

차량 포그 컴퓨팅 : 현황 및 과제

홍지연*, 이정현**, 김치용***, 윤주상****

*동의대학교 디지털미디어공학과

**동의대학교 IT융합학과

***동의대학교 게임애니메이션공학전공

****동의대학교 산업ICT기술공학과

e-mail : anasis6095@gmail.com, kimchee@deu.ac.kr

Vehicular Fog Computing: Status and Challenges

Ji-Yeon Hong*, Gyeong-Heon Lee**, Chee-Yong Kim***, Joo-Sang Youn****

*Dept. of Digital Media Engineering, Dong-Eui University

**Dept. of IT Convergence, Dong-Eui University

***Major of Game Animation Engineering, Dong-Eui University

****Dept. of Industrial ICT Technology, Dong-Eui University

요 약

셀룰러 네트워크, RSU(Road-side Unit) 및 모바일 클라우드 컴퓨팅과 같은 기존 솔루션은 추가 인프라 구축 비용에 크게 의존하고 부담해야하기 때문에 완벽하지 않다. 따라서 우리는 통신(Communication) 및 계산(Computing)을 수행하기 위해 최종 사용자 클라이언트 또는 가까운 사용자의 가장자리 장치(Edge)를 사용하는 아키텍처인 차량 포그 컴퓨팅(VFC)이라는 인프라로 차량을 활용한다. 높은 신뢰성과 낮은 레이턴시의 요구 사항을 가진 데이터의 폭발적인 성장은 차량 네트워크에 큰 도전이 되었다. 하나의 잠재적인 솔루션은 포그 컴퓨팅 서버를 지리적으로 차량에 더 가깝게 배치하여 차량 기반 애플리케이션을 실시간으로 제공하는 것이다. 차량 애플리케이션은 연산이 집약적이고 레이턴시에 민감한 작업에서 탁월한 컴퓨팅과 통신 용량을 요구하는데 컴퓨팅 리소스를 네트워크 엣지로 이동시키는 데 주력하는 포그 컴퓨팅은 레이턴시 제한을 해결하고 클라우드에 대한 유입 트래픽을 줄임으로써 클라우드 컴퓨팅을 보완한다. 연결된 차량의 급속한 성장으로 포그를 지원하는 VANET(Vehicular Ad-Hoc Network)은 새로운 연구분야이다. VANET에서 포그의 신뢰할 수 있는 적용 가능성을 위해 많은 공개된 연구 과제들을 확인하고, 본 논문은 급속도로 발전하고 있는 차량에 대한 기존 시스템 설계 외에도 남아있는 기술적 과제에 대해 논의했다.

1. 서론

기존의 IoT(Internet of Things)는 인터넷(Internet)의 의미를 가지고 사용했다면, 지금은 지능(Intelligent)의 의미를 가지고 사용한다. 2019년 2월 스페인 바로셀로나에서 개최된 MWC(Mobile World Congress)에서는 지능형 연결성(Intelligent connectivity)을 주제로 내세웠는데 5G(Fifth-generation)와 AI(embedded Artificial Intelligence) 인프라를 지원하는 기술들이 주가 되었다. 그 중 ICT업체들이 참석하여 자율주행 차량(autonomous vehicle)을 주제로 하드웨어 기반의 단순한 이동 수단의 개념에서 벗어나 소프트웨어 플랫폼과의 융합을 제시하여 자율주행 차량에 대한 관심과 연구가 집중되고 있다[1].

자율주행 차량의 애플리케이션의 경우 연산이 집약적이고 레이턴시에 민감한 작업에서 탁월한 컴퓨팅 및 통신 용량을 요구한다. 컴퓨팅 리소스를 네트워크 엣지(Edge)로 이동시키는데 주력하는 포그 컴퓨팅(Fog computing)은 레이턴시 제한을 해결하고 클라우드에 대한 유입 트래픽을 줄임으로써 클라우드 컴퓨팅을 보완하고[1], 레이턴시

의 컴퓨팅 및 용량 문제를 해결하기 위해 3G, 4G, 셀룰러 네트워크, RSU(Roadside Unit), 모바일 클라우드 컴퓨팅은 다음과 같은 이유로 충분하지 않다. 셀룰러 네트워크는 통신 기능을 향상 시키지만 매우 제한적이며 네트워크 운영자에 의해 주로 제어된다. 이는 애플리케이션 측면에서 효과적일 수도 있고 아닐 수도 있다. RSU는 네트워크 통신 용량을 확대하지만 실제로는 비싸고 특히 도시 전체와 같이 대규모로 도로를 따라 완전히 배치하기가 어렵다. 모바일 클라우드 컴퓨팅은 모바일 사용자에게 풍부한 컴퓨팅 자원을 제공할 수 있지만 모바일 클라우드 컴퓨팅이 클라이언트-서버 통신 모델을 사용하기 때문에 실시간 정보를 업로드 할 때 값이 비싸고 많은 시간이 소요된다. 또한 원격 인프라와 높은 수준의 네트워크 연결이 필요하다. 본 논문에서는 포그 컴퓨팅에 대해 소개 하고, 차량 포그 컴퓨팅에 대한 개념을 제시한다. 세 번째로 안정적인 체계를 개발하기 위해 고려해야 하는 과제에 대해 설명하고 네 번째에서 포그 컴퓨팅 기반의 차량에 대한 필요성 대해 논의한 후 마지막으로 결론에서 향후 방향에 대해 애

기한다.

2. 관련 연구

1) 포그 컴퓨팅

포그 컴퓨팅이라는 용어는 Cisco가 발명했다. 시스코의 로베르토 데라모라 수석 이사가 “포그 컴퓨팅은 클라우드 컴퓨팅과 서비스를 네트워크의 종단부로 확장한 패러다임이다”라고 말하면서 중앙보다 종단(Edge)에 더 주목하고 마치 안개가 종단에 자욱하게 있다는 의미로 사용된다[2]. 이 시나리오에서는 차량 대신 클라우드 서버로 빅 데이터의 중복 대부분을 보내는, 로컬 리소스를 공유하는 통신 허브 및 중개 역할을 할 수 있다. 포그 서버는 소셜 네트워크 및 차량 네트워크에서 얻은 데이터를 수정하여 가능한 상호의존성을 예측할 수 있다. 지연을 줄이기 위해 로컬에서의 의사 결정 및 지리적 분포 특성을 모두 포함한다.

기존 기술은 3G 및 4G, 셀룰러 네트워크에서 RSU와 함께 제안되었다. 그러나 이 기술들은 무제한의 통신을 제공하기 위해 셀룰러 네트워크에 충분하지 않다. 기존 한계를 극복하기 위해 포그 컴퓨팅, 소프트웨어 정의 네트워크(SDN) 및 5G 네트워크가 보다 나은 방법으로 지원될 수 있다. 그림 1은 RSU를 통한 차량 및 교통 시스템 액세스와 같은 포그 서버에 액세스하는 두 가지 방법을 보여준다. 포그 서버는 서로 다른 로컬 포그 서버 간의 로드 밸런싱 및 작업 공유를 위한 배포 개념을 가지고 있다.



그림 1. RSU를 사용하는 운송 시스템, 사용자 및 스마트 장치를 위한 안개 서버 기반 아키텍처

2) VANET 및 아키텍처

VANET은 서로 간에 정보를 교환하기 위해 무선 연결이 가능한 차량으로 구성된다. 현재 VANET은 차량의 에너지, 저장 및 통신 기능이 풍부한 가장 보편적인 네트워크이다. 또한 네트워크 토폴로지는 빠른 이동성으로 인해 자주 변경된다.

차량은 V2X 통신으로 통칭되는 V2V(Vehicle-to-Vehicle) 및 V2I(Vehicle-to-Infrastructure)의 두 가지 시나리오

에서 통신할 수 있다. VANET 아키텍처는 WLAN 또는 셀룰러, ad-hoc 및 하이브리드 아키텍처의 세 가지 유형으로 분류할 수 있는데, WLAN은 다음 표준을 따르는 무선 기술이다. 예로 미국에서는 IEEE 1609 무선 액세스가 차량 환경 프로토콜 스택이 IEEE 802.11p WLAN에 구축된다. 인프라의 경우 WLAN/셀룰러 또는 WIMAX 액세스 포인트가 필요하다. 셀룰러 네트워크는 차량 통신 시스템을 강화시킬 수 있는 넓은 영역과 거대한 사용자를 대상으로 한다. 이 경우 차량 및 RSU는 액세스 포인트를 사용하여 WLAN 및 셀룰러 네트워크와 상호 작용할 수 있다. VANET에서는 영구적인 셀룰러 게이트웨이와 액세스 포인트를 도로 교차로에 배치하여 교통 관련 정보를 교환할 수 있으며 차량과의 연결성을 향상시킬 수는 있지만 인프라 비용이 추가된다. WLAN은 저렴하지만 통신 범위는 제한되어 있다. ad-hoc 네트워크의 경우 차량은 액세스 포인트 없이 통신한다. 하이브리드 아키텍처는 인프라와 ad-hoc를 포함한다. 이것은 저 지연과 함께 셀룰러 기술에 의한 IEEE 802.11p 따르면, 최대의 최소 비용을 제공한다. 포그를 지원하는 VANET(FAV) 아키텍처의 통신을 기반으로 하는 혼잡 관리, 긴급 상황을 포그 서버에 보고하기 위해 RSU 외에 휴대폰이나 스마트 차량이 BS와 통신할 수 있다.

3) VANET 과제

VANET 장점이 세계에 이목을 집중시켰지만 최근의 연구 분야에는 여전히 많은 어려움이 있다. 원활한 교통과 도로 안전을 위해 이러한 과제를 탐구해야 한다. 교통 상황에서 효율적인 교통 신호를 사용하여 도로의 차단을 피할 필요가 있다. 도로에서 긴급 상황시 적시에 구조하기 위해 사고를 정보를 받아 회피해서 갈 필요가 있다. 차량 간의 정보 분배를 위한 VANET 기반 애플리케이션은 네트워크의 대역폭에 집중해야 하며 레이턴시, 처리량, 라우팅, 보안, 가용성, 정제, 노드 이동성 및 시간제한을 비롯한 몇 가지 과제는 포그 컴퓨팅을 사용하여 향상시킬 수 있다.

1) 레이턴시

데이터 레이턴시는 목적지 차량에서 하나의 소스 차량과 수신 시간 사이와 전송 시간 사이의 시간을 의미한다. 포그 컴퓨팅의 로컬 서버를 사용하여 향상시킬 수 있다. 데이터 패킷을 송수신하는 주요 매개 변수는 전송 시간이며 이를 사용하여 처리량 비율을 계산할 수 있다.

2) 처리량

초당 비트 수와 같은 시간 단위당 통신 속도를 기반으로 한다. 처리량은 보낸 사람이 보낸 패킷 수와 대상에서 받은 패킷 수의 비율인 패킷 전달 비율과 연결된다. 기본적으로 패킷 포워딩에서도 고려해야 할 주요 사항이다. 패킷 크기, 동작 범위, 노드 이동성 및 클러스터 크기와 같

은 몇 가지 필수 요소가 영향을 준다. 강력한 메시지 브로드 캐스트는 100% 패킷 배포로 설명된다[3].

3) 혼잡

비상 통신, 메시지 보고와 V2V 통신, 도로에서 발생하는 차량의 물리적, 네트워크 정체를 포함하는 두 가지 유형으로 분류될 수 있다. 위에서 보았듯이 차량 간의 통신은 주요 문제이다. 통신이 약한 차량 통신은 도로 사고로 이어지고 사고 식별을 지연시킨다. 사고에 대한 보고도 제대로 이루어지지 않을 수도 있다. 위에서 언급 한 문제를 해결하기 위해 VANET에는 주 서버가 있어 시간이 오래 걸리고 고장이 발생할 확률이 높다. 이는 지연이 크고 가용성이 떨어진다는 의미이다. 이것을 포그 보조 VANET을 사용하여 해결할 수 있다. 로컬 서버는 지연을 줄이고 정보 손실 가능성도 줄인다.

4) 가용성

사고 후 경고 메시지를 전달하는 안전 애플리케이션에서, 무선 브로드캐스트 신호는 경고 메시지를 수신하고, 차량 통신을 위해 액세스가 가능해야 한다. 주파수 채널에 문제가 발생하면(방해 전파), 경고 메시지는 방송될 수 없으며 애플리케이션 자체는 쓸모 없게 된다. 메시지 혼잡이 발생하는 경우, 시스템을 원활히 사용할 수 없으며 더 많은 패킷 손실이 발생할 수 있다. 따라서 통신 시스템의 높은 가용성은 매우 어렵다.

5) 라우팅

출발지에서 목적지까지의 최적 경로를 찾는 것은 아주 어려운 일이다. 차량 네트워크에서 토폴로지는 차량의 예측 불가능한 이동성으로 인해 급속하게 변한다. 이 경우 중단 간 경로는 발견되지 않고 목적지까지의 차량의 방향, 속도 및 위치에 따라 다음 홉 차량이 선택된다. 효율적인 위치 기반 라우팅을 통해 패킷 전달 지연을 줄일 수 있다. 데이터를 전송하기 위해 홉 연결이 적어 최적의 경로로 이어진다. 라우팅 오버 헤드는 라우트 당 전송된 패킷 수를 포함한다.

6) 보안

VANET의 보안은 공격을 피하는 의미에서 중요한 연구 과제이다. 충돌 회피와 같은 애플리케이션 요구 사항을 충족시키기 위해 차량 간의 직접 통신을 기반으로 하는 IVC에 대한 가짜 공격과 같은 몇 가지 공격이 있다. 이 시스템의 가장 큰 문제점 중 하나는 전송된 데이터에 대한 보안 보증과 사용자 접근성을 위한 인증이다. 예로 차량용 소셜 네트워크에서 비상 메시지에 대한 안전한 메시지 보급은 QR 코드 기반 인증을 사용하여 해당 지역의 소셜 네트워크의 활성 사용자로부터 토폴로지를 준비함으로써 수행할 수 있다. 새로운 모델은 데이터 수집을 보장하기 위해 필수적이다.

3. 개방형 연구 과제

이 부문에서는 VAVET 및 ITS와 함께 포그 서버를 활용하여 안정적인 체계를 개발하기 위해 고려해야 하는 많은 공개된 연구 과제를 탐구한다.

A. 무선 네트워킹

차량의 연결 상태가 불확실하고 네트워크 토폴로지가 자주 변경되므로 최근의 현장 테스트에서 802.11p가 대부분 안정적으로 수행되었지만 차량 네트워킹의 안정성은 여전히 어려움이 있다. 반면, D2D 기반 차량 네트워크의 기존 성능 분석은 시뮬레이션에 기반을 두고있다[4]-[5]. D2D 기반 솔루션이 실생활에서 레거시 802.11p를 능가하는지 여부는 여전히 열려있다. 셀룰러 네트워크가 모든 도시와 교외 지역을 완전히 커버하지 못하고, 셀룰러 네트워크의 대역폭 리소스가 제한된다는 사실과 관련하여 두 가지 장점을 결합한 이 기종 차량 네트워킹 시스템을 만드는 옵션을 고려해야 한다.

D2D와 WLAN 기반 접근법이 공존하는 차량 포그 컴퓨팅 시나리오에서, 공동 스케줄링은 성능 요구 사항(즉, 대역폭, 레이턴시)과 사용 가능한 용량을 고려해야 한다. 지금까지의 공동 스케줄링 메커니즘은 여전히 부족하다.

B. 응용 프로그램 프로비저닝

차량 및 레이턴시에 민감한 모바일 애플리케이션은 중앙 클라우드, 셀룰러 포그 노드 또는 차량 포그 노드에 배치할 수 있다. 응용 프로그램을 배포할 위치는 기본 차량 네트워크의 토폴로지, 응용 프로그램의 허용하는 지연 범위와 차량 포그 노드, 응용 프로그램, 서비스 사용자의 예측된 이동성을 비롯한 여러 요소에 따라 다르다.

이전 연구는 포그 노드가 정적인 시나리오에 중점을 둔다. 예를 들어, [6]은 임대된 클라우드 노드와 자신의 포그 노드 사이의 작업 스케줄링에 중점을 두었고 클라우드 리소스의 비용과 화환의 균형을 맞추기 위해 발견적 기반의 알고리즘을 제안했다. [7]은 모바일 장치의 이동성을 고려하여 모바일 장치로의 실시간 스트리밍을 위한 클라우드 및 포그 노드의 리소스를 예약하는 적응형 콘텐츠 예약 기법을 제안했다. [8]는 게임 비디오 렌더링과 주변 플레이어에게 스트리밍하기 위해 게임 플레이어 및 조직의 유휴 머신을 포그 노드로 활용하는 Cloudfog를 개발했다. 포그 노드가 움직일 때 새로운 과제가 나타난다. 하나의 문제는 차량 포그 노드와 데이터 소스와 사용자의 동시 이동성 때문이다. 또 다른 문제는 컴퓨팅과 통신 리소스의 일정을 조정하는 복잡성에서 기인한다.

C. 보안 및 개인 정보

포그 킨 노드의 이동성과 동적 차량 네트워크 토폴로지는 새로운 보안 및 개인 정보 보호 문제를 야기한다. 주요 관심사는 인증 보안이다. 분배된 차량용 포그 노드는 포그 노드와 중앙 클라우드로 구성된 하이브리드 클라우드의

게이트웨이 역할을 한다. 예를 들어, 해커가 포그 노드 중 하나에 액세스하면 악의적인 메시지와 불법적인 명령을 보내 네트워크 서비스의 신뢰성을 파괴할 수 있다. 게다가 공격자는 차량의 포그 노드를 해킹하여 고객의 개인 정보를 복제할 수 있으므로 고객의 개인 정보를 심각하게 위협할 수 있다. 악의적인 공격을 막기 위해 [9]은 HoneyBots를 구현하여 D2D 네트워크에서의 악성 통신 활동을 탐지하고 추적한다. 공개키 기반 구조와 디피-헬만 키 교환(Diffie - Hellman key exchange)은 스마트 그리드 네트워크에서 인증의 보안을 강화하기 위해 사용된다. 그러나 차량 포그 플랫폼은 앞으로 더 많은 보안 문제를 지속적으로 발생 시킬 것이다. 이러한 문제를 해결하기 위해 효과적인 암호화 방법과 강력한 미들웨어가 개발되어야 한다.

4. Fog Computing 기반 Vehicular 관련 연구의 필요성

최근에는 차량과 인간, 차량과 교통 인프라 간의 네트워크를 이루려고 하는 추세가 빠르게 이뤄지고 있으며 다양한 표준화 작업이 이루어지고 있다. V2X 기술을 통해 자동차끼리 직접 또는 주변 시설과 전방 교통정보, 차량접근, 충돌 가능성 등의 다양한 정보를 주고받음으로써 운전자에게 안정성과 편리함을 제공하는 것을 목표로 한다.

V2X통신은 도로 환경의 요구사항에 따라 차량 서비스 제공을 위한 고효율의 주파수 전송률과 측위 정확도를 요구하게 되며 통신기술의 융합이 필수적으로 요구되고 있다. 그러나 특정 기술만으로 사용자의 요구조건을 모두 충족시키기 어렵고 기존 인프라와 새로운 기술의 융합으로 사용자가 언제 어디서나 끊김 없이 서비스를 이용할 수 있도록 사용자들과 근접한 위치에 포그 서버를 배치함으로써 사용자에게 보다 더 효율적인 서비스를 제공할 수 있다.

6. 결론

차량용 포그 컴퓨팅의 핵심 아이디어는 버스 및 택시와 같은 이동 차량을 주변 차량 및 승객을 위한 컴퓨팅 및 통신 서비스를 제공하는 모바일 포그 노드로 전환하는 것이다. 포그 컴퓨팅은 도로 및 교통 상황을 공유하고 차량 간의 통신 기능을 개선하기 위해 차량 네트워크에서 중요한 역할을 할 수 있다. 차량용 포그 컴퓨팅은 주문형 포그 컴퓨팅 (on-demand fog computing)이라는 아이디어를 실현하며, 컴퓨팅 리소스는 요청시 필요한 곳으로 전달된다.[1] 주요 초점은 포그를 보조하기 위해 VANET에 대한 VANET의 진보와 주요 기회 및 문제점을 파악하는 것이다. 마지막으로 많은 새롭게 공개된 연구 과제가 확인되었다. 우리는 포그를 지원하는 VANET에서 정책 회피에 대한 확인된 문제를 고려하여 새롭고 신뢰할 수 있는 솔루션을 제시할 필요성이 있다.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) (NRF-2017 R1D1A1B03034689) and by the BB21+ Project in 2019

참고문헌

- [1] Y. Xiao and C. Zhu, "Vehicular fog computing: Vision and challenges," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), 2017, pp. 6 - 9.
- [2] 김귀훈, 홍용근, 표철식 (2017). "IoT와 AI를 위한 에지 컴퓨팅 표준화 및 기술 동향". 한국통신학회지(정보와 통신), 34(12), 49-56.
- [3] R. Kumar, M. Dave, "A comparative study of various routing protocols in VANET", Int. J. Comput. Sci., vol. 8, no. 4, pp. 643-648, 2011.
- [4] H. Liu, H. Ning, Y. Zhang, M. Guizani, "Battery status-aware authentication scheme for V2G networks in smart grid", IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 99-110, Mar. 2013.
- [5] A. Paranjothi, M. S. Khan, M. Nijim, and R. Chaloo, "MAvanet: Message authentication in VANET using social networks," in Proc. IEEE 7th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON), New York, NY, USA, Oct. 2016, pp. 18.
- [6] X.-Q. Pham and E.-N. Huh, "Towards task scheduling in a cloud-fog computing system," in 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS), Oct 2016, pp. 1 - 4.
- [7] C. Y. Huang and K. Xu, "Reliable realtime streaming in vehicular cloudfog computing networks," in 2016 IEEE/CIC International Conference on Communications in China (ICCC), July 2016, pp. 1 - 6.
- [8] Y. Lin and H. Shen, "Cloud fog: Towards high quality of experience in cloud gaming," in 2015 44th International Conference on Parallel Processing (ICPP), Sept 2015, pp. 500 - 509.
- [9] A. Mtibaa, K. Harras, and H. Alnuweiri, "Friend or foe? detecting and isolating malicious nodes in mobile edge computing platforms," in 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Nov 2015, pp. 42 - 49.