논문 2011-3-25

VANETs을 위한 가중치 기반 침입탐지 방법의 설계 및 평가

Design and Evaluation of a Weighted Intrusion Detection Method for VANETs

오선진*

Sun-Jin Oh

요 약 무선 네트워크와 모바일 컴퓨팅 응용의 급속한 보급과 더불어, 최근 네트워크 보안의 배경도 많은 변화를 가져왔다. 특히 이동성이 높은 차량 노드들로 네트워크 위상을 유지하는 차량 애드 혹 네트워크(Vehicular Ad Hoc Networks: VANETs)는 일반적으로 불안정한 통신 링크를 갖는 자기 조직화 P2P 망으로, 고정된 인프라 구조나 중앙 통제 라우팅 장비 없이 자동으로 망을 구성하고, 시간에 따라 고속으로 이동하며 망에 결합하거나 이탈하는 개방 망이므로 중앙 집중 제어 없이 누구나 접속이 허용되기 때문에 네트워크상에 해로운 비정상 행위 노드들에 대한 침입에 매우 취약하다. 본 논문에서는 VANETs에서의 노드들의 활동에 대한 비정상 행위를 효율적으로 식별하여 침입을 탐지할 수 있는 러프집합을 이용한 가중치 기반 침입탐지 방법을 제안하고, 그 성능을 모의실험을 통해 임계 허용 오차 ϵ에 대한 비정상 행위로 인한 침입 탐지율과 거짓 경고율로 평가한다.

Abstract With the rapid proliferation of wireless networks and mobile computing applications, the landscape of the network security has greatly changed recently. Especially, Vehicular Ad Hoc Networks maintaining network topology with vehicle nodes of high mobility are self-organizing Peer-to-Peer networks that typically have short-lasting and unstable communication links. VANETs are formed with neither fixed infrastructure, centralized administration, nor dedicated routing equipment, and vehicle nodes are moving, joining and leaving the network with very high speed over time. So, VANET-security is very vulnerable for the intrusion of malicious and misbehaving nodes in the network, since VANETs are mostly open networks, allowing everyone connection without centralized control. In this paper, we propose a weighted intrusion detection method using rough set that can identify malicious behavior of vehicle node's activity and detect intrusions efficiently in VANETs. The performance of the proposed scheme is evaluated by a simulation study in terms of intrusion detection rate and false alarm rate for the threshold of deviation number ϵ.

Key Words : VANETs, MANETs, Intrusion Detection, Rough Set. Anomaly

Ⅰ. 서 론

모바일 애드 혹 망(Mobile Ad Hoc Networks: MANETs)은 무선 기반의 자기 조직화 망으로 고정된 인프라 구조 없이 이동성을 가진 노드들이 자동적으로 네트워크를 구성하며, 동적으로 망을 이탈하거나 참여하기 때문에 노드들 사이의 링크가 불안정하고 노드들의 이동성에 따라 망이 단절되는 경우도 발생할 수 있다. 만약

*종신회원, 세명대학교 정보통신학부 교수
접수일자 2011.4.18, 수정일자 2011.5.18
게재확정일자 2011.6.10

MANETs 내의 노드들이 차량들로 구성된다면 이 망을 차량 애드 혹 망 (Vehicular Ad Hoc Networks: VANETs)이라 한다. VANETs은 일반적으로 이동성이 높은 노드들로 구성되어 짧은 시간 망 위상이 지속되므로 불안정한 통신 링크를 갖게 된다. VANETs은 고정된 도로변의 게이트웨이와 연결할 수 있는 메커니즘을 가지며 인터넷과 같은 공통 망을 이들 게이트웨이를 통해 접근할 수 있다.

VANETs의 주요 장점으로는 고정 인프라 구조, 중앙 통제 관련 라우팅 장비로부터의 독립이다. 그러나 보안 측면에서는 이러한 장점들 역시 커다란 도전이 된다. VANETs은 개방 망으로 중앙 집중식 제어 없이 누구나 접속을 허용하기 때문에 네트워크상에 해로운 비정상 행위 노드들에 대한 침입이나 공격에 매우 취약하다. 따라서 효과적인 보안을 위해서 비정상 행위 노드의 공격이나 침입에 대한 탐지기법이 필요하다. 이때 침입 탐지는 시스템 상태와 노드 행위의 정상 프로파일을 생성하여 그것을 현재 활동과 비교해서 만약 정상 상태로부터 상당한 이탈이 관찰되면 침입이나 공격으로 간주한다. 이 기법은 아직 알려지지 않은 공격을 탐지할 수 있으며, 분명 VANETs 환경에서는 사전에 모든 공격 패턴을 아는 것이 불가능하므로 이 기법이 매우 유용하다. 그러나 VANETs에서는 노드들의 높은 이동성 때문에 정상 프로파일 구축이 어려우므로 효율적인 침입 탐지 알고리즘의 설계가 중요하다.

본 논문에서는 VANETs에서의 차량 노드들의 비정상 행위를 효율적으로 식별할 수 있는 러프집합을 이용한 가중치 기반 침입 탐지방법을 제안한다. VANETs 상에서 정상상태의 차량 노드 활동패턴으로 노드의 정상 프로파일을 갖는 정상 특징 정보 시스템을 구축하고, 러프집합을 이용하여 어떤 노드의 활동 패턴에 대한 정상으로부터의 이탈 정도를 러프 소속 함수를 이용하여 계산하여 그 이탈 정도가 허용 임계치보다 크면 침입으로 간주하고 경고 메시지를 발령하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 VANETs과 보안문제에 대한 관련 연구를 살펴보고, 3장에서 제안한 가중치 기반 침입 탐지방법의 시스템 모델을 서술하였으며, 4장에서 가중치 기반 침입 탐지 알고리즘을 제안한다. 5장에서는 제안한 가중치 기반 침입 탐지 방법에 대한 성능평가를 하였고, 마지막으로 6장에서 향후 연구 내용과 함께 결론을 맺는다.

II. 관련 연구

오늘날 자동차는 그동안 기계적이고 전기적인 특징에서 매우 복잡한 모바일 컴퓨터 시스템으로 진화하고 있다. 차량 내의 컴퓨터 하드웨어와 소프트웨어의 양은 폭발적으로 증가해 왔으며 폐쇄된 플랫폼이 아닌 개방된 소프트웨어와 서비스 플랫폼 상에서 모바일 애드 혹 망의 노드 역할을 하게 되었다. 이렇게 차량들로 이루어진 애드 혹 망을 차량 애드 혹 망이라 하며 노드들은 이동성이 높아 불안정한 통신 링크를 갖는다.[1, 2] 그림 1은 VANETs의 예를 보여준다. VANETs에서의 통신은 전통 망에서 알려진 유니캐스트 방식이 아닌 노드 그룹을 기반으로 메시지를 전송하는 지오캐스트(geocast) 통신 패턴을 사용한다.[3]

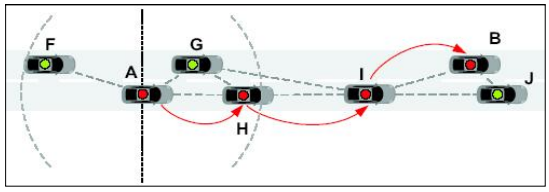

그림 1. 차량 애드 혹 네트워크(VANETs)
Fig. 1. Vehicular Ad Hoc Networks

대부분 전통 망들은 망 위상에 기반한 라우팅 접근방법을 사용하지만 VANETs에서는 위상기반 라우팅이 가능하지 않다.[4] VANETs의 위상은 계속해서 변화하고 노드들은 고속으로 이동하며 지속적으로 망에 결합하거나 이탈하면서 불안정한 통신 링크를 만든다. 따라서 대부분의 VANETs 시스템은 위치기반 라우팅 접근방법을 사용한다.[4] 그러나 위치기반 라우팅 메커니즘은 노드들의 위치에 종속적이며 어드레싱과 라우팅 방법에서 위치를 사용하기 때문에 제 3자에게 이동 패턴을 노출하여 노드 수명동안 추적되는 것이 가능하므로 망에 대한 거대한 보안 문제를 초래한다. VANETs에서는 라우팅에 대한 공격이 가장 큰 문제이다. 그들의 위치에 대한 노드 위조나 부당 변경은 거짓된 지리적 지역에 대한 메시지를 발생할 수 있고 VANETs 일부의 모든 트래픽을 블록하거나 가로챌 수 있으며 또는 망 분할을 초래할 수 있다.[5, 6] VANETs에서의 주요 보안 문제는 거짓 경고 메시지의 유포, 실제 경고 메시지의 억제 또는 블로킹, 다른 메시지를 위한 시스템의 남용, 차량 노드들의 위치에 대

한 노드 위조나 부당 변경, 그리고 그로 인한 거짓된 지리적 지역에 대한 메시지 발생 등을 들 수 있다. VANETs 라우팅의 보안을 위한 한 예로 이렇게 위치를 부당 변경한 노드를 탐지하고 라우팅 프로세스에서 그들을 제외시키는 방법이다. 위험감지 모듈에 대한 센서입력 보안 역시 고려되어야만 한다.[7, 8]

VANETs을 위한 능동적 안전 시스템의 한 예로 WILLWARN[9] 프로젝트가 있으며 VANETs 안전 응용 생성에 목표를 두고 있다. 이 프로젝트는 EU가 주도하는 PReVENT 프로젝트의 일부로 여기서 보안 스레드는 거짓 경고 메시지의 유포, 실제 경고 메시지의 억제 또는 블로킹, 다른 메시지를 위한 시스템의 남용 등의 탐지 및 경고등을 수행한다.[10]

현존하는 MANETs에서의 가능한 침입탐지시스템(IDS)의 구조는 다음을 포함한다.[7, 11]

- 독립형 IDS : 각 호스트가 IDS를 가지고 독립적으로 공격을 탐지하는 방식으로 노드들 사이에서의 협력은 없고 모든 결정은 지역노드가 한다. 이 구조는 비효율적이며 모든 노드에서 IDS를 구동시킬 수 없는 환경에 적용된다.
- 분산협력형 IDS : 각 노드들이 IDS 에이전트를 가지고 지역 탐지 결정을 하며, 동시에 모든 노드들이 전역 탐지 결정에 참여한다. 이는 flat 애드 혹 망에 적합한 구조이다.
- 계층형 IDS : 다중 계층 애드 혹 망을 위해 설계되었으며 클러스터 헤드 노드가 클러스터내의 모든 노드들에 대한 중앙 집중식 라우팅을 수행하면서 보안 수단을 지원한다. 이 구조는 가상 백본 라우팅 프로토콜에 대한 공격을 탐지할 수 있다.

Chen[8]은 연속적인 경로 스트림에 대한 지역 클러스터를 구축하기 위해 경로의 지역 연관성을 이용하고 가지치기 정책을 통해 anomaly를 감시하는 프레임워크를 제안하였다. Guizani[12]는 패턴 인식에서 기인한 통계적 방법에 기초하여 MANETs의 이동성 패턴 같은 anomaly를 식별하는 침입탐지 알고리즘을 제안하였다.

Ⅲ. 시스템 모델

VANETs은 개방 네트워크로 어느 차량이건 네트워크에 접속을 허용하기 때문에 네트워크상에 해로운 비정상 행위 노드들에 대한 침입이나 공격에 매우 취약하여 거대한 보안 문제를 초래하기 쉽다. 또한 망을 구성하는 노드들이 고속으로 진행하면서 망에 접속하거나 이탈하기 때문에 VANETs 망의 위상이 계속 변화하고 불안정한 링크를 가지게 되므로 대부분 위치기반 라우팅 방법을 사용하게 되는데 이때 라우팅에 대한 침입이나 공격이 큰 문제가 된다. VANETs에서 라우팅 공격의 대표적 사례로 노드 위치에 대한 위조나 부당 변경, 노드 트래픽의 블록이나 가로 챔 행위, 그리고 비인증 노드들의 거짓 경고 메시지 유포나 시스템 남용을 들 수 있다.

위치기반 라우팅 메커니즘은 노드 위치에 종속적이며 어드레싱과 라우팅 방법에서 위치를 사용한다. 노드들은 비컨이라는 작은 데이터 패킷을 통해 그들의 직접 이웃에게 자신의 위치를 방송한다. 그러나 노드 위치는 어드레싱의 일부이기 때문에 노드는 메시지를 간접 이웃들에게 전송하기를 원한다면 그들의 위치 또한 알아야 한다. 즉, 현재 노드의 위치를 탐색할 수 있는 네트워크상의 위치 서비스가 있어야 한다.

위치기반 서비스는 현재 환경과 차량의 상황 그리고 운전자에 적합한 맞춤형 정보를 제공할 것이다. 이것은 유동적인 차량 데이터 또는 트래픽 센터에 기반한 실시간 트래픽 정보, 차량 근처에서의 흥미로운 이벤트에 대한 전자적 안내이고, 각각의 경우에 이 정보는 운전자/승객의 개인 프로파일에 적용될 수 있다.

이렇게 수집된 차량 노드활동에 대한 정보와 프로파일 정보는 이후에 발생하는 이벤트에 대한 정규성을 판단하는 기준이 될 수 있으며 이를 근거로 발생한 이벤트에 대한 비정상 행위 정도를 판가름하는 척도로 사용될 수 있다. 비정상 행위는 그 정도에 따라 시스템에 대한 침입이나 공격으로 인식되며 침입 탐지 시스템은 이러한 이벤트에 대한 경고 메시지를 발령하게 된다. 시간의 흐름에 따라 수집되는 차량 노드활동과 프로파일 정보를 기반으로 특정 이벤트에 대한 모호한 정도에 따른 비정상 행위 정도를 나타내기 위해 본 논문에서는 러프 집합을 사용한다.

러프 집합의 기본 개념은 식별(classification)과 근사(approximation)이다. 외계로부터 얻어진 정보에 대하여 우리들은 이들 정보에 대한 주 개체를 속성에 따라 구별하여 추론하기도하고 결정하면서 행동한다. 이때 정보에 대한 식별은 수학적인 분명한 개념에 국한되지 않으며

모호하고, 부정확하며, 확실하지 않고, 복잡한 자료를 바탕으로 추론, 결정, 귀납, 학습 등으로 이루어진다. 러프 집합은 관심 도메인의 분류가 서로 독립적인 카테고리인 하한과 상한 근사라 불리는 명확한 개념의 쌍에 의한 모호한 개념에 대한 근사이다. 불완전한 자료의 처리를 위한 러프 집합 어프로치는 이러한 근사에 기반한다.[13] 전체 집합을 U, 동치관계를 R이라하면 $E=(U,R)$을 근사공간이라 하고 이때 관계 R의 동치 클래스는 E의 기본 집합이다. $x \in U$에 대해 $[x]_R$을 x를 포함하는 R의 동치 클래스라 하면 각 $X \subseteq U$에 대해 하한과 상한 근사는 다음 수식 (1)과 같다.

$$\underline{E}X = [x \in U | [x]_R \subseteq X$$
$$\overline{E}X = x \in U | [x]_R \cap X \neq \varnothing \quad (1)$$

여기서 동치관계 R에 의한 근사 공간에 대한 X의 근사의 정확도는 수식 (2)와같이 정의된다.

$$\alpha_R(X) = \frac{Card\,\underline{E}X}{Card\,\overline{E}X}, 0 \leq \alpha_R(X) \leq 1 \quad (2)$$

따라서 퍼지 포함 관계에 있지 않는 조건 클래스와 결정 클래스는 퍼지 포함으로 표현될 수 있으며 이는 멤버 함수의 불일치의 정도를 나타낸다. 그 이탈 정도가 퍼지 포함 허용범위 안에 있는 한 어느 정도 오차를 허용한다. 주어진 모델에 대한 퍼지 포함은 수식 (3)의 러프 소속 함수에 의해 계산된다.

$$\mu_R(X) = 1 - \alpha_R(X) \quad (3)$$

러프니스는 집합 X에 대한 지식 E의 불완전 정도를 나타내며[14] 본 논문에서는 이 값이 주어진 허용 오차 범위를 벗어나 이탈 정도가 큰 경우 이를 비정상 행위로 간주하고 그 정도에 따라 시스템에 대한 침입이나 공격으로 인식되며 침입 탐지 시스템은 이러한 이벤트에 대한 경고 메시지를 발령하게 된다.

Ⅳ. 가중치 기반 동적 침입 탐지 방법

가중치 기반 동적 침입 탐지 방법은 VANETs에서의 정상 차량 노드들의 활동에서 가지는 특징 값을 가지고 애드 혹 망이 정상상태일 때의 VANETs에 대한 정상 특징 정보시스템을 구축하여 시간에 따른 차량 노드들의 활동에 대한 정상으로부터의 이탈 정도를 러프 집합을 이용하여 동적으로 계산해서 그 노드에 대한 비정상 행위 정도를 측정하고 이를 기반으로 시스템에 대한 침입을 탐지하게 된다. 본 논문에서 제안한 가중치 기반 동적 침입탐지 알고리즘은 다음과 같다.

1. 차량노드의 이동경로와 패턴으로부터 특징 추출

차량 노드들의 활동으로부터 가지는 특징 값은 차량 노드의 이동 경로와 이동 패턴으로부터 특징을 추출한 것으로 단위 시간 동안의 차량 노드의 상대적 위치 변화량(LOC), 도로에서 차량 노드들의 주요 트래픽 변화량(TRF), 각 차량 노드에서 단위 시간 동안의 상대적인 홉수에 따른 전달 패킷 라우팅 변화량(ROT), 그리고 정상 특징 정보 시스템에 등록된 각 정상 엔트리의 신뢰도(RLY)를 신뢰 등급에 따라 평가한 사용자 프로파일을 사용한다.

2. VANETs에 대한 정상 특징 정보 시스템 구축

VANETs 상에서 정상상태의 차량 노드들의 활동으로부터 가지는 특징 값을 추출하여 얻어진 LOC, TRF, ROT와 각 정상 엔트리의 신뢰도 RLY에 추가로 프로파일 엔트리의 나이 등급을 더하여 VANETs에 대한 정상 특징 정보 시스템을 구축한다. 여기서 정상 특징 정보 시스템의 마지막 엔트리 항목으로 AGE를 두었는데 이 항목은 사용자 프로파일 엔트리의 나이를 나타내는 것으로 각 엔트리의 시스템 존속 시간에 따른 등급으로 나누어 분류한다. 시스템의 프로파일 엔트리는 시간에 따라 계속 생성되고 소멸되면서 존속 시간이 길어질수록 나이를 먹게 되는데, 이때 나이가 적을수록 시스템에 최근 입력된 최신의 프로파일 엔트리를 나타내며 그 신뢰도가 과거의 데이터에 비해 참신하고 높음을 의미하고, 상대적으로 나이가 많은 엔트리는 이미 시간이 경과한 데이터로 현재 시스템의 상황에 대한 정확도가 떨어지는 낮은 신뢰도를 나타내는 것으로 노드 활동에 대한 정상 이탈 정도를 계산할 때 AGE에 따른 차별화된 가중치가 적용되게 한다.

3. 러프집합 이용 프로파일 동치관계 클래스 추출

구축된 정상 특징 정보시스템으로부터 LOC, TRF, ROT 등을 조건 속성으로 하여 러프 집합을 이용 이에 대한 조건 클래스라 불리는 프로파일 동치관계 클래스를 구성하였으며 이들 조건 속성들 간의 시스템에 미치는 영향에 대한 중요도를 고려하여 각각 가중치를 부여하였다. 결정 속성으로는 정상 특징 정보 시스템에 등록된 각 정상 엔트리의 신뢰도(RLY)를 사용해서 러프 집합을 이용 결정 클래스라 불리는 프로파일 동치관계 클래스를 구성하였다.

이렇게 구축된 VANETs에 대한 정상 특징 정보시스템으로부터 러프 집합을 이용하여 프로파일 동치 관계 클래스를 추출하고 이들 클래스들로부터 퍼지 포함 관계를 다음과 같이 결정한다.

$$V_i = \overline{R}X_i \cup \overline{R}Y$$
$$W_i = \overline{R}X_i \cap \overline{R}Y \quad (4)$$

여기서, X_i : i번째 조건속성, Y : 결정속성

$$\alpha(V_i, W_i) = \frac{\sum_{AGE=1}^{n} [Card(W_i) \times (\omega_{X_i} + \omega_Y) \times \omega_{AGE}]}{\sum_{AGE=1}^{n} [Card(V_i) \times (MAX(\omega_{X_i}) + \omega_Y) \times \omega_{AGE}]} \quad (5)$$

여기서, ω_{X_i} : i번째 조건속성의 가중치

ω_Y : 결정속성의 가중

ω_{AGE} : AGE의 가중치, n : AGE 등급 수

4. 러프 소속 함수에 의한 이탈정도 계산

어느 주어진 시점에 차량 노드 활동이 발생하면 이 노드 활동에 대한 정상 프로파일로 부터의 비정상 행위 정도를 수식 (6)의 러프 소속 함수를 이용 기존의 정상 특징 정보시스템으로부터 이탈 정도를 계산한다.

$$\mu(X, Y) = MIN(1 - \alpha(V_i, W_i)), \text{ for } 1 \le i \le m \quad (6)$$

여기서, m : 조건 속성의 개수

5. 허용 임계오차 ϵ과 비교

러프 소속 함수에 의해 구해진 러프니스 정도를 시스템에서 허용하는 임계오차 범위 내에 있는지 비교하여 그 오차 범위를 벗어나는 경우(즉, $\mu(X, Y) > \epsilon$) 이 차량 노드의 활동이 비정상 행위로 분류되어 시스템에 대한 공격이나 침입으로 간주하여 경고 메시지를 발령하게 된다.

V. 성능 평가

본 논문에서 제안한 가중치 기반 동적 침입 탐지 방법은 차량 노드들의 활동이 가지는 특징 값을 추출하여 정상상태에서의 VANETs에 대한 정상 특징 정보 시스템을 구축하고 이를 근거로 어떤 차량 노드의 활동이 시스템에 대한 공격이나 침입인지 여부를 탐지한다. 제안하는 가중치 기반 침입탐지 방법의 성능 평가를 위해 차량 노드들의 활동으로부터 가지는 특징 값으로 단위 시간 동안의 차량 노드의 위치 변화(LOC)를 상대적인 변화량에 따라 {S, M, L}의 3등급으로 구분하였고, 도로에서의 차량 노드들의 주요 트래픽 변화(TRF)를 그 변화량에 따라 {U, M, O}의 3등급으로 구분하였으며, 차량 노드에서의 패킷 전달을 위한 라우팅 변화량(ROT)을 단위시간 동안의 상대적인 홉 수에 따라 {D, E, U}의 3등급으로 구분하였다. 그리고 각 정상 엔트리의 신뢰도(RLY)를 그 신뢰 등급에 따라 {1, 2, 3}의 3등급으로 평가한 사용자 프로파일을 갖는 정상 특징 정보 시스템을 구축하였다. 구축된 정상 특징 정보 시스템의 노드의 상대적 위치 변화량, 주요 트래픽 변화량, 그리고 라우팅 홉 수 변화량 등의 정상상태 시스템 프로파일 정보에 기초하여 러프집합을 이용해 조건 동치관계 클래스를 추출하였고, 각 정상 엔트리의 신뢰도 등급에 따라 러프집합을 이용하여 결정 동치관계 클래스를 추출하여 이를 바탕으로 지금까지의 정상 시스템에서의 퍼지 포함 관계를 결정하였다.

이때 만약 어떤 차량 노드의 활동이 발생하였다면 시스템은 이 노드의 활동에 대한 공격이나 침입 여부를 판단하기 위해 지금까지의 정상 활동에 대한 이탈 정도를 계산하게 되고 그 이탈 정도가 시스템이 정한 허용 임계오차 범위를 벗어나는 노드에 대해서는 비정상 행위로 간주하고 침입 경고 메시지를 발령하게 된다.

본 논문에서 제안한 가중치 기반 침입 탐지 방법의 성

능 평가는 모의실험을 통해 허용 임계오차에 대한 침입 탐지율(detection rate)과 거짓 경고율(false alarm rate) 등 2가지로 평가하였다. 여기서 침입 탐지율은 모의실험 기간 중 발생한 총 비정상 행위 중에서 정상적으로 침입 행위를 탐지한 비율을 말하며, 거짓 경고율은 모의실험 기간 중 침입 행위가 아닌 활동을 침입으로 잘못 탐지한 비율을 말한다. 모의실험은 인텔 펜티엄 4 PC상에서 MS 비주얼 C++로 모의실험 프로그램을 작성하였으며, 이때 모의실험에 사용한 파라미터는 다음의 표 1과 같다. 여기서 VANETs의 정상 차량 노드 활동 특징 값, 즉 LOC, TRF, ROT, RLY, AGE의 등급 값의 증감은 모의실험 결과에 영향을 미치지 않으므로 본 논문에서는 이들 등급의 증감에 따른 변화를 고려하지 않는다.

표 1. 모의실험 파라미터
Table 1. Simulation Parameters

Parameters	Value	
Total # of Node Activities	100	
Degree of LOC	random(1, 3)	
Degree of TRF	random(1, 3)	
Degree of ROT	random(1, 3)	
Degree of RLY	random(1, 3)	
Degree of AGE	random(1, 3)	
Threshold ϵ	[0.2-0.6]	
Weighted Value of (X,Y)	A	(0.5, 0.15, 0.15, 0.2)
	B	(0.4, 0.2, 0.2, 0.2)
	C	(0.3, 0.25, 0.25, 0.2)
Weighted Value of AGE	D	(1.0, 0.5, 0.1)
	E	(1.0, 0.7, 0.3)
	F	(1.0, 1.0, 1.0)

VANETs에서 차량 노드들의 활동이 가지는 특징 값들에 대한 가중치가 제안하는 침입탐지 방법의 성능에 미치는 영향을 분석하기 위해 서로 간의 가중치 차이가 큰 것부터 거의 비슷한 것까지 3단계로 비교하였고, 정상 특징 시스템 내에서 각 엔트리의 참신도에 따른 AGE의 가중치가 제안하는 침입탐지 방법의 성능에 미치는 영향을 분석하기 위해 또한 3단계로 비교하였다.

우선 차량 노드들의 활동이 가지는 특징 값들에 대한 가중치가 제안하는 침입탐지 방법의 성능에 미치는 영향을 분석하기 위해 차량 노드의 활동을 다음과 같이 4가지 부류로 나누어 모의실험을 하였다.

1. 차량 노드 활동이 완전 퍼지 포함 관계에 있는 경우
2. 차량 노드 활동이 부분 퍼지 포함 관계에 있는 경우
3. 차량 노드 활동이 퍼지 포함 관계는 아니지만 비정상 행위가 아닌 경우
4. 차량 노드 활동이 퍼지 포함 관계도 아니고 비정상 행위인 경우

표 2. 노드활동의 가중치에 따른 러프니스
Table 2. Roughness for Weighted Values of Node Activities

노드활동 / 가중치	1	2	3	4
AD	0	0.135	0.465	0.625
AE	0	0.149	0.457	0.585
AF	0	0.143	0.441	0.542
BD	0	0.142	0.407	0.554
BE	0	0.155	0.392	0.471
BF	0	0.151	0.368	0.463
CD	0	0.135	0.373	0.488
CE	0	0.149	0.316	0.434
CF	0	0.143	0.279	0.375

표2는 4가지의 노드 활동 유형에 대해 각각 3가지의 조건 속성에 대한 가중치와 3가지의 AGE 속성에 대한 가중치를 적용하여 모의실험을 통해 러프 소속 함수를 통해 구해진 평균 러프니스를 보여준다. 표에서 보인바와 같이 차량 노드 활동이 완전 퍼지 포함 관계에 있는 경우에는 각 조건 속성이나 AGE 속성에 대한 가중치의 변화에 러프니스가 전혀 영향을 받지 않는 것으로 나타났다. 또한 차량 노드 활동이 부분 퍼지 포함 관계에 있는 경우에도 속성들의 가중치 변화에 거의 영향을 받지 않고 안정적으로 허용 임계 오차 범위 내에서 약간의 변화를 보이고 있다. 이때 AGE 속성에 대한 가중치는 차이를 크게 주는 경우가 그렇지 않은 경우보다 약 1.4%정도 저하되는 것을 확인할 수 있다. 하지만 차량 노드 활동이 퍼지 포함 관계에 있지 않은 경우에는 가중치의 변화에 대한 러프니스의 변화가 두드러지게 영향을 받는 것으로 나타났다. 특히 차량 노드 활동이 비정상 행위인 경우 그 영향은 더욱 두드러져서 러프니스의 변화가 약 16%정도 저하하는 것을 알 수 있다. 이는 분명한 비정상 행위임에도 불구하고 가중치의 변화에 따라 그 활동이 침입으로 탐지가 되지 않는 경우가 발생할 확률이 매우 높아짐을

알 수 있다. AGE 속성에 대한 이들 차량 활동에 대한 가중치의 영향 역시도 매우 커서 AGE 속성에 가중치를 적용하지 않는 경우보다 최대 약 11%정도 러프니스가 저하됨을 알 수 있다. 이 또한 AGE의 가중치의 변화에 따라 침입 탐지율의 저하나 거짓 경고율의 상승을 초래하게 된다.

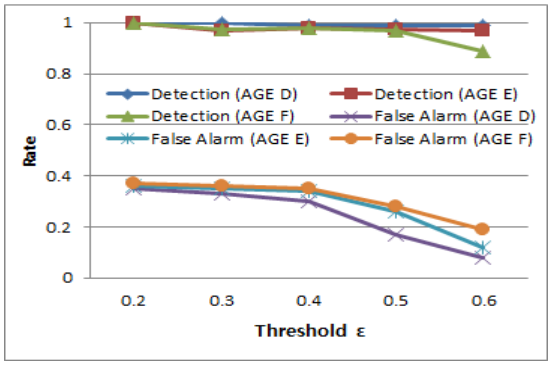

그림 2. 모의실험 결과
Fig. 2. Simulation Results

그림 2는 본 논문에서 제안한 가중치 기반 침입 탐지 방법에서 AGE 속성에 서로 다른 가중치를 적용했을 때의 허용 임계오차에 따른 침입 탐지율과 거짓 경고율에 대한 모의실험 결과를 보여준다. 그림에서 보는 바와 같이 제안한 가중치 기반 침입 탐지 방법은 허용 임계 오차 ϵ이 작을수록 침입 탐지율은 높아지나 동시에 거짓 경고율도 상대적으로 높아지는 것을 알 수 있다. 이는 정상 활동에 대한 엄격한 행위 패턴을 적용함으로써 정상 활동에서 조금이라도 벗어나면 비정상 행위로 간주하여 침입으로 탐지하기 때문으로 생각되며, 이로 인해 실제 정상행위에 대해서도 침입으로 오인한 경고가 발령되는 경우가 잦아져서 거짓 경고율이 높아지는 것으로 판단된다. 하지만 허용 임계오차 ϵ이 커질수록 침입 탐지율은 저하되나 거짓 경고율도 역시 저하되는 것을 알 수 있다. 이는 정상 활동에 대한 느슨한 행위 패턴을 적용함으로써 이들 정상 활동에 유사한 경우 모두 정상 활동으로 간주하여 비정상 행위에 대한 침입 탐지가 낮아지는 반면에, 이로 인해 실제 정상 활동에 대해서 침입으로 오인한 경고가 발령되는 경우가 낮아지므로 거짓 경고율도 낮아지는 것으로 판단된다. 특히 허용 임계오차 ϵ이 0.4 부근 이후에서 침입 탐지율의 하락 정도는 미미한 반면 거짓 경고율은 크게 저하되는 것으로 나타났다. 따라서 이 부근에서의 적당한 허용 임계오차 ϵ의 선택이 중요하다. 침입 탐지율과 거짓 경고율에 대한 AGE 속성의 가중치에 따른 영향은 그림에서 보는바와 같이 AGE 속성에 대한 가중치 차이를 크게 주는 것이 적게 주는 경우 보다 침입 탐지율과 거짓 경고율에서 모두 우수하게 나타나는 것을 확인 할 수 있다.

Ⅵ. 결 론

VANETs은 이동성이 높은 차량 노드들이 일시적으로 망을 구성하는 자기 조직화 망으로 고정된 인프라 구조 없이 동적으로 차량 노드들이 망에 결합하거나 이탈하므로 불안정한 통신 링크를 갖는다. VANETs은 개방망으로 중앙 집중식 제어 없이 누구나 접속을 허용하므로 망상에 해로운 비정상 행위 노드들에 대한 침입이나 공격의 기회가 높아 보안에 매우 취약하다. 본 논문에서는 이렇게 보안이 취약한 VANETs에서의 차량 노드들의 활동에 대한 비정상 행위를 효율적으로 식별하여 침입을 탐지할 수 있는 가중치 기반 침입 탐지 방법을 제안하고 그 성능을 모의실험을 통해 각 속성에 대한 가중치에 따른 러프니스와 임계 허용오차에 대한 침입 탐지율 및 거짓 경고율로 평가하였다.

성능 평가 결과 조건 속성에 대한 가중치의 러프니스에 미치는 영향은 노드의 활동이 퍼지 포함 관계 안에 있는 경우에는 그 정도가 미미한 반면 차량 노드의 활동이 퍼지 포함 관계 안에 있지 않은 경우에는 그 영향이 크게 나타나서 탐지 오류 등의 문제를 초래하게 된다. AGE 속성에 대한 가중치의 러프니스에 미치는 영향 역시 차량 노드의 활동이 퍼지 포함 관계 안에 있지 않은 비정상 행위의 경우 더욱 두드러져 침입 탐지율과 거짓 경고율에 크게 영향을 미치는 것으로 나타났다. 또한 AGE 속성에 서로 다른 가중치를 적용했을 때의 허용 임계오차에 따른 침입 탐지율과 거짓 경고율에 대한 모의실험 결과는 비교적 낮은 허용 임계오차 범위 내에서 높은 침입 탐지율과 거짓 경고율을 나타내는 것을 알았다. 반면에 높은 허용 임계 오차 범위 내에서는 거짓 경고율이 낮아지고 동시에 침입 탐지율도 낮아지는 것을 알았다. 그리고 허용 임계오차가 0,4 부근에서 침입 탐지율은 높게 유지하면서 거짓 경고율이 급격히 낮아지는 것을 알았다. AGE 속성의 가중치에 대한 영향은 가중치 차이를 크게 주는

것이 더욱 우수한 성능을 보임을 알 수 있었다. 향후 연구과제로는 VANETs에서의 신뢰도가 높은 차량 노드 활동의 특징 값의 추출 방법과 이들에 대한 적절한 가중치 부여 방안에 관한 것이다.

참 고 문 헌

[1] B. Karp and H. T. Kung, “GPSR: greedy perimeter stateless routing for wireless networks,” *Proc. in Mobile Computing and Networking*, pp. 243 - 254, 2000.

[2] C. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers,” *Proc. in ACM SIG-COMM'94 Conference on Communications Architectures, Protocols and Applications*, pp. 234 - 244, 1994.

[3] W. Franz and C. Maihoefer, “Geographical addressing and forwarding in fleetnet,” *Proc. in Mobile Computing and Networking*, 2002.

[4] H. Fuessler, M. Mauve, H. Hartenstein, M. Kaesemann, and D. Vollmer, “A Comparison of Routing Strategies for Vehicular Ad Hoc Networks,” Department of Computer Science, University of Mannheim, Mannheim, *Tech. Rep. TR-3-2002*, 2002.

[5] T. Leinmueller, E. Schoch, F. Kargl, and C. Maihoefer, “Influence of Falsified Position Data on Geographic Ad-hoc Routing,” *Proc. in ESAS 2005, 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks*, 2005.

[6] H. Deng et al., "Agent-based Distributed Intrusion Detection Methodology for MANETs," *Proc. of the 2006 International Conference on Security & Management*, pp. 200-206, 2006.

[7] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad-Hoc Networks", *Proc. of the 2003 Symposium on Applications and the Internet Workshop*, pp. 368-373, 2003.

[8] B. Chen, L. Fu and D. Liu, "Efficient Anomaly Monitoring over Moving Object Trajectory Streams", *KDD'2009*, pp. 159-167, 2009.

[9] The PReVENT WILLWARN subproject website. [Online]. Available: http://www.prevent-ip.org/en/prevent_subprojects/safe_speedand safe_following/willwarn/

[10] The PReVENT project website. [Online]. Available: http://www.prevent-ip.org/

[11] D. Stern et al., "A General Cooperative Intrusion Detection Architecture for MANETs," *Proc. of the 3rd IEEE International Workshop on Information Assurance*, pp. 57-70, 2005.

[12] C. Guizani and A. Al-Fuqaha, "Constructing an Efficient Mobility Profile of Ad-Hoc for Mobility-Pattern-Based Anomaly Detection in MANET," *GLOBECOM'2006*, pp. 1-5, 2006.

[13] R. Jensen and Q. Shen, Fuzzy-Rough Sets for Descriptive Dimensionality Reduction, *Proc. of the 11th International Conference on Fuzzy Systems*, pp. 29-34., 2002.

[14] Z. Pawlak, *Rough Sets Theoretical Aspects of Reasoning about Data*, Kluwer Academic Pub., 1991.

저자 소개

오 선 진(종신회원)

- 제6권 제2호 참조
- 현재 세명대학교 정보통신학부 교수

<주 관심분야 : VANETs, MANETs, USN, P2P, Mobile Computing, 스마트 응용 등>