DTN 에서 보안 강화를 위한 Queue 관리 방법

박종권, 홍충선*
경희대학교

jkpark@networking.khu.ac.kr, cshong@networking.khu.ac.kr

A Study on the Robust Secure Queue management Scheme in Delay Tolerant Network

Jong Kwon Park, Choong Seon Hong*
Department of Computer Engineering, Kyung Hee University

요 약

본 논문은 Delay Tolerant Network(DTN)에서 발생할 수 있는 네트워크 공격 유형 중 Flooding attack 에 대하여 Queue 를 효과적으로 관리하기 위한 관한 연구이다. 불필요한 메시지나 악의적인 메시지 구분을 하기 위하여, 라우터에서 정상 메시지인지 유 무를 판별하며, 이후 메시지에 저장 된 다음 Queue 관리 정책을 통해 효율적으로 메시지를 폐기하는 절차를 시행한다. 이러한 매커니즘을 사용하면, Flooding attack 이 발생 하였을 경우, queue 안에 있는 메시지의 우선순위를 높게 설정하여, 메시지가 전송률을 높였으며, 무작위 메시지 생성 공격으로부터 보다 안전함을 시뮬레이션을 통해 입증하였다.

Ⅰ. 서 론

Delay Tolerant Network(DTN)는 기존 인프라가 충분히 갖춰지지 않은 지역이나 네트워크가 정상적으로 동작하기 힘든 지역에서 사용되도록 설계되었다[1]. End-to-End 간에 전송만을 지원하는 TCP/IP 는 기본적인 handshake 를 통해 통신 하므로 양 방향이 지속적으로 연결 되어야 하며, 짧은 round-trip 과 높은 에러 발생으로 인해 빈번한 전송 지연이 발생하게 된다. 반면, DTN 의 경우 비대칭 통신을 하여 중간 노드와의 연결성을 보장하고, 에러 발생과 전송 지연에 대하여 보다 견고하다. DTN 의 가장 큰 특징이 Store-and forward 정책이며, Storage 를 기반으로 위와 같은 특징을 유지하고 있다. 따라서, 저장 공간에는 정상 적인 메시지도 있지만, 불필요하게 남아있거나 공격자가 의도적으로 flooding 할 수도 있다. 또한 노드 자체가 가지는 이동성에 의하여 메시지를 전달 하므로 메시지 전송을 위해서는 중간 릴레이 노드의 역할이 중요하다.

현재까지 DTN 에서 제안된 라우팅 알고리즘들은 모두 명시적 또는 묵시적인 가정을 기반으로 하고 있으며, 제안된 환경에 따라 알고리즘이 서로 다르게 적용될 수 있으므로, 라우팅 또한 중요한 이슈이다.

본 논문은 이러한 라우팅 알고리즘 중 flooding 을 기반으로 하는 Epidemic 라우팅을[2] 전제로 발생할 수 있는 보안 위협에 대하여 이야기하고 Queue 관리를 통해 메시지를 효율적으로 관리할 수 있는 방법에 대하여 알아 보고, 번들의 특성에 적합한 보안 매커니즘을 제안 하였다.

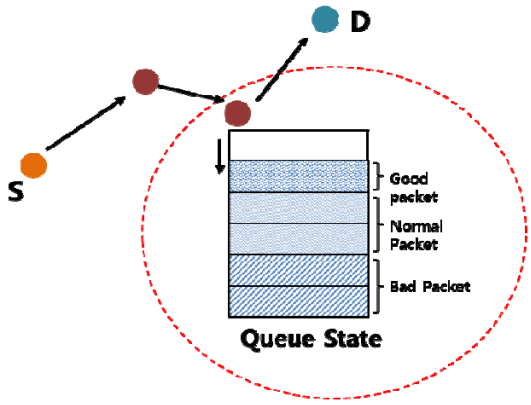
본 논문의 2 장에서는 DTN 보안 위협 모델 및 제안 사항에 대하여 말하고 3 장에서는 결론 및 시뮬레이션 결과에 대하여 말한다.

Ⅱ. 본론

1. 위협 모델

DTN 에서의 보안 위협 모델로 메시지가 유효한지 기밀성과 무결성을 입증 하는 것은 쉽지 않다. 기밀성과 무결성을 입증하기 위해서 암호화 알고리즘을 이용한 방법과 bundle 레이어 구조에 인증 메시지를 사용하여 hop-by-hop 으로 인증하는 방법이 사용되기도 하였으며, 이러한 구조에서 오버헤드를 최소화 하기 위한 방법에 관한 연구도 진행 중이다[3]. 전송 측면에서는 악의적인 메시지를 무차별하게 전송하여 노드의 리소스를 고갈되게 할 수 있으며, 이러한 공격은 서비스 거부 공격(Denial of Service)의 범주 안에 들며 Secure Routing 을 위한 측면에서 발생하는 대부분의 문제는 Mobile ad-hoc Network(MANET)에서의 보안 위협 모델과 매우 흡사하다.

Internet-Draft 문서인 " Delay-Tolerant Networking Security Overview" 에서는 DTN 에서 발생할 수 있는 보안 위협 모델에 대하여 이야기 하고 있으며, open issue 로 key management, 라우팅 프로토콜 보안, 성능 및 보안 디자인 고려사항에 대하여 언급하고 있으며, 특히, 트래픽을 이용한 공격 유형에 대처하기 위하여 프로토콜 설계의 중요성을 언급하고 있다[4].



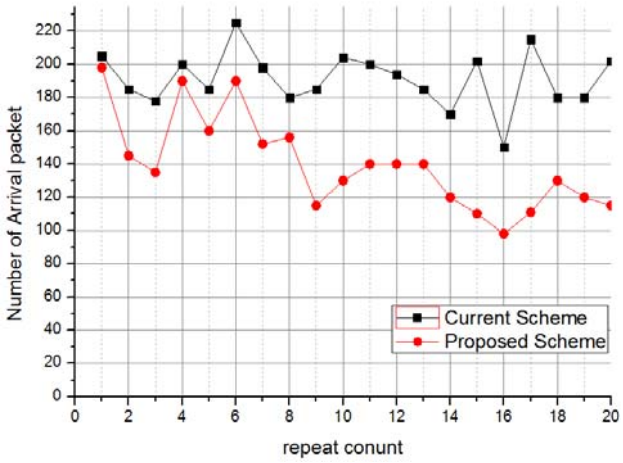
[그림 1] 노드 별 queue 상태

위의 그림 1 과 같이 각 노드의 큐에는 정상 메시지 및 악의적인 메시지 또는 폐기되지 않은 메시지가 존재 할 수 있다.

2. 제안 사항

본문에서는 Queue 의 효율성을 높이기 위하여 RFC 5050[6]문서에 명시된 ' Creation Timestamp time' 을 조절하여, 노드에 들어오는 메시지의 drop 시간을 조절하도록 하였다. 각각의 노드는 메시지를 전송 할 때 노드의 고유 ID 를 포함하며, 한 클러스터 내의 노드들은 각자의 주변 노드의 정보를 공유하고 있다고 가정하였다. 따라서, 전송되는 메시지의 ID 가 섞인 고유 값이 변경 되었다면, 불량 메시지나 악의적인 메시지로 판별 하도록 설정 하였다. 네트워크 상황이나 무선 노드의 상태에 따라 데이터의 값이 유동적으로 바뀔 수 있기 때문에 값이 바뀐 메시지를 무작위로 폐기 한다면 비효율 적일 수 있기 때문에, 본 논문에서는 Bundle 프로토콜의 Timestamp 필드를 수정하여 비정상 적으로 의심 되는 패킷의 drop 시간을 짧게 조절 하였다. 단, Queue 상태가 포화 되었을 때에 이러한 절차를 실행 하도록 설정 하였다.

Ⅲ. 결론



[그림 2] 메시지 전송 및 평가 결과

1. 성능 평가

제안된 방법은 기존의 방법에서 메시지의 이상 유무를 판별하여 drop 순위를 높이기 때문에 기존의 방법으로 메시지를 전송했을 때보다 도달하는 메시지의 양이 줄어드는 것을 그림 2 를 통해 확인할 수 있다. 실험의 정확성을 높이기 위해 20 번을 반복하였으며, 전체 메시지가 수신된 양을 그래프에 나타나도록 하였다. 또한 송신 노드와 수신 노드사이에 2 개의 attack 노드를 임의로 삽입하여 불필요한 메시지가 생성 되도록 설정하였으며, 각각의 노드가 지니고 있는 통신 범위에 다른 노드가 감지되면 비콘 메시지를 수신 할 수 있도록 설정 하였다. 따라서, 무작위 Spoofing attack[7]과 같이 네트워크에 악의적으로 메시지가 전송 된다면, 본문에서 제시된 방법으로 네트워크 트래픽 부하를 줄 일 수 있음을 입증하였다.

2. 결론

많은 네트워크 모델과 가정 아래 DTN 에 관한 연구가 이루어지고 있으며, 현재 라우팅 및 future internet testbed 로서의 연구도 활발히 진행 중이다. 본 논문에서는 DTN Bundle layer 프레임을 통한 효율적인 Queue 관리 방법에 관해서 제시 하였으며, 각 노드에서 수신된 고유의 값을 통해 메시지가 수신될 때에 timestamp 값을 조절하여 네트워크 상에서 발생할 수 있는 무작위 flooding attack 에 대하여 대처 할 수 있는 방안에 대하여 제안 하였다.

DTN 에서 보안에 관한 연구는 Delay Tolerant Networking Working Group 의 메일링을 통해서 현재 진행 사항을 확인 할 수 있으며, RFC 문서를 통해 기본적인 요구사항을 확인 할 수 있으며, 무선 환경에서 일어날 수 있는 공격 유형이 유사하게 DTN 에서도 발생할 수 있다. 따라서, 기존 무선 환경에서의 공격 유형 특징을 파악하고 이를 활용하여 대처하는 것이 바람직하다.

ACKNOWLEDGMENT

" 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2010-(C1090-1031-0005)), Dr. CS Hong is corresponding author.

참 고 문 헌

[1] Delay Tolerant Networks (DTNs), A Tutorial, 2003 http://www.dtnrg.org

[2] A. Vahdat and D. Becker, " Epidemic routing for partially connected ad hoc networks", Department of computer Science, Duke University, Durhan, NC, Tech 2000.

[3] Haojin Zhu, Xiaodong Lin, Rongxing Lu, Xuemin Shen, Pin-Han Ho, " BBA: An Efficient Batch Bundle Authentication Scheme for Delay Tolerant Networks", IEEE GLOBECOM. 2008

[4] Farrell, S., Symington, s., and Weiss, H., " Delay-Tolerant Networking Security Overview," Internet draft, draft-irtf-dtnrg-sec-overview, July 2007

[5] K. Scott, " Bundle Protocol Specification", delay tolerant networking reaching group, November 2007

[7] Fai cheong Choo, Mun Choon Chan, Ee-Chien Chang, Dept of Comput. Sci., Nat. Univ. of Singapore " Robustness of DTN against Routing Attacks", Communication System and Networks(COMSNETS) Jan 2010