

링크 에러 모델링을 이용한 MANET 환경에서의 IPv6 자동주소 설정 방식의 확장성 분석

(Scalability Analysis of MANET IPv6 Address Auto-configuration Protocols based on Link Error Modeling)

김 상 철 [†]

(Sang-chul Kim)

요 약 본 논문에서는 무선 노드의 이동성에 따른 링크 에러로 인한 *Mobile Ad hoc Network (MANET) IP* 자동 네트워크 프로토콜(*Address Autoconfiguration Protocol: AAP*)의 메시지 복잡도를 분석하고자 한다. 링크 에러로 인해 목적지까지 전달되지 못한 메시지는 재전송되어야 하고, 이러한 재전송 횟수 (S)를 링크 에러 확률 (P_e)에 따라 계산하는 알고리즘을 제안하였다. 또한, O -표기법에 따라 N 개의 노드에 의해 발생된 메시지의 *Upper Bound*를 각 *AAP*에서 유도하였다. 본 연구에서 검토된 *AAP*는 *Strong Duplicate Address Detection (DAD)*, *Weak DAD with proactive routing protocol (WDP)*, *Weak DAD with on-demand routing protocol (WDO)*, *MANETconf*이다. 컴퓨터 기반 시뮬레이션에서, 제안된 알고리즘에 의해 링크 에러가 있을 때, 각 *AAP*의 성능을 분석해본 결과, *WDP*가 가장 낮은 메시지 복잡도를 가졌고, *MANETconf*가 가장 높은 메시지 복잡도를 보였다.

키워드 : IP 자동 네트워크 프로토콜, 메시지 복잡도, 이동성 특별 네트워크, 링크에러, 성능분석

Abstract This paper focuses on message complexity performance analysis of *MANET AAPs* in reference to link errors generated by the mobile wireless nodes. To obtain the message complexity performance of *AAPs* in reference to the link error probability (P_e), an enhancement was made by proposing the retransmission limit (S) to be computed for error recovery (based on the link error probability), and then for each of the *AAPs* the control procedures for the retransmission limit have been properly included. The O -notation has been applied in analyzing the upper bound of the number of messages generated by a *MANET* group of N nodes. Based on a link error probability range of $P_e = 0$ to 0.8 , the *AAPs* investigated in this paper are *Strong DAD*, *Weak DAD with proactive routing protocol (WDP)*, *Weak DAD with on-demand routing protocol (WDO)*, and *MANETconf*. Based on the simulation results and analysis of the message complexity, for nominal situations, the message complexity of *WDP* was lowest, closely followed by *WDO*. The message complexity of *MANETconf* is higher than that of *WDO*, and *Strong DAD* results to be most complex among the four *AAPs*.

Key words : IP Address Autoconfiguration Protocol, Message Complexity, Mobile Ad hoc Network, Link Error, Performance Analysis

· 이 논문은 2008년도 서울시 산학연 협력사업의 지원을 받아 연구되었음

[†] 정 회 원 : 국민대학교 컴퓨터공학부 교수
sckim7@kookmin.ac.kr

논문접수 : 2008년 1월 16일

심사완료 : 2008년 5월 21일

Copyright © 2008 한국정보과학회 : 개인 목적이나 교육 목적인 경우, 이 작품의 전체 또는 일부에 대한 복사본 혹은 디지털 사본의 제작을 허가합니다. 이 때, 사본은 상업적 수단으로 사용할 수 없으며 첫 페이지에 본 문구와 출처를 반드시 명시해야 합니다. 이 외의 목적으로 복제, 배포, 출판, 전송 등 모든 유형의 사용행위를 하는 경우에 대하여는 사전에 허가를 얻고 비용을 지불해야 합니다.

정보과학회논문지: 정보통신 제35권 제4호(2008.8)

1. 서 론

포터블 컴퓨팅 및 무선 네트워크 기술의 급속한 발전에 따라서, 무선 통신은 셀룰러 네트워크(Cellular Network, 2G/2.5G/3G), Wireless Local Area Network(LAN, IEEE 802.11), Wireless Personal Area Network(PAN, IEEE 802.15) 및 Wireless Metropolitan Area Network(MAN, IEEE 802.16) 등과 같은 다양한 무선 네트워크 기반 시설에 적용되어 왔다. 무선 애드혹 네트워크는 무선 통신 기술을 이용하여 어디서나 그리고 어느 때나 구성될 수 있고 다수의 이동 가능한 노드들로 구

성되며, 네트워크 토폴로지는 노드의 이동성에 따라 달라진다. 따라서, 노드 이동성을 실시간으로 파악하는 네트워크 토폴로지 기술은 라우팅 프로토콜의 성능에 많은 영향을 끼친다. MANET는 자가-구성(self-organizing) 무선 네트워크이며, 이동 노드들은 베이스 스테이션(base station) 또는 액세스 포인트(access point)와 같은 고정 통신 기반 시설이 없이도 다중 홉(multi-hop) 무선 링크를 통해 서로 통신하기 위해 패킷을 전송할 수 있는 라우팅 성능을 가지고 있다. MANET 노드들은 경로를 통해 목적지 노드에 데이터 패킷을 직접 전송한다. 따라서, 노드들은 모든 노드들에 대한 최신 라우팅 테이블을 가지거나(proactive approach) 요청이 있는 경우(on-demand approach) 즉시 경로를 찾아야 할 필요가 있다[1]. 또한, MANET 내에서 데이터 패킷의 적절한 라우팅을 위해 모든 노드들은 유일한 주소 구성에 필요한 작업을 수행할 수 있어야 한다. MANET에서는 주소의 사전 구성(pre-configuration)이 항상 가능한 것은 아니므로, 주소의 자동 구성(auto-configuration)은 MANET에서의 중요한 이슈이다.

또한, 노드 이동성에 기인한 링크 실패율은 애드혹 네트워크의 라우팅에 있어서 주요한 관심사이다[2]. MANET 노드들은 라우팅 프로토콜을 수행하면서 동시에 이동 시나리오에 따라 이동한다. 따라서, 이동 패턴 및 이동성-기초 프레임워크에 대한 연구가 많은 연구자들에 의해 수행되고 있다. Alparslan의 다수 [3]는, 일반화된 랜덤 이동 모델을 제안하였고, 종래의 무선 애드혹 모델용 이동 모델을 분류하였으며, 이동 프로파일에서 사용된 가정을 요약하였다. 또한, 랜덤 이동 모델이 성능 평가용으로 적당하다고 지적하였는데, 여기서 이동 모델이란 랜덤 프로세스에 기인한 노드들의 이동을 의미한다. 랜덤 이동 모델은 이동 에포크(movement epoch)로 불리는 연속적인 랜덤한 길이 구간으로 이동 호스트의 이동 패턴을 설명한다. 각 에포크의 속도와 방향은 이전 에포크 값과 서로 관련될 수 있거나 관련되지 않을 수 있다.

Random Waypoint Model(RWP)은 MANET 라우팅 알고리즘의 성능을 분석적으로 측정하기 위해 광범위하게 사용되는 랜덤 이동 모델들 중의 하나로[4], 노드의 상대 이동성을 정의하기 위해 remoteness 함수가 사용된다[5]. 위상 변화에 따른 far-reaching effects를 감소시키기 위해, [6]의 저자들은 클러스터 위상 구조 알고리즘을 제안하였다.

Amid의 다수는, 라우팅 알고리즘을 평가하기 위해, 시뮬레이션에 사용된 현 이동 모델을 조사하였고, 패킷 전송률, 제어 오버헤드 및 데이터 패킷 지연 등과 같은 애드혹 라우팅 알고리즘 성능이 이동 모델에 의해 지대

한 영향을 받는다는 점을 기술하였다. 또한, 그들은 현 이동 모델이 실제 이동을 시뮬레이션 하는데 있어서 완벽한 것이 아니라고 주장하였다[7]. 이러한 연구 결과를 바탕으로 본 논문에서는 수학적 동적 링크 에러 표현을 이용하여, MANET내에서의 노드 이동성에 기인한 피어-투-피어(peer-to-peer) 무선 링크 연결의 링크 단절을 모델링 하는 기법을 제안하고자 한다.

2. 복잡도 분석

데이터 패킷을 라우팅하기 위한 선결조건은 각 이동 단말이 유일한 IP 주소를 가지게 하는 것이며, 이러한 동작을 하게 하는 프로토콜이 MANET 자동 네트워킹 프로토콜이다. 이 프로토콜은 IP 주소 할당을 다른 외부 인터넷 서버의 도움 없이 자체적으로 할당하는 프로토콜이다. MANET에서는 단말의 이동성(mobility)과 무선통신 채널(wireless channel)의 제한된 대역폭 때문에 항상 자동 네트워킹이 지원되는 것은 아니다. 따라서, MANET에서의 원활한 자동 네트워킹 기술은 현재 중요한 연구 항목으로 대두되고 있다.

종래의 자동 네트워킹 기술은 stateless 접근과 stateful 접근방식으로 분류될 수 있다. Stateless 접근은 IP 주소가 유일하고 라우터블(routable)해야 되지만 정확한 IP 주소 할당이 네트워크에 요구되지 않을 때 사용된다. Stateful 접근은 정확한 IP 주소 할당을 네트워크가 요구할 때 사용된다. Dynamic host configuration 프로토콜(DHCP)는 DHCP 서버가 유일한 주소를 이동단말에 할당하고, 할당된 주소 정보를 DHCP 서버의 주소 할당 테이블에 보관하여 두는 stateful 프로토콜의 한 예이다.

Stateless 프로토콜에서는 DAD 알고리즘을 채택하여 이동단말 스스로 IP 주소를 선택하고, 선택된 IP 주소를 네트워크에 배포함으로써, 주소의 유일성 및 정확성을 검증하도록 한다. 따라서, DAD 알고리즘 사용으로 스스로 선택한 후보 IP 주소가 사용가능한지를 결정할 수 있다. 또한, 이미 IP 주소를 사용하고 있는 단말은 또 다른 단말이 자신의 IP 주소를 중복 사용하는 것을 막기 위해 DAD 알고리즘이 사용한다.

DAD 알고리즘은 Strong DAD[8]와 Weak DAD[9]로 분류된다. Strong DAD는 단말이 임의적으로 한 개의 IP 주소를 선택하고, 이 선택된 주소가 MANET에서 사용되는지를 조사하는 중복 주소 발견(duplicate address detection) 메커니즘을 사용한다. 만약, 단말이 IP 주소가 중복여부를 묻는 요청(request) 메시지에 대한 응답으로 응답(reply) 메시지를 일정 시간 안에 받으면, 이동단말은 자신이 선택한 IP 주소가 중복되었음을 발견할 수 있다.

Weak DAD는 Strong DAD에서 사용하는 중복 주소 발견 메커니즘을 사용하며, 라우팅 프로토콜 패킷 형태를 변경하여 IP 주소가 중복되는지를 확인한다.

MANET은 그래프 $G(V, E)$ 로서 표현되며, 여기서 V 는 유한하며 공집합이 아닌 노드 집합이며 이는 $V = \{V_1^G, V_2^G, \dots, V_W^G\}$ 로 표현될 수 있고 $|V|=W$ 이며, E 는 링크를 형성하는 V 로부터의 별개 노드 쌍의 집합이며 이는 $E = \{E_1^G, E_2^G, \dots, E_w^G\}$ 로 표현될 수 있다[10].

Strong DAD, Weak DAD, MANETconf [11]에 사용된 메시지 및 중요 변수들을 표 1에 나타내었다. AAP에서 각 이동단말은 엄격하게 일련의 단계(step)의 연속인 절차(procedure)를 따른다. 각 단계는 이동단말이 메시지를 발생해야 하는 상황인지 일반적인 결정을 할 수 있도록 하여 준다. 또한, 각 단계는 이동단말이 같은 절차를 다시 반복(recursive 절차라고 불린다) 해야 하는지 아니면, 다른 절차를 시작해야 되는지 또는 현재 단계를 수행 후 동작을 멈추는지 등에 관한 결정을 할 수 있도록 인도한다.

정의 1. MANET $P(V, E)$ 에서, 시도(trial)는, 노드에 의한 Address Query(예를 들어, Strong DAD에서의 AQ메시지, Weak DAD에서의 IQ메시지, 또는 MANETconf에서의 IQ메시지)의 브로드캐스팅으로 정의된다.

1. 성공 시도(success trial)는, 노드가 Address Query 메시지를 브로드캐스트한 후 특정 시간 구간 내에 어떠한 Address Reply 메시지(예를 들면, Strong DAD에서의 AP메시지, Weak DAD에서의 AE메시지, 또는 MANETconf에서의 negative IR메시지)도 받지 못한 이벤트로서 정의된다.
2. 실패 시도(failure trial)는, 노드가 Address Query 메시지를 브로드캐스트한 후 특정 시간 구간 내에 적어도 하나의 Address Reply 메시지를 받는 이벤트로서 정의된다.
3. 성공된 IP 인증 절차(successful IP verification procedure)는 m 번의 연속 성공 시도로부터 정의된다.

- A. 따라서, 노드는 확인된 IP 주소를 얻기 위해 m 개의 독립 시도를 연속적으로 수행해야 하며, 여기서 각 시도는 성공 시도 이어야 한다.
 - B. Strong DAD에서, m 은 1보다 큰 양수로 정의된다($m > 1$).
 - C. Weak DAD 및 MANETconf에서, m 이 1로 설정되기 때문에($m=1$), 성공된 IP 인증 절차는 성공 시도와 동일하다.
4. IP 인증 절차가 실패 시도를 포함함으로써 실패 IP 인증 절차(failure IP verification procedure)가 발생된다.
 - A. Strong DAD에서, 실패 IP 인증 절차는 $x-1$ 개의 연속 성공 시도와 x 번째 시도에서의 실패 시도로 구성된다(여기서 $x=1, 2, \dots, m$).
 - B. Weak DAD 및 MANETconf에서, m 이 1로 설정되기 때문에($m=1$), 성공된 IP 인증 절차는 성공 시도와 동일하다.
 5. 세션은 성공 또는 실패 절차의 연속(sequence)으로서 정의된다. 세션에서 수행된 절차의 최대 개수는 Strong DAD, Weak DAD 및 MANETconf에서의 n 으로 제한된다.
 - A. Strong DAD의 상한을 계산하는 경우, 성공한 세션의 최악의 케이스는 $n-1$ 개의 연속 실패 IP 인증 절차와 n 번째 IP 인증 절차에서의 성공된 IP 인증 절차로 구성된다. 실패 세션은 n 개의 실패 IP 인증 절차로 구성된다.
 - Weak DAD 및 MANETconf의 상한을 계산하는 경우, 성공한 세션의 최악의 케이스는 $n-1$ 개의 연속 실패 시도와 n 번째 IP 인증 절차에서의 성공 시도로 구성된다. 실패 세션은 n 개의 실패 시도로 구성된다.
- 본 논문에서, Address Query 메시지는 일반적인 플러딩 방법으로 브로드캐스트되며 상기 방법에서 모든 노드는 Address Query 메시지의 첫 번째 복사본을 받을 때마다 Address Request 메시지를 그 노드의 전체

표 1 메시지 및 중요 변수 [*: 논문에 사용된 변수 이름]

메시지	역할	메시지	역할
AB	Abort	LS	Link State
AC	Address Cleanup	NR	Neighbor Reply
AD	Advertised	NQ	Neighbor Query
AE	Address Error	RR	Route Reply
AL	Allocated	RQ	Route Request
AO	Allocation	RT	Requester Request
AP	Address Reply	m^*	DAD retry count limit
AQ	Address Request	n^*	retry count limit
IR	Initiator Reply	S^*	retransmission count limit
IQ	Initiator Request	P_e^*	probability of link error

one-hop 이웃 노드로 재전송한다 [12]. MANET의 각 멤버 노드는 임의의 노드 V_i 에서 최초로 전송된 Address Query 메시지를 중계하기 때문에, 중복 패킷 폐기 기법 (Duplicated Packet Discard Scheme)이 적용되면, Address Query 메시지를 중계하는 최대 노드 개수는 $N-1$ 개이다. 따라서, 트리 내에서 브로드캐스트되거나 중계된 Address Query 메시지의 최대 개수는 N 개이며, 이는 완전한 무선 채널(perfect wireless channel)인 경우 $O(N)$ 으로 표시될 수 있고, 이는 MANET 내에서 링크 에러가 없음을 의미한다.

MANET 내에서의 노드 이동성에 기인한 피어-투-피어 무선 링크 연결의 링크 단절을 표시하기 위해, 본 논문은 노드 이동성의 효과를 라우팅 알고리즘으로 표현하기 위해 링크 에러 확률(P_e)이라는 수학적 표현을 도입하였다.

MANET의 링크 에러 확률이 P_e 인 경우, 식 (1)에서 정의된 변수 S (재전송 횟수)는 Address Query 메시지를 다시 브로드캐스팅하거나 Address Reply 메시지를 다시 유니캐스팅하는 평균 개수를 산정하는 하나의 해법이 된다. 링크 에러는 AQ메시지를 이웃 노드로 처음 전송하거나 중계하는 노드로부터의 AQ메시지 전송을 중단시키기 때문에, 노드는 AQ메시지를 이웃 노드로 전달하기 위해 AQ메시지를 브로드캐스트하기 위해 재시도 한다. 노드는 하부 계층으로부터의 부정 응답(passive acknowledgment)을 이용함으로써 전송이 중단되었음을 알 수 있다. 중간 노드에서의 재전송 횟수의 평균값은 아래와 같이 정의된 S 로 표현된다.

$$S = \frac{1}{1 - P_e}, \quad 0 \leq P_e < 1 \quad (1)$$

MAC(Medium Access Control) 또는 물리적 계층과 같은 하부 계층으로부터 링크 에러 확률값(P_e)이 통지된 경우, 네트워크 계층은 제안된 알고리즘의 메시지 복잡도의 상한을 산정하기 위해 S 를 사용할 수 있다. 따라서, MANET의 링크 에러 확률이 P_e 로 알려진 경우, MANET에서 브로드캐스트되거나 중계된 Address Query 메시지의 최대 개수는 $SO(N)$ 로 표현될 수 있다. 상기 내용은 아래 정의로 일반화될 수 있다.

정의 2. N 개의 노드를 가진 MANET에서, $SO(N)$ 은, 링크 에러 확률이 고려되는 조건에서 Address Query 메시지가 브로드캐스트될 때, 브로드캐스트되거나 중계된 Address Query 메시지의 최대 개수의 상한이다.

보조정의 1. 최대 길이 경로에서 t 개의 노드를 가진 MANET 라우팅 트리에서, $SO(t)$ 는, 링크 에러 확률이 고려된 조건에서 노드가 Address Reply 메시지를 유니캐스트할 때, 유니캐스트되거나 중계된 Address Reply 메시지의 최대 개수의 상한이다.

증명. $d(j, i)$ hop 경로의 각 멤버 노드는 Address Reply 메시지를 중계하기 때문에, Address Reply 메시지를 중계하는 노드의 최대 개수는 $t-2$ 이며, 이때 중복 메시지 폐기 규칙이 노드에 적용되면 노드 V_i 는 Address Reply 메시지를 중계하지 않는다. 따라서, 트리 내에서 유니캐스트되거나 중계된 Address Reply 메시지의 최대 개수는 $t-1$ 이며, 무선 채널이 완벽할 경우, 메시지 복잡도 한계는 $O(t)$ 로 표현될 수 있다. 링크 에러 확률이 고려되는 경우, 재전송 횟수 S 가 $O(t)$ 의 앞에 곱해진다. □

2.1 Strong DAD

Strong DAD 프로토콜의 메시지 복잡도의 상한을 유도하기 위해, 그림 1에 도시된 바와 같은 Strong DAD의 의사 코드가 사용된다.

메시지 복잡도의 상한을 계산하기 위해, 노드가 실패 IP 인증 절차를 경험하는 시나리오가 고려된다. 상기 절차는 총 $(m-1)$ 개의 성공 시도와 m 번째 시도에서의 실패 시도로 구성되기 때문에, 실패 IP 인증 절차의 메시지 복잡도는 $S(mO(N)+O(t))$ 로 표현될 수 있다. 상기 결과에 기초하여, 아래의 보조정의가 주어진다.

보조정의 2. IP 주소 확인 절차에서, $S(mO(N)+O(t))$ 는, 노드가 Strong DAD 프로토콜을 가진 MANET에서 IP 주소를 확인한 필요가 있는 경우 브로드캐스트된/중계된 AQ메시지 및 유니캐스트된/중계된 AP메시지의 최대 개수의 상한이다.

증명. m 번째 시도에서 실패 시도를 포함한 IP 인증 절차는, 정의 2에 기초한 브로드캐스트되거나 중계된 AQ메시지가 $S(m-1)O(N)$ 개임을 나타내는 $m-1$ 개의 성공 시도와, 정의 2에 기초한 브로드캐스트되거나 중계된 AQ메시지가 $SO(N)$ 개인 것과 보조정의 1에 기초한 브로드캐스트되거나 중계된 AP메시지가 $SO(t)$ 개임을 나타내는 m 번째 시도에서의 실패 시도로 구성된다. 따라서, 실패 IP 인증 절차의 메시지 복잡도는 $S(m-1)O(N)+SO(N)+SO(t)$ 로 표현될 수 있고, 이는 $m-1$ 개의 성공 시도와 m 번째 시도에서의 실패 시도에서 브로드캐스트되고, 유니캐스트되고, 중계된 AQ 및 AP메시지의 최대 개수의 상한을 합한 것이다. $S(m-1)O(N)+SO(N)+SO(t)$ 를 재배열하면 $S(mO(N)+O(t))$ 가 된다. □

보조정의 3. Session에서, $nS(mO(N)+O(t))$ 는 Strong DAD 프로토콜을 사용하여 브로드캐스트된/중계된 AQ 메시지 및 유니캐스트된/중계된 AP메시지의 최대 개수의 상한이다.

증명. Strong DAD의 세션에서의 IP 인증 절차의 최대 재시도 횟수는 n 으로 제한된다. 즉, Session은 최대 개수가 n 인 IP 인증 절차로 구성되고, IP 인증 절차의 최대 개수의 상한이 보조정의 2에 따라 $S(mO(N)+O(t))$

```

Start
Step 01: A node selects a temporary address
        and configures it as its network interface address
Step 02:  $n=0$ ; (Set retry count ( $n$ ) =0)
Step 03:  $m=0$ ; (Set DAD retry count ( $m$ ) = 0 )
Step 04:  $n++$ ; (Increase the retry count ( $n$ ) by 1)
Step 05:  $m++$ ; (Increase the DAD retry count ( $m$ ) by 1)
Step 06: The node randomly selects a source IP address
        and makes an AQ message for the IP address
Step 07: The node broadcasts the AQ
Step 08: if (all MANET nodes receive the AQ in the situation
        that there might be link errors in a MANET == TRUE)
Step 09:   if (an AP arrives to the node before timer expires
        in the situation that there might be link errors in a MANET == TRUE)
Step 10:     if ((retry count <=  $n$ ) == TRUE)
Step 11:       goto Step 4;
Step 12:     else (the corresponding if is in if in Step 10)
Step 13:       goto Step 21;
Step 14:   else (the corresponding if is the if in Step 9)
Step 15:     if ((DAD retry count <=  $m$ ) == TRUE)
Step 16:       The node replaces the source IP address with its IP address
        break;
Step 17:     else (the corresponding if is the if in Step 15)
Step 18:       goto Step 5;
Step 19:   else (the corresponding if is in if in Step 8)
Step 20:     goto Step 7;
Step 21: The node fails to get a source IP address
End

```

그림 1 Strong DAD AAP 동작을 나타내는 의사 코드

로 나타남에 따라 세션의 메시지 복잡도는 $nS(mO(N)+$

2.2 Weak DAD

Weak DAD 프로토콜의 메시지 복잡도의 상한을 유
□ 도하기 위해, 그림 2에 도시된 바와 같은 Weak DAD
의 의사 코드가 사용된다.

```

Start
Step 01: A node selects a temporary address
        and configures it as its network interface address
Step 02:  $n=0$ ; (Set retry count ( $n$ ) =0)
Step 03:  $n++$ ; (increase the retry count ( $n$ ) by 1)
Step 04: The node randomly selects a source IP address and picks a
        unique key value (e.g., MAC address) as the identification of the node;
Step 05: if (Proactive routing protocol is used == TRUE)
Step 06:   The node broadcasts a LS periodically
Step 07:   if (all MANET nodes receive the LS in the situation
        that there might be link errors in a MANET == TRUE)
Step 08:     if (the node receives an AE for the selected IP address
        in the situation that there might be link errors in a MANET == TRUE)
Step 09:       if (retry count <=  $n$ )
Step 10:         Goto Step 3;
Step 11:       else
Step 12:         The node fails to get a source IP address, goto End
Step 13:     else
Step 14:       The node replaces the source IP address with its IP address, goto End
Step 15:   else
Step 16:     goto Step 6;
Step 17:   else
Step 18:     The node broadcasts a RQ when it needs to
Step 19:     if (all MANET nodes receive the RQ in the situation that there might
        be link error in a MANET)
Step 20:       if (the node is the destination of a RQ)
Step 21:         The node unicasts a RP in the situation that there might be
        link errors in a MANET.
Step 22:       else
Step 23:         goto Step 8
Step 24:     else
Step 25:       goto Step 18
End

```

그림 2 Weak DAD AAP 동작을 나타내는 의사 코드

WDP에서, 노드는 다른 노드에게 네트워크 토폴로지를 알리기 위해 LS메시지를 주기적으로 브로드캐스트한다. WDO에서, 소스 노드가 목적지까지의 경로를 가지고 있지 않은 조건에서 데이터를 목적지 노드에 전송할 필요가 있을 때에만, 소스 노드는 목적지 노드까지의 경로를 찾기 위해 RQ메시지를 브로드캐스트하며, 목적지 노드 또는 새로운 경로를 가진 노드는 RQ메시지에 대한 응답으로 RR메시지를 유니캐스트한다. 노드가 LS, RQ 또는 RR메시지에서 IP 주소를 조사한 후 자신의 라우팅 테이블에 등재된 것과 중복된 IP 주소를 발견한 경우, 노드는 다른 노드들에게 중복된 주소를 통지하는 추가 단계를 수행한다. 이 경우, IP 주소를 이미 사용하고 있던 노드는 AE메시지를 중복된 IP 주소를 가진 노드로 유니캐스트한다. 만일 노드가 LS, RQ 또는 RR메시지에서 IP 주소를 조사한 후 어떠한 중복된 IP 주소도 발견하지 못한 경우, 노드는 LS, RQ 또는 RR메시지를 정상적으로 중계한다. 상술한 내용에 기초하여, 아래의 보조정의가 유도될 수 있다.

보조정의 4. IP 인증 절차에서, $S(O(N)+O(t))$ 는, 노드가 WDP를 이용하여 MANET 내의 IP 주소를 확인할 필요가 있을 때, 브로드캐스트된/중계된 LS메시지 및 유니캐스트된/중계된 AE메시지의 최대 개수의 상한이다.

증명. IP 인증 절차의 결과가 실패 시도일 때 메시지 개수가 최대가 된다. 실패 시도는 정의 2에 기초한 $SO(N)$ 개의 브로드캐스트되거나 중계된 LS메시지와 보조정의 1에 기초한 $SO(t)$ 개의 유니캐스트되거나 중계된 AP메시지를 제공하기 때문에, 실패 시도의 메시지 복잡도는 $S(O(N)+O(t))$ 로 표현될 수 있으며, 이는 브로드캐스트되고 중계된 LS메시지 및 유니캐스트되고 중계된 AE메시지의 최대 개수의 상한의 합이며, 여기서 S는 MANET 내에서의 링크 에러를 고려하기 위해 도입되었다. □

보조정의 5. 세션에서, $nS(O(N)+O(t))$ 는 WDP를 사용하여 브로드캐스트된/중계된 LS메시지와 유니캐스트된/중계된 AE메시지의 최대 개수의 상한이다.

증명. WDP는 세션을 가지며, IP 인증 절차의 최대 재시도 횟수는 세션의 n 으로 제한된다. 세션이 최대 개수가 n 인 IP 인증 절차로 구성되고 IP 인증 절차의 최대 개수의 상한이 보조정의 4에 기초하여 $S(O(N)+O(t))$ 이기 때문에, 세션의 메시지 복잡도는 $nS(O(N)+O(t))$ 로 표현될 수 있고, 여기서 n 은 IP 인증 절차의 재시도 횟수이다.

WDO에서, 노드는 RQ메시지를 브로드캐스트하거나 중계하며, 만일 노드가 정상 라우팅 절차에 기초한 목적지 노드라면 RP메시지를 유니캐스트할 수 있다. 또한,

노드는 중복된 IP 주소를 발견한 경우 AE메시지를 유니캐스트한다. 상기 결과에 기초하여, WDP와 유사한 아래의 추론이 얻어진다. □

추론 1. IP 인증 절차에서, $S(O(N)+2O(t))$ 는, 노드가 WDO를 사용하여 MANET 내의 IP 주소를 확인하고자 할 때, 브로드캐스트된/중계된 RQ메시지 및 유니캐스트된/중계된 RP메시지와 AE메시지의 최대 개수의 상한이다.

증명. IP 인증 절차의 결과가 실패 시도일 때 메시지 개수가 최대가 된다. 실패 시도는 정의 2에 기초한 $SO(N)$ 개의 브로드캐스트되거나 중계된 LS메시지와 보조정의 1에 기초한 $2SO(t)$ 개의 유니캐스트되거나 중계된 AP메시지를 제공하기 때문에, 실패 시도의 메시지 복잡도는 $S(O(N)+2O(t))$ 으로 표현될 수 있으며, 이는 브로드캐스트되고 중계된 RQ메시지와 유니캐스트되고 중계된 RP 및 AE메시지의 최대 개수의 상한을 합한 것이다. □

추론 2. Session에서, $nS(O(N)+2O(t))$ 는 WDO에서 브로드캐스트된/중계된 RQ메시지와 유니캐스트된/중계된 RP메시지 및 AE메시지의 최대 개수의 상한이다.

증명. WDO는 세션을 가지며, IP 인증 절차의 최대 재시도 횟수는 세션의 n 으로 제한된다. 세션이 최대 개수가 n 인 IP 인증 절차로 구성되고 IP 인증 절차의 최대 개수의 상한이 추론 1에 기초한 $S(O(N)+2O(t))$ 이기 때문에, 세션의 메시지 복잡도는 $nS(O(N)+2O(t))$ 로 표현될 수 있고, 여기서 n 은 IP 인증 절차의 재시도 횟수이다. □

2.3 MANETconf

MANETconf의 메시지 복잡도의 상한을 유도하기 위해, 그림 3에 도시된 바와 같은 의사 코드가 사용된다. 요청 노드(requestor)가 MANET에 포함되어 인증된 IP 주소를 얻으려 할 때, 노드는 그 이웃들에게 NQ메시지를 브로드캐스트한다. 요청 노드는 이웃 응답 타이머가 끝나기 전에 어떠한 NR메시지도 받지 못한 경우, NQ메시지의 브로드캐스팅을 임계 횟수만큼 반복한다. 반복을 마친 후, 요청 노드는 단지 하나의 노드만이 존재한다고 판단하고 그 자신을 IP 주소로 구성한다. 메시지 복잡도는 MANET 그룹에 연결되는 단일 노드의 절차에 초점이 맞추어져 있기 때문에, 상술한 MANETconf의 초기화 절차는 메시지 복잡도에서 고려되지 않는다.

만일 요청 노드가 NR메시지를 받는다면, 요청 노드는 시작 노드(initiator)를 선택하고, 시작 노드는 RR메시지를 유니캐스트한다. RR메시지 유니캐스팅의 메시지 복잡도는 $SO(1)$ 로 표현될 수 있으며, 여기서 Pe_0 가 0인 경우 S는 1이다. RR메시지를 받은 후, 시작 노드는 요청 노드의 IP 주소를 확인하기 위해 MANET그룹의 모든 노드들에게 IQ메시지를 브로드캐스트한다. IQ메시지 브

```

Start
Step 01: A requester (new joining node) selects an initiator and
unicasts RR to the initiator
Step 02: n=0; (Set retry count (n) =0)
Step 03: n++; (Increase the retry count (n) by 1)
Step 04: The initiator broadcasts an IQ to all the nodes of the MANET group
with the address of the requester
Step 05: if (all MANET nodes receive the IQ in the situation that there might
be link errors in a MANET == TRUE)
Step 06: Recipient nodes reply with an affirmative or a negative response (IR)
to the initiator in the situation that there might be link errors in a MANET
Step 07: else
Step 08: goto Step 4;
Step 09: if (the initiator receives affirmative IR messages from all nodes == TRUE)
Step 10: The initiator assigns the IP address to the requester
Step 11: The initiator broadcasts an AO message to all recipient nodes of the MANET group, goto End
Step 12: else
Step 13: The initiator selects another IP address
Step 14: if (retry count <= n)
Step 15: The initiator sends an AB message to the requester, goto End
Step 16: else
Step 17: goto Step 3;
End

```

그림 3 MANETConf AAP 동작을 나타내는 의사 코드

로드캐스팅의 메시지 복잡도는 정의 2에 기초하여 $SO(N)$ 으로 표현될 수 있다. 수신 노드들은 시작 노드에 대해 긍정적이거나 부정적으로 응답할 것이다. MANET 그룹 내의 모든 노드에 의한 IR메시지 유니캐스팅의 메시지 복잡도는, 모든 N 개의 노드가 IR메시지를 유니캐스트하고 각 IR메시지는 보조정의 1에 기초하여 메시지 복잡도 $SO(t)$ 를 가지기 때문에, $SO(tN)$ 으로 표현될 수 있다. 만일 시작 노드가 모든 수신 노드로부터 긍정적인 IR메시지를 받았다면, 시작 노드는 MANET 그룹 내의 모든 수신 노드들에게 AO메시지를 브로드캐스트한다. AO메시지 브로드캐스팅의 메시지 복잡도는 정의 2에 기초하여 $SO(N)$ 으로 표현될 수 있다. 만일 시작 노드가 수신 노드로부터 부정적인 IR메시지를 받았다면, 시작 노드는 다른 IP 주소를 선택하고, 재시도 횟수가 본 논문에서 n 으로 설정된 시작 노드 Request Retry에 도달할 때까지 IQ메시지를 브로드캐스팅하는 단계와 IR메시지를 수신하는 단계를 반복한다. 상기 결과에 기초하여, 아래의 보조정의가 유도된다.

보조정의 6. 단일 노드가 연결된 경우의 IP 인증 절차에서, $SO((t+1)N)$ 은, 노드가 MANETconf를 포함한 MANET 내에서 IP 주소를 확인할 필요가 있을 때, 브로드캐스트된/중계된 IQ메시지 및 유니캐스트된/중계된 IR메시지의 최대 개수의 상한이며, 여기서 S 는 링크 에러 확률이 Pe 인 경우 메시지의 브로드캐스팅, 중계 또는 유니캐스팅의 평균 재전송 횟수를 나타낸다.

증명. 메시지 개수는 IP 인증 절차의 결과가 실패 시도일 때 최대가 된다. 실패 시도는 정의 2에 기초한 $SO(N)$ 개의 브로드캐스트되거나 중계된 IQ메시지와, 보조정의 1에 기초한 $SO(tN)$ 개의 유니캐스트된/중계된

IR메시지를 제공하기 때문에, 실패 시도의 메시지 복잡도는 $SO(N)+SO(tN)$ 으로 표현될 수 있으며, 이는 브로드캐스트되고 중계된 IQ메시지와 유니캐스트되고 중계된 IR메시지의 최대 개수의 상한을 합한 것이다. 이는 $SO((t+1)N)$ 으로 재배열될 수 있다. □

따라서, 재시도 횟수가 n 에 도달할 때까지의 IQ메시지의 브로드캐스팅 및 IR메시지 수신에 대한 메시지 복잡도는 $nSO((t+1)N)$ 로 표현될 수 있다. n 번 반복 이후, 만일 시작 노드가 부정적인 IR메시지를 받으면, 시작 노드는 요청 노드에게 AB메시지를 전송한다. AB메시지 유니캐스팅의 메시지 복잡도는 $SO(1)$ 로 표현될 수 있다. 따라서, 단일 노드가 연결된 경우의 메시지 복잡도는 $nSO((t+1)N)+SO(N)+SO(2)$ 로 표현될 수 있고, 여기서 $SO(2)$ 는 RR메시지와 AB메시지 유니캐스팅의 메시지 복잡도를 나타낸다. 상기 결과에 기초하여, 아래의 보조정의가 유도된다.

보조정의 7. 단일 노드가 연결된 경우의 세션에서, $nSO((t+1)N)+SO(N)+SO(2)$ 는 MANETconf에서 브로드캐스트되거나 중계된 IQ메시지와 AO메시지 및 유니캐스트되거나 중계된 IR, RR, 및 AB메시지의 최대 개수의 상한이다.

증명. MANETconf는 세션을 가지며, IP 인증 절차의 최대 재시도 횟수는 세션의 n 으로 제한된다. 세션이 최대 개수가 n 인 IP 인증 절차로 구성되고 IP 인증 절차의 최대 개수의 상한이 보조정의 6에 기초하여 $SO((t+1)N)$ 이기 때문에, 세션의 메시지 복잡도는 $nSO((t+1)N)+SO(N)+SO(2)$ 로 표현될 수 있고, 여기서 n 은 IP 인증 절차의 개수이고, $SO(N)$ 은 AO메시지 브로드캐스팅의 메시지 복잡도를 나타내며, $SO(2)$ 는 RR메시

지와 AB메시지 유니캐스팅의 메시지 복잡도를 나타낸다. □

3. 시뮬레이션 분석 결과

AAP의 메시지 복잡도를 분석하기 위해, 불연속-이벤트 특성을 갖는 Matlab 시뮬레이터가 개발되었고, 이 시뮬레이터의 특징은 1km²의 네트워크 영역안에 다양한 네트워크 토폴로지를 생성하고, AAP를 수행할 때의 메시지 복잡도를 계산한다. 또한, 시뮬레이터 성능을 입증하기 위해 QualNet에 의해 수행된 ADB 알고리즘 [13]을 비교 테스트하였고, 그 결과 100, 125, 150 및 175개의 노드에 대해 클러스터당 평균 노드 개수가 [13]의 결과와 1% 이하의 차이를 나타냄을 보였다.

충돌 확률(P)은, 요청된 IP 주소가 MANET 그룹 내에서 이미 사용되고 있는 확률로서 정의된다. 충돌 확률은 MANET 그룹 내의 주소의 크기와 노드 개수에 따라 달라진다. [14]의 저자는, 300개 노드 네트워크 내의 MANET 로컬 주소에서 16비트의 주소 공간 크기가 사용된 경우 충돌 확률을 50%로 계산한다. 충돌 확률이 1인 경우, 선택 또는 재 선택된 IP 주소는 MANET 그룹내의 IP 주소들 중 하나의 주소와 항상 중복된다.

WDO의 시뮬레이션에 있어서, 특정 충돌 확률 조건에서 서로 다른 RP메시지 유니캐스팅 발생 확률을 가짐으로 인해 다른 메시지 복잡도 값을 가지게 됨을 예상할 수 있다. 따라서, 아래의 시뮬레이션 실험에서는, 노드에서 RP메시지 유니캐스팅의 발생 확률은 0이 아니며, 요청 IP 주소의 충돌 확률과 동일하다고 가정된 후에 실험을 수행하였다.

시뮬레이션에서는 충돌 확률(P)을 0.1로 고정한 후, 링크 에러 확률(Pe)을 고려하였다. Pe값이 0.2에서 0.25, 0.5, 0.75 및 0.8까지 변하는 경우, 재전송 횟수 S는 개별적으로 식 (1)에 기초한 1.25, 1.33, 2, 4 및 5로 정의된다.

시뮬레이션에서 사용된 가장 일반적인 플러딩 방법은, 모든 노드가 Address Request 메시지의 첫 번째 복사본을 받을 때마다 Address Request 메시지를 모든 one-hop 이웃 노드들에게 재전송하게 한다[12]. 각 노드에서의 적용된 Dijkstra의 최단 경로 알고리즘은, 유니캐스팅된 Address Reply 메시지를 목적지 노드에서 소스 노드로 유니캐스팅하거나 중계할 경우 hop 개수를 계산하는 데 사용된다. 노드의 전송 범위는 hop 개수를 변경시킨다. 메시지 복잡도의 상한은 이전 장의 유도식에 기초하여 계산되며, 여기서 각 유니캐스트 케이스에서 반대 경로의 최대 노드 개수는 각 상한 식에서 O(t)를 계산하는 데 사용된다.

Strong DAD 프로토콜, Weak DAD 및 MANET-

conf 프로토콜에서, 재전송 횟수(retry count limit: n)은 5이고 DAD 재전송 횟수(DAD retry count limit: m)은 Strong DAD 프로토콜에서 3으로 Weak DAD 및 MANETconf 프로토콜에서는 1로 설정하였다. 향후 연구 항목으로는 네트워크의 환경과 각 프로토콜의 성능에 따라 n과 m 값을 최적으로 설정해주는 것이다. 노드의 전송 범위는 100m이며, 노드 개수는 50에서 350까지 변한다.

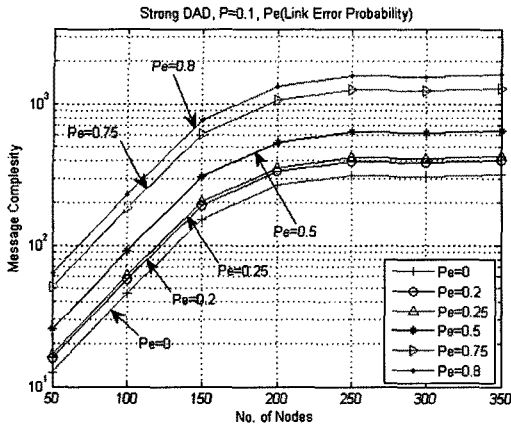
그림 4에서 $P_e = 0$ 는 에러가 없는 무선 통신 환경을 의미한다. 또한, 주어진 무선 링크 에러 확률에서, 링크 에러는 Address Query 메시지의 재보트캐스트와 Address Reply 메시지의 재유니캐스트를 발생시켰고, 이로 인해 각 AAP는 서로 다른 제어 오버헤드를 가지는 것을 보였다. 다른 P_e 값에 대해, Strong DAD는 WDP에 대비하여 45% 많은 제어 (control) 오버헤드를 가지는 것을 보였다. WDO는 WDP에 대비하여 1.1%의 오버헤드를 가지는 것을 보였다. MANETconf는 WDP에 대비하여 174%의 제어 오버헤드를 가지는 것을 보였다.

그림 5에서는 링크 에러 확률이 0.2, 0.5, 0.8로 변화될 때, Strong DAD, WDP, WDO,와 MANETconf의 메시지 복잡도를 비교한 그래프이다. 각각의 링크 에러 확률에서 WDP와 WDO가 가장 낮은 메시지 복잡도를 가졌고, MANETconf가 가장 높은 메시지 복잡도를 보였다. 또한, WDO의 메시지 복잡도는 WDP의 메시지 복잡도와 거의 유사함을 보였다.

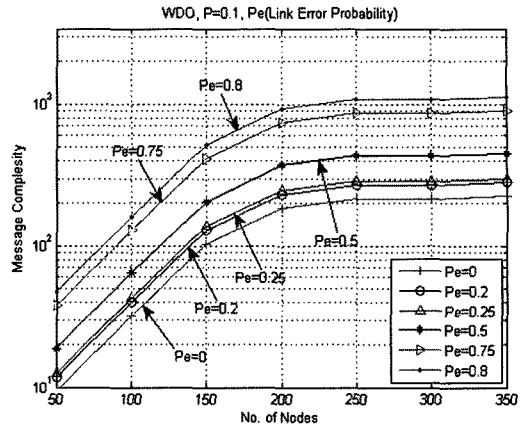
표 2는 Strong DAD, WDP, WDO 및 MANETconf에서 단일 노드 연결 케이스의 메시지 복잡도를 요약한 것이다. 시뮬레이션 결과와 표 2의 메시지 복잡도 분석에 기초하여, n, m, t, S, N, 및 전송 범위값이 적절한 값들을 가질 경우, $P \leq 1$ 인 단일 노드 IP 주소 할당 케이스에서, 메시지 복잡도는 아래와 같이 비교될 수 있다: $WDP < WDO < Strong\ DAD < MANETconf$.

AAP의 원래 논문들은 실제 MANET에 적용될 수 없는 불완전한 부분을 가지고 있었으며, 본 연구에서는 아래와 같은 개념을 새로 첨가함으로써, 프로토콜이 작동되게 수정하였다.

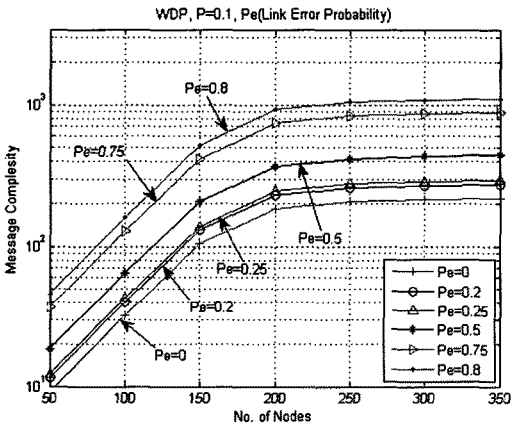
1. End to end 무선 연결에서 발생한 링크 에러를 시뮬레이션 하기 위해 재전송 횟수 (S)를 도입함으로써, 다중경로 전파, 페이딩, 노드 이동성, 및 방해물에 의한 실제 무선 채널 환경이 메시지 복잡도에서 고려되었다.
2. Strong DAD에서 세션의 재전송 횟수 (n)을 도입함으로써, 무한 루프가 발생할 확률을 제거하였다. 원래의 Strong DAD는 IP 인증 절차에 대한 최대 재시도 횟수를 정의하지 않았다.
3. [9]에서 도입된 AE메시지 응답 매커니즘을 채택함으



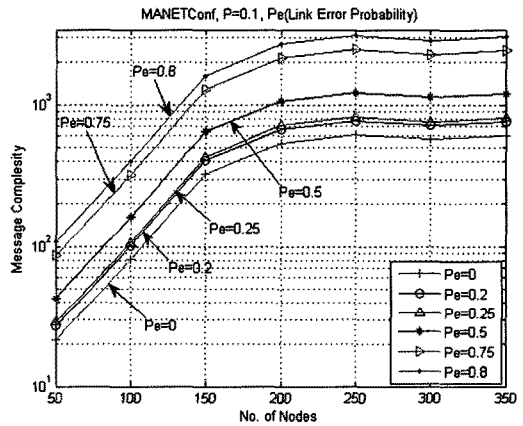
(a) Strong DAD



(c) WDO



(b) WDP



(d) MANETconf

그림 4 다른 링크 에러 확률을 가질 때 AAPs ((a) Strong DAD, (b) WDP, (c) WDO, (d) MANETconf)의 메시지 복잡도

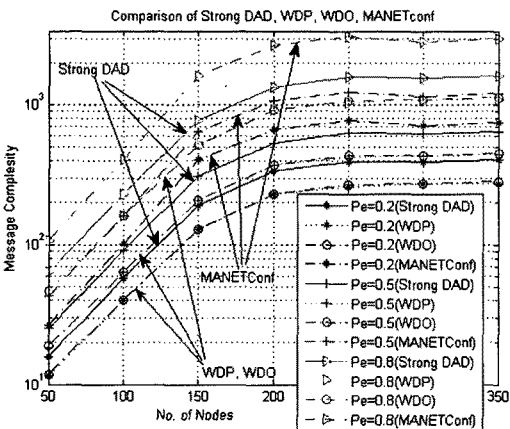


그림 5 Strong DAD, WDP, WDO,와 MANETconf의 메시지 복잡도(링크 에러 확률: 0.2, 0.5, 0.8)

표 2 각 AAP의 메시지 복잡도

AAP	메시지 복잡도
Strong DAD	$nS(mO(N)+O(t))$
WDP	$nS(O(N)+O(t))$
WDO	$nS(O(N)+2O(t))$
MANETconf	$nSO((t+1)N)+SO(N)+SO(2)$

로써, Weak DAD 프로토콜은 IP 주소가 중복된 상황을 해결할 때 적절히 작용되게 하였다.

4. MANETconf에서, 더 높은 Partition Identity를 가진 중복된 주소 노드가 그 이웃 노드에게 그의 시작 노드가 될 것을 요구하는 요청 노드가 되는 개념을 보완하였다.

4. 결론

무선 통신 환경에서 단말의 이동은 링크 에러를 만들고, 하나의 MANET 그룹에서 다른 그룹으로 소속을 바꾸게 한다. 새로운 그룹에서는 신규 노드로서 주소의 재구성이 필요하다. 따라서, 본 논문에서는, 이러한 주소의 자동 할당을 위해 필요한 각 MANET AAP의 메시지 복잡도의 정량적 분석을 수행하고 AAP들의 메시지 복잡도를 비교하는 독창적인 방법을 제안하였다. 메시지 복잡도의 정량적 분석을 수행하기 위해, 본 논문에서는 최악의 경우의 시나리오에 대한 분석을 수행하였다.

노드 이동성은 라우팅, 리소스 관리 및 서비스 제공 품질과 같은 네트워크 작업에 상당한 과제를 부여하기 때문에, 본 논문은 무선 링크의 빈번한 분리와 동적 네트워크 토폴로지를 모델링하기 위해 링크 에러 확률을 사용하였다. 재전송 횟수 S는 MANET의 링크 에러 확률로부터 계산될 수 있다. 링크 에러 확률이 1에 가까울 정도로 큰 경우 재전송 횟수가 무한대에 접근한다는 사실은 주의할 만하다. 실제 환경에서는 링크 에러율이 각 링크마다 그리고 시간이 흐름에 따라 다르게 나타난다. 이러한 링크 에러를 적정 시간 동안 관찰한 후 평균 링크 에러 값을 구할 수 있고, 이 값을 본 논문에서 사용하는 링크 에러 확률로 사용한다.

메시지 복잡도 관점에서, MANET 영역이 높은 충돌 확률로 구성된 경우, MANET 라우팅 프로토콜을 가진 Weak DAD가 MANETconf 및 Strong DAD보다 더욱 적당한 프로토콜이 될 것이며, 이는 MANET 라우팅 프로토콜을 가진 Weak DAD가 라우팅과 주소 자동 구성을 제공하며 MANETconf 및 Strong DAD와 비교하여 더 작은 메시지 복잡도를 제공하기 때문이다.

참 고 문 헌

[1] Z. J. Haas and B. Liang, "Ad hoc mobility management with uniform quorum systems," *IEEE Trans. Network*, Vol.7, No.2, pp. 228-240, Apr. 1999.

[2] A. B. McDonald and T. F. Znati, "A mobility-based framework for adaptive clustering in wireless ad hoc networks," *IEEE J. Select. Areas Commun.*, Vol.17, No.8, pp. 1466-1487, Aug. 1999.

[3] D. N. Alparslan and K. Sohraby, "A Generalized Random Mobility Model for Wireless Ad Hoc Networks and Its Analysis One-Dimensional Case," *IEEE Trans. Network*, Vol.15, No.3, pp. 602-615, Jun. 2007.

[4] E. Hyttia, P. Lassila, and J. Virtamo, "Spatial node distribution of the random waypoint mobility model with applications," *IEEE Trans. Mobile Computing*, Vol.5, No.6, pp. 18-32, Jun. 2006.

[5] B-. J. Kwak, N-. O Song, and L. E. Miller. "A mobility measure for mobile ad hoc networks,"

IEEE Commun. Lett., Vol.7, No.8, pp. 379-381, Aug. 2003.

[6] A.P. Jardosh, E.M.Belding-Royer, K.C. Almeroth, and S. Suri, "Real-world environment models for mobile network evaluation," *IEEE J. Select. Areas Commun.*, Vol.23, No.3, pp. 622-632, Mar. 2005.

[7] A.P. Jardosh, E.M.Belding-Royer, K.C. Almeroth, and S. Suri, "Real-world environment models for mobile network evaluation," *IEEE J. Select. Areas Commun.*, Vol.23, No.3, pp. 622-632, Mar. 2005.

[8] J-. P. Jeong, J. Park, H. Kim, and D. Kim, "Ad hoc IP address autoconfiguration," *IETF draft*, July 2004.

[9] N. H. Vaidya, "Weak duplicate address detection in mobile ad hoc networks," *Proc. ACM MobiHoc 2002*, pp. 206-216, June 2002, Lausanne, Switzerland.

[10] J. Gross and J. Yellen, *Graph Theory and Its Applications*, CRC Press, 1998.

[11] S. Nesargi and R. Prakash, "MANETconf: Configuration of hosts in a mobile ad hoc network," *Proc. IEEE Infocom 2002*, June 2002, New York, USA.

[12] M. Sheng, J. Li, and Y. Shi, "Relative Degree Adaptive Flooding Broadcast Algorithm for Ad Hoc Networks," *IEEE Trans. on Broadcasting*, Vol.51, No.2, pp. 216-222, June 2005.

[13] C-. C. Shen, and C. Srisathapornphat, and R. L. Z. Huang, and C. Jaikaeo, and E. L. Lloyd, "CLTC: A cluster-based topology control framework for ad hoc networks," *IEEE Trans. Mobile Computing*, Vol.3, No.1, pp. 18-32, Jan.-Mar. 2004.

[14] K. Weniger, "PACMAN: passive autoconfiguration for mobile ad hoc networks," *IEEE J. Select. Areas Commun.*, Vol.23, No.3, pp. 507-519, Mar. 2005.



김 상 철

2005년 12월 미국 Oklahoma State University, Electrical & Computer Eng., 공학박사. 2006년 2월 미국 Univ. of Nevada Las Vegas, Computer Science, Post Doctoral Research Fellow. 1994년 3월~2000년 7월 (주)삼성 테크윈, (주)삼성SDS 시스템 엔지니어. 2006년 3월~현재 국민대학교 컴퓨터공학과 조교수. 관심분야는 디지털 유무선 통신공학, 로봇공학