논문 2010-2-12

VANETs의 보안을 위한 비정상 행위 탐지 방법

An Anomaly Detection Method for the Security of VANETs

오선진*

Sun Jin Oh

요 약 차량 애드 혹 망 (Vehicular Ad Hoc Networks: VANETs)은 일반적으로 이동성이 높은 차량 노드들로 구성되어 매우 짧은 시간 망 위상이 지속되므로 불안정한 통신 링크를 갖는 자기 조직화 P2P 망이다. VANETs은 고정된 인프라 구조나 중앙 통제 라우팅 장비 없이 자동적으로 망구조를 구성하고, 차량 노드들은 시간에 따라 고속으로 이동하며 망에 결합하거나 이탈하는 개방 망이므로 중앙 집중식 제어 없이 누구나 접속을 허용하기 때문에 망상에 해롭고 비정상 행위 노드들에 대한 침입에 매우 취약하다. 본 논문에서는 이러한 VANETs에서의 노드들의 활동에 대한 비정상 행위를 효율적으로 식별할 수 있는 러프집합기반 비정상 행위 탐지방법을 제안하고, 그 성능을 모의실험을 통해 임계 허용 오차에 대한 비정상 행위 탐지율과 거짓 경고율로 평가하였다.

Abstract Vehicular Ad Hoc Networks are self-organizing Peer-to-Peer networks that typically have highly mobile vehicle nodes, moving at high speeds, very short-lasting and unstable communication links. VANETs are formed without fixed infrastructure, central administration, and dedicated routing equipment, and network nodes are mobile, joining and leaving the network 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 connect, without centralized control. In this paper, we propose a rough set based anomaly detection method that efficiently identify malicious behavior of vehicle node activities in these VANETs, and the performance of a proposed scheme is evaluated by a simulation in terms of anomaly detection rate and false alarm rate for the threshold ϵ.

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

Ⅰ. 서 론

모바일 애드 혹 망(Mobile Ad Hoc Networks: MANETs)은 특별한 특징을 가진 자기 조직화 P2P망이다. 고정된 인프라 구조 없이 참여하는 노드들은 수동적 방해 없이 자동적으로 망구조를 구성하며 동적인 노드의 망 이탈이나 결합에 대처할 수 있다. 망의 노드들은 시간에 따라 이동하고 결합하며 이탈한다. 주로 무선 통신을 사용하면서 노드들 사이의 링크는 매우 불안정하여 노드들은 지속적으로 통신 범위를 벗어나 다른 노드의 통신 범위에 도달한다. 만약 MANETs 내의 노드들이 차량들로 구성된다면 이 망을 차량 애드 혹 망 (Vehicular Ad Hoc Networks: VANETs)이라 부른다. VANETs은 일반적으로 이동성이 높은 노드들로 구성되어 매우 짧은 시간 망 위상이 지속되므로 불안정한 통신 링크를 갖는다. VANETs은 고정된 도로변의 게이트웨이와 연결할 수 있는 메커니즘을 가질 수 있고 인터넷과 같은 공통 망을 이들 게이트웨이를 통해 접근할 수 있다.

VANETs의 주요 장점 중 하나는 고정된 인프라 구조, 중앙 통제 관련 라우팅 장비로부터의 독립이다. 그러나 보안 측면에서는 이러한 장점들 역시 커다란 도전이 된다. VANETs의 인프라 구조는 망 내에 참여하는 모든 노

*종신회원, 세명대학교 정보통신학부 교수
접수일자 2010.3.17, 수정일자 2010.4.16

드들에 의해 형성되기 때문에 망의 신뢰는 단일 노드의 신뢰에 종속적이다. VANETs은 대부분 개방 망으로 중앙 집중식 제어 없이 누구나 접속을 허용하기 때문에 망 상에 해롭고 비정상 행위 노드들에 대한 침입이나 공격에 매우 취약하다.

VANETs에서의 보안은 중요한 속성으로 과연 VANETs이 성공적이고 사용 가능 기술이 될지를 결정하게 될 것이다. 보안에 가장 중요한 응용은 안전 응용이다. 거짓이거나 지연된 경고 메시지는 사고를 야기하므로 예방되어야 한다. 만약 비인증 노드들이 거짓 경고 메시지를 유포할 수 있다면 트래픽 흐름상의 충격은 엄청날 것이고 주요 도로를 완전히 블록 시키거나 다른 트래픽의 방해를 초래할 것이다. 비안전 분야에서도 많은 응용들은 강력한 안전을 요구한다. 만약 VANETs을 통해 비지니스가 이루어지거나 차량 내 소프트웨어 갱신 또는 원격 진단 같은 중요한 작업이 수행된다면 종단 간 보안이 필요하다.

VANETs에서의 효과적인 보안을 위해서 비정상 행위를 하는 노드들의 탐지기법이 필요하다. 비정상 행위 탐지기법은 시스템 상태와 노드 행위의 정상 프로파일을 생성하고 그것을 현재 활동과 비교하여 만약 정상상태로부터 상당한 이탈이 관찰되면 경고를 발생한다. 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 침입탐지 알고리즘의 설계가 중요하다.

본 논문에서는 VANETs에서의 차량 노드들의 활동에 대한 비정상 행위를 효율적으로 식별할 수 있는 러프집합기반 비정상 행위 탐지방법을 제안한다. VANETs 상에서 정상상태의 차량 노드 활동패턴으로 노드의 정상 프로파일을 가지는 정상 특징 정보 시스템을 구축하고, 러프집합을 이용하여 어떤 노드의 활동 패턴에 대한 정상으로 부터의 이탈 정도를 계산한다. 그 이탈 정도가 허용 임계치보다 크면 경고 메시지를 생성하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 VANETs과 라우팅 그리고 보안문제에 대한 관련 연구를 살펴보았고, 3장에서는 본 논문에서 제안한 러프집합 기반 비정상 행위 탐지방법을 서술하였으며, 4장에서는 제안한 비정상 행위 탐지모델의 분석과 성능평가를 했고, 마지막으로 5장에서 향후 연구내용과 함께 결론을 맺는다.

Ⅱ. VANETs과 보안문제

지난 20년 동안 자동차는 주로 기계적이고 전기적인 상품으로부터 매우 복잡한 모바일 컴퓨터 시스템으로 진화하였다. 지난 수 년 동안 차량 내의 컴퓨터 하드웨어와 소프트웨어의 양은 폭발적으로 증가해 왔으며 현재는 폐쇄된 소프트웨어 플랫폼 상에서 작동하나 앞으로 10년 내에 자동차는 개방된 소프트웨어와 서비스 플랫폼에서 작동할 연결된 모바일 애드 혹 망의 노드가 될 것이다. 이렇게 차량들로 이루어진 애드 혹 망을 차량 애드 혹 망이라 하며 차량 노드들은 매우 이동성이 높아 상대 속도가 500Km/h에 이르기도 하므로 매우 짧게 망 위상이 지속되어 불안정한 통신 링크를 갖는다. 이러한 VANETs에서의 통신은 전통 망에서 알려진 것과는 다른 통신 패턴을 사용한다. 인접한 노드들과의 직접 단일 홉 통신뿐만 아니라 멀리 떨어진 노드들과는 중간 노드로 다른 노드들을 사용하는 멀티 홉 통신을 사용해야 하고 특별한 라우팅 프로토콜[1, 2]로 메시지를 목적지로 전송하게 된다. 그림 1은 VANETs의 예를 보여준다. 7개의 노드가 차량 애드 혹 망을 형성하고 거기서 메시지가 차량 노드 A와 B사이에 중간노드 H와 I를 통해 전달된다.

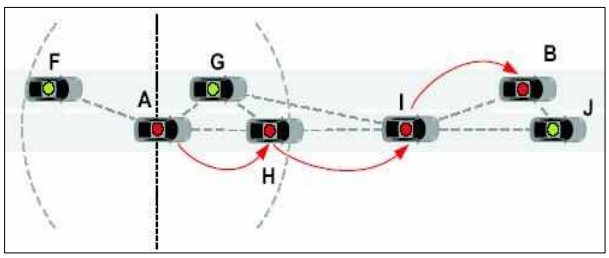

그림 1 차량 애드 혹 네트워크(VANETs)
Fig. 1. Vehicular Ad Hoc Networks

또한 전통 망에서 가장 일반적인 형태의 통신은 유니캐스트로 하나의 노드가 망 주소를 통해 어드레스된 다른 노드에 메시지를 송신하는 반면 많은 VANETs 응용들은 특별한 노드로가 아닌 노드 그룹으로 메시지를 보내는데 이러한 통신 패턴을 지오캐스트(geocast)라 한다.[3]

대부분 전통 망은 망 위상에 기반한 라우팅 접근방법

을 사용하지만 VANETs에서는 위상기반 라우팅이 가능하지 않다.[4] VANETs의 위상은 계속해서 변화하고 노드들은 고속으로 이동하며 지속적으로 망에 결합하거나 이탈하고, 불안정하고 변화하는 링크를 만든다. 따라서 대부분의 VANETs 시스템은 위치기반 라우팅 접근방법을 사용한다. 이때 패킷들은 송신자와 수신자의 위치에 따라 라우트 된다.

그러나 위치기반 라우팅 메커니즘은 노드들의 위치에 종속적이며 어드레싱과 라우팅 방법에서 위치를 사용하기 때문에 제 3자에 이동 패턴을 노출하여 노드의 수명 동안에 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 VANETs의 어떤 부분의 모든 트래픽을 블록하거나 가로챌 수 있으며 또는 망 분할을 초래할 수 있다.[5, 6]

VANETs을 위한 능동적 안전 시스템의 한 예로 WILLWARN[7] 프로젝트가 있는데 VANETs 안전 응용의 생성에 목표를 두고 있다. WILLWARN 프로젝트는 "Wireless Local Danger Warning"의 약자로 EU가 펀드를 제공하는 PReVENT 프로젝트의 서브 프로젝트이다.[8] 이 프로젝트에서의 보안 스레드는 거짓 경고 메시지의 유포, 실제 경고 메시지의 억제 또는 블로킹, 다른 메시지를 위한 시스템의 남용 등을 들 수 있다.

VANETs에서의 위치기반 라우팅 메커니즘은 노드의 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 적응될 수 있다.

차량 간 통신은 새로운 안전 응용을 허용한다. 근처 차량과의 끊임없는 통신을 통해 센서 데이터나 정보의 교환, 사고 예방 그리고 운전 지원이 가능하게 되고 도로상에서의 재난이나 부상을 줄일 수 있다. 사고 예방 응용들은 다가올 위험과 특별한 상황(그림 2참조)에 대해 운전자에게 능동적으로 경고한다. 차선 머징 지원, 추월 지원, 트래픽 관리, 가상 경고신호 그리고 비상등과 같은 응용들 역시 사고 횟수나 도로 위험을 줄인다.

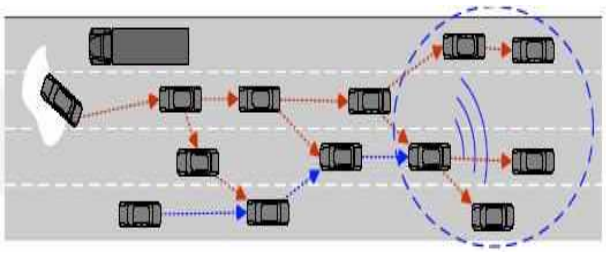

그림 2. 위험 경고 다중 홉 시나리오
Fig. 2. Hazard Warning Multi-hop Scenario

VANETs에서의 주요 보안 문제는 거짓 경고 메시지의 유포, 실제 경고 메시지의 억제 또는 블로킹, 다른 메시지를 위한 시스템의 남용, 차량 노드들의 위치에 대한 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 센서 입력의 보안 역시 고려되어야만 한다.[9, 10]

Ⅲ. 러프집합 기반 비정상 행위 탐지 알고리즘

본 논문에서 제안하는 러프집합 기반 비정상 행위 탐지 알고리즘은 그림 3과 같다. VANETs에서의 비정상 행위를 탐지하기 위해 먼저 정상상태의 VANETs으로부터 차량 노드 활동 특징을 추출하여 정상 특징 정보 시스템을 구축하고, 러프집합을 이용하여 그 사용자 프로파일의 동치류를 계산한다. 그리고 차량 노드 활동에 대한 정보와 그 프로파일에 대한 동치류 정보를 기초로 러프집합을 이용하여 특정 노드의 정상 행위로부터의 이탈 정도(deviation number)를 계산하고, 그 이탈 정도가 시스템에 설정된 허용 임계오차를 초과하면, 비정상 행위로 간주하여 시스템에 경고 메시지를 생성한다.

<VANETs에서의 비정상 행위 탐지 방법>

1. 차량노드의 이동경로와 패턴으로부터 특징 추출

   단위 시간 동안의 노드 상대적 위치 변화량(LC),
   단위 시간 동안의 주요 트래픽 변화량(TR),
   단위 시간 동안의 노드의 라우팅 변화량(RT),
   각 엔트리의 신뢰도(RY)를 갖는 노드의 정상 특징 정보 기초

2. VANET에 대한 정상 특징 정보 시스템 구축

   (RQ#, LC, TR, RT, RY, AGE)
   AGE : 프로파일 엔트리 나이 등급

3. 러프집합을 이용 프로파일 동치관계 클래스 추출

   1) 결정 동치 클래스 : $X = \{RY\}$
   2) 조건 동치 클래스 : $Y = \{LC, TR, RT\}$
   3) 퍼지 포함관계 결정

4. 이탈정도(deviation number) 계산

$$\mu(X,Y) = 1 - \frac{\sum_{AGE=1}^{n} [Card(\overline{R}X \cap \overline{R}Y) \times \omega_{AGE}]}{\sum_{AGE=1}^{n} [Card(\overline{R}X \cup \overline{R}Y) \times \omega_{AGE}]}$$

5. 허용 임계오차 ϵ과 비교

   if $\mu(X,Y) > \epsilon$, 노드 비정상 행위 탐지 경고

그림 3. 러프집합 기반 비정상 행위 탐지 알고리즘
Fig. 3. Rough Set based Anomaly Detection Algorithm

VANETs에서 라우팅 공격의 대표적인 사례로 차량 노드의 위치에 대한 노드 위조나 부당 변경, 노드 트래픽의 블록이나 가로 챔 행위, 그리고 비인증 노드들의 거짓 경고 메시지의 유포나 시스템 남용을 들 수 있다. 따라서 본 논문에서 제안한 러프집합 기반 비정상 행위 탐지 알고리즘은 VANETs의 정상 차량 노드 활동 특징 값으로 단위 시간 동안의 노드 위치의 변화량(LC)을 상대적인 변화에 따라 {S, M, L}의 3등급으로, 주요 트래픽 변화량(TR)을 {U, M, O}의 3등급으로, 노드에서의 라우팅 변화량(RT)을 단위시간 동안의 상대적인 홉 수에 따라 {-, 0, +)의 3등급으로, 그리고 각 정상 엔트리의 신뢰도(RY)를 신뢰 등급에 따라 {a, b, c, d)의 4 등급으로 평가한 사용자 프로파일을 갖는 정상 특징 정보 시스템을 구축한다.

여기서 정상 특징 정보 시스템의 마지막 항목으로 AGE는 사용자 프로파일 엔트리의 나이를 나타내는 것으로 각 프로파일 엔트리의 시스템 존속 시간에 따라 {1, 2, 3}의 3등급으로 분류한다. 시스템의 프로파일 엔트리는 시간에 따라 계속 생성되고 소멸되면서 존속 시간이 길어질수록 나이를 먹게 되는데, 이때 나이가 적을수록 시스템에 최근 입력된 새로운 프로파일 엔트리를 나타내며 그 신뢰도가 비교적 낮음을 의미하고, 상대적으로 나이가 많은 엔트리는 보다 높은 정상 신뢰도를 나타내는 것으로 노드 활동에 대한 정상 이탈 정도를 계산할 때 AGE에 따른 차별화된 가중치를 부여한다.

Ⅳ. 분석 및 성능평가

본 논문에서 제안한 러프집합 기반 비정상 행위 탐지 알고리즘에서는 정상 상태의 VANETs으로부터 차량 노드들의 과거 일정기간 동안의 상대적 위치 변화량, 주요 트래픽 변화량, 그리고 라우팅 홉 수 변화량을 갖는 정상 상태의 시스템 프로파일 정보에 기초하여 러프집합을 이용하여 동치관계 클래스를 추출하여 정상 특징 정보 시스템을 구축한다. 그리고 어떤 노드의 활동에 대한 이탈 정도를 계산하여 시스템이 정한 허용 임계오차를 벗어나는 노드에 대한 비정상 행위를 탐지하여 경고 메시지를 생성한다.

표 1. 정상 특징 정보 시스템
Table 1. Normal Characteristic Information System

RQ#	LC	TR	RT	RY	AGE
1	M	O	+	c	3
2	S	U	-	a	3
3	S	O	0	d	2
4	L	M	0	b	2
5	M	U	-	b	2
6	S	U	-	a	2
7	S	O	0	c	1
8	L	M	0	d	1
9	M	O	+	c	1

표 1은 VANETs에서의 차량 노드의 이동경로와 패턴으로부터 특징을 추출한 정상 특징 정보 시스템의 예를 보여준다. 여기서 RQ#, LC, TR, RT, RY, AGE는 각각 사용자 채널의 요청 번호, 노드의 상대적 위치 변화량, 주요 트래픽 변화량, 라우팅 홉 수 변화량, 엔트리의 신뢰

도, 그리고 프로파일 엔트리의 나이 등급을 각각 나타낸다.

표 1의 예에서, 속성 RY를 결정 속성이라 하면, 결정 클래스라 불리는 다음의 4가지 동치 클래스를 가진다.[11, 12]

$$\begin{aligned} &DE1=\{1, 7, 9\}=\{c\} \\ &DE2=\{2, 6\}=\{a\} \\ &DE3=\{3, 8\}=\{d\} \\ &DE4=\{4, 5\}=\{b\} \end{aligned} \quad (1)$$

조건 속성 (LC, TR, RT)에 대해, 우리는 조건 클래스라 불리는 다음의 5가지 동치 클래스를 가진다.

$$\begin{aligned} &CE1=\{1, 9\} \\ &CE2=\{2, 6\} \\ &CE3=\{3, 7\} \\ &CE4=\{4, 8\} \\ &CE5=\{5\} \end{aligned} \quad (2)$$

상기 조건 클래스와 결정 클래스를 비교하면 다음의 포함관계를 얻을 수 있다.

$$\begin{aligned} &CE1 \subseteq DE1 \\ &CE2 \subseteq DE2 \\ &CE5 \subseteq DE4 \end{aligned} \quad (3)$$

차량 노드활동의 이탈 정도의 계산은 다음의 식에 의해 퍼지포함 관계를 얻을 수 있다.

$$\mu(X,Y) = 1 - \frac{\sum_{AGE=1}^{n} [Card(\overline{R}X \cap \overline{R}Y) \times \omega_{AGE}]}{\sum_{AGE=1}^{n} [Card(\overline{R}X \cup \overline{R}Y) \times \omega_{AGE}]} \quad (4)$$

비정상 행위 탐지 시스템의 정상 상태로부터 허용하는 오차(ϵ)를 0.35라 하면, 차량 노드활동 (S, U, -, a)가 발생한 경우, Y={a} = DE2, X={S, U, -} = CE2라 두면 $\overline{R}X$={2, 3, 6, 7}이고 $\overline{R}Y$={2, 6}이다. 그러므로 차량 노드 활동의 이탈 정도는 식 4로 부터 $\mu \approx 0.33$이다. 따라서 $\mu \leq \epsilon$이므로 차량 노드 활동은 정상 행위로 수용된다. 그러나 만일 차량 노드 활동에 대한 이탈 정도 μ가 허용 임계오차 ϵ보다 크면 비정상 행위 탐지 알고리즘은 이 차량 노드의 활동에 대해 비정상 행위로 간주하고 경고 메시지를 전송하게 된다.

본 논문에서 제안한 비정상 행위 탐지 방법의 성능 을 모의실험을 통해 허용 임계오차에 대한 비정상 행위 탐지율(detection rate)과 거짓 경고율(false alarm rate)등 2가지로 평가하였다. 여기서 비정상 행위 탐지율은 모의실험 기간 중 발생한 총 비정상 행위 중에서 정상적으로 비정상 행위를 탐지한 비율을 말하며, 거짓 경고율은 모의실험 기간 중 비정상 행위가 아닌 활동을 비정상 행위로 잘못 탐지한 비율을 말한다. 모의실험은 인텔 펜티엄 4 PC상에서 MS 비주얼 C++로 프로그램을 작성하였으며, 이때 모의실험에 사용한 파라미터는 다음의 표 2와 같다. 여기서 VANETs의 정상 차량 노드 활동 특징 값, 즉 LC, TR, RT, RY, AGE의 등급값의 증가는 모의실험 결과에 크게 영향을 미치지 않으므로 본 논문에서는 이들 등급값의 증가에 따른 변화를 고려하지 않는다.

표 2. 모의실험 파라미터
Table 2. Parameters for Simulation

Parameters	Value
Total # of Node Activities	200
Degree of LC	random(1, 3)
Degree of TR	random(1, 3)
Degree of RT	random(1, 3)
Degree of RY	random(1, 4)
Degree of AGE	random(1, 3)
Threshold ϵ	[0.2-0.6]

본 논문에서 제안한 비정상 행위 탐지 알고리즘의 허용 임계오차에 따른 비정상 행위 탐지율(detection rate)과 거짓 경고율(false alarm rate)에 대한 성능평가 결과는 다음의 그림 4와 같다.

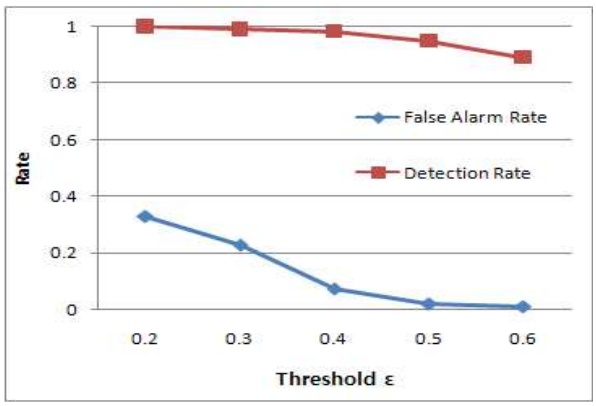

그림 4. 시뮬레이션 결과
Fig. 4. Simulation Result

그림 4에서 보는 바와 같이 본 논문에서 제안한 러프집합 기반 비정상 행위 탐지 알고리즘은 허용 임계 오차 ϵ이 작을수록 비정상 행위 탐지율은 높아지고 동시에 거짓 경고율도 상대적으로 높아지는 것을 알 수 있다. 이는 정상 행위에 대한 엄격한 행위 패턴을 적용함으로써 이들 정상 활동에 조금이라도 벗어나면 비정상 행위로 간주하여 경고를 전송하기 때문으로 생각되며, 이로 인해 실제 정상행위에 대해서도 경고가 발령되는 경우가 잦아져서 거짓 경고율이 높아지는 것으로 판단된다. 하지만 허용 임계오차 ϵ이 커질수록 비정상 행위 탐지율은 낮아지고 거짓 경고율도 역시 낮아지는 것을 알 수 있다. 이는 정상 활동에 대한 느슨한 행위 패턴을 적용함으로써 이들 정상 활동에 유사한 경우 정상 행위로 간주하여 비정상 행위에 대한 탐지가 낮아지고 반면에, 이로 인해 실제 정상행위에 대해서 경고가 발령되는 경우가 낮아지므로 거짓 경고율이 낮아지는 것으로 판단된다. 특히 허용 임계오차 ϵ이 0.4 부근에서 비정상행위 탐지율의 하락은 미미한 반면 거짓 경고율은 크게 낮아지는 것으로 나타났다. 따라서 이들 사이에서의 적당한 허용 임계오차 ϵ의 선택이 중요하다.

V. 결 론

차량 애드 혹 망은 이동성이 높은 차량 노드들로 구성되어 망을 이루는 특별한 모바일 애드 혹 망으로 고정된 인프라 구조가 없고 매우 짧은 시간 망 위상이 지속되므로 불안정한 통신 링크를 갖는다. VANETs은 대부분 개방 망으로 중앙 집중식 제어 없이 누구나 접속을 허용하기 때문에 망상에 해롭고 비정상 행위 노드들에 대한 침입이나 공격의 기회가 매우 높다. VANETs에서는 라우팅에 대한 공격이 가장 큰 문제이다. 그들의 위치에 대한 노드 위조나 부당 변경은 거짓된 지리적 지역에 대한 메시지를 발생할 수 있고, VANETs의 어떤 부분의 모든 트래픽을 블록하거나 가로챌 수 있으며 또는 망 분할을 초래할 수도 있다. VANETs에서의 주요 보안 문제는 거짓 경고 메시지의 유포, 실제 경고 메시지의 억제 또는 블로킹, 다른 메시지를 위한 시스템의 남용 등을 들 수 있다.

본 논문에서는 이렇게 보안이 취약한 VANETs에서의 차량 노드들의 활동에 대한 비정상 행위를 효율적으로 식별할 수 있는 러프집합 기반 비정상 행위 탐지방법을 제안한다. VANETs 상에서 정상상태의 차량 노드 활동패턴으로 노드의 정상 프로파일을 가지는 정상 특징 정보 시스템을 구축하고, 러프집합을 이용하여 어떤 노드의 활동 패턴에 대한 정상으로 부터의 이탈 정도를 계산한다. 그 이탈 정도가 허용 임계치보다 크면 경고 메시지를 생성하게 된다. 본 논문에서 제안한 비정상 행위 탐지 알고리즘의 성능은 모의실험을 통해 임계 허용오차에 대한 비정상 행위 탐지율과 거짓 경고율로 평가하였고, 그 결과 낮은 허용 임계오차 범위 내에서 높은 비정상 행위 탐지율과 거짓 경고율을 나타내는 것을 알았다. 반면에 높은 허용 임계 오차 범위 내에서는 거짓 경고율이 낮아지고 동시에 비정상 행위 탐지율도 낮아지는 것을 알았다. 그리고 허용 임계오차가 0.4 부근에서 비정상행위 탐지율은 높게 유지한 채 거짓 경고율이 급격히 낮아지는 것을 알았다. 향후 연구과제로는 VANETs에서의 보다 높은 신뢰도의 효율적인 정상 특징 정보 시스템의 구축과 VANETs의 정상 차량 노드 활동 특징 값에 따른 성능 평가 모델에 관한 것이다.

참고문헌

[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] C. Cai et al., "Constructing an Efficient Mobility Profile of Ad-Hoc for Mobility-Pattern-Based Anomaly Detection in MANET," *Proc. in the Global Telecommunications Conference*, pp. 1-5, 2006.

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

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

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

[10] 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.

[11] 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.

[12] 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

<주관심분야 : VANETs, MANETs, 무선 센서 망, P2P망, 스마트 폰 응용 등>