DTN 네트워크 환경에서 노드간 인증을 통한 신뢰성 있는 메시지 전송 기법

이준*, 홍충선**
경희대학교 컴퓨터 공학과
e-mail: *junlee@networking.khu.ac.kr, **cshong@khu.ac.kr

Reliable Message Delivery Scheme for Delay Tolerant Network Using Inter-Node Authentication

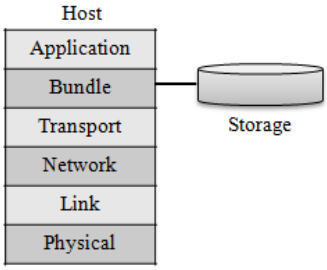
Jun Lee*, Choong Seon Hong**
Department of Computer Engineering, Kyung Hee University

요 약

Delay-Disruption Tolerant Network(DTN)는 store-and-forward를 통한 통신을 기본으로 하며 이러한 통신에 적합한 라우팅 프로토콜 연구가 진행 되고 있다. DTN 라우팅 프로토콜은 불안정한 링크 연결 환경 극복을 위해 스토리지를 이용하여 메시지를 전달한다. 이는 수신한 메시지를 보존하여 전달 할 수 있는 장점이 있지만 스토리지의 특성에 따른 보안 취약점이 존재 한다. 따라서 본 논문에서는 DTN 라우팅 프로토콜의 취약점을 분석하여 가능한 공격 유형을 제시하고 이를 탐지하기위한 메커니즘을 제안하고자 한다.

1. 서론

Delay Tolerant Network(DTN)는 빈번히 발생하는 네트워크 변화로 인해서 상대적으로 긴 전송 지연시간, 불안정한 링크 연결 등으로 종단간 연결이 보장되지 않는다. 이런 DTN의 특성으로 인해서 기존의 TCP/IP 프로토콜이 적용 될 수 없기 때문에 DTN은 종단간 연결성이 보장되지 않는 환경에서의 통신을 위해 store and forward 방식의 메시지 전달을 기본으로 하는 라우팅 방식을 사용하여 목적지 까지 메시지 전달 확률을 높이고 있다[1]. 메시지를 전달 받은 노드가 목적지까지 메시지 전달을 위한 릴레이 노드를 찾지 못한 경우에는 메시지를 저장 하고 이동을 하면서 노드와의 연결이 이루어 질 때 까지 기다리게 된다. 이와 같은 메시지 전달을 위해 DTN 아키텍쳐는 전송 계층 상위에 번들(Bundle) 계층[2]이 추가 되며 이 번들 계층에는 메시지를 저장 할 수 있는 스토리지가 존재 한다. 아래 그림 1 은 메시지 전달을 위한 DTN의 아키텍쳐 이다. 그림 1 과 같은 아키텍쳐를 가지는 DTN 노드는 메시지 저장에 따른 높은 스토리지 오버헤드와 유한한 저장 공간에 따른 메시지 손실 때문에 네트워크 안정성에 대하여 매우 취약 하다[3]. 이와 같은 DTN 네트워크의 특성 때문에 그에 상응하는 유형의 공격들이 등장 할 것이다. 따라서 본 논문에서는 DTN 라우팅 프로토콜의



(그림 1) DTN의 아키텍쳐

특성을 이용하여 시도 될수 있는 공격 유형을 분석하고 공격을 탐지하기 위한 메커니즘을 제안한다. 본 논문의 구성은 다음과 같다 2장에서는 관련 연구를 설명하고 3장에서는 DTN 라우팅 보안 취약점 및 네트워크상에서 가능한 공격 형태를 분석하고, 4장에서는 3장에서 제안한 공격에 대한 탐지 메커니즘을 제안한다. 그리고 5장에서는 Omnet++ 시뮬레이터를 이용하여 검증 하였고 6장에서 결론 및 앞으로 필요한 연구를 설명한다.

2. 관련연구

2.1 DTN 라우팅 프로토콜

DTN 라우팅 프로토콜은 크게 전달기반(forwarding based)프로토콜과 복제기반(replicated)프로토콜로 구분 된다[4]. 전달 기반 프로토콜의 경우 노드간 연결이 이루어 졌을때 상대편 노드가 자신이 전달 하고자 하는 메시지를 가지고 있지 않을 경우에만 메시지를 전달 한다. 이는 목적지까지 전달하고자 하는 메시지를 네트워크 상에 한 개

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

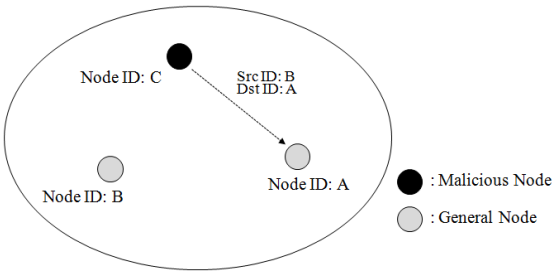
만 유지 될 수 있도록 하여 목적지까지의 메시지 도달 확률은 낮지만 노드의 에너지, 스토리지 공간, 네트워크 대역폭 소비와 같은 네트워크 자원의 소비 측면에서는 높은 효율을 보인다. Scale Free Routing, Seek and Focus 이 대표적인 전달 기반 라우팅 프로토콜들 이다. 복제기반 프로토콜의 경우 노드간 연결이 이루어 졌을때 상대편 노드가 전달하고자 하는 메시지를 이미 가지고 있을 경우에도 메시지를 복제하여 전달한다. 이는 목적지까지 전달하고자 하는 메시지를 네트워크상에 가능한 많이 존재 하도록 하여 목적지까지 전달 확률을 높이는 것이다. 메시지 전달 확률은 높지만 네트워크 자원의 소비 측면에서는 비효율적이다. Epidemic 라우팅 프로토콜과 Spray and Wait 라우팅 프로토콜이 대표적인 복제기반 라우팅 프로토콜들이다.

3. DTN 라우팅 보안 취약점 및 공격 유형 분석

3.1 DTN 라우팅 보안 취약점

DTN 라우팅 프로토콜은 주로 버퍼에 저장하고 전달하는 방식을 기본으로 하고 각 노드의 메시지 저장 공간은 한정 되어 있기 때문에 이는 악의적인 공격에 이용 될 수 있다. 앞에서 설명한 바와 같이 복제기반의 라우팅 프로토콜의 경우 메시지의 전달 확률은 네트워크상에 존재하는 유효한 메시지의 수에 비례한다고 볼 수 있다.하지만 악의적인 노드가 상당량의 위조된 메시지를 일반적인 노드에게 전송 한다면 일반적인 노드의 버퍼는 위조된 메시지들로 꽉차서 더 이상 메시지를 수신 할 수 없거나 Tail drop 방식을 사용하는 기존의 버퍼관리 특성상 유효한 메시지들이 삭제되어 전체적으로 유효한 메시지의 수가 감소하여 메시지의 전달 확률을 낮추는 결과를 가져 온다.

3.2 공격 유형 분석



(그림 2) Spoofing에 의한 flooding 공격

위 그림 2는 Spoofing에 의한 flooding 공격의 한 예이다. 공격 노드는 자신의 ID를 네트워크에 존재하는 다른 노드로 위장하여 공격 대상에게 위조된 메시지를 연속적으로 보내 공격 대상의 버퍼를 채우게 된다.또한 버퍼에 있는 메시지들은 다른 노드에게 전달되어 네트워크 전체에 영향을 미치게 된다.이와 같은 스푸핑 형태의 공격은 공격 노드를 추적 하거나 위조된 메시지의 탐지가 어렵기 때문에 적합한 대처법 연구가 필요 하다.

4. 제안하는 메커니즘

본 논문에서는 제안하는 메커니즘은 다음과 같은 환경을 가정한다.

- 네트워크를 구성하는 노드의 수는 항상 고정이다.
- 노드는 지정된 영역 만을 자유롭게 이동 한다.

DTN 네트워크에서 Spoofing에 의한 flooding 공격에 대한 탐지를 위해서는 인증 되지 않은 메시지에 대한 정의와 공격이 의심되는 메시지를 처리하기위한 시스템 구조가 필요하다. 네트워크를 구성하는 노드들은 처음 연결이 생성 되었을 때 상대편 노드를 인증하는 인증정보를 교환하게 되고 그다음에 연결이 생성 되었을 경우에는 기존에 교환한 인증 정보를 검사하여 인증 정보가 불일치 하는 노드는 공격이 의심되는 노드로 판단하여 수신되는 메시지는 낮은 우선순위를 갖게 하여 메시지 저장 스토리지가 찼을 경우 우선적으로 삭제 되도록 한다.

4.1 노드간 인증

본 논문에서는 각 노드가 이동중에 연결된 노드들의 인증 정보를 생성하여 저장하는 방법을 통해서 각 노드를 인증하는 방식을 제안한다. 노드의 인증 정보는 스마트 카드나 휴대폰등과 같이 작은 메모리를 가지고 있는 시스템에 적합한 ECC(Eliptic Curve Crypto)공개 암호시스템[5]을 이용하여 인증 정보를 생성한다.

<표 1> 노드간 인증 및 세션을 형성하는 과정

Node A		*Node B*
$KeyPair(d_A, Q_A)$		$KeyPair(d_B, Q_B)$
$d_A : A's\,PrivateKey$	$Connection$	$d_B : B's\,PrivateKey$
$Q_A = d_A G$ $(A's\,PublicKey)$	$G: (generator)$	$Q_B = d_B G$ $(B's\,PublicKey)$
	$Send\,Q_A\,to\,Node\,B$	$Q_s = d_B Q_A (session\,key)$
$Q_s = d_A Q_B (session\,key)$	$Send\,Q_B\,to\,Node\,A$	
$Q_s(x_s, y_s) = d_A d_B G$		$Q_s(x_s, y_s) = d_A d_B G$
$S_A = k^{-1}(h + d_A x_s)(\mathrm{mod} n)$ $h = SHA^{-1}(ID_A)$	$select\,a\,random\,number\,k$	$S_B = k^{-1}(h + d_B x_s)(\mathrm{mod} n)$ $h = SHA^{-1}(ID_B)$
	$Send\,S_A, ID_A\,to\,Node\,B$	$store\,S_A$ and ID_A
$store\,S_B$ and ID_B	$Send\,S_B, ID_B\,to\,Node\,A$	

위 표 1 은 최초로 연결이 생성된 노드 사이에 인증 및 세션을 형성하는 과정이다. 각 노드들은 사전에 정의되어진 비밀키를 가지고 있으며 노드간 연결이 이루어 졌을 경우에 generator 에 의해서 기준점 G를 생성한다. 각 노드는 비밀키와 기준점 G를 이용하여 각 노드는 공개키

Q_A, Q_B를 생성한다. 생성된 공개키를 상대편 노드에게 전송하여 세션을 위한 Q_s를 생성한다. 세션키 Q_s와 각 노드의 고유 ID를 이용하여 상대편 노드와의 연결을 인증하는 $Signature$ S_A, S_B를 생성하고 서로 교환하여 저장 한다.

<표 2> 노드에 저장된 인증 정보

$Table\ of\ Node\ A$		
$Node\ ID$	$Signature$	$Session\ Key$
ID_B	S_B	Q_S

위 표2 는 연결이 생성된 노드들의 정보를 저장하는 테이블의 구조이다. $Node\ ID$는 상대편 노드의 고유한 ID를, $signature$는 상대편 노드로부터 수신한 각 노드의 인증 정보를, $Session\ Key$는 연결된 노드사이에 생성된 비밀키를 의미한다. 테이블에 존재하는 노드와 연결이 생성될 경우에는 $Signature$값과 Q_s를 이용하여 처음으로 연결이 생성된 노드인지 확인한다. 확인 과정은 아래 표 3 과 같다.

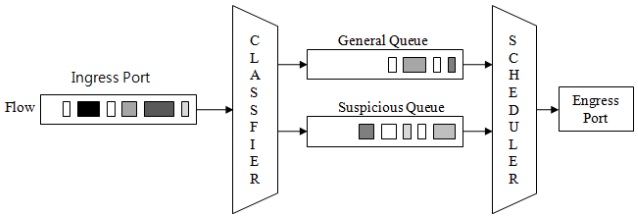
<표 3> 메시지 수신을 위한 노드 확인 과정

$Node\ A$	$Node\ B$
• $Receive$	• $Sender$
$Search\ on\ the\ Table$: $Session\ Key\ Q_s(x_s, y_s)$	$Search\ on\ the\ Table$: $S_A(Signature\ of\ S_A)$
$Send\ S_A\ to\ Node\ A$	
$Verify\ the\ S_A$	
$w = S_A^{-1}(\mathrm{mod}n)$ $u_1 = h \times w(\mathrm{mod}n)$ $u_2 = x_s \times w(\mathrm{mod}n)$	
$X = u_1 G + u_2 G$ $X = (x, y)$	
$\mathrm{if}(x_s == x)$ $then\ input\ message$ $to\ General\ Queue$	
$else\ \mathrm{if}(x_s \neq x)$ $then\ input\ message$ $to\ Suspicious\ Queue$	

전달할 메시지가 있는 노드B는 노드A로부터 얻은 인증정보 S_A를 노드A에게 전송하고 노드A는 두 노드사이에 생성된 Q_s를 이용하여 이를 확인 한다. 인증이 성공하면 이를 General Queue에 저장하고 만약 인증이 실패 하면 이를 Suspicious Queue에 저장한다. 이는 처음에 연결이 생성된 노드가 아닌 스푸핑 공격으로 인한 다른 노드로부터 수신한 메시지일 가능성이 크기 때문에 정상적인 메시지와 구분하기 위함 이다.

4.2 버퍼 관리 시스템 구조

DTN의 불안정한 연결성 때문에 각 노드에는 메시지 위의 그림 3과 같은 노드 인증 절차에 따라서 정상적인 메시지는 General Queue에 저장하고 공격이 의심되는 메



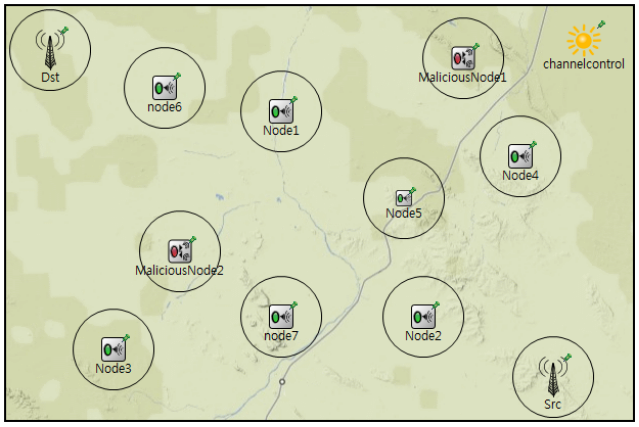
(그림 3) 메시지 관리를 위한 버퍼 시스템 구조

시지들은 Suspicious Queue에 저장한다. Suspicious Queue에 저장 되어진 메시지들은 버퍼안의 Scheduler에 의해서 General Queue에 저장 되어진 패킷보다 낮은 우선순위를 갖게 한다. 따라서 서비스 시에는 정상적인 메시지들 보다 나중에 전송되고 버퍼가 찼을 경우에는 우선적으로 삭제 되도록 하여 네트워크로 인증되지 않은 메시지가 전파되는 확률을 낮춘다.

5. 성능평가

5.1 시뮬레이션 환경 구성

본 챕터에서는 제안하는 메커니즘에 대한 성능 평가를 위해 네트워크 시뮬레이터인 Omnet++[6]를 이용하여 진행 하였다. DTN 특성을 가지는 노드들을 구현하였고 각 노드들을 배치하여 아래 그림 4 와 같은 실험 환경을 구축 하였다.



(그림 4) 실험을 위한 환경 구성

아래 표 4, 표 5의 실험 환경을 바탕으로 출발지(Src)에서 전송된 메시지가 목적지(Dst)까지 도달한 개수를 측정하여 현재의 메커니즘과 본 논문에서 제안하는 메커니즘을 비교 분석 하였다.

<표 4>

Parameters for Simulation	
Area Size (m)	4000 x 3000
Number of Nodes	7 ~ 10
Number of Malicious Nodes	2 ~ 4

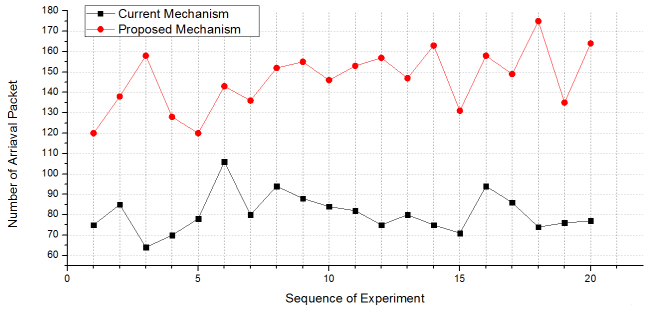
<표 5>

Parameters for Nodes	
Mobility Type	Random way point
Mobility Speed (m/s)	4 ~ 15
Frequency (2.4GHz)	2.4
Data rate (Mbps)	19 ~ 54
Buffer Size(MB)	50
Transmission Range (m)	10
Routing Protocol	Epidemic Routing

네트워크를 구성하는 노드들은 지정된 구간을 이동 패턴에 따라서 움직이게 된다. 이때 각 노드들은 다른 노드에 인접 했을 때 서로의 Transmission Range 안에 들어오게 되면 메시지 교환을 시도한다. Malicious Node 들은 지정된 구간을 이동하면서 네트워크를 구성 하는 노드들의 ID로 위장하여 다량의 메시지를 연결이 생성된 노드에게 전송한다.

5.3 Omnet++ 시뮬레이터를 이용한 성능평가

시뮬레이션을 통해 다음과 같은 결과를 얻었다.
아래 그림 5는 출발지에서 연속으로 일정량의 패킷을 전송할 때 현재의 메커니즘과 본 논문에서 제안하는 메커니즘을 이용했을 때 목적지에 도착하는 패킷의 수를 비교한 그래프 이다.



(그림 5) 목적지에 도달하는 패킷의 수

반복적인 실험을 통하여 목적지에 도달하는 패킷의 수를 비교해 봤을 때 Malicious 노드의 스푸핑에 의한 Flooding 공격에도 불구하고 본 논문에서 제안하는 메커니즘을 적용한 노드들은 상대적으로 높은 메시지 전달 확률을 보이는 것을 알 수 있다.

6. 결론 및 향후 계획

본 논문에서는 DTN 라우팅 프로토콜의 취약점을 분석하고 발생 가능한 공격과 그 탐지 메커니즘을 설명하고 제안 하였다. 본 논문의 제안사항을 사용 할 경우 Malicious 노드의 공격에도 불구하고 해당 메시지의 목적지까지의 전송률을 향상 시켰다. 하지만 본 논문에서 노드가 네트워크 간 이동이 없는 지정된 네트워크 영역만을 움직이는 것을 가정 하였다. 이동성을 갖는 노드의 특성상 노드가 다른 영역으로 이동 할 경우를 고려할 필요성이 있다. 따라서 네트워크 간 이동이 있을 경우에 어떻게 노드를 인증하고 노드에서 수신한 메시지를 효율적으로 분석하여 공격을 탐지 하는 메커니즘과 실제 시스템에 적용될 수 있는지 판단하며, 이러한 관점에서의 향후 연구가 진행 되어야 할 것이다.

참고문헌

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

[2] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss."Delay tolerant network architecture, draft-irtf-dtnrg-arch-02.txt", July 2004

[3] Samuel, H, Weihua Zhuang. "Preventing Unauthorized Messages in DTN Based Mobile Ad Hoc Networks", Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE

[4] Thrasyvoulos Spyropoulos, Konstantinos Psounis Cauligi S. Raghavendra. "Spray and wait: an efficient routing scheme for intermittently connected mobile networks", Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking

[5] Eun-Jun Yoon, Kee-Young Yoo. "ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC", Computational Science and Engineering, 2009. CSE '09. International Conference on

[6] OMNET++, http://www.omnetpp.org