Journal of the Korean Data & Information Science Society
2011, **22**(6), 1153–1166

한국데이터정보과학회지

차량애드혹망을 위한 가변정밀도 러프집합 기반 부정행위 탐지 방법의 설계 및 평가

김칠화[1] · 배인한[2]

[12]대구가톨릭대학교 컴퓨터정보통신공학과

접수 2011년 10월 31일, 수정 2011년 11월 15일, 게재확정 2011년 11월 20일

요 약

차량 네트워크에서 부정행위를 탐지하는 것은 안전 관련 응용 및 혼잡 완화 응용을 포함하는 광범위한 영향을 갖는 매우 중요한 문제이다. 대부분 부정행위 탐지 방법들은 악의적인 노드들의 탐지와 관련이 있다. 대부분 상황들에서, 차량들은 운전자의 이기적인 이유 때문에 틀린 정보를 보낼 수 있다. 합리적인 행위 때문에 부정행위를 하는 노드를 식별하는 것보다 거짓 경보 정보를 탐지하는 것이 더 중요하다. 이 논문에서, 우리는 경보 메시지를 전송한 후, 부정행위를 한 노드들의 행위를 관찰하여 거짓 경보 메시지를 탐지하는 가변 정밀도 러프집합 기반 부정행위 탐지 방법을 제안한다. 차량 네트워크에서 이동하는 노드의 타당한 행위들로부터 경보 프로파일인 경보 정보 시스템이 먼저 구축되어진다. 어떤 이동하는 차량이 다른 차량으로부터 경보 메시지를 받으면, 수신차량은 그 메시지로부터 경보종류를 알아낸다. 경과시간 후, 수신차량이 경보 전송차량으로부터 비콘을 받으면, 수신차량은 경보 정보 시스템으로부터 가변 정밀도 러프집합을 사용하여 상대적 분류 오차를 계산한다. 만일 그 상대적 분류 오차가 그 경보종류의 최대 허용 가능한 분류 오차보다 크면, 수신 차량은 그 메시지를 거짓 경보 메시지로 결정한다. 제안하는 방법의 성능은 모의실험을 통하여 2가지 척도, 즉 정확률과 부정확률로 평가되어진다.

주요용어: 러프집합, 보안, 부정행위 탐지, 이기적인 행위, 차량 네트워크.

1. 서 론

차량애드혹망 (VANET: vehicular ad hoc network)은 차량들, 노변 장치들 (RSUs: road side units), 도로 안전을 보장하고 메시지와 데이터의 안전한 전송을 돕는 것이 목표인 인증 기관 (CAs: certification authorities)으로 구성되어 진다. 통신은 V2V (vehicle-to-vehicle)이거나 V2I (vehicle-to-infrastructure)일 수 있다. 어떤 차량에 의해 보내진 메시지는 사고 예방과 같은 중요한 결과를 가져올 수도 있기 때문에 VANETs에서 보안은 중요하다.

VANET은 차량 간의 연결이 매우 짧게 생존하는 일시적인 네트워크의 한 부류이다. 차량들이 서로 통신 범위를 들락거리는 만큼 망 위상이 아주 자주 변한다. 망의 밀도는 시간에 따라 역시 변한다. 그러한 특성들은 VANET에서 보안 문제 처리를 매우 어렵게 만들었다.

각 차량은 위치, 속도, 가속/감속, 경보 신호 등에 대한 메시지를 방송하는 차량용 단말기 (OBU: on board unit)을 가지고 있다. OBU는 입력되는 메시지가 유효한 엔티티에 의해 방송되어진 것인지를 검

[1] (712-702) 경북 경산시 하양읍 금락로 5, 대구가톨릭대학교 컴퓨터정보통신공학과, 박사과정.
[2] 교신저자: (712-702) 경북 경산시 하양읍 금락로 5, 대구가톨릭대학교 컴퓨터정보통신공학과, 교수.
E-mail: ihbae@cu.ac.kr

증하는 인증 기능도 역시 가지고 있다. RSUs는 차량 행위를 조정하는 것을 돕고, 근처 차량들과 그것들의 행위에 대한 정보를 수집한다. 결함이 있는 차량들은 몇몇 내부 고장에 기인하여 오작동을 발생시키거나 이기적인 이유로 의도적으로 거짓 경보, 거짓 위치나 속도를 알려줄 수 있다. 악의의 차량은 다른 사용자들에 대한 민감한 정보의 수집을 시도할 수도 있다 (Ruj 등, 2011).

본 논문에서, 차량들은 그것들의 목적지에 더 빨리 도착하기 위한 이기적인 이유로 주로 비행을 저지른다고 가정한다. 예를 들어, 차량은 혼잡, 사고 또는 도로 차단에 대한 거짓 보고를 전송할 수 있다. 따라서 우리는 어떤 차량으로부터 수신된 정확한 정보와 거짓 정보 간의 차이를 구별하는 것을 논의한다.

본 논문에서는 경보 메시지를 전송한 후, 그것들의 행위를 관찰하여 거짓 경보 메시지를 발송한 노드들을 탐지하는 가변 정밀도 러프집합 기반 부정행위 탐지 방법, VPRSMDS (Variable Precision Rough Set based Misbehavior Detection Scheme)를 제안한다. 그리고 성능을 모의실험을 통하여 평가한다.

본 논문의 구성은 다음과 같다. 2절에서는 VANETs의 기본 배경과 부분집합 연산자를 완화하여 러프 집합 이론 향상을 시도한 가변 정밀도 러프 집합과 VANETs에서의 부정행위 탐지에 대한 관련연구를 살펴본다. 3절에서는 부정행위 노드들과 부정확한 데이터를 탐지하고, 네트워크의 프라이버시를 지키기 위한 가변 정밀도 기반 부정행위 탐지 방법을 설계한다. 4절에서는 모의실험을 통하여 제안하는 VPRS 기반 부정행위 탐지 방법의 성능을 평가한다. 마지막으로 5절에서는 결론 및 향후 연구과제에 대하여 논의한다.

2. 관련연구

2.1. 차량애드혹망

텔레매틱스 (Telematics)는 'Telecommunication'과 'Informatics'의 합성어로 차량과 무선 통신망이 접속되어 운전자에게 교통정보안내, 긴급구조, 인터넷 서비스를 제공하여 편리함과 안전성을 증대시키는 서비스이다. 텔레매틱스는 차량과 IT 통신기술이 융합된 대표적인 기술로서 새로운 부가가치를 얻을 수 있을 뿐만 아니라 잠재 시장이 매우 큰 기술로 주목을 받고 있다. 또한 전 세계적으로 차량과 IT 기술이 융합되는 차량 통신 네트워크 기술과 차량 통신 기술을 활용한 텔레매틱스, ITS, 차량 안전 서비스 등이 활발하게 연구되고 있다.

VANET은 그림 2.1과 같이 차량을 중심으로 차량 내부 망과 외부 망으로 구분할 수 있는데, 차량 내부망은 일반적으로 IVN (in-vehicle communication network)라고 부르며, 차량 외부망은 차량 간 통신망 (V2V communication network), 차량과 인프라 통신망 (V2I communication network)으로 분류된다. IVN은 차량의 바디나 섀시 부분을 연결하고 제어하는 CAN, 차량의 오디오, 앰프, CDP 등 멀티미디어 기기 접속을 위한 MOST, 그리고 브레이크나 조향장치를 연결하고 제어하는 X-by-Wire (Flexray)가 있다 (이소연, 2008). V2V는 차량 간 통신을 기반으로 통신망을 구성하고 정보를 전달하는 인프라 도움 없이 구성될 수 있는 차량통신망을 형성하고, V2I는 차량과 유무선 통신 인프라 망이 접속되어 단말과 서버 간에 통신을 지원할 수 있는 통신망을 제공한다. V2V는 차량 간 통신을 기반으로 차량 추돌경보 서비스와 그룹통신을 제공하며, V2I는 차량에 IP 기반의 교통정보 및 안전 지원, 다운로드 서비스를 제공할 수가 있다 (Papadimitratos 등, 2006). 표 2.1은 IVN, V2V, V2I의 대표적인 서비스를 보여준다.

2.2. 가변정밀도 러프집합

가변정밀도 러프집합 (VPRS: variable precision rough sets)은 부분집합 연산자를 완화하여 러프 집

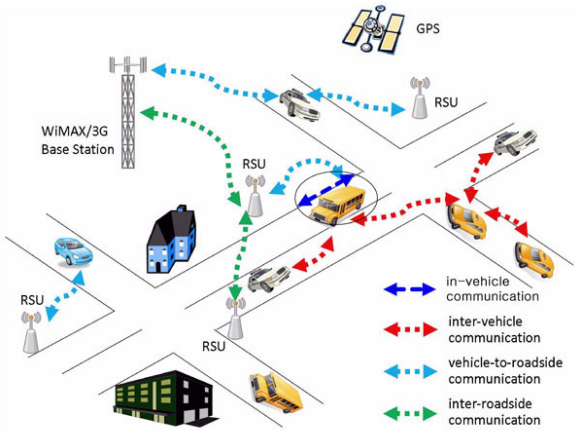


그림 2.1 VANET의 구조

표 2.1 차량 통신 서비스

분류	서비스
IVN	- 차량 멀티미디어 서비스 지원: MOST - 개인 편의 서비스 지원: CAN - 개인 안전 서비스 지원: Flexray
V2V	- 차량 추돌 경보 - 차량 간 그룹 통신
V2I	- 탐침 데이터 수집 - 교통 및 안전 정보 - 다운로드 (Map, POI) - IP 기반 패킷

합 이론 향상을 시도한다. 그것은 통계적 추세로 표현되는 데이터 패턴을 분석하고 식별하기 위하여 제안되었다. VPRS의 주된 아이디어는 객체들을 어떤 미리 정해진 수준보다 작은 오차로 분류하는 것을 허용하는 것이다 (Shen과 Jensen, 2007).

이 방법은 분류 프레임워크에서 이해하기 가장 쉽다. $X, Y \subseteq U$라 두면, 상대적 분류 오차는 식 (2.1)과 같이 정의되어진다.

$$c(X,Y) = 1 - \frac{|X \cap Y|}{|X|} \tag{2.1}$$

만일 $X \subseteq Y$이면 $c(X,Y) = 0$이다. 포함정도는 분류에서 어떤 수준의 오차 β를 허용하여 얻을 수 있다.

$$X \subseteq_\beta Y \ \textit{iff} \ c(X,Y) \leq \beta, 0 \leq \beta < 0.5$$

$\subseteq$대신에 $\subseteq_\beta$를 사용하여, 집합 X의 β-상한 근사와 β-하한근사는 다음과 같이 정의될 수 있다.

$$\underline{R_\beta} X = \cup \left\{ [x]_R \in U/R | \, [x]_R \subseteq_\beta X \right\}$$
$$\overline{R_\beta} X = \cup \left\{ [x]_R \in U/R | c([x]_R, X) < 1 - \beta \right\}$$

$\beta = 0$이면 $\underline{R_\beta}X = \overline{R_\beta}X$이다.

러프집합이론에서 긍정, 부정, 경계영역은 다음과 같이 확장될 수 있다.

$$POS_{R,\beta}(X) = \underline{R_\beta}X \tag{2.2}$$

$$NEG_{R,\beta}(X) = U - \overline{R_\beta}X \tag{2.3}$$

$$BND_{R,\beta}(X) = \overline{R_\beta}X - \underline{R_\beta}X \tag{2.4}$$

표 2.2 데이터 집합의 예

$x \in U$	a	b	c	d	==>	e
0	S	R	T	T		R
1	R	S	S	S		T
2	T	R	R	S		S
3	S	S	R	T		T
4	S	R	T	R		S
5	T	T	R	S		S
6	T	S	S	S		T
7	R	S	S	R		S

표 2.2의 데이터 집합에서 식 (2.2)는 $R = \{b, c\}, X = \{e\}$, $\beta = 0.4$에 대한 β-긍정영역을 계산하는데 사용될 수 있다. β를 0.4로 설정하는 것은 어떤 집합과 다른 집합의 부분집합이 원소개수의 거의 절반을 공유한다면 그 집합은 다른 집합의 부분집합인 것으로 간주된다는 것을 의미한다.

R과 X에 대한 전체의 객체 분할은 다음과 같다.

$$U/R = \{\{2\}, \{0, 4\}, \{3\}, \{1, 6, 7\}, \{5\}\}$$

$$U/X = \{\{0\}, \{1, 3, 6\}, \{2, 4, 5, 7\}\}$$

$A \in U/R$과 $B \in U/X$에 대해, 만일 동치류 A가 β-긍정영역에 포함된다면, $c(A, B)$의 값은 β보다 작아야 한다. $A = \{2\}$를 고려하면 다음과 같다.

$$c(\{2\}, \{0\}) = 1 > \beta$$

$$c(\{2\}, \{1, 3, 6\}) = 1 > \beta$$

$$c(\{2\}, \{2, 4, 5, 7\}) = 0 < \beta$$

따라서 객체 2는 그것이 $\{2, 4, 5, 7\}$의 β-부분집합인 것처럼 β-긍정영역에 추가된다.

$A = \{1, 6, 7\}$를 취하면, 더 흥미로운 경우가 발생된다.

$$c(\{1, 6, 7\}, \{0\}) = 1 > \beta$$

$$c(\{1, 6, 7\}, \{1, 3, 6\}) = 0.3333 < \beta$$

$$c(\{1, 6, 7\}, \{2, 4, 5, 7\}) = 0.6667 > \beta$$

여기에서 객체 1, 6과 7는 집합 $\{1, 6, 7\}$이 $\{1, 3, 6\}$의 β-부분 집합인 것처럼 β-긍정영역에 포함된다. 이런 방식으로 부분집합을 계산하는 것은 다음과 같은 β-긍정영역을 유도한다.

$$POS_{R,\beta}(X) = \{1, 2, 3, 5, 6, 7\}$$

이전에 생성된 긍정영역과 $\{2,3,5\}$를 비교한다. 부분집합 연산자의 완화에 기인하여 객체 1, 6, 7이 포함되어진다. 결정테이블 $(U, C \cup D)$를 고려한다. 여기서 C는 조건속성집합이고, D는 결정속성집합이다. U와 동치류인 Q의 β-긍정영역은 다음 식에 의해 결정된다.

$$POS_{R,\beta}(Q) = U_{X \in U/Q} \underline{R_\beta} X$$

여기서 R은 또한 U와 동치류이다. 이것은 종속성을 계산하고 β-감축을 결정하는데 사용될 수 있다. 종속함수는 다음과 같다.

$$\gamma_{R,\beta}(Q) = \frac{|POS_{R,\beta}(Q)|}{|U|}$$

2.3. 부정행위 탐지

본 논문의 초점은 VANETs의 응용 계층에서 부정행위 탐지를 이해하는 것이다. 침입 탐지는 무선 애드혹 망에서 널리 연구되고 있다. 그러나 기존 해결책들은 VANETs에서 악의적인 행위를 탐지하는데 적용할 수 없다.

안전한 V2V 통신 시스템의 경우에 부정행위를 탐지하고, 부정행위 노드를 축출하는 문제는 어려워진다. 이 문제는 다수의 다른 소스들이 같은 종류의 부정행위로 이어질 때 훨씬 더 복잡해진다. 예로서, 충돌된 차량이 PCN (Post-Crash Notification) 경보를 보내는 PCN 응용을 고려한다. PCN 경보는 충돌된 차량과 방향의 위치, 차량 상태를 포함한다 (The CAMP Vehicle Safety Communications Consortium, 2005). 악의 있는 차량은 어떤 파손이 없을지라도 틀린 위치 정보를 가진 틀린 PCN 경보를 발생시킬 수 있다. 또는, 충돌된 차량의 센서에 결함이 있어 부정확한 위치 정보를 전송할 수도 있다. 부정행위 탐지로 취해진 행동은 부정행위 근원의 잠재적 결과 강도에 따라 변할 수 있다.

VANETs에서 부정행위 탐지 문제에 대하여 Golle 등 (2009)은 네트워크 모델을 생성하였다. 네트워크 모델은 그 네트워크에서 모든 가능한 이벤트들의 집합이다. 다른 노드에 의해 관찰된 어떤 이벤트는 그 모델과 대조되어진다. 그 이벤트가 그 모델에 따라 유효하면, 그것은 정확한 메시지로 고려되고, 아니면 거짓이다. 이 방법이 갖는 주된 문제는 이 모델이 어떻게 생성되고 관리되는지에 대한 방법이 제시되지 않았다는 것이다. 다수의 노드들로 구성되는 VANETs에서, 광역 데이터베이스를 구축하는 것은 매우 비용이 많이 들고 실행 불가능할 수도 있다.

Zhou 등 (2007)과 Park 등 (2009)은 VANETs에서 노드들이 독립된 ID로 가장하고, 다수결에 의존하는 취소와 MDS의 결정에 영향을 미치는 Sybil 공격 (Douceur, 2002)에 저항하는 방법들을 제안하였다. 그 방법들은 노드들의 정확한 위치가 알려진다고 가정한다. 그러나 그러한 방법들은 노드들에 의해 발생한 거짓 경보를 탐지할 수 없다.

Ghosh 등 (2010)은 충돌 후 시나리오를 조사하였다. 만일 어떤 노드가 정확한 충돌 후 알림 (PCN) 경보를 전송하였는지를 결정하기 위하여 예상 궤도와 실제 궤도를 비교한다. 예상 궤도는 노드의 가능 행위를 사용하여 모델 되어 진다. 그러한 방법에는 2가지 단점이 있다. 첫째로, 어떤 악의의 노드는 항상 그것의 정확한 위치 정보를 전송한다고 가정한다. 그러한 노드들이 틀린 위치 정보를 보낼 수 있기 때문에 이것은 유효한 가정이 아니다. 둘째로, 실제 궤도는 이동 모델링에 의해 예측된 궤도와 합법적으로 다를 수 있다.

Raya 등 (2007)은 LEAVE 프로토콜을 사용한 지역 취소 방법을 제안하였다. 부정행위를 하는 노드는 일반적으로 투표에 의해 이웃으로부터 철회된다.

Moore 등 (2008)은 스팅이라 불리는 'suicide' 메커니즘을 사용하였고, 취소는 지역적으로 실행되어진다. 노드를 고발하는 노드는 고발한 노드와 함께 인접 노드에 의해 블랙리스트에 오른다. 이 희생 행

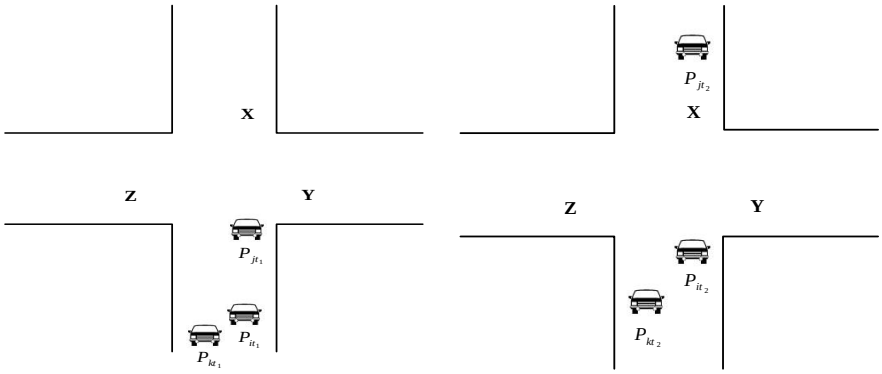
동은 첫 번째 노드가 정직하다는 것을 입증해야 한다. 이 메카니즘은 아래와 같은 방법으로 공격되어질 수 있다. 부정행위를 하는 노드에 둘러싸여 있는 정직한 노드가 있는 상황을 고려한다. 정직한 노드가 고발 신호를 발생시켜 철회되면, 다른 부정행위를 하는 노드를 고발할 수 없다. 또한, 부정행위를 하는 노드 중 하나가 정직한 노드를 고발하여 철회되면, 다른 악의의 노드는 여전히 네트워크에 남아 있다. 부정행위를 하는 노드는 또 다른 부정행위를 하는 노드를 고발하고 다른 노드에 의해 정직한 것으로 간주될 수도 있다.

두 가지 게임 이론 기반 취소 설계가 제안되었다 (Raya 등, 2008; Bilogrevic 등, 2010). 그리고 배인한 (2010)은 모바일 애드 혹 망에서 모바일 장치의 위성항법장치로부터 이동특징 정보를 계산하여 정상 프로파일을 구축하고, 모바일 장치의 현재 이동 특징 정보와 정상 프로파일내의 이동 특징 정보간의 퍼지 비유사도를 기초로 그 모바일 장치의 비정상 행위를 탐지하는 퍼지 비정상 행위 탐지 알고리즘을 제안하였다.

3. 가변정밀도 러프집합 기반 부정행위 탐지 방법

부정행위 차량의 탐지는 참여하는 엔티티로 부터 피드백을 요구한다. 참여하는 차량은 차량이 CA에 연결된 RSE에 접촉할 때 부정행위를 탐지하기 위한 다소의 부정행위 탐지 방법 (MDS: misbehavior detection scheme)을 실행하고, CA에 보고되어진다. CA는 인증서를 취소하고 대응하는 CRL (certification revocation list)에 추가하기 전에 어떤 인증서에 대하여 부정행위 보고의 횟수를 누적시킨다. CRL를 요청한 어떤 차량은 최신 정보를 받고, 새롭게 탐지되는 부정행위를 한 차량들의 축출을 가져온다. 어떠한 차량 요청은 최근에 탐색되는 부정행위 차량의 축출로 이어지면서, 최종 보안 성능은 탐지 지연, 기록 지연과 축출 지연에 의존한다. 부정행위 보고와 축출은 부정행위를 한 노드들에 대한 정보를 주고받을 것을 그 차량들에게 요구한다. 이것은 중앙 엔티티로 부터 V2V 시스템의 참여자에 이르기까지 통신을 가능하게 하는 인프라구조 지원 또는 기술을 분명히 요구한다. 그러므로 보고와 축출 지연은 예측 불가능할 수 있다. 본 연구에서, 우리는 부정행위 탐지 방법의 설계에만 집중한다.

이 논문에서, 우리는 부정행위 노드들과 부정확한 데이터를 탐지하고, 네트워크의 프라이버시를 지키기 위한 가변정밀도 기반 부정행위 탐지 방법, VPRSMDS를 제안한다. 차량들은 주기적으로 비콘 메시지를 전송하므로 이웃 차량들의 위치는 시간에 따라 감시되어진다. 만일 보고되어진 위치가 경보 발생된 위치와 일치하지 않으면 수신 노드는 그 메시지를 부정확한 것으로 선언하고 그것을 취소한다.



(a)노드 n_j가 경보 '위치 X에서 도로 차단' 전송 (b) 노드 n_j가 최근에 위치 X 지남

그림 3.1 메시지 비일관성이 부정행위를 증명하는 예

그림 3.1의 상황에서, 시점 t_1에 노드 n_j가 '위치 X에서 도로 차단' 경보를 전송하고, 시점 t_1과 가까운 시점 t_2에 그것의 위치가 최근에 X를 지나갔다면, 이것은 위치 X에 도로 차단이 없었거나 n_j의 위치 정보가 틀린 것을 암시한다.

차량 네트워크는 $|N|$=N의 노드들의 집합 N, RSUs의 집합 R, CAs의 집합 C로 구성된다. 차량들은 n_i로, RSUs는 R_i로, CAs는 C_i로, 그리고 MA (master authority)는 M_i로 각각 나타낸다.

대부분 바람직하지 않은 행위는 이기적인 동기에 기인하여 발생됨으로, '좋은' 노드와 '나쁜' 노드의 분류는 정확한 정보와 거짓 정보 간의 구별만큼 중요하지 않다. 우리는 그 노드가 '좋다' 또는 '나쁘다' 보다는 어떤 노드에 의해 생성된 메시지 또는 경보 신호가 정확한 것인지 틀린 것인지를 알아내는 것에 더 신경 쓸 것이다.

어떤 노드는 도로 상에서 차량의 안전을 보장하기 위하여 다음과 같은 경보 메시지들을 전송할 수 있다.

- 긴급 전자 제동장치등 (EEBL: Emergency Electronic Brake Light): 어떤 차량이 갑자기 감속하면 EEBL 경보를 발생시키고, 뒤 차량들은 후미 충돌을 예방할 수 있다.
- 충돌 후 알림 (PCN): 이미 발생되어진 사고를 다른 차량들에게 경보하는 차량에 의해 전송된다.
- 도로 위험 상태 알림 (RHCN: Road Hazard Control Notification): 도로 상의 미끄러운 구간, 빙판길 또는 위험한 잔해와 같은 도로 상태를 보고한다.
- 도로 특징 알림 (RFN: Road Feature Notification): 학교 근처 속도 제한 또는 급커브 또는 급경사 경보를 발생시킨다.
- 도로 차단 알림 (RBN: Road Break Notification): 공사 또는 자연재해 등으로 도로가 차단되어 차량 진행이 불가능하면, 도로 차단 정보를 전송한다.
- 혼잡 도로 알림 (CRN: Congested Road Notification): 진행 중인 도로에 교통 혼잡으로 정체가 발생하면 혼잡 도로 정보를 전송한다.
- 정지/저속 차량 알림 (SVN: Stopped/Slow Vehicle Notification): 도로에 고장으로 차량이 정차해 있거나 천천히 이동하는 차량이 있으면 경보를 발생시킨다.
- 협동 충돌 경보 (CCW: Cooperate Collision Warning): 피할 수 있는 가능 충돌에 대한 정보를 전송한다.
- 긴급 차량 접근 (EVA: Emergency Vehicle approaching): 뒤에서 접근하는 다른 차량들을 위하여 노드에 의해 전송되어진다.

노드 n_i는 시점 t에 5개의 속성 값을 갖는 $M_A \in M$으로 표현되는 경보 메시지를 전송한다.

$$M_A = (p_{it}, T, L_i, t, v_{it}, l_{it})$$

여기서 p_{it}는 노드 n_i의 가명, T는 경보 종류이고, L_i는 경보가 발생한 이벤트 E_i의 위치이고, t는 경보 메시지가 전송된 시간이고, v_{it}는 시점 t에 노드 n_i의 속도이고, 그리고 l_{it}는 시점 t에 경보를 발생시킨 노드 n_i의 위치이다.

어떤 노드 n_j가 어떤 노드 n_i로부터 경보 메시지를 받으면, 그 경보 메시지로부터 경보 종류를 알아낸다. 여기서 그 경보 종류는 부정행위 탐지를 위한 정보 시스템에서 결정속성이 된다.

노드 n_j는 경과 시간 Δt후에 노드 n_i로부터 다음과 같은 비론을 받는다.

$$(B_i = p_{it}, t, v_{it}, l_{it})$$

노드 n_j는 노드 n_i로부터 받은 경보 메시지가 정확한 경보 메시지인지 틀린 경보 메시지인지를 검사하기 위하여, 이전에 받은 경보 메시지와 비콘 메시지의 전송 시간, 속도 그리고 위치 정보를 이용하여 이동거리, 감속도, 동일차선, 동일진로를 각각 계산한다. 여기서 노드 n_j가 경보를 발생한 시점과 비콘을 받은 시점의 차선과 진로가 같으면 동일차선과 동일진로 속성 값은 'Y (yes)'이고 아니면 'N (no)'다. 그리고 계산된 이동거리와 감속도 값들은 각 속성의 소속함수에 의하여 퍼지집합으로 사상되어진다.

Δt동안의 차량은 가까운 거리를 이동하기 때문에 차량의 이동거리, $D = dist(l_{jt_1}, l_{jt_2})$는 GPS의 위치데이터로부터 피타고라스의 정리를 사용하여 계산되어진다. 그리고 Δt 동안의 차량 이동거리는 그림 3.2의 소속함수를 사용하여 5개의 기본 퍼지집합인 VL (Very Long), L (Long), M (Medium), S (Short), VS (Very Short)로 사상되어진다.

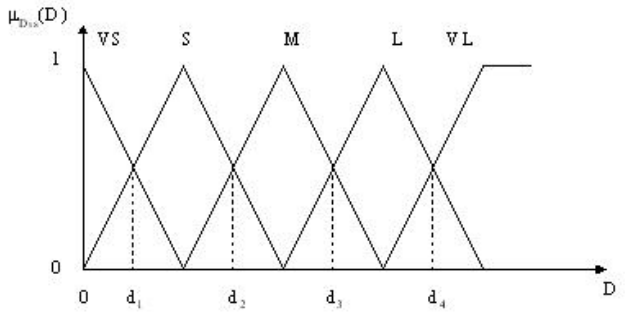


그림 3.2 차량의 이동거리에 대한 소속함수

전방 차량이 현재 가속도를 유지할 때의 충돌 회피 감속도인 ODCA (Overt Deceleration for Collision Avoidance)는 기호 α로 표현되어진다.

$$\alpha = -\frac{v_{r_0}^2 + 2a_{p_0}x_{r_0}}{2x_{r_0} + 2v_{r_0}T - a_{p_0}T^2} \ (a_{p_0} \geq 0, v_{p_0} < v_{f_0}) \tag{3.1}$$

식 (3.1)에서 $v_{p_0}, a_{p_0}, v_{f_0}$는 현재시점에서의 전방 차량의 속도와 가속도, 그리고 뒤 차량의 속도를 각각 나타낸다. x_{r_0}는 현재시점에서의 상대위치를 나타낸다. 충돌 회피를 위한 감속 기반 충돌 위험 평가 지수 연구 (Hiraoka 등, 2009)에서, 0.8[s]에서 1.4[s]까지의 운전자의 반응시간 설정에 대한 경보준비 조건 $\alpha \geq 4.0[m/s^2]$임을 보였다. 따라서 Δt 동안의 감속도 값을 단위시간 1초 동안의 감속도 값으로 변환한 다음, 그림 3.3의 소속함수를 사용하여 6개의 기본 퍼지집합인 N (None), VW (Very Weak), W (Weak), M (Medium), S (Strong), VS (Very Strong)으로 사상되어진다. 사상된 속성 값들은 부정행위 탐지를 위한 정보 시스템의 조건속성이 된다.

VANETs에서 운전자와 차량의 안전에 큰 영향을 미치는 사건의 경보 메시지에 대한 부정행위 탐지를 위한 정보 시스템의 구조는 표 3.1과 같다. 여기서 조건속성인 Dis, Dec, Slane 그리고 Srout는 노드의 이동거리, 감속도, 동일차선, 동일진로를 각각 나타내고, 결정속성인 Type는 경보 메시지 종류를 나타낸다. 그리고 Error는 해당 규칙에서 최대 허용 가능한 상대적 분류 오차 값으로 (1-확신도)로 계산되어진다.

정보 시스템을 구성하는 규칙들은 약간의 오차를 허용할 뿐만 아니라 센서로부터 획득한 데이터에는 차량 전자장치의 고장과 무선통신망의 특성에 기인하여 약간의 오차를 포함할 수 있다. 따라서 본 논문에서는 정보 시스템의 조건속성으로부터 VPRS 기반 근사 경보 메시지를 식별하여 부정행위를 탐지한

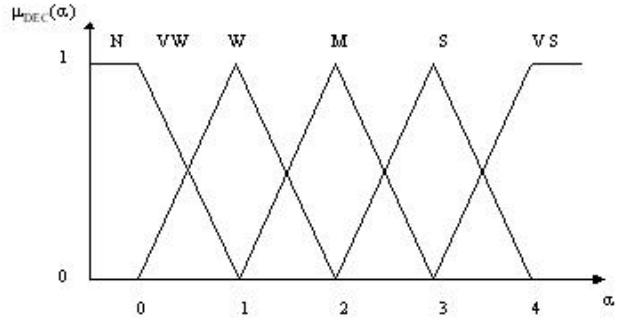


그림 3.3 차량의 감속도에 대한 소속함수

표 3.1 부정행위 탐지를 위한 정보 시스템

U	Dis	Dec	Slane	Srout	Type	Error
x_1	M	W	-	Y	PCN	0.3
x_2	S	W	-	Y	RHCN	0.2
x_3	M	M	-	N	RBN	0.3
x_4	VS	M	Y	Y	CRN	0.2
x_5	S	W	N	Y	CRN	0.2
x_6	M	N	-	N	CRN	0.2
x_7	S	M	-	Y	SVN	0.2
x_8	M	W	-	Y	SVN	0.2
x_9	S	S	Y	Y	CCW	0.1

다. 결정속성인 경보 종류의 상대적 분류 오차는 식 (3.2)와 같이 계산되어진다.

$$c(X,Y) = \min_{Y \in T_d} \left(1 - \frac{\sum_{k=1}^{l} w(x_k, y_k)}{l}\right) \tag{3.2}$$

여기서 X는 경보 메시지의 결정속성인 경보 종류 T_d를 발송한 노드의 현재 조건속성들이고, Y는 정보 시스템의 경보 종류 T_d에 대한 정상 조건속성들을 나타낸다. 그리고 l은 조건속성의 길이를 나타내고, $w(x_k, y_k)$는 현재 조건속성의 k-번째 원소와 정상 조건속성의 k-번째 원소 간의 유사도 가중치를 나타낸다.표 3.1에서 조건속성 P={Dis, Dec, Slane, Srout}에 따른 동치류는 다음과 같다.

$$U/Dis = \{\{x_1, x_3, x_6, x_8\}, \{x_2, x_5, x_7, x_9\}, \{x_4\}\}$$
$$U/Dec = \{\{x_1, x_2, x_5, x_8\}, \{x_3, x_4, x_7\}, \{x_6\}, \{x_9\}\}$$
$$U/Slane = \{\{x_1, x_2, x_3, x_6, x_7, x_8\}, \{x_4, x_9\}, \{x_5\}\}$$
$$U/Srout = \{\{x_1, x_2, x_4, x_5, x_7, x_8, x_9\}, \{x_3, x_6\}\}$$

P에서의 식별불가능 관계 (indiscernibility relation)는 다음과 같다.

$$IND(P) = \{\{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_5\}, \{x_6\}, \{x_7\}, \{x_8\}\}$$

예를 들어, 어떤 노드가 다른 노드로부터 CRN 경보 메시지를 수신하였다면 CRN 경보가 결정속성이 되고, 경과시간 Δt후에 그 경보 수신 노드는 경보 메시지를 전송한 노드로부터 비콘 메시지를 받는

다. 그러면 이전에 받은 경보 메시지와 비콘 메시지의 전송 시간, 속도 그리고 위치 정보를 이용하여 조건속성인 이동거리, 감속도, 동일차선, 동일진로를 각각 계산한다. 계산된 조건속성이 CA=(S, N, -, N)이면, 결정속성인 Type이 CRN인 부분집합 $Q = \{x_4, x_5, x_6\}$이다. 그러므로 긍정영역 $POS_P(Q) = \{x_4, x_5, x_6\}$이다. CA은 부정행위 탐지를 위한 정보 시스템의 긍정영역 $POS_P(Q) = \{x_4, x_5, x_6\}$에 존재하지 않는다. 따라서 $\forall x \in POS_P(Q)$에 대해 표 3.1에서 CRN 경보 메시지의 최대 허용 가능한 상대적 분류 오차가 0.2이므로 β=0.2인 β-긍정영역을 계산한다.

$$c(CA, x_4) = 1 - (1.0/4) = 0.75,$$
$$c(CA, x_5) = 1 - (1.8/4) = 0.55,$$
$$c(CA, x_6) = 1 - (2.8/3) \approx 0.667.$$

여기서 유사도 가중치는 언어 변수 값이 1 단계 다르면 0.8, 2 단계 다르면 0.5, 3 단계 다르면 0.2 그리고 4 단계 이상 다르면 0.0을 적용하였다. 따라서 계산된 조건속성 $POS_{P,\beta}(Q) = \{x_6\}$이므로, 수신된 CRN 경보 메시지는 정확한 경보 메시지로 식별되어진다.

다른 예로, 어떤 노드가 다른 노드로부터 SVN 경보 메시지를 수신하였다면 SVN 경보가 결정속성이 되고, 경과시간 Δt 후에 그 경보 수신 노드는 경보 메시지를 전송한 노드로부터 비콘 메시지를 받는다. 그러면 이전에 받은 경보 메시지와 비콘 메시지의 전송 시간, 속도 그리고 위치 정보를 이용하여 조건속성인 이동거리, 감속도, 동일차선, 동일진로를 각각 계산한다. 계산된 조건속성은 CA=(M, VW, -, N)이면, 결정속성인 Type이 SVN인 부분집합 $Q = \{x_7, x_8\}$이다. 그러므로 긍정영역 $POS_P(Q) = \{x_7, x_8\}$이다. CA은 부정행위 탐지를 위한 정보 시스템의 긍정영역 $POS_P(Q) = \{x_7, x_8\}$에 존재하지 않는다. 따라서 $\forall x \in POS_P(Q)$에 대해 표 3.1에서 SVN 경보 메시지의 최대 허용 가능한 상대적 분류 오차가 0.2이므로 β=0.2인 β-긍정영역을 상기 예와 동일한 유사도 가중치를 적용하여 계산한다.

$$c(CA, x_7) = 1 - (1.3/3) \approx 0.567,$$
$$c(CA, x_8) = 1 - (1.8/3) = 0.4.$$

따라서 계산된 조건속성 $POS_{P,\beta}(Q) = \phi$이므로, 수신된 SVN 경보 메시지는 거짓 경보 메시지로 식별되고, CRL에 추가되어진다.

4. 성능 평가

본 논문에서 제안하는 VPRSMDS의 성능을 평가하기 위하여 다음 변수들을 정의한다.

- MB: 부정행위 (Mis-Behavior) 발생 횟수
- RB: 정상행위(Rational Behavior) 발생 횟수
- RR: 정상행위를 정상행위로 예측한 횟수
- MM: 부정행위를 부정행위로 예측한 횟수
- RM: 정상행위를 부정행위로 예측한 횟수

상기 변수를 사용하여 2가지 성능 척도인 정확률과 부정확률을 사용한다.

- 정확률 (correct rate): 부정행위로 측정된다. MB개의 부정행위에 대하여 MM개가 부정행위인 것으로 탐지되면, 정확률은 MM/MB으로 정의된다.

$$correct\ rate = \frac{MM}{MB}$$

- 부정확률 (incorrect rate): 정상행위로 측정된다. RB개의 정상행위에 대하여 RM개가 부정행위인 것으로 식별되면, 부정확률은 RM/RB으로 정의된다.

$$incorrect\ rate = \frac{RM}{RB}$$

모의실험 프로그램은 인텔 코어 2 쿼드 Q9400에서 MATLAB 7.0 (Kay, 2009)을 사용하여 개발되었다. 모의실험에서 결정속성인 경보종류에 따르는 조건속성이 다음과 같은 경우 그 경보 메시지는 정확한 경보 메시지로 식별된다고 가정한다.

- 계산된 조건속성이 정보시스템의 조건속성과 일치하는 경우
- 계산된 조건속성이 정보시스템의 조건속성에서 이동차선과 이동진로가 같으면서 이동거리의 언어 변수 값과 감속도의 언어 변수 값 중 하나가 1 단계 다르거나 각각 1 단계 다른 경우

상기의 조건속성을 제외한 모든 조건속성에서 발생한 경보 메시지는 거짓 경보 메시지라 가정한다.

표 4.1은 모의실험에서 사용된 매개 변수와 값을 보여준다.

표 4.1 모의실험 매개변수와 값

매개변수	값
경보 메시지 발생 횟수	4000
경보 종류의 개수	6
경보 당 조건속성의 개수	3∼4
언어 변수 값의 단계별 유사도 가중치	1.0, 0.8, 0.5, 0.3, 0.0

그림 4.1과 그림 4.2는 4000번의 경보 메시지를 확률적으로 발생시킨 후, 실제 발생한 정상행위 횟수 (RB, Baseline)와 VPRSMDS가 예측한 정상행위의 횟수 (RR, VPRSMDS), 실제 발생한 부정행위 횟수 (MB, Baseline)와 VPRSMDS가 예측한 부정행위의 횟수 (MM, VPRSMDS)를 경보 메시지의 종류별로 각각 보여준다.

모의실험 결과, 제안하는 VPRSMDS는 경보 메시지의 종류에 대해 거의 비슷한 성능을 갖는다는 것을 알 수 있었다. 그러나 조건속성이 4개인 경보종류 CRN과 CCW에서 상대적으로 조금 좋은 행위 식별 성능을 보였고, 반면에 경보종류 PCN과 RHCN에서 상대적으로 조금 낮은 행위 식별 성능을 보였다.

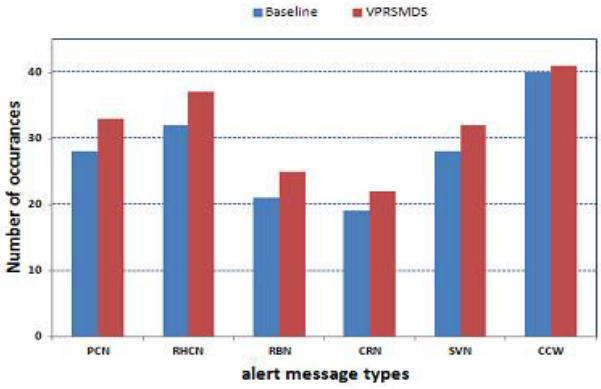


그림 4.1 경보종류별 정상행위의 발생횟수 대 예측횟수

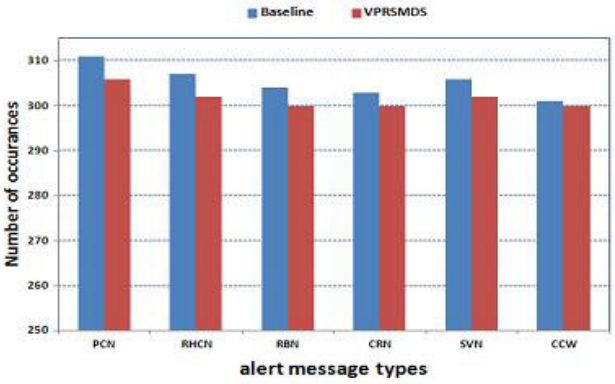


그림 4.2 경보종류별 부정행위의 발생횟수 대 예측횟수

그림 4.3은 경보 메시지 발생회수에 따른 정확률과 부정확률을 각각 보여준다. 여기서 사례 A는 조건속성이 3개인 경보종류와 4개인 경보종류의 최대 허용 가능한 상대적 분류 오차를 각각 0.15와 0.1로 설정한 경우이고, 그리고 사례 B는 조건속성이 3개인 경보종류와 4개인 경보종류의 최대 허용 가능한 상대적 분류 오차를 각각 0.2와 0.1로 설정한 경우이다. 전체적으로 사례 A의 성능이 사례 B의 성능보다 약간 우수함을 알 수 있었다. 특히 경보 발생 횟수가 500번일 때, 사례 B의 정확률이 0.965로 가장 높았고, 그리고 경보 발생 횟수가 300∼500번일 때, 사례 A와 B의 부정확률이 0.076로 가장 낮음을 알 수 있었다.

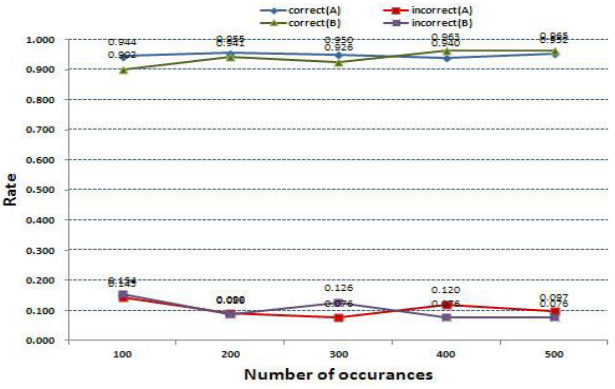


그림 4.3 경보메시지 발생횟수에 따른 정확률과 부정확률

5. 결 론

결함이 있는 차량들은 몇몇 내부 고장에 기인하여 오작동을 발생시키거나 이기적인 이유로 의도적으로 거짓 경보, 거짓 위치나 속도를 알려줄 수 있다. 악의의 차량은 다른 사용자들에 대한 민감한 정보의 수집을 시도할 수도 있다. 따라서 차량 네트워크는 거짓 경보를 방지하거나 약화시키기 위하여 위조된

데이터의 인젝션 (Injection)에 대해 안전해야 한다. 부정행위는 전체 시스템, 즉 안전 응용과 그것들의 결과로 초래된 결정을 방해할 것이다.

본 논문에서는 경보 메시지를 전송한 후, 부정행위를 한 노드들의 행위를 관찰하여 거짓 경보 메시지를 탐지하는 VPRSMDS를 제안하였다. 어떤 노드가 발송한 경보 메시지의 상대적 분류 오차가 그 경보종류의 최대 허용 가능한 분류 오차 보다 작으면, 정확한 경보 신호로 결정하고, 아니면, 수신 차량은 그 메시지를 거짓 경보 메시지로 식별한다. 본 논문에서 VPRSMDS의 성능을 모의실험으로 평가하였다. 그 결과, VPRS는 경보종류에 상관없이 차량의 정상행위와 부정행위에 대하여 높고 고른 식별 성능을 보였다. 그리고 경보 발생 횟수에 상관없이 높은 정확률과 낮은 부정확률을 제공함을 알 수 있었다.

모의실험 결과로부터 경보종류에 대한 조건속성이 많을수록 좋은 성능을 제공함을 알 수 있었다. 따라서 향후 연구과제는 더 많은 경보종류와 각 경보종류에 대하여 많은 조건속성을 개발하고 추가하여 제안하는 VPRSMDS를 확장하는 것, 모의실험을 통하여 기존의 다른 부정행위 탐지 방법들과 성능을 평가하고 비교하는 것, 그리고 필드 테스트를 통하여 제안하는 VPRSMDS의 성능을 평가하는 것 등을 포함한다.

참고문헌

배인한 (2010). 모바일 애드-혹 망을 위한 퍼지 비정상 행위 탐지 알고리즘. <한국데이터정보과학회지>, **21**, 1125-1136.

이소연 (2008). 차내망 인터페이스. <TTA 저널>, **117**, 114-117.

오현서, 박종현 (2008). 차량 통신 네트워크 기술 동향. <전자통신동향분석>, **23**, 49-55.

Bilogrevic, I., Manshaei, M., Raya, M. and Hubaux, J. P. (2010). Optimal revocations in ephemeral networks: A gametheoretic framework. *Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks,* 184-193.

Douceur, J. R. (2002). The sybil attack. *Proceeding of the First International Workshop on Peer-to-Peer Systems,* 251-260.

Ghosh M., Varghese, A., Gupta, A., Kherani A. A. and Muthaiah, S. N. (2010). Detecting misbehaviors in vanet with integrated root-cause analysis. *Journal of Ad Hoc Networks*, **8**, 778-790.

Golle, P., Greene, D. and Staddon J. (2009). Detecting and correcting malicious data in vanets. *Proceedings of Vehicular Ad Hoc Networks*, 29-37.

Hiraoka, T., Tanaka, M., Takeuchi, S., Kumamoto, H., Isumi, T. and Hatanaka, K. (2009). Collision risk evaluation index based on deceleration for collision avoidance (second report). *Review of Automotive Engineering,* **30**, 439-447.

Moore, T., Raya, M., Clulow, J., Papadimitratos, P., Andeson, R. and Hubaux, J. P. (2008). Fast exclusion of errant devices from vehicular networks. *Proceeding of Sensor, Mesh and Ad Hoc Communications and Networks,* **21**, 135-143.

Papadimitratos, P., Gligor, V. and Hubaux, J. P. (2006). Securing vehicluar communications - assumptions, requirements and principles. *Proceeding of the workshop on Embedded Security in Cars*, 5-14.

Park, S., Aslam, B., Turgut, D. and Zou, C. C. (2009). Defence against sybil attack in vehicular ad hoc network based on roadside unit support. *Proceedings of Military Communications Conference*, 1-7.

Raya, M., Manshaei, M. H., Felegyhazi, M. and Hubaux, J. P. (2008). Revocation games in ephemeral networks. *Procedings of ACM Computer and Communications Security*, 199-210.

Raya, M., Papadimitratos, P., Aad, I., Jungels, D. and Hubaux, J. P. (2007). Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, **25**, 1557-1568.

Ruj, S., Cavenaghi, M. A., Huang, Z., Nayak, A., and Stojmenovic, I. (2011). On data-centric misbehavior detection in vanets. *Proceeding of Vehicular Technology Conference*.

Shen, Q. and Jensen, R (2007). Rough sets, their extensions and applications. *International Journal of Automation and Computing,* **4**, 217-228.

The CAMP Vehicle Safety Communications Consortium. (2005) *Vehicle safety communications project, task 3 final report.*

Zhou, T., Choudhury, R. R., Ning, P. and Chakrabarty, K. (2007). Privacy-preserving detection of sybil attacks in vehicular ad hoc networks. *Proceeding of Mobile and Ubiquitous Systems: Networking & Services*, 1-8.

Journal of the Korean Data & Information Science Society
2011, **22**(6), 1153–1166

한국데이터정보과학회지

Design and evaluation of a VPRS-based misbehavior detection scheme for VANETs

Chil-Hwa Kim[1] · Ihn-Han Bae[2]

[12]Department of Computer and Information Communication, Catholic University of Daegu

Received 31 October 2011, revised 15 November 2011, accepted 20 November 2011

Abstract

Detecting misbehavior in vehicular ad-hoc networks is very important problem with wide range of implications including safety related and congestion avoidance applications. Most misbehavior detection schemes are concerned with detection of malicious nodes. In most situations, vehicles would send wrong information because of selfish reasons of their owners. Because of rational behavior, it is more important to detect false information than to identify misbehaving nodes. In this paper, we propose the variable precision rough sets based misbehavior detection scheme which detects false alert message and misbehaving nodes by observing their action after sending out the alert messages. In the proposed scheme, the alert information system, alert profile is constructed from valid actions of moving nodes in vehicular ad-hoc networks. Once a moving vehicle receives an alert message from another vehicle, it finds out the alert type from the alert message. When the vehicle later receives a beacon from alert raised vehicle after an elapse of time, then it computes the relative classification error by using variable precision rough sets from the alert information system. If the relative classification error is lager than the maximum allowable relative classification error of the alert type, the vehicle decides the message as false alert message. Th performance of the proposed scheme is evaluated as two metrics: correct ratio and incorrect ratio through a simulation.

Keywords: Misbehavior detection, rough sets, security, selfish behavior, VANET.

[1] Graduate student, Department of Computer and Information Communication, Cathloic University of Daegu, Gyeongbuk 712-702, Korea.
[2] Corresponding author: Professor, School of Computer and Information Communication, Catholic University of Daegu, Gyeongbuk 712-702, Korea. E-mail: ihbae@cu.ac.kr