

## 차량간 애드혹 네트워크에서의 전자상거래

박준상  
홍익대학교

### 요 약

도로상의 이동 중의 차량 등으로 구성된 차량간 애드혹 네트워크는 과거에는 볼 수 없었던 수준으로 인간과 주변 환경과의 소통을 가능케 해 줄 미래 사물지능통신(M2M: Machine-to-Machine)의 한 축으로써 많은 역할을 수행할 것으로 예상되고 가까운 미래에 현실화될 사물지능통신의 한 예로서 많은 관심을 받고 있다.

도심 전역에 산재하는 무수한 차량들을 연결하여 다양한 서비스의 제공이 가능한 새로운 광대역 기간망등으로 활용될 수 있을 뿐 아니라 각기 차량에 설치된 센서들이 기존의 시스템으로는 채집 불가능했던 다양한 자료의 수집을 가능하게 하여 인간의 주변 환경에 대한 이해를 높이는데 도움을 줄 것이다.

차량간 애드혹 네트워크는 위상 변화가 매우 심하고 구성원이 무수한 대규모 네트워크라는 특성이 있어 기존의 네트워크에서 볼 수 없었던 이동성 기반 정보 확산 (mobility-assisted data dissemination) 기법 등 새로운 형태의 정보 전송 기법들이 활용될 것이다.

본고에서는 향후 차량간 애드혹 네트워크등의 사물지능통신의 기반 기술이 될 이동성 기반 정보 확산 기법에 대하여 소개하고 어떻게 차량간 애드혹 네트워크에서 활용되어 여러 서비스들의 구현이 가능한지 전자상거래 서비스들을 중심으로 설명한다.

### 1. 서 론

과거와 현재의 통신망 기술은 인간간의 소통에 중심을 두었으나 미래에는 인간이 타인을 포함한 주변 환경, 즉, 주변의 모든 사물에 내재된 센서 또는 컴퓨터들과의 소통을 가능하게 해 줄 기술로 발달할 것으로 예상되고 이러한 기술을 현재 사물지능통신(M2M: Machine-to-Machine) 기술이라 부른다. 가까운 미래에 활성화 될 차량간 애드혹 네트워크(VANET: Vehicular Ad hoc Networks)는 무선 통신 기능을 갖춘 차량들과 노변 고정 장치들이 서로 노면 이상, 사고 발생 여부, 급정거 신호, 정체 상황 등 운행 정보를 교환함으로써 차량 운행 안전과 편의를 도모한다. 즉, 차량간 애드혹 네트워크는 각기 다른 차량들에서 수집된 다양한 정보가 차량간 통신으로 전달되어 운전자 또는 보행자의 주변 환경에 대한 이해도를 높여 차량 운행 안전 및 편의를 가져다주고 더 나아가 위급 상황 발생 시 차량간 통신과 차량 자체의 판단으로 적극적인 사고 방지 기능을 수행할 수 있게 해 준다. 이와 같이 사물(차량)간의 통신과 인간(운전자)과 주변 환경과의 활발한 소통을 가능하게 해 주는 차량간 애드혹 네트워크는 가장 가까운 미래에 우리의 실생활의 일부가 될 사물지능통신의 실레라 할 수 있다.

차량간 애드혹 네트워크는 교통안전 향상과 운행 편의를 가져다주는 역할 뿐 아니라 우리의 일상생활에서 발생하는 다양한 정보 수요를 충족시켜줄 수 있는 또 하나의 광대역 망으로서의 역할 또한 수행할 것으로 예상된다. 차량간 애드혹 네트워크에서는 기본적으로 운행 안전을 위한 서비스

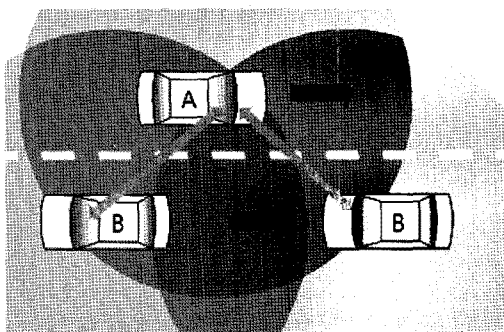
가 최우선적으로 제공되고 이와 함께 별도의 허가 주파수 대역에서 운영되는 허가된 서비스들과 비허가 주파수 대역에서 운영되는 다수의 불특정 서비스가 존재할 것으로 예상된다. 본고에서는 비허가 주파수 대역을 사용하고 인프라 또는 고정 기반 시설에 의존하지 않는 서비스들에 초점을 맞춘다. 비허가 주파수 대역에 기반하고 인프라에 의존하지 않는 차량간 애드혹 네트워크에서는 각 구성원이 제한된 전파 도달 범위를 갖는 단거리 무선 통신만이 가능한데 이로 인하여 원거리에 있는 구성원간의 통신을 위해서는 멀티홉(multihop) 통신이 필수적이다. 따라서 많은 경우 MANET(Mobile Ad hoc Networks) 한 형태로 분류하기도 한다.

차량간 애드혹 네트워크에서는 네트워크의 구성원인 차량의 빠른 이동성으로 인한 네트워크 연결성(connectivity) 또는 위상(topology)의 심한 변화가 존재하고 매우 많은 수의 차량 및 노변 고정 장치 등의 구성원이 존재할 수 있다. 이는 기존의 MANET 기술들의 차량간 애드혹 네트워크에서의 활용을 저해하는 요소로서 작용하는데 이에 대한 대안으로 DTN(Delay/Disruption Tolerant Networks)[1] 기법의 활용이 제안되고 있다. 대표적인 DTN 기법으로 구성원의 이동성을 활용하여 네트워크상에서의 정보 전달을 가능하게 해주는 이동성 기반 정보 확산 기법(Mobility-assisted Data Dissemination)[2]이 있다. 그러나 DTN 기술이라고 할 수 있는 이동성 기반 정보 확산 기법을 차량간 네트워크에서 활용하는 경우 데이터 전송 시 종단간(end-to-end) 지연시간(delay)이 매우 큰 단점이 있어 이를 사용하는 서비스는 종단간 지연시간에 민감하지 않아야 하는 제약 조건이 있다. 이러한 조건을 만족하는 차량간 네트워크에서 제공 가능한

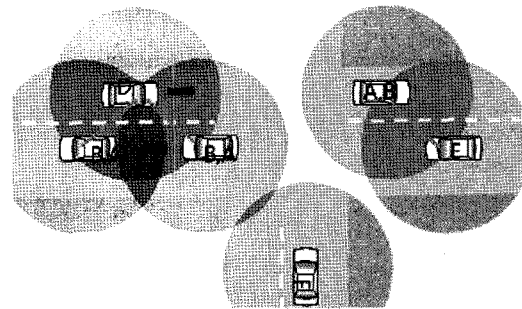
서비스들 중 현재 많은 관심을 받고 있는 광고 서비스와 일명 오픈 마켓이라 지칭되는 전자상거래 매개 서비스에 대하여 본고에서는 소개하고자 한다.

## II. FleaNet: 차량간 네트워크 전자상거래 시스템

FleaNet[3][4]은 차량간 네트워크상에서 동작되도록 설계된, 사용자가 원하는 물품을 사고팔고자 할 때 상거래 상대의 검색을 가능하게 해주는 전자상거래 매개 시스템이다. FleaNet의 사용자는 인터넷 연결성 또는 인프라가 없는 차량간 네트워크에서 상거래가 가능하도록 설계되어 있다. 현재 많이 사용되고 있는 인터넷의 오픈 마켓 시스템들과 유사하게 B2C(Business-to-Customer) 및 C2C(Customer-to-Customer) 거래가 가능하나 인터넷 또는 인프라의 의존성이 없기 때문에 사용자에게 인터넷 사용료 또는 거래 수수료를 부가할 필요가 없는 장점이 있다. FleaNet에서 활용되는 핵심적인 기술은 이동성 기반 데이터 확산 기법(mobility-assisted data dissemination)이다. 예를 들면, (그림 1(a))에서와 같이 어떤 차량은 A란 정보를 가지고 있고, 다른 차량들은 B란 정보를 가지고 있다. 이 차량들이 서로 통신할 수 있는 거리에 도달하면, 무선 통신을 이용하여 서로의 정보를 교환할 수 있게 된다. 원래 A의 정보만 가지고 있던 차량은 B의 정보를 얻게 되고 또한 B란 정보를 가지고 있던 차량은 A란 정보를 얻게 된다. 이 후 (그림 1(b))에서와



(a)



(b)

(그림 1) 움직임을 이용한 정보의 확산

같이 정보 A,B를 가진 차량이 새로운 정보 E 또는 D를 가진 새로운 차량을 만나게 되면 추가적으로 E 또는 D라는 정보는 획득하게 된다. 이와 같이 각각의 차량들이 이동하여 또 다른 차량을 만나게 되면, 더 많은 정보를 얻을 수 있게 되고, 더 많이 움직일수록 더 많은 정보를 획득하게 된다. 따라서 이동성 기반 데이터 확산 기법을 사용하는 경우 데이터의 전달 또는 확산 속도는 노드의 움직임 속도 그리고 움직임 패턴에 따라 증가 또는 감소한다.

FleaNet에서는 각 노드들이 네트워크를 통해서 확산 또는 전송하고자 하는 정보는 상거래 상대의 탐색을 위한 질의(query) 패킷이다. 어떤 물건을 구매 또는 판매하고자 하는 상거래 의도를 가진 노드는 상거래 상대 탐색을 위한 질의 패킷을 자신의 전파 도달 범위 안에 있는 이웃 노드들에게 주기적으로 전송한다. 판매와 구매 의사 모두 각각의 질의 패킷으로 생성되어 전송된다. 그러한 질의 패킷을 수신한 노드는 다른 노드에게 재전송하지 않고 자신의 저장 공간에 저장한다. 특정 노드의 질의 패킷들은 직접 전송이 가능한 이웃 노드에게만 전달됨에도 불구하고 시간이 지남에 따라 네트워크 전역으로 확산된다. 전부 또는 일부 노드의 이동성으로 인하여 시간이 지남에 따라 특정 노드의 이웃 노드 자체가 바뀌어 질의 패킷을 수신하는 서로 다른 노드의 개수는 시간이 지남에 따라 지속적으로 증가하고 또한 질의 패킷을 수신한 노드들의 물리적 위치 이동으로 인하여 질의 패킷을 저장하고 있는 노드들이 네트워크 전역에 분포할 가능성이 높다. FleaNet에서 노드의 물리적 움직임을 이용하여 질의 패킷을 확산시키고 패킷 전송은 단일홉(single-hop) 전송으로 제한한 이유는 차량간 네트워크의 특성 상 밀도 높게 분포되어 있는 무수한 차량들로 이루어져 있을 가능성과 주변 노드와의 연결의 단속성(intermittent connectivity)이 고려되었기 때문이다.

특정 질의 패킷을 수신한 노드는 자신의 저장공간에 저장되어 있는 다른 질의 패킷을 비교하여 질의 간의 정합(matching) 발생 여부를 판단한다. 즉, 특정 물품을 판매하고자 하는 의도를 가진 노드1에 의하여 생성된 질의 Q1가 어떤 노드 3에 저장되어 있을 때, 동일한 물품을 구매하고자 하는 의도를 가진 노드2가 생성한 질의 패킷 Q2가 노드 3에게 전달이 되면 Q1, Q2는 노드 3에서 정합되었다고 표현하고 이를 Q1과 Q2의 생성자 노드1, 노드2에게 상대방 정보

와 함께 정합 사실을 알려준다.

다음은 FleaNet을 이용한 하나의 사례이다. 특정 제품의 중고 자전거의 구매를 원하는 A가 있다. A는 자동차로 서울 강남구역삼동의 사무실과 경기도 성남시의 집 사이를 출퇴근을 위해서 매일 왕복 이동한다. 또한 경기도 일산과 서울 마포구 상수동에서 출근퇴근을 위하여 매일 왕복 이동하는 B는 A가 원하는 제품과 동일한 중고 자전거의 판매의사를 가지고 있다. A와 B는 출근 전 FleaNet 시스템이 운영되는 차량 컴퓨터에 특정 제품 자전거 구매 의사와 판매 의사를 각각 등록한다. A와 B의 차량 컴퓨터는 A와 B가 출근을 위해서 이동하는 동안 만나는 차량들과 정보를 교환한다. 이 때, C의 차량이 서울 마포구 상수동에서 B의 차량을 만나 B의 차량이 발생시킨 질의를 수신, 저장한 상태에서 타 지역으로 이동하였는데 이 후 서울 강남구 역삼동에서 A의 차량을 만나 A의 질의 패킷을 수신하게 된다. C는 A의 질의 패킷의 수신 즉시 자신이 저장하고 있던 B의 질의와 A의 질의가 정합됨을 알고 A와 B에게 질의 정합 사실과 상거래 상대방에 대한 정보를 전송한다. A와 B는 자신이 원하던 제품인 것을 확인하고 상대방 구매/판매자에게 구매/판매 의사를 전달하여 상거래를 성사시킨다.

FleaNet에서 두 질의간의 정합이 발생했을 경우에 상거래 당사자 한쪽은 질의 정합 발생 노드의 직접 통신이 가능한 주변 이웃 노드이어서 정합 사실의 통보가 쉽다. 그러나 다른 한쪽은 원거리의 노드일 가능성이 있다. 이러한 원거리 당사자에게의 통보는 Last Encounter Routing(LER)[5]을 이용한다. LER은 별도의 위치 추적 서비스(location service) 없이 지좌표 또는 지리적 라우팅(geographic routing)을 가능하게 해 주는 방법이다. 앞서 언급한 바와 같이 차량간 네트워크와 같이 위상 변화가 심한 대규모 네트워크의 경우 라우팅 테이블의 유지가 거의 불가능하기 때문에 라우팅 테이블에 크게 의존하지 않는 geographic routing의 사용이 주로 제안된다. 일반적인 geographic routing의 동작 원리는 모든 노드가 GPS등 위치 정보 제공 서비스를 이용할 수 있다고 가정할 때, 패킷의 전송자는 패킷의 수신자 노드의 좌표를 알아 내 수신자에 가장 가까이에 있는 주변 노드에게 패킷을 전송함으로써 중국에는 수신자에게 패킷이 전달되는 방식인데 구성원이 움직임이 있는 이동 네트워크에서는 먼저 수신자의 현 좌표를 알아올 수 있는 방법이 있어야 하고 특정 노

드의 현 좌표를 알려주는 서비스를 일반적으로 위치 추적 서비스(location service)라고 한다. 그러나 때로는 location service의 구축/운영 자체가 일반 라우팅 프로토콜에서 라우팅 테이블 유지에 비견될 만큼 매우 자원 소모적이라, 즉, 네트워크 상에서 많은 정보의 교환을 필요로 해서, 이를 채용하면 geographic routing의 장점이 사라지는 문제가 있다. LER에서는 location service와 geographic routing을 통합하여 별도의 location service 없이 geographic routing을 가능하게 해 준다. 몇 가지 변형된 방식들이 있으나 일반적으로 LER에서 모든 노드는 다른 모든 노드와의 가장 최근 접촉지점과 접촉시간을 기록하고 패킷은 언제나 수신자의 최근 접촉지점 방향으로 전송된다. 즉, 노드 B에 기록된 노드 A와의 접촉 정보가 시점  $t_1$ , 위치  $L_1$ 이라면 B는 A에게 보내려는 패킷에  $t_1$ ,  $L_1$  정보를 기록한 후 현 B의 위치를 기준으로  $L_1$  지점에 제일 가까운 이웃 노드에게 패킷을 전송한다. 패킷을 수신한 이웃 노드는 자신이 가지고 있는 A와 접촉점 정보, 예를 들면  $t_2$  시점에  $L_2$  지점에서 A와 접촉한 기록과 비교하여  $t_1$ 이  $t_2$  보다 최신인 경우  $L_1$  지점에 가장 가까운 이웃 노드에게 전송하고  $t_2$ 가  $t_1$ 보다 최신인 경우  $L_2$  지점에 가장 가까운 이웃노드에게 전송한다. 패킷을 여러 중계 노드를 거쳐 목적지 까지 전달되는 동안 점진적으로 최신 정보를 획득한 노드의 중계를 받아 종국에는 목적지의 현 위치에 정확히 다다르게 된다.

FleaNet에서 질의 패킷들은 각각의 질의 패킷 생성자에 의해서만 이웃 노드들에게 전파된다. 질의 생성자가 아닌 노드는 타 노드로부터 전송된 질의 패킷의 수신 시 저장만 하고 재전송하지 않는다. 이와 같은 제약 조건은 구성원간의 정보 교환량을 줄여 네트워크에 참여할 수 있는 참여자 수를 늘리는 등 네트워크 수용능력을 증가시킬 수 있으나 매개 지연 시간이 클 수 있다. 즉, 정보의 확산 속도가 느려 원하는 상거래 상대자를 찾는 데 오래 걸릴 수 있다. 대략적으로 정보의 확산 속도는 노드의 이동 속도와 비례한다. 만일 확산 속도를 증가시켜 거래 성립 시간을 단축시키고자 한다면 생성자와 함께 질의 패킷의 확산을 담당할 대리인(proxy)을 여럿 두는 방법이 있다. 이들 대리인은 질의 패킷 생성자와 마찬가지로 이동하면서 접촉하는 모든 주변 노드들에게 질의 패킷을 지속적으로 전송한다. FleaNet에서는 질의 패킷 전달 대리인을 설정하는 기법으로 RW(Random

Walk)라 불리는 방식이 있다. RW방식에서는 질의 생성자가 특정 주변 노드에 대리인 설정 패킷을 전송한다. 대리인 설정 패킷에는 최대 대리인 수인  $k$ 가 기록되어 있는데 이 패킷을 수신한 노드는 수신 즉시 대리인 역할의 수행을 시작하고, 즉, 질의 패킷을 주변 노드에게 광고하고,  $k-1$ 을 기록한 대리인 설정 패킷을 특정 이웃 노드에게 재전송한다. 위와 같은 방법으로  $k$ 개의 대리인이 설정된다.

### III. SSD: 차량간 네트워크에서의 광고 배포를 위한 인센티브 시스템

FleaNet에서는 모든 네트워크 구성원이 상호 협조적이라는 가정이 있다. 다른 많은 차량간 네트워크 또는 MANET 상에서 운용되는 프로토콜들 또한 구성원 모두가 상호 협조적이라는 가정에 기반을 두고 있다. MANET은 군사 전술망 등 특수 목적 네트워크로서 운용될 가능성이 크기 때문에 단일 운영주체가 존재하고 따라서 모든 구성원이 어떠한 공통 목표를 위하여 상호 협조한다는 가정이 일반적으로 받아들여지고 있으나 일반 차량간 네트워크의 경우 다양한 소유주의 차량 및 장치로 이루어져 있고 그러한 구성원 모두가 어떠한 공통된 목표를 위해 상호 협조한다는 가정은 때로는 성립하지 않는다. FleaNet을 예로 들면, 특정 노드는 다른 노드로부터 발생된 질의를 비교하여 정합이 일어날 경우 질의 생성자에게 통보해 준다. 그러나 소유주가 다양한 차량들로 이루어진 실제 차량간 네트워크에서 특정 소유주 소유의 차량이 다른 소유주의 차량의 질의를 수신, 저장한 후 다른 질의와 비교 및 정합 발생 시 통보하기 위하여 자신의 자원을 사용할 의무가 없으면 아무런 경제적 이익이 없는 위와 같은 행위를 자발적으로 수행할 가능성은 매우 낮아 보인다. 또한 차량간 네트워크에서는 개인 사생활 보호 문제가 대두될 수 있다. 일반적으로 네트워크 구성원은 여러 가지 이유로 개별 구성원의 구별자 역할을 하는 특정 아이디를 사용하도록 요구 받는데 만일 특정 차량이 동일한 아이디를 지속적으로 사용한다면 해당 아이디를 차량간 네트워크 상에서 여러 가지 방법으로 추적함으로써 개인 사생활 정보를 보다 손쉽게 취득할 수 있게 된다. 이러한 이유로 차량간 네

트위크에서 때로는 구성원의 아이디를 수시로 바꾸도록 요구받고 구성원의 아이디가 고정되어 있다는 가정하게 상호 협력이 가능하도록 설계되어있는 프로토콜은 차량간 네트워크에서의 운용이 불가능 할 수도 있다.

이렇듯 상호 협조 가정이 성립하지 않는 차량간 네트워크에서 운용되는 프로토콜은 따라서 구성원들의 자발적인 참여를 유도할 수 있는 동기 부여 장치 또한 마련되어 있어야 하는데, 일반적으로 참여자에게 적절한 경제적 보상이 주어지도록 하는데 초점을 맞춘 인센티브 시스템을 많이 채택하고 있다. 이러한 인센티브 시스템에서 중요한 요소는 참여자에게 적절한 보상이 주어지도록 하는데 있어서 참여도에 상당하는 만큼만의 보상이 필히 이루어지도록 하는데 있다. 즉, 시스템의 허점을 이용한 참여자의 부당 이득의 취함을 불가능한 수준으로 만들어야 한다.

SSD(Signature Seeking Drive)[6]는 상호 협력적이지 않은 구성원들로 이루어진 차량간 네트워크를 광고 미디어로서 사용할 수 있도록 하는 인센티브 시스템이다. 기본 동작 원리는 다음과 같다. 특정 광고주가 주변 차량들에게 광고의 배포를 요청한다. 광고의 배포를 요청받은 차량이 배포 요청을 수용한다면 광고를 전송받아 이동하면서 접촉하는 모든 차량들에게 광고를 재전송한다. 광고 배포를 수행한 차량은 자신으로부터 광고를 수신한 차량들에게 수신 확인서를 수거해 수거된 확인서의 수 만큼에 해당하는 경제적 보상을 전자화폐 형태로 광고주로부터 받고 또한 광고를 수신한 차량 또한 광고주로부터 광고 수신에 대가로 경제적 보상을 받는다.

SSD에서는 암호화 기법을 이용하여 참여자 보상 체계를 구축한다. 기존의 유사 차량간 네트워크 또는 MANET 인센티브 체계들은 대부분 개조 불가능 (tamper-proof) 하드웨어 나 게임 이론 (game theory)을 이용한 방법들이었으나 SSD에서는 보다 단순한 공개키 기반구조 (Public Key Infrastructure: PKI)의 존재만을 가정한다. 공개키 기반구조에서는 신뢰할 수 있는 기관에서 부여한 한 쌍의 공개키와 개인키를 이용하여 특정 목적을 달성할 수 있도록 정보의 암호화/복호화 작업을 수행한다. 인터넷 사이트에서 디지털 공인 인증서를 이용한 본인 확인이 특정 목적의 하나의 예이다. 공개키 기반구조는 이미 일반적으로 많이 사용되고 있는 체계이므로 보다 현실적인 가정이라 할 수 있다.

SSD의 구성은 CA(Certificate Authority), VA(Vehicular Authority), 광고주(advertiser), 그리고 차량 등의 일반 구성원으로 이루어져 있다. CA는 공개키와 개인키를 발급하는 기관으로 SSD의 모든 참여 주체는 CA로부터 공개키와 개인키를 발급받아야 한다. VA는 광고의 허가를 맡는 기관으로 무분별한 사용의 방지와 보상금 지급을 위한 기록 보존 및 보증을 맡는다. 어떤 광고주  $I$ 가  $ADI$  라는 광고의 배포를 시작하려고 할 때 다음과 같은 방법으로 VA로부터 광고 허가서(Ad permit)를 발급받는다.

$$I \rightarrow VA : C_I, AD_I, \{AD_I\}_{K_I^*}$$

$$VA \rightarrow I : \{AD_I\}_{K_{VA}^-}$$

이 때,  $u \rightarrow v$  는  $u$ 로부터 어떤 정보가 전송되었다는 의미를 그리고  $C_I$ 는  $I$ 의 디지털 인증서를 나타내고,  $K_I^*$ 와  $K_I^-$ 는 각각  $I$ 의 공개키와 개인키를 나타낸다. 또한  $M1 \parallel M2$ 는  $M1$ 과  $M2$ 의 결합된 메시지를 나타내고  $\{M\}_{K_I^-}$ 은  $I$ 에 의하여 전자서명된 메시지  $M$ 을 나타낸다. 즉,  $I$ 는 먼저 VA에게 광고 내용과 신원 확인을 위한  $I$ 의 인증서 그리고 전자서명된 광고 내용을 전송하면 VA는 전자서명된 광고와 인증서를 이용하여 허가를 받으려는 주체의 신원이  $I$ 가 정확인지 확인하고 허가서를 발급한다. 허가서는 VA에 의하여 전자서명되어 있는데 이는 VA가 차후 참여자에 대한 경제적 보상이 이루어짐을 보증한다는 의미로 해석할 수 있다.

허가서를 발급받은  $I$ 는 지나가는 차량들과 다음과 같은 방법으로 광고 배포 합의를 이룬다.

$$I \rightarrow * : C_I, AD_I, \{AD_I\}_{K_{VA}^-}$$

$$u \rightarrow I : C_u, \{AD_I\}_{K_u^-}$$

즉, 광고주  $I$ 는  $I$  주변을 지나쳐가는 불특정 다수(\*로 표시) 차량들에게 광고 배포 의뢰를 하면 광고 배포 의사가 있는 노드  $u$ 는 응답을 하는데 이 때  $u$ 는 자신의 신원을 확인할 수 있도록 인증서와 전자서명된 광고를  $I$ 에게 전송한다.  $I$ 는 특정 광고와  $u$ 의 신원을 나타낼 수 있는 아이디와 함께 전자서명한 voucher를  $u$ 에게 전송한다. 이 voucher는 차후 지정된 특정 광고가  $u$ 에 의해서 배포되었는지를 확인을 위해서 발행된다.

Voucher를 획득한  $u$ 는 이동하며 접촉하는 다른 구성원들에게 다음과 같은 방법으로 광고를 배포하고 수신확인서를 수거한다.

$$u \rightarrow * : C_u, AD_I, I, \left\{ \left\{ AD_I | I \right\}_{K_{VA}^-} \right\}_{K_u^-}$$

$$u \rightarrow u : C_v, \left\{ AD_I | u \right\}_{K_v^-}$$

광고와 함께 배포되는 내용은 인증서와 전자서명된 광고 허가서인데 이를 통해  $u$ 의 신원을 확인할 수 있고 또한 광고가 허가된 광고임을 알 수 있다. 허가된 광고는 또한 지불 보증된 광고로 해석할 수 있고 광고를 수신한 대가를 지불받을 수 있음을 나타낸다.  $u$ 로부터 광고를 수신한  $v$ 는 수신 확인서를 발급하여야 한다.  $u$ 는 이러한 수신확인서를 모두 수거해 전자화폐 교환처(Virtual Cashier : VC)에 제출하면 광고 배포의 대가로서 전자화폐를 보상 받을 수 있고  $v$  또한 광고 수신의 대가로서  $u$ 에게 지불되는 보상액의 일부를 제공받는다.  $u$ 는 다음과 같은 정보를 VC에게 제출한다.

$$u \rightarrow VC : C_u, AD_I, I, \left\{ \left\{ AD_I | I \right\}_{K_{VA}^-} \right\}_{K_u^-}, R_u$$

$$R_u = (C_v, \left\{ AD_I | u \right\}_{K_v^-}), (C_w, \left\{ AD_I | u \right\}_{K_w^-}), \dots$$

위와 같은 정보를  $u$ 로부터 수신한 VC는 광고허가서와 수신확인서등의 진위를 먼저 확인한 후, VA에게 문의하여  $u$ 가 이미 동일한 수신확인서로 보상을 받지 않았는지 확인한다. 문제가 없음이 확인되면  $u$ 와 수신 확인서를 발급한 모든 주체들에게 합당한 보상액을 지급한다.

상기된 방법은 SSD에서 광고 배포시의 광고주로부터 직접 광고 배포 의뢰를 받은 차량들만 광고 배포를 할 수 있도록 제한된 방법이다. 이는 광고주가 광고 배포자의 수를 제한함으로써 광고비용등을 어느 정도 제한할 수 있도록 하지만 광고 배포 속도 또한 제한되는 문제가 있다. 때로는 광고비용 보다는 광고 확산 속도가 중요한 문제가 될 수 있는데 광고 확산 속도의 증가를 위해서는 광고주와의 직접 접촉을 통하여 배포 의뢰를 받지 않은 노드들도 광고를 배포할 수 있도록 하는 방법이 필요하다. 만일 광고주가 비용을 고려치 않고 광고의 빠른 확산을 원한다면 광고주가 접촉하는 모든 차량들에게 다음과 같은 정보를 전송한다.

$$S \rightarrow * : C_S, AD_S, \left\{ AD_S | S \right\}_{K_{VA}^-}$$

이 방법에서는 발급 대상이 지정된 Voucher가 없으므로 수신확인서를 이용하여 VC에게서 보상을 받을 때에도 Voucher의 확인을 수행하지 않는다. 따라서 광고를 수신한 모든 차량들이 광고를 재배포하며 수신확인서를 수거한다면 어떠한 참여자라도 보상의 제공 대상이 된다. Voucher를 사용하는 경우 Voucher에 명시된 참여자만이 VC로부터 보상을 받을 수 있다.

## IV. 결 론

본고에서는 가장 가까운 미래에 현실화 될 사물지능통신의 실례로서 차량간 애드혹 네트워크를 제시하고 차량간 애드혹 네트워크에서의 기본 기술로 많이 활용될 이동성 기반 정보 확산 기법과 이의 활용법으로써 차량간 애드혹 네트워크에서 운영 가능한 전자상거래 서비스들에 대하여 소개하였다. 사물지능통신 기술은 차량간 애드혹 네트워크와 같이 구성원의 이동성이 매우 높고 구성원의 수가 매우 많은 대규모 네트워크에의 대응이 가능하도록 개발되어야 할 것이다. 차량간 애드혹 네트워크에서 제공될 많은 서비스들이 이를 고려하여 차량간 애드혹 네트워크의 확장성을 어느 정도 보장해 주는 이동성 기반 정보 확산 기법을 이용하도록 설계되고 있다. 차량간 네트워크에서의 오픈 마켓 구축을 가능하게 하는 FleaNet과 비협조적 구성원으로 이루어진 차량간 애드혹 네트워크를 광고 미디어로서의 활용을 가능하게 해 주는 SSD 인센티브 시스템들이 이러한 서비스들의 예이다. (2장의 일부는 [4]에서 발췌하였음을 밝혀둔다.)

참 고 문 헌

[1] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," In Proc. ACM SIGCOMM, Aug. 2003.

[2] R. Groenevelt, P. Nain, and G. Koole, "Message delay in mobile ad hoc networks," In Proc. Performance, Oct. 2005.

[3] U. Lee, J. Lee, J.-S. Park, and M. Gerla, "FleaNet: A Virtual Market Place on Vehicular Networks," IEEE Transactions on Vehicular Technology, Vol. 59 (1), Jan. 2010.

[4] 유희훈, 박준상, 모바일 P2P 오픈마켓 시스템, 한국정보과학회, 정보과학회지 제28권 6호, 2010.6.

[5] M. Grossglauser and M. Vetterli, "Locating nodes with

EASE: Mobility diffusion of last encounters in ad hoc networks," In Proc. IEEE INFOCOM, Mar./Apr. 2003.

[6] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure Incentives for Commercial Ad Dissemination in Vehicular Networks," In Proc. of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC) 2007.

약 력



박 준 상

1996년 홍익대학교 공학사  
 2001년 University of Southern California 공학석사  
 2006년 University of California, Los Angeles 공학박사  
 2006년 ~ 2007년 UCLA Postdoctoral Researcher  
 2007년 ~ 현재 홍익대학교 컴퓨터공학과 조교수  
 관심분야: 유무선 통신 및 통신망

