http://dx.doi.org/10.7840/kics.2014.39B.5.304

CCN 기반 이동 애드혹 환경에서의 안전한 라우팅 방안

이 주 용◆, 이 지 훈°

Secure Routing Scheme in CCN-Based Mobile Ad-Hoc Networking Environments

Ju-Yong Lee◆, Ji-Hoon Lee°

요 약

이동통신 기술의 발달과 스마트폰의 폭발적 보급으로 인해 사용자들이 언제 어디서든 컨텐츠를 생성하고 공유하게 하게 됨에 따라, CCN (Content-centric networking)과 같은 컨텐츠 중심의 새로운 네트워킹 방식이 등장하게 되었다. 그러나, CCN은 일대일 전송 구조를 근간으로 하고 있어 사용자 단말로만 구성된 애드혹 환경에 적합한 라우팅 프로토콜이 요구된다. 이에 본 논문에서는 애드혹 환경에 적합한 주문형 방식의 CCN 라우팅 방식을 제안한다. 또한, 허위 라우팅 정보 구축을 방지하기 위한 해쉬 기반 라우팅 정보 교환 구조 또한 제안한다. 성능 평가를 통해 이중 라우팅 구조로 인해 제안 방식이 기존 방식 대비 제어 메시지 오버헤드를 감소시킴을 확인하였다.

Key Words : Content-centric networking, Ad-hoc network, Secure routing

ABSTRACT

As users generate lots of contents anytime and anywhere with an explosive growth of the number of mobile devices, Content centric networking (CCN) has emerged as a new networking architecture. However, the efficient CCN routing scheme is required for ad hoc network support because of its one to one message exchange characteristics. So, this paper proposes the new CCN ad hoc routing scheme using on-demand approach, which includes the secure routing configuration scheme based on multiple hash operation. It is shown from the simulation that the proposed method can provide lower control overhead because of its two-fold routing configuration architecture.

Ⅰ. 서 론

이동통신 기술의 발달과 함께 스마트폰 기반 이동통신 기기의 보급이 증가함에 따라, 사용자들은 시간과 장소에 제한받지 않는, 언제 어디서나 사용 가능한 네트워크 환경을 요구하고 있다. 이러한 무선 네트워크 기술의 발달과 무선기기의 다양화로 인해 등장하게 된 것이 애드혹 네트워크다.

애드혹 네트워크는 기지국이나 AP (Access Point) 등의 고정된 기반 시설의 도움 없이 이동 노드들만으로 자율적으로 망을 구성하여, 고정적이고 계층적인 기존 네트워크에 자율성과 융통성을 부여한 구조를 갖고 있다. 애드혹 네트워크를 구성하는 노드들은 무선 인터페이스를 가지며, 호스트와 라우팅 기능을 동시에 수행한다. 애드혹 네트워크에서 사용되는 라우팅 프로토콜들은 크게 테이블 기반 방식 (Table-driven

※ 본 연구는 상명대학교 교내과제 (2014-A000-0311)로 수행되었습니다.
◆ First Author : Sangmyung University Department of Information Communication, goal0208@sangmyung.kr, 학생회원
° Corresponding Author : Sangmyung University Department of Information Communication, vincent@smu.ac.kr, 정회원
논문번호 : KICS2014-04-119, Received April 7, 2014; Revised May 12, 2014; Accepted May 12, 2014

scheme)과 주문형 방식 (On-demand scheme)으로 구분된다[1]. 테이블 기반 방식은 사전에 애드혹 노드들이 라우팅 정보를 구축하고, 주기적 또는 변경사항이 발생할 경우에만 네트워크 내의 모든 이동 노드들이 라우팅 정보를 네트워크 전체로 전파하게 하는 구조를 갖고 있으며, 대표적인 예로 OLSR (Optimized link state routing)이 있다. 한편, 주문형 방식은 데이터 전송을 위해 경로가 필요한 경우에만 경로를 탐색하는 방식을 말한다. 이 방식은 주기적인 라우팅 정보를 전파하고 갱신 및 저장하면서 발생하는 오버헤드를 줄일 수 있지만 데이터 전송 시점에서 경로를 탐색하기 때문에 경로 탐색으로 인해 데이터가 전송될 때까지 지연이 발생하게 된다. 대표적으로 AODV (Ad hoc on-demand distance vector routing), DSR (Dynamic source routing) 등이 있다.

또한, 사용자간 컨텐츠 공유와 소셜 네트워킹 기반 컨텐츠 공유가 인터넷 사용 패턴의 주를 이루고 있다. 이러한 추세에 따라, 기존 종단간 통신 기반의 인터넷 구조를 변화시키려는 움직임이 나타나고 있으며, 대표적인 예가 CCN (Content-centric networking) 기술이다 [2-6].

본 논문에서는 주문형 방식 애드혹 라우팅 프로토콜의 일종인 AODV 기반으로 CCN과 애드혹 환경을 연동시키기 위한 구조와 이때 라우팅 정보 교환의 오류를 피하기 위한 안전한 라우팅 구조를 제시한다.

Ⅱ. 관련 연구

CCN은 다음과 같은 특징들을 갖고 있다[2-6]. 첫째, CCN은 기존의 네트워킹 기술과는 달리 주소 자체가 데이터를 명명한다. 즉, 호스트 주소가 아닌 데이터 이름으로써 패킷 전달 경로를 처리한다. 둘째, 수신자 중심의 모형이라는 특징을 가진다. 즉, 전송 제어는 수신자가 보내는 컨텐츠 요청 패킷인 Interest 패킷의 전달에 의해서만 이루어진다. 셋째, 네트워크에서 컨텐츠 패킷을 저장하는 기능 (in-network caching)이 있다. 콘텐츠 패킷들이 네트워크내 노드에서 저장되어, 동일한 콘텐츠에 대한 요청이 전달되면 원래의 컨텐츠 생성자가 아닌 중간 노드에서 컨텐츠 패킷을 전달하게 하여 네트워크내 트래픽의 부하를 감소시킬 수 있다. 마지막으로, 내재된 보안 기능을 갖고 있다. 즉, 각 컨텐츠 패킷들은 그 자체가 디지털 서명이 되고 효율적으로 암호화가 가능하다. 따라서, HTTPS (Hypertext transfer protocol over secure socket layer)와 같은 프로토콜을 사용하지 않아도 된다는 것이다.

CCN에는 그림 1과 같이 Interest 패킷과 Data 패킷이라는 두 가지 타입의 패킷이 존재한다. Interest 패킷은 콘텐츠의 이름을 지시하며, Selector라는 부분을 통해 콘텐츠를 내보내는 순서와 전송 범위 등을 지정하게 된다. 그리고 Nonce를 통해 수신된 Interest 패킷의 재전송 여부를 구분하게 한다. Data 패킷은 chunk라는 다수의 컨텐츠 객체 단위로 나눌 수 있다.

CCN 노드들은 독특한 포워딩 모델을 갖는데, 여기에는 세 가지 테이블이 존재한다. 컨텐츠 저장을 위한 Content store (CS), 패킷 전달 경로 정보를 구성하고 있는 Forwarding information base (FIB), 그리고 Data 패킷의 전달을 위해 interest 패킷이 수신된 face의 정보를 가지고 있는 Pending interest table (PIT)이다. CCN 포워딩은 다음과 같은 과정을 진행된다. 우선 interest 패킷이 도착하면, 재수신 여부를 감지하기 위해 PIT 정보를 확인하고, 재수신된 경우라면 별도의 동작 수행 없이 바로 폐기한다. 그렇지 않으면, 저장되어 있는 데이터 패킷이 존재하는지 확인하기 위해 CS를 검사한다. 저장되어 있는 데이터 패킷이 있는 경우 interest 패킷의 포워딩 없이 데이터 패킷을 interest 패킷이 수신된 face로 전송한다. 저장되어 있는 데이터 패킷이 없으면, 차후 수신된 데이터 패킷을 전달하기 위한 경로 구성을 위해 PIT에 목록을 생성하고 FIB를 통해 interest 패킷을 포워딩한다. 이러한 과정을 통해 패킷의 중복 전송을 차단하게 되고 또한,

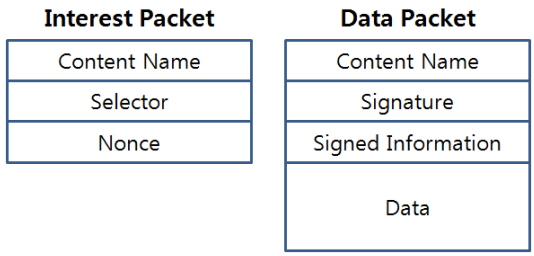

그림 1. CCN 패킷: Interest vs. Data
Fig. 1. CCN Packet: Interest vs. Data

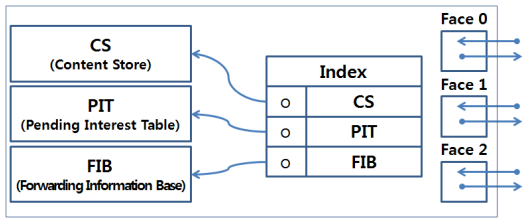

그림 2. CCN 포워딩 모델
Fig. 2. CCN Forwarding Model

CS를 통한 트래픽 부하의 감소 효과를 가질 수 있게 된다.

또한, AODV 라우팅 프로토콜은 RREQ/RREP 메시지 교환을 통해 종단간 경로를 구성하게 된다. 이때 Routing request (RREQ) 메시지는 전체 네트워크로 플러딩되며, Routing reply (RREP) 메시지는 유니캐스트로 전송되어 소스와 목적지 노드간 종단 경로를 구성한다.

CCN 노드들은 독특한 포워딩 모델을 갖는데, 여기에는 세 가지 테이블이 존재한다. 컨텐츠 저장을 위한 Content store (CS), 패킷 전달 경로 정보를 구성하고 있는 Forwarding information base (FIB), 그리고 Data 패킷의 전달을 위해 interest 패킷이 수신된 face의 정보를 가지고 있는 Pending interest table (PIT)이다. CCN 포워딩은 다음과 같은 과정을 진행된다. 우선 interest 패킷이 도착하면, 재수신 여부를 감지하기 위해 PIT 정보를 확인하고, 재수신된 경우라면 별도의 동작 수행 없이 바로 폐기한다. 그렇지 않으면, 저장되어 있는 데이터 패킷이 존재하는지 확인하기 위해 CS를 검사한다. 저장되어 있는 데이터 패킷이 있는 경우 interest 패킷의 포워딩 없이 데이터 패킷을 interest 패킷이 수신된 face로 전송한다. 저장되어 있는 데이터 패킷이 없으면, 차후 수신된 데이터 패킷을 전달하기 위한 경로 구성을 위해 PIT에 목록을 생성하고 FIB를 통해 interest 패킷을 포워딩한다. 이러한 과정을 통해 패킷의 중복 전송을 차단하게 되고 또한, CS를 통한 트래픽 부하의 감소 효과를 가질 수 있게 된다.

또한, AODV 라우팅 프로토콜은 RREQ/RREP 메시지 교환을 통해 종단간 경로를 구성하게 된다. 이때 Routing request (RREQ) 메시지는 전체 네트워크로 플러딩되며, Routing reply (RREP) 메시지는 유니캐스트로 전송되어 소스와 목적지 노드간 종단 경로를 구성한다.

CCN은 기본적으로 chunk 단위의 개별 패킷 전송이 이루어지므로, 애드혹 환경에 적합한 새로운 라우팅 방안이 필요하다. 또한, 잘못된 경로 구성을 막기 위한 정보 전달이 필수적이다. 따라서, 본 논문에서는 애드혹 환경에 적합한 안전한 CCN 라우팅 구조를 제안한다.

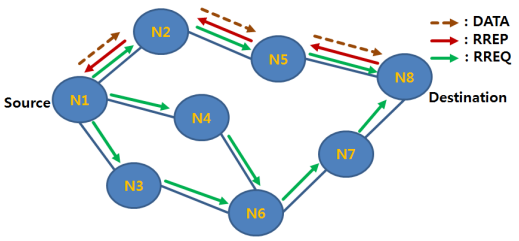

그림 3. AODV 경로 발견
Fig. 3. AODV root discovery

Ⅲ. 제안 방식

본 논문은 CCN 구조와 애드혹 라우팅 구조 연동시 나타나는 경로 발견의 비효율성 문제 및 허위 라우팅 정보 구축을 방지하기 위한 안전한 라우팅 정보 교환 구조를 제시한다.

3.1 경로 발견 과정

CCN 기반 애드혹 라우팅 방안은 먼저 경로 발견 과정으로 이루어진다. 하위 호환성 (backward compatibility)을 위해 CCN의 interest/data 패킷 구조를 활용하여 경로를 구성한다. 즉, 첫 번째 interest 패킷을 플러딩 (flooding) 기반으로 전송하여 관련 컨텐츠 생성자로만 전달될 수 있게 하기 위해 첫 번째 interest 패킷은 옵션 정보를 포함하는 것을 가정한다. 이는 중간 노드가 모든 컨텐츠를 캐쉬하지 않은 경우에 따른 경로 재발견 과정 가능성을 차단하기 위한 것이다. 경로 발견을 위한 interest 패킷을 수신한 컨텐츠 생성자는 데이터 패킷을 CCN 포워딩 모델에 따라서 컨텐츠 요청자에게 전달한다.

RREQ 기능을 수행하는 interest 패킷 처리 후에 해당 경로에 포함되는 모든 CCN 노드들은 애드혹 라우팅을 위한 별도의 Temporary FIB (TFIB)을 구축한다. 이후부터는 interest 패킷 포워딩시에 FIB와 TFIB 검사를 수행하여 패킷 포워딩을 수행한다. 따라서, interest 패킷의 플러딩 전송이 한 차례로 제한되는 구조를 갖는다.

3.2 경로 안정성 검증

본 논문에서 제시하는 CCN 애드혹 라우팅 방안은 허위 라우팅 정보 구성이 가능하다는 보안 취약점을 갖는다. 즉, RREQ 기능을 수행하는 interest 패킷 교환시에 악의적 사용자가 허위 라우팅 정보 구성을 위한 RREP 데이터 패킷을 전달하게 되면 이후 전달되는 모든 interest 패킷이 bad guy에 전달되게 된다. 이러한 취약점을 해결하기 위해 RREP 데이터 패킷에 포함된 인증 정보를 컨텐츠 요청자가 확인하는 과정이 필요하다. 이를 위해 컨텐츠 요청자는 컨텐츠 생성시, 랜덤 값 R을 생성한 후, 컨텐츠 청크 수 만큼 해쉬

값을 반복해서 계산해서 해쉬 체인 값들을 생성한다. 이 후, 첫 번째 interest 패킷에 해쉬 체인의 마지막 해쉬 값을 동봉해서 전송한다. i 번째 interest에 포함된 해쉬 값을 중간에 가로채더라도 $i+1$번째 interest에 포함된 해쉬 값을 예측할 수 없다. 이러한 해쉬값 동봉 전송 및 해쉬 값 확인을 통해 원래의 컨텐츠 요청자와 생성자간에서만 데이터 교환이 가능하게 된다. 간소화된 해쉬 기반 안정적 경로 구성은 그림 4와 같다.

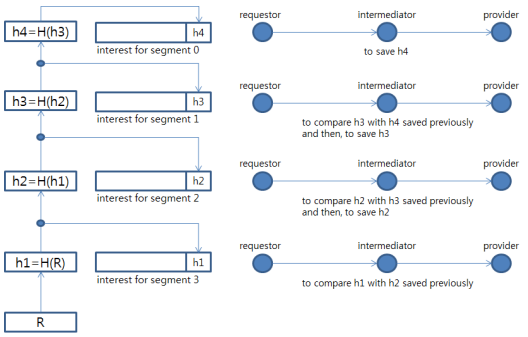

그림 4. 해쉬 기반 경로 안정성 검증
Fig. 4. Root reliability verification base on hash

Ⅳ. 성능 분석

본 절에서는 제안 방식과 플러딩 기반 CCN 애드혹 시스템을 비교 분석하기 위한 시뮬레이션 결과를 제시한다. 무선 채널 특성은 IEEE 802.11b 규격을 따르며, 11Mbps의 채널 비트율을 갖는다. 무선 전송 범위는 250 미터로 가정하였으며, IEEE 802.11 DCF (Distributed coordination protocol) 프로토콜 위에 CCN 애드혹 라우팅 프로토콜을 추가하는 구조를 갖는다. 제안 방안의 효율성 검증을 위해 경로 구성과 컨텐츠 교환시 요구되는 제어 메시지 오버헤드를 네트워크 크기의 변화에 따라 평가한다. 즉, 기존 애드혹 라우팅 방안 적용시 나타나는 플러딩 오버헤드와 제안 방안에서 추가적으로 이루어지는 안전한 정보 교환을 위한 제어 메시지 오버헤드를 비교 분석한다. 제안 방식에서 노드간 신뢰성 확보를 위한 secure relationship 구성에 따른 제어 메시지는 사전에 완료된 것으로 가정하며, CCN의 in-network caching에 의한 환경 구축을 위해 시뮬레이션 초기에 해당 컨텐츠에 대한 임의의 노드간에 교환이 이루어지는 것으로 가정한다.

그림 5는 경로 구성과 컨텐츠 전달을 위해 교환되는 제어 메시지의 발생량을 측정하였다. 그림 5에서

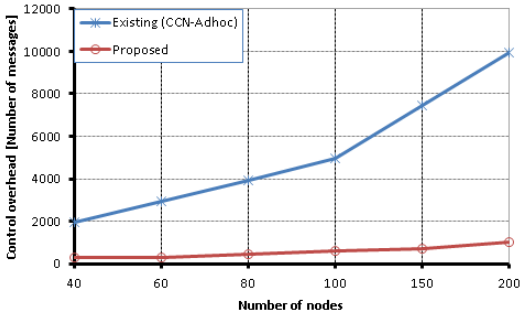

그림 5. 제어 메시지 오버헤드
Fig. 5. Control message overhead

보이는 바와 같이 기존 방안은 경로 구성을 위해 모든 제어 패킷이 플러딩되므로, CCN이 갖는 in-network caching에 의한 트래픽 감소 및 전달 경로 단축 효과를 거의 보지 못한다. 특히, 모든 interest 패킷이 플러딩되므로 높은 제어 오버헤드를 갖는다. 반면, 제안 방안은 초기 패킷만 경로 구성을 위해 플러딩되고 이후에 전달되는 제어 패킷들은 구축된 경로를 통해 유니캐스트 전송이 이루어지므로 기존 방안 대비 낮은 메시지 오버헤드를 가지며, 네트워크내에 저장되어 있는 데이터 캐쉬에 의해 제어 메시지의 수가 더욱 적은 경로를 갖게 되어 제어 메시지의 수가 크게 감소됨을 확인할 수 있다.

Ⅴ. 결 론

본 논문은 이중 라우팅 구조와 안전한 라우팅 정보 구축을 위한 해쉬 기반 정보 전달 구조를 통한 애드혹 환경에 적합한 CCN 정보 전달 방식을 제안하며, 제안 방식이 갖는 특징은 다음과 같다. 첫째, 주문형 애드혹 방식 적용시 나타나는 반복적인 플러딩 전송에 따른 오버헤드 감소를 위해 이중 라우팅 구조를 채택하였다. 두 번째로, 허위 라우팅 정보 구축에 따른 정보 전달 오류 문제를 해결하기 위해 경로 발견 단계에서 해쉬 정보 교환 구조를 제시하였다.

References

[1] T. Santhamurthy, “A quantitative study and comparison of AODV, OLSR and TORA routing protocols in MANET,” *Int. J. Computer Sci.*, vol. 9, no. 1, pp. 364-369, Jan. 2012.

[2] J. Choi, J. Han, E. Cho, T. Kwon, and Y. Choi, “Survey on content-oriented networking

for efficient content delivery," *IEEE Commun. Mag.,* vol. 49, no. 3, pp. 123-127, Mar. 2011.

[3] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," *ACM CoNEXT,* pp. 1-12, Dec. 2009.

[4] J. Lee, S. Cho, and D. Kim, "Device mobility management in content centric networking," *IEEE Commun. Mag.,* vol. 50, no. 12, pp. 28-34, Dec. 2012.

[5] M. Meisel, V. Pappas, and L. Zhang, "Ad hoc networking via named data," *ACM MobiArch,* pp. 3-8, Sept. 2010.

[6] J. Lee, T. Chung, T. Kwon, and Y. Choi, "A study on flooding-based routing designs for CCNx testbed," in *Proc. KICS,* pp. 325-326, Seoul, Korea, Nov. 2011.

[7] S. Jung, H. Park, and T. Kwon, "A study on the data push using push table in content centric networking," in *Proc. KICS,* pp. 667-668, Pyeongchang, Korea, Jan. 2014.

[8] O. Lee and J. Lee, "Proposal of handover using CCN with comparison of the handover in current LTE system," in *Proc. KICS,* pp. 297-298, Pyeongchang, Korea, Jan. 2014.

이 주 용 (Ju-Yong Lee)

2010년 3월~2014년 2월 : 상명대학교 정보통신공학과 학사

2014년 3월~현재 : 상명대학교 정보통신공학과석사 과정

<관심분야> 미래인터넷, 네트워크 보안, Electric vehicle

이 지 훈 (Ji-Hoon Lee)

1998년 3월~2001년 8월 : 고려대학교 대학원 전자공학과 공학 박사

2001년 9월~2002년 3월 : 고려대학교 차세대인터넷 센터 Research fellow

2002년 4월~2012년 2월 : 삼성전자 종합기술원 전문 연구원

2012년 3월~현재 : 상명대 정보통신공학과 조교수

<관심분야> 미래인터넷, CCN, M2M, 네트워크 보안, Electric Vehicle