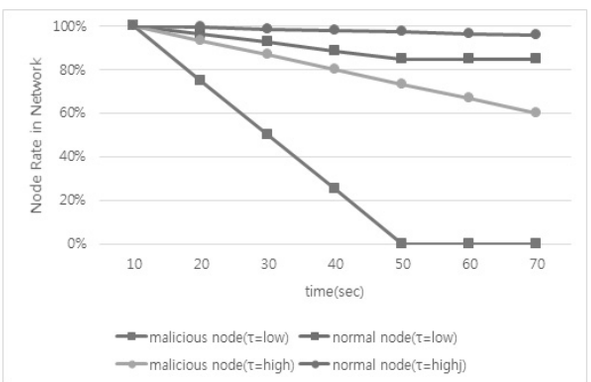

Fig. 4. Node Rate in Network Against Time(sec)

Fig. 2, Fig. 3, Fig. 4는 각 기법에 대해서 시간의 흐름에 따른 두 가지 노드의 비율 변화를 나타낸 그래프이다. 각 기법은 시간이 지남에 따라 네트워크의 상태변화를 나타낸다. 먼저 Fig. 2는 Revogame의 특성을 잘 나타내고 있다. Revogame에서는 투표게임이 진행이 될 때 선택할 수 있는 전략이 3가지가 있는데 그 중 자살이라는 전략이 존재한다. 이 전략은 자신을 희생함으로써 네트워크내의 고발된 노드를 제거하는 전략에 해당이 된다. 이러한 특성 때문에 악의적인 노드의 공격이 쉽게 성공될 수 있다. 그렇기 때문에 일정한 시간의 흐름에 따라 네트워크 내의 존재하는 일반적인 노드의 비율도 감소하게 된다. 이와는 달리 제안된 기법은 악의적인 노드의 결탁으로 인해 처음에는 일반적인 노드가 감소될 수 있지만 일정한 시간이 흐른 뒤 러닝비율이 증가하고 이에 따라 악의적인 노드의 폐지는 쉽게 이루어지고 악의적인 노드의 공격에는 일반적인 노드의 폐지가 되지 않는 것을 확인할 수 있다.

Revogame과 제안된 기법과는 달리 임계 값 기반 기법에서의 노드 비율 변화는 시간의 변화와 임계 값(τ)에 영향을 많이 받는다. 고정된 임계 값에 의해서 임계 값을 낮게 설정하면 악의적인 노드의 폐지뿐만 아니라 일반적인 노드의 폐지도 쉽게 이루어진다. 그렇기 때문에 악의적인 노드의 폐지가 빠르게 이루어지고 일반적인 노드의 폐지도 다른 기법에 비해 많이 이루어지는 것을 볼 수 있다. 반대로 값을 높게 설정하게 되면 악의적인 노드의 폐지도 어려울 뿐만 아니라 공격에 대한 일반적인 노드의 폐지도 거의 이루어지지 않는 것을 확인할 수 있다. 그래서 적절한 임계 값 설정이 필요하다.

고정된 임계 값과는 달리 제안된 기법은 동적으로 러닝을 통한 적절한 임계 값을 설정하기 때문에 효율적으로 악의적인 노드를 폐지할 뿐만 아니라 공격에 대한 방어도 뛰어난 것을 확인하였다.

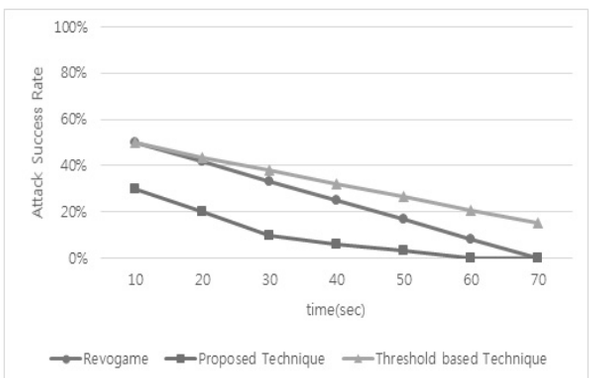

Fig. 5. Attack Success Rate Against Time(sec)

Fig. 5는 악의적인 노드의 평균 공격 성공률을 각각 나타낸 그래프이다. 실험결과, 시간의 흐름에 따라 반복되는 고발과 투표에 의해 악의적인 노드가 평균적, 상대적으로 감소하기 때문에 공격 성공확률이 감소하는 것을 확인 할 수 있다. 고정된 임계 값 기반기법의 경우 임계 값이 높을 경우와 낮을 경우 중간일 경우를 모두 평균한 결과 악의적인 노드가 네트워크에서 가장 늦게 제거되며 존재하는 악의적인 노드에 의해 네트워크가 불안정한 것을 확인할 수 있다. Revogame의 경우 평균적으로 공격성공 확률이 감소하고 제안된 기법의 경우 계속적으로 반복된 투표에 의해 네트워크 내 악의적인 노드의 입지는 줄어들고 러닝비율은 증가한다. 결국 일정한 시간 때부터는 공격확률이 0이 되며 다른 타 기법들과 비교했을 때 성능이 우수하다는 것을 확인할 수 있다.

5. 결 론

본 논문에서는 안정화된 이동 애드혹 네트워크 서비스를 제공하기 위해 가중투표게임을 이용한 악의적인 노드의 인증서 폐지기법을 제안하였다. 또한 악의적인 노드의 폐지에 관한 의사결정을 하기 위해 일정 범위의 임계 값을 설정하고 확률러닝을 통해 임계 값은 확률 값을 가지고 확률 값에 따라 임계 값을 선택하는 기법을 제안하였다. 시뮬레이션을 통해 제안기법이 기존에 존재하는 임계 값 기반의 폐지기법과 Revogame에 비해 악의적인 노드 폐지에 대한 더 높은 성공률을 기록하였으며 더 짧은 시간 내에 네트워크가 안정화 되었으며 악의적인 노드의 공격성공률이 현저히 낮은 것

을 확인할 수 있다. 제안된 기법은 네트워크내의 악의적인 노드수가 증가해도 더 좋은 성능을 유지할 수 있고 노드의 네트워크 참가와 이탈이 자유로운 상황에서도 탄력적으로 대응할 수 있음을 확인하였다. 또한 시간의 흐름에 따라 임계 값 선택에 대한 학습이 반복되어 악의적인 노드의 공격 성공률이 급격히 감소하고 악의적인 노드가 더 이상 네트워크에 존재하지 않는 것을 확인하여 기존의 다른 기법에 비해 더욱 효율적인 인증서 폐지기법임을 증명하였다.

References

[1] M. Gowsalayy, N. Karthick, S. Keerthana, and R. Durga, "Certificate Revocation Using Public Key Infrastructure For MANET's," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, pp. 1032-1035, 2014.

[2] G. Mohan and R. Ramachandran, "An improved Approach for MANET Security using Cluster Based Certificate Revocation," *International Journal of Computer Science and Information Technologies (IJCSIT)*, pp.5781-5784, 2014.

[3] W. Liu, H. Nishiyama, N. Ansari, J. Yang, and N. Kato "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks," *Parallel and Distributed Systems, IEEE Transactions on,* pp.239-249, 2013.

[4] P. Virada, "Intrusion Detection System (IDS) for Secure MANETs: A Study," *International Journal of Computational Engineering Research* (ijceronline.com), pp.75-79, 2007.

[5] S. Madhavi and Dr. T. Kim, "An Intrusion Detection System in Mobile Ad hoc Networks," *International Journal of Security and its Application*, pp.1-16, 2008.

[6] M. Raya, M. Manshaei, M. Felegyhazi, and J.-P.Hubaux, "Revocation Games in Ephemeral Networks," *Proceedings of the 15th ACM conference on Computer and communications security*, pp.199-210, 2008.

[7] E. Elkind, G. Chalkiadakis, and N. R. Jennings, "Coalition structures in weighted voting games," *Proc. 18th European Conf on AI (ECAI)*, pp.393-397, 2008.

[8] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," *Proc. IEEE 71st Vehicular Technology Conference (VTC)*, pp.16-19, 2010.

[9] K. Shalini and D. Swapna Mtech, "Certificate Revocation Using Threshold Based Approach in MANETs," *International Journal for Development of Computer Science and Technology (IJDCST)*, pp. 1-7, 2013.

[10] H. Dahshan, F. Elsayed, A. Rohiem, A. Elgmoghazy, and J. Irvine, "A Trust Based Threshold Revocation Scheme for MANETs," *Proc. IEEE 78st Vehicular Technology Conference (VTC)*, pp.1-5, 2013.

김 민 정

e-mail : kmj2136@gmail.com
2014년 동서대학교 컴퓨터공학과(학사)
2016년 서강대학교 컴퓨터공학과(석사)
2016년~현 재 삼성SDS(주) 네트워크 관리자
관심분야 : 게임이론, 애드 혹 네트워크

김 승 욱

e-mail : swkim01@sogang.ac.kr
1993년 서강대학교 전자계산학과(학사)
1995년 서강대학교 전자계산학과(석사)
2003년 Syracuse University, Computer Science(박사)
2004년~2005년 Post Doc. The Center for Advanced Systems and Engineering (CASE), Syracuse, NY. U.S.A
2006년~현 재 서강대학교 컴퓨터공학과 교수
관심분야 : 게임이론, 이동통신, 멀티미디어 통신, 네트워크 자원관리, QoS