The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 6, pp.175-181, Dec. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.6.175
JIIBC 2014-6-26

VANETs에서 비정상 행위 탐지를 위한 빅 데이터 응용

A Big Data Application for Anomaly Detection in VANETs

김식*, 오선진**

Sik Kim*, Sun-Jin Oh**

요 약 무선 기반의 모바일 컴퓨팅 네트워크 기술의 급속한 발전과 더불어, 다양한 관련 기술과의 융합을 통한 획기적인 모바일 애드 혹 네트워크 응용들이 빠르게 확산되고 있는 실정이다. 차량 애드 혹 망 (Vehicular Ad Hoc Networks: VANETs)은 일반적으로 높은 이동성을 갖는 차량 노드들로 구성되어 망 위상이 짧은 시간 유지되고 통신 링크가 불안정한 자기 조직화 모바일 애드 혹 망이다. 따라서 VANETs은 네트워크상에 센서들의 해로운 노이즈나 차량 노드들의 비정상 행위에 매우 취약하다. 본 논문에서는 이러한 VANETs에서 센싱된 센서로 부터의 상황정보에 대한 해로운 오동작이나 노이즈와 차량 노드들의 활동에 대한 비정상 행위를 효율적으로 식별할 수 있는 빅 데이터 처리 기술을 응용한 비정상 행위 탐지 방법을 제안하고, 그 성능을 모의실험을 통해 임계 허용 오차에 대한 비정상 행위 탐지율과 거짓 경고율로 평가하였다.

Abstract With rapid growth of the wireless mobile computing network technologies, various mobile ad hoc network applications converged with other related technologies are rapidly disseminated nowadays. Vehicular Ad Hoc Networks are self-organizing mobile ad hoc networks that typically have moving vehicle nodes with high speeds and maintaining its topology very short with unstable communication links. Therefore, VANETs are very vulnerable for the malicious noise of sensors and anomalies of the nodes in the network system. In this paper, we propose an anomaly detection method by using big data techniques that efficiently identify malicious behaviors or noises of sensors and anomalies of vehicle node activities in these VANETs, and the performance of the proposed scheme is evaluated by a simulation study in terms of anomaly detection rate and false alarm rate for the threshold ϵ.

Key Words : VANETs, Anomaly Detection, Big Data

Ⅰ. 서 론

지능 교통 시스템 (Intelligent Transportation System : ITS)의 많은 흥미롭고 바람직한 응용들이 새로운 유형의 애드 혹 망인 차량 애드 혹 네트워크 (Vehicular Ad Hoc Networks: VANETs)의 개발과 발전을 촉발시켰다. 차량 애드 혹 네트워크에서는 주행 중인 차량들 간 통신 (Vehicle-to-Vehicle Communication: V2V)으로 서로 메시지를 교환하고, 또한 자동차 도로변 망 인프라 구조 (Vehicle-to-Roadside Communication: V2R)를 통해 메시지를 교환할 수 있는 통신 장비를 장착하고 있다.[1]. 차량 애드 혹 망은 특별한 특징을 가진 애드 혹 망이다. VANETs은 일반적으로 매우 이동성이 높은 망 노드들을 가지며 노드들 사이의 상대 속도가 고속으로 이동하

*정회원, 세명대학교 정보통신학부
**종신회원, 세명대학교 정보통신학부(교신저자)
접수일자 : 2014년 9월 20일, 수정완료 : 2014년 10월 30일
게재확정일자 : 2014년 12월 12일

Received: 20 September, 2014 / Revised: 30 October, 2014 / Accepted: 12 December, 2014
**Corresponding Author: sjoh@semyung.ac.kr
Dept. of Computer & Information Science, Semyung University, Korea

여 매우 짧은 시간 지속되며 불안정한 통신 링크를 갖는다. 주로 무선 통신을 사용하면서 노드들 사이의 링크는 매우 불안정하여 노드들은 지속적으로 통신 범위를 벗어나 다른 노드의 통신 범위에 도달한다. VANETs은 고정된 자동차 도로변의 게이트웨이와 연결할 수 있는 메커니즘을 가질 수 있고 인터넷과 같은 공통 망을 이들 게이트웨이를 통해 접근할 수 있다.[2]

모바일 애드 혹 망의 주요 장점 중의 하나는 그들의 고정된 인프라 구조, 중앙 통제 관련 라우팅 장비로부터의 완전 독립이다. 그러나 보안 측면에서는 이러한 장점들도 역시 커다란 도전 과제가 된다. VANETs의 인프라 구조는 망 내에 참여하는 모든 차량 노드들에 의해 형성되기 때문에 망의 신뢰도는 단일 노드의 신뢰도에 종속적이다. VANETs은 대부분 개방 망으로 중앙 집중식 제어 없이 누구나 접속을 허용하기 때문에 망상에 고장이 나거나 해롭고 비정상적인 행위를 하는 노드들에 대한 참여 기회가 매우 높다. 많은 기존의 전통적인 망 보안 메커니즘들은 중앙의 컴포넌트나 노드 간 사전 통신 상호작용을 요구하지만 VANETs에서는 이러한 요구사항을 충족시키기가 어려운 실정이다. VANETs에서의 비정상 행위로부터의 보안은 중요한 속성으로 과연 VANETs이 성공적이고 사용 가능한 기술이 될지를 결정하는 중요한 요인이 될 것이다. 보안에서 가장 중요한 응용은 안전 응용이다. 거짓이거나 지연된 경고 메시지는 사고를 야기하므로 사전에 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 비즈니스가 이루어지거나 차량 내 소프트웨어 갱신 또는 원격 진단 같은 중요한 작업이 수행된다면 종단 간 보안이 절실히 요구된다.

본 논문에서는 VANETs에서의 다양한 센서로 부터 센싱된 상황정보에 대한 노이즈나 오동작과 차량 노드들의 활동에 대한 비정상 행위를 효율적으로 식별하여 처리할 수 있도록 하는 빅 데이터 처리 기술을 응용한 VANETs에서의 비정상 행위 탐지 방법을 제안한다. VANETs 상에서 정상상태로 센싱된 상황정보나 차량 노드 활동패턴으로부터 크게 벗어나는 이상 신호나 상황정보와 차량 노드의 비정상 행위를 빅 데이터 기법을 이용하여 구분하고 이에 대한 이상 상태 정도를 정상 활동 패턴으로부터의 이탈 정도를 고려하여 허용 임계치보다 크면 비정상 행위로 인식하고 이에 대한 경고 메시지를 생성하여 VANETs 망을 통해 경고 방송하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 살펴보았고, 3장에서는 제안한 VANETs에서의 빅 데이터 기법을 이용한 비정상 행위 탐지방법을 위한 시스템 모델을 서술하였으며, 4장에서는 제안한 빅 데이터 응용 기반 비정상 행위 탐지모델의 주요 알고리즘을 분석하였고, 5장에서는 제안한 알고리즘에 대한 모의실험과 고찰을 하였으며, 마지막으로 6장에서 향후 연구내용과 함께 결론을 맺는다.

II. 관련 연구

오늘날 자동차는 지금까지 기계적 • 전기적인 특징에서 벗어나 매우 복잡한 모바일 컴퓨팅 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 VANETs이라 하며 노드들은 이동성이 높아 불안정한 통신 링크를 갖는다.[1, 2] 그림 1은 VANETs의 일반적인 구조와 VANETs에서의 비상상황 발생 시 이를 감지하고 대처하는 도로의 센서와 라우터 등 통신장비 동작과 위기 상황을 알리고 대처하기 위한 통신기술의 예를 보여준다.[1]

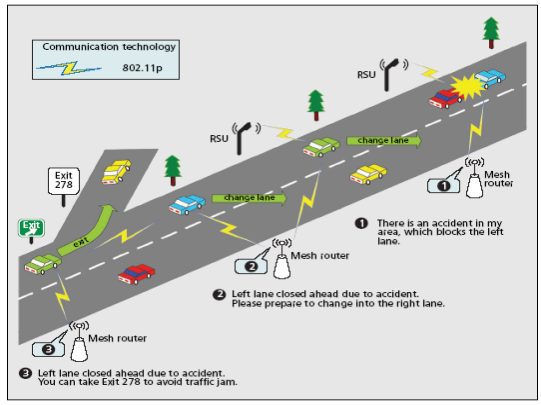

그림 1. VANETs에서의 비상 통신기술
Fig. 1. Emergency Communication Technologies in VANETs

그림에서 보인바와 같이, 도로상에서 차량들의 접촉 사고와 같은 비상 상황이 발생했을 때 도로 주변의 센서들로부터 도로 상황정보를 인지하고 사고를 감지하여 뒤따르는 도로위의 차량들에게 사고 정보를 알리고 도로 정체에 대처할 수 있도록 각 차량의 위치정보에 따라 차선 변경이나 인근 도로 출구를 통해 우회할 수 있도록 안내하는 메시지를 발령하게 된다.

VANETs에서의 통신은 전통 망에서 알려진 유니캐스트 방식이 아닌 노드 그룹을 기반으로 메시지를 전송하는 지오캐스트(geocast) 통신 패턴을 사용한다.[3] 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 만들기 때문에 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 수명 동안 추적되는 것이 가능하므로 망에 대한 거대한 보안 문제를 초래한다. VANETs에서는 위치기반 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 대한 노드 위조나 부당 변경, 그리고 그로 인한 거짓된 지리적 지역에 대한 메시지 발생, 도로 주변 상황정보를 수집하는 센서들의 잡음과 오동작이나 고장으로 인한 비정상 행위 등을 들 수 있다. 위험감지 모듈에 대한 센서 입출력 보안 역시 고려되어야만 한다.[7]

Ⅲ. 시스템 모델

VANETs은 도로변을 따라 설치된 라우터와 센서 노드들로 구성된 도로를 따라 빠른 속도로 질주하는 차량들이 네트워크 노드들로 일시적으로 구성되는 일종의 모바일 애드 혹 망이다. 이러한 VANETs은 실시간으로 센서들로 부터 센싱된 위치기반의 상황 정보들을 양산하고, 도로에 설치된 라우터나 차량들이 라우터 역할을 하며 시시각각 도로의 상황정보를 VANETs을 통해 유포하고 사고와 같은 비상상황이 발생했을 때 이를 알리고 대처할 수 있는 경고 메시지를 발령하고 전파하게 된다. 따라서 VANETs은 짧은 시간동안 수많은 정보들을 양산하고 유통하는 거대한 망으로 이러한 많은 정보에 대한 효율적인 처리와 관리가 절실하다. 아울러 이들 센서나 라우팅 장비로부터 유포되는 각종 정보들은 노이즈, 고장으로 인한 오동작 비정상 행위 정보, 보안을 위협하는 해로운 정보 등을 포함할 수 있다. 따라서 이러한 거대한 량의 정보로부터 빠르고 정확하게 필요한 핵심 정보를 찾아내어 처리하는 기술이 요구된다.

빅 데이터 처리 기법은 대용량의 데이터를 병렬로 빠르게 수집하고 분류하여 정확한 상황정보를 찾아내는데 매우 유용한 처리 기술이다. 빅 데이터는 데이터의 양, 생성 주기, 형식 등에서 과거의 데이터에 비해 규모가 크고 형태가 다양하여 기존의 방법으로는 수집, 저장, 검색, 분석이 어려운 방대한 크기의 데이터를 말하며 따라서 빅 데이터는 이러한 방대한 양의 데이터와 데이터 생성속도, 데이터 종류의 다양성을 통합적으로 고려할 수 있는 빅 데이터 처리기술이 필요하다. 빅 데이터 처리기술은 컴퓨터 학습기법 등을 사용하여 데이터로부터 지식을 자동으로 분석하거나 추출하는 과정으로 구성되며 이 과정을 통해 데이터 속에 감춰있는 어떠한 경향이나 패턴을 찾을 수 있다. 빅 데이터 분석에 사용되는 기술은 대부분 통계학과 전산학 특히 기계학습과 데이터 마이닝 분야에서 사용되는 기술로 비정형 데이터로부터 정보를 추출하거나 다른 데이터와의 연계성을 파악하여 분류나 군집화 기술을 이용하여 빅 데이터에 숨겨진 의미있는 정보를 발견하는 것이다.[8] 본 연구에서는 VANETs에서 유포되는 방대한 양의 도로 상황정보와 비상 상황 메시지들로부터 위치정보 기반 연계성에 따른 분류와 군집화 기술을 이용하여 전반적인 VANETs의 정규상황을 파악하고 센싱된 상황정보나 차량 노드 활동패턴이 정상 상태로부터 크게 벗어나는 이상 신호나 상황정보와 차량 노드의 비정상 행위를 빅 데이터 기법을 이용하여 구별하고 이에 대한 이상 상태 정도를 정상 활동 패턴으로부터의 이탈 정도를 고려하여 그 이탈 정도가 허용 임계치보다 크면 비정상 행위로 인식하게 된다.

Ⅳ. 빅 데이터 응용 설계

이 장에서는 본 논문에서 제안한 VANETs에서의 빅 데이터 기법을 이용한 비정상 행위 탐지방법을 설계하고 주요 알고리즘을 분석하였다. 기존의 네트워크들은 망 위상에 기반한 라우팅 접근 방법을 주로 사용하지만 VANETs의 위상은 지속적으로 고속으로 이동하는 노드들로 구성되어 있어 불안정하고 취약한 링크를 가지므로 VANETs에서는 위상기반 라우팅이 가능하지 않다. 따라서 대부분의 VANETs 시스템은 위치기반 라우팅 접근 방법을 사용하며 이때 전송 패킷들은 송신자와 수신자의 위치정보에 따라 라우트되게 된다. VANETs에서의 위치기반 라우팅 메커니즘은 노드의 위치에 종속적이며 어드레싱과 라우팅 방법에서 위치를 사용한다. 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.

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 상황에 대해 운전자에게 능동적으로 경고한다. 차선 머징 지원, 추월 지원, 트래픽 관리, 가상 경고신호 그리고 비상등과 같은 응용들 역시 사고 횟수나 도로 위험을 줄인다.

VANETs에서 발생하는 빅 데이터에 대한 분석은 우선 이들 데이터들이 위치 정보에 민감한 정보로서 도로를 주행하고 있는 차량의 위치정보에 따라 차별하여 적용이 되어야 하기 때문에 우선 위치정보에 대한 군집화 기술을 적용하였다. 군집화 기술은 데이터 분석 방법 중 데이터 마이닝 기술의 한 방법으로, 주어진 빅 데이터에서 데이터들의 특성을 고려하여 군집을 정의하고 군집을 대표할 수 있는 대표점을 찾는 것이다. 본 연구에서는 발생하는 데이터들이 위치정보에 매우 민감하므로 우선 위치 정보에 따라 군집화 기술을 적용하여 분류하였다. 이렇게 분류된 군집 데이터들을 대상으로 데이터 유형별 발생 빈도에 따라 분류하여 각 위치기반 군집의 하위계층에 계층별로 구분하여 이들에서 의미있는 상황정보를

```
public static void main(String[] args) throws Exception {
  Configuration conf = new Configuration();
  Job job = new Job(conf, "TokenCount"); //입력 토큰 카운트
  job.setJarByClass(TokenCount.class);
  job.setMapperClass(MyMapper.class);
  job.setCombinerClass(MyReducer.class);
  job.setReducerClass(MyReducer.class);
  /만약 mapper 출력이 다르면, setMapOutputKeyClass 호출
  job.setOutputKeyClass(Text.class);
  job.setOutputValueClass(LongWritable.class);
  job.setInputFormatClass(KeyValueTextInputFormat.class);
  - 중략 - }
public class TokenCount { //토큰 카운트 클래스
  public static class MyMapper extends Mapper<Text, Text, Text,
    LongWritable> {
    private final static LongWritable one = new LongWritable(1);
    private Text word = new Text();
    public void map (Text key, Text value, Context context) throws
      IOException, InterruptedException {
      String line = value.toString();
      StringTokenizer tokenizer = new StringTokenizer(line, "\t\r\n\f;
      while(tokenizer.hasMoreTokens()){
        word.set(tokenizer.nextToken().toLowerCase());
        context.write(word, one); } } }
public static class MyReducer extends Reducer //MapReducer 클래스
            <Text, LongWritable, Text, LongWritable> {
  private LongWritable sumWritable = new LongWritable();
  public void reduce(Text key, Iterable<LongWritable> Values, Context
    context) throws IOException, InterruptedException {
    long sum = 0; //토큰 카운트의 개수 합 - 발생빈도
    for(LongWritable val : values) {
      sum += val.get();      }
    sumWritable.set(sum);
    context.write(key, sumWritable);
    context.getCounter("Words Stats", "Unique Words").increment(1);
  } }
```

그림 2. 빅데이터 분석에서 상황정보 발생빈도 추출 알고리즘
Fig. 2. MapReduce Algorithm for Context in a Big Data Analysis.

추출하고자 하였다. 이때 고장이나 오동작으로 인해 생성된 데이터나 노이즈 그리고 해로운 비정상행위 정보들은 상대적으로 정상 상태에서의 발생된 데이터에 비해 노출 빈도가 적게 나타나게 될 것이다. 이러한 데이터가 가지는 속성을 이용하여 정상상태에서의 발생 데이터로부터 비정상 행위를 구별하고자 한다. 다음의 그림 2는 VANETs에서 발생하는 각종 빅 데이터를 우선 위치정보 기반의 군집화를 이룬 다음 각 위치 정보에 해당하는 데이터에 대한 상황정보의 추출을 위해 각각의 데이터 유형별 발생 빈도에 따른 분류를 하는 알고리즘을 보여

준다.[8] 이 알고리즘을 통해 발생 데이터로부터 발생 빈도가 높은 순서로 상황정보를 추출할 수 있고 이를 통해 현재 위치에서의 정상상태 상황정보를 구별해 낼 수 있게 된다.

V. 모의실험 및 고찰

이 장에서는 본 논문에서 제안한 VANETs에서의 비정상행위 탐지를 위한 빅 데이터 응용을 모의실험을 통해 그 성능을 임계 허용 오차에 대한 비정상 행위 탐지율과 거짓 경고율로 평가하였다. 여기서 비정상행위 탐지율은 정상 상태로부터 이탈한 총 데이터의 양에 대한 비정상 행위를 나타내는 데이터의 비율을 의미하며, 거짓 경고율은 총 검출된 비정상 행위 의심 데이터 중에서 정상상태의 데이터 비율을 의미한다. 다음의 표 1은 본 논문에서 제안한 VANETs에서의 비정상행위 탐지를 위한 빅 데이터 응용의 모의실험을 위해 사용된 파라미터를 보여준다.

표 1. 모의실험 파라미터
Table 1. Parameters for Simulation

Parameters	Value
단위시간 데이터 발생량	100
총 시뮬레이션 시간	30 time unit
기준 위치 개수	3
발생 데이터 분포	log-normal Dis.
발생 데이터 종류	random
발생 데이터 값	random
Threshold ϵ	[0.1, 0.15, 0.2, 0.25, 0.3]

표 1에 보인바와 같이 총 모의실험 시간은 30 단위 시간으로 하였고 단위 시간동안 발생하는 빅 데이터의 량은 각 기준 위치마다 100개로 하였으며, 이 때 도로상의 기준 위치 지점의 개수를 3곳으로 가정하였다. 상황 정보를 포함하는 발생되는 빅 데이터의 분포는 비교적 정상상태에서 발생하는 정상행위 데이터가 높은 비율을 차지하도록 로그-노말 분포를 가진다고 가정하였으며 각 기준 위치 지점에서 발생하는 데이터의 종류와 그 값은 random하다고 가정한다.

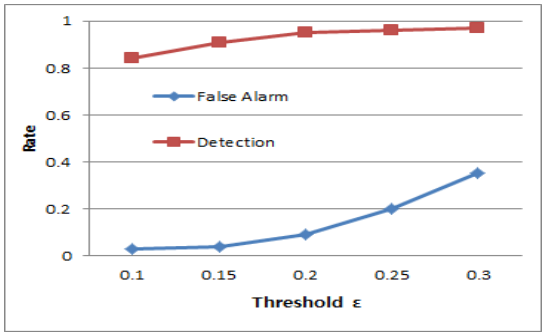

그림 3. 모의실험 결과
Fig. 3. Results of the Simulation Study

그림 3은 본 논문에서 제안한 VANETs에서의 비정상행위 탐지를 위한 빅 데이터 응용을 모의실험을 통해 비정상 행위 탐지율과 거짓 경고율에 대해 그 성능을 평가한 결과이다. 그림에서 보인바와 같이 발생하는 데이터 중에서 비정상 행위에 해당하는 데이터 탐지율은 임계값이 작을 때 낮게 나타나며 임계값을 높이면서 탐지율이 상승함을 알 수 있다. 하지만 그 차이는 그리 크지 않으며 특히 임계값 0.15 이후에는 큰 차이없이 탐지율이 높게 나타남을 알 수 있다. 반면, 거짓 경고율의 경우 임계값이 증가할수록 거짓 경고율이 급속히 높아짐을 알 수 있는데 이는 임계값이 높아짐에 따라 비정상 행위로 간주되어 탐지된 데이터 중에 정상행위 데이터의 비율이 급속히 증가하여 거짓 경고율이 높아지는 것으로 사료된다. 따라서 최적의 조건은 임계값이 0.15 부근에서 비정상 행위 탐지율은 높으면서 거짓 경고율은 최소화가 되는 것으로 나타났다.

VI. 결 론

지능형 교통 시스템의 많은 흥미롭고 유용한 응용들이 새로운 유형의 일시적인 애드 혹 망인 차량 애드 혹 네트워크의 개발과 연구를 발전시켰다. VANETs의 인프라 구조는 망 내에 참여하는 모든 차량 노드들에 의해 형성되며 중앙 집중식 제어 없이 누구나 접속을 허용하기 때문에 망상에 고장이 나거나 해롭고 비정상적인 행위를 하는 노드들에 대한 참여 기회가 매우 높다. 본 논문에서는 VANETs에서의 다양한 센서로 부터 센싱된 상황정보에 대한 노이즈나 오동작과 차량 노드들의 활동에 대한 비정상 행위를 효율적으로 식별하여 처리할 수 있도

록 하는 빅 데이터 처리 기술을 응용한 VANETs에서의 비정상 행위 탐지 방법을 제안한다. VANETs 상에서 정상상태의 센싱된 상황정보나 차량 노드 활동패턴으로부터 크게 벗어나는 이상 신호나 상황정보와 차량 노드의 비정상 행위를 빅 데이터 기법을 이용하여 구별하고 이에 대한 이상 상태 정도를 정상 활동 패턴으로부터의 이탈 정도를 고려하여 그 이탈 정도가 허용 임계치보다 크면 비정상 행위로 인식하였다.

본 논문에서 제안한 VANETs에서의 비정상행위 탐지를 위한 빅 데이터 응용은 모의실험을 통해 비정상 행위 탐지율과 거짓 경고율에 대해 그 성능을 평가하였다.

모의실험 결과 발생하는 데이터 중에서 비정상 행위에 해당하는 데이터 탐지율은 임계값이 작을 때 낮게 나타나며 임계값을 높이면서 탐지율이 상승함을 알 수 있다. 반면, 거짓 경고율의 경우 임계값이 증가할수록 거짓 경고율이 급속히 높아짐을 알 수 있었다. 최적의 비정상 행위 탐지 조건은 임계값이 0.15 부근으로 탐지율은 높으면서 거짓 경고율은 최소화가 되는 것으로 나타났다. 여기서 발생하는 데이터의 분포가 모의실험 결과에 크게 영향을 미칠 수 있음을 알 수 있었다. 따라서 향후 연구로는 이러한 VANETs에서 발생하는 데이터 속성과 빅 데이터 분석방법에 따른 영향에 관한 연구이다.

References

[1] A. Boukerche, H. A. Oliveria, E. F. Nakamura, A. A. Loureiro, "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems, Computer Communications, Vol. 31, pp. 2838 - 2849, 2008.

[2] W. Franz, C. Wagner, C. Maihoefer, and H. Hartenstein, "Fleetnet: Plat-form for inter- vehicle communications," in 1th International Workshop on Intelligent Transportation, Hamburg, Germany, 2004.

[3] 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.

[4] S. J. Oh, "An Anomaly Detection Method for the Security of VANETs", Journal of the Institute of Webcasting, Internet and Telecommunication, Vol. 10, No. 2, pp. 77 - 84, 2010.

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

[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] S. J. Oh, "Design and Evaluation of a Weighted Intrusion Detection Method for VANETs", Journal of the Institute of Webcasting, Internet and Telecommunication, Vol. 11, No. 3, pp. 181 - 188, 2011

[8] H. Wickham, "The Split-Apply-Combine Strategy for Big Data Analysis. Journal of Statistical Software, Vol. 40, No. 1, pp. 1 - 29, 2011.

저자 소개

김 식(정회원)

- 1979년 : 경북대학교 컴퓨터공학사
- 1991년 : 미국 Taxas A&M 컴퓨터공석사
- 2004년 : 일본 오카야마 현립대학 정통신공학 박사
- 현재 : 세명대학교 정보통신학부 교수

<주관심분야 : 임베디드 S/W, Real-time OS, 센서네트워크>

※ 이 논문은 2013학년도 세명대학교 교내학술연구비 지원에 의해 수행된 연구임

오 선 진(종신회원)

- 제 6권 제2호 참조
- 현재 : 세명대학교 정보통신학부 교수

<주관심분야 : 스마트 응용, 그린IT, VANETs, 모바일컴퓨팅, USN 등>