(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월04일
(11) 등록번호 10-2021852
(24) 등록일자 2019년09월09일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)
H04W 40/02 (2009.01)
(52) CPC특허분류
H04L 67/1065 (2013.01)
H04L 63/0807 (2013.01)
(21) 출원번호 10-2017-0171648
(22) 출원일자 2017년12월13일
심사청구일자 2017년12월13일
(65) 공개번호 10-2019-0070780
(43) 공개일자 2019년06월21일
(56) 선행기술조사문헌
KR1020130087918 A*
이광수, 'MIPv6에서의 바인딩 갱신 인증', TTA 표준기술동향, 2002.05*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
상명대학교 천안산학협력단
충청남도 천안시 동남구 상명대길 31, 상명대학교내 (안서동)
(72) 발명자
이종혁
충청남도 천안시 서북구 북일로 21, 104동 1503호(두정동, e편한세상 두정3차)
(74) 대리인
김정수

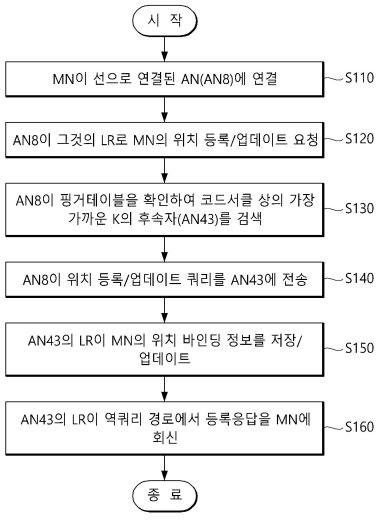
전체 청구항 수 : 총 5 항 심사관 : 채정목

(54) 발명의 명칭 **지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법**

(57) 요 약

본 발명은 지능형 5G(fifth-Generation) 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 관한 것으로, 특히 분산 위치 관리를 위한 액세스 노드의 분산 해시 테이블을 이용하고 MN(Mobile Node)의 보안 인증을 제공하면서 인증 성능을 향상시키기 위해 티켓 재사용 방법을 채택한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04W 40/02 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 GK17P0400
부처명 과학기술정보통신부
연구관리전문기관 (재)기가코리아사업단
연구사업명 범부처 Giga KOREA 사업
연구과제명 저지연 융합서비스를 위한 모바일 에지 컴퓨팅 플랫폼 기술 개발
기 여 율 1/1
주관기관 한국전자통신연구원
연구기간 2017.04.01 ~ 2017.12.31

명 세 서

청구범위

청구항 1

분산 위치 서버에서 K[이동노드(MN)의 고유 아이디(ID_{MN})의 해시]-V[MN의 현재 IP 어드레스] 쌍의 메인 복사본을 추가 또는 업데이트하는 단계;

상기 분산 위치 서버에서 K-V 쌍의 백업 복사본을 추가 또는 업데이트하는 단계; 및

TALM(ticket-based authentication mechanism) 프로토콜을 수행하는 단계를 포함하고,

상기 K-V 쌍의 메인 복사본을 추가 또는 업데이트 단계는,

상기 이동 노드(MN)가 그 위치를 등록 또는 업데이트하기 위해 코드 서클 내에서 선으로 연결되어 있는 액세스 노드(AN8)에 연결하는 단계;

상기 액세스 노드(AN8)가 그것의 위치 레지스터(LR)로 상기 이동 노드(MN) 위치의 등록 또는 업데이트를 요청하는 단계;

상기 액세스 노드(AN8)가 핑거 테이블을 확인하여 코드 서클상의 가장 가까운 K의 후속자(AN43)를 검색하는 단계;

상기 액세스 노드(AN8)가 위치의 등록 쿼리 또는 업데이트 쿼리를 상기 후속자(AN43)에게 전송하는 단계;

상기 후속자(AN43)의 위치 레지스터(LR)가 상기 이동 노드(MN)의 위치 바인딩 정보를 저장 또는 업데이트하는 단계; 및

상기 후속자(AN43)의 위치 레지스터(LR)가 역 쿼리 경로에서 등록 응답을 상기 이동 노드(MN)에 회신하는 단계를 포함하는, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

상기 K-V 쌍의 백업 복사본을 추가 또는 업데이트하는 단계는 상기 K-V 쌍의 메인 복사본을 추가 또는 업데이트 단계와 동일한, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법.

청구항 4

제 1 항에 있어서,

상기 TALM 프로토콜을 수행하는 단계는 티켓의 생성 및 만료 단계와 이전의 액세스 라우터(AR)에서 티켓을 수집하는 단계를 포함하는, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법.

청구항 5

제 4 항에 있어서,

상기 티켓의 생성 및 만료 단계는,

상기 이동 노드(MN)가 온(On) 된 직후 액세스 라우터(AR)를 등록 할 필요가 있을 때, 상기 이동 노드(MN)에서 상기 액세스 라우터(AR)에 초기 메시지(MN_{Reg})를 송신하는 단계;

상기 액세스 라우터(AR)가 상기 초기 메시지(MN_{Reg})를 수신하면 자신의 난수를 추가하여 메시지($MN_{Reg}AS_{Msg}$)을 생

성하여 인증 서버(AS)에 송신하는 단계:

상기 인증 서버(AS)가 키(K_{TK})에 의해 암호화된 티켓을 생성하는 단계;

상기 인증 서버(AS)가 상기 액세스 라우터(AR)에 이동 노드(MN)와 액세스 라우터(AR)가 공유하는 키(K_{MN-AR})를 전송할 메시지(AS_{Res})를 송부하는 단계;

상기 액세스 라우터(AR)가 메시지(RegRes)를 사용하여 K와 이동 노드(MN)가 통신하게 하는 단계; 및

상기 이동 노드(MN)가 위치 업데이트 메시지와 함께 마지막 메시지(AuthMsg)를 상기 액세스 라우터(AR)로 전송하는 단계를 포함하는, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법.

청구항 6

제 4 항에 있어서,

상기 티켓을 수집하는 단계는,

상기 이동 노드(MN)가 nAR[이동 노드(MN)의 새롭게 첨부된 액세스 라우터]에 메시지(nAR_{Reg})를 전송하는 단계;

상기 nAR이 상기 메시지를 수신하고 pAR[이전에 첨부된 이동 노드(MN)의 액세스 라우터]에 메시지($MN_{Reg-pAR}$)를 전송하는 단계; 및

상기 pAR이 티켓 유효 시간 및 키(K_{TK})에 대한 정보를 추가하여 메시지 (MN_{RegRes})를 nAR에게 전송하는 단계를 포함하는, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 지능형 5G(fifth-Generation) 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 관한 것으로, 특히 분산 위치 관리를 위한 액세스 노드의 분산 해시 테이블을 이용하고 MN(Mobile Node)의 보안 인증을 제공하면서 인증 성능을 향상시키기 위해 티켓 재사용 방법을 채택한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 관한 것이다.

배 경 기 술

[0002] 통상, 모바일 IPv6 (MIPv6)[비특허문헌1]이나 프록시 모바일 IPv6 (PMIPv6)[비특허문헌 2] 등의 기존의 이동성 관리 프로토콜은 셀룰러 네트워크 아키텍처가 중앙 집중화되어있는 것을 전제로 개발되었다. 그러나 전제는 변경되고 있다. 셀룰러 네트워크 아키텍처는 성능과 확장성을 향상시키기 위해 평탄화(flattened) 되어 있는 반면, 집중 형 네트워크 아키텍처와 이동성 관리 프로토콜은 네트워크의 병목 현상을 유발하고 단일 실패 지점이 발생한다는 보고가 많이 있다. 집중형 이동성 관리 프로토콜의 문제를 해결하기 위해, 분산 셀룰러 네트워크 아키텍처[비특허문헌 3]를 조작하도록 설계된 DMM 프로토콜을 개발하기 위해 IETF 분산형 이동성 관리(DMM) 워킹 그룹이 제안되었다. DMM에서 데이터 플레인(plane)과 컨트롤 플레인이 분리되고, 데이터 플레인은 분산되어 네트워크 아키텍처의 보다 좋은 성능 및 확장성을 제공한다.

[0003] 그러나 위치 관리를 용이하게 하기 위해 컨트롤 플레인을 분산(즉, 완전 분산형 DMM) 또는 중앙 집중식(즉, 반분산 DMM)으로 할 수 있다 [비특허문헌 4] [비특허문헌 5]. 예를 들어, [비특허문헌 6]에서는 집중 형 SIP 레지스터가 DMM 환경에서 사용되는 것이 제안되었다. 그러나 그 SIP 레지스터는 신뢰성을 향상시키기 위해 복제될 수 있지만 완전히 분산된 아키텍처에서 얻을 수 있는 복원력(resilience) 수준에 미치지 않는다.

[0004] 따라서 DMM과 완전히 호환될 수 있는 아키텍처를 정의해야 할 필요가 있다. DMM의 배경과 접근 방법에 대한 자세한 내용은 [비특허문헌 4] 및 [비특허문헌 5]를 참조하십시오. 또한 예비 연구 [비특허문헌 7]로서, PMIPv6와 비교하여 Dynamic Mobility Anchoring(DMA)[비특허문헌 8]이라는 DMM 기법의 성능을 분석했다.

[0005] 무선 네트워크 액세스를 확보하지 않고, 부정한(불법) 모바일 노드(MN)는 네트워크 리소스에 액세스하여 다양한 공격을 시작할 수 있다. 인증되어 허용된 MN(즉, 정당한 MN) 만이 네트워크 리소스에 액세스 할 것이며, 예를 들어 정당화 된(합법적인) MN 만이 안전한 인증 후 핸드 오버 동안 그 위치를 등록하고, 업데이트한다. 무선 네

트워크 액세스 보안이 제공되지 않은 경우 불법 MN은 정당한 MN 대신 악의적인 위치 업데이트 메시지를 보내거나, 위치 업데이트 관련 데이터 패킷을 방향전환(redirect) 또는 차단할 수 있다. DMM 환경에서 이러한 공격을 방지하기 위해, MN 인증시 인증 성능을 향상시키기 위해 티켓 재사용 방법이 채택되는 동안, 분산 위치 관리를 위해 액세스 노드의 분산 해시 테이블을 이용하는 위치 관리용 티켓 기반 인증 메커니즘(TALM)이 필요하게 되었다.

선행기술문헌

비특허문헌

[0006] (비특허문헌 0001) Johnson, D., Perkins, C., Arkko, J. (2004). Mobility Support for IPv6. IETF RFC 3775. http://www.ietf.org/rfc/rfc3775.txt. Accessed 22 August 2016.

(비특허문헌 0002) Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B. (2008). Proxy Mobile IPv6. IETF RFC 5213. http://www.ietf.org/rfc/rfc5213.txt. Accessed 22 August 2016.

(비특허문헌 0003) http://datatracker.ietf.org/wg/dmm/. Accessed 22 August 2016.

(비특허문헌 0004) Chan, H.-A., Yokota, H., Xie, J., Seite, P., Liu, D. (2011). Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues. Journal of Communications. 6(1). 4-15.

(비특허문헌 0005) J.-H. Lee, J.-M. Bonnin, P. Seite, and H. Anthony Chan, "Distributed IP Mobility Management from the Perspective of the IETF: Motivations, Requirements, Approaches, Comparison, and Challenges," IEEE Wireless Communications Magazine, vol. 20, no. 5, pp. 159-168, October 2013.

(비특허문헌 0006) Ali-Ahmad, Hassan, Kashif Munir, Philippe Bertin, Karine Guillouard, Meryem Ouzzif, and Xavier Lagrange (2016). Processing loads analysis of distributed mobility management and SIP-based reachability. Springer Telecommunication Systems: 1-16.

(비특허문헌 0007) Munir, K., Lagrange, X., Bertin, P., Guillouard, K., Ouzzif, M. (2015). Performance analysis of mobility management architectures in cellular networks. Springer Telecommunication Systems, 59(2). 211-227.

(비특허문헌 0008) Bertin, P., Bonjour, S., Bonnin, J.-M. (2008). A distributed dynamic mobility management scheme designed for flat IP architectures. In Proceedings of 3rd international conference on new technologies, mobility and security (NTMS 2008).

(비특허문헌 0009) Xie, J., Akyildiz, I.F. (2002). A novel distributed dynamic location management scheme for minimizing signaling costs in mobile IP. IEEE Trans. Mobile Computing. 1(3). 163-175.

(비특허문헌 0010) Zhai, YuJia, XinYu Mao, Yue Wang, Jian Yuan, and Yong Ren (2013). A DHT-based fast handover management scheme for mobile identifier/locator separation networks. Science China Information Sciences. 56(12). 1-15.

(비특허문헌 0011) Bezahaf, Mehdi, Luigi Iannone, Marcelo Dias De Amorim, and Serge Fdida (2009). Transparent and distributed localization of mobile users in wireless mesh networks. In International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer Berlin Heidelberg. 513-529.

(비특허문헌 0012) Stoica, I., Morris, R., Karger, D., Kaashoek, M.F., Balakrishnan, H.(2001). Chord: A scalable peer-to-peer lookup service for internet applications. In Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '01). ACM, New York, NY, USA, 149-160.

(비특허문헌 0013) Imtiaz, Waqas Ahmed, Muhammad Afaq, and Muhammad Asmatullah Khan Babar (2011). mSCTP Based Decentralized Mobility Framework. International Journal of Advanced Computer Science and Applications. 2(9). 106-112.

(비특허문헌 0014) Imtiaz, Waqas A (2013). Two-Tier CHORD for Decentralized Location Management. International Journal of Computer Applications. 69(4).

(비특허문헌 0015) D. Simon, B. Aboba, R. Hurst (2008). The EAP-TLS Authentication Protocol, RFC 5216 (Proposed Standard), March 2008.

(비특허문헌 0016) H. Zhou, H. Zhang, Y. Qin (2009). An authentication method for Proxy Mobile IPv6 and performance analysis. Security and Communication Networks 2(5). 445-454.

(비특허문헌 0017) Lee, J.-H., Bonnin, J.-M. (2013). HOTA: Handover optimized ticketbased authentication in network-based mobility management. Elsevier Information Sciences. Volume 230. 64-77.

(비특허문헌 0018) Steinmetz, Ralf, and Klaus Wehrle (2005). P2P Systems and Applications, LNCS 3485. Springer Berlin Heidelberg. pp. 95-117.

(비특허문헌 0019) Akl, R.G., Hegde, M.V., Naraghi-Pour, M. (2005). Mobility-Based CAC Algorithm for Arbitrary Call-Arrival Rates in CDMA Cellular Systems. IEEE Transactions on Vehicular Technology. 54(2). 639-651.

(비특허문헌 0020) Hong, Rappaport, S.-S. (1986). Traffic Model and Performance Analysis for Cellular Mobile Radio Telephone Systems with Prioritized and Non-Prioritized Handoff Procedures. IEEE Transactions on Vehicular Technology. 35(3). 77-92.

(비특허문헌 0021) Thomas, R., Gilbert, H., Maziotto, G. (1988). Influence of the Moving of the Mobile Stations on the Performance of a Radio Mobile Cellular Network. Proc of the 3rd Nordic Seminar on Digital Land Mobile Radio Communications.

발명의 내용

해결하려는 과제

[0007] 따라서 본 발명은 상기와 같은 필요성에 의해 이루어진 것으로서, 본 발명의 목적은 평균 인증 대기 시간이 적고, 위치 업데이트당 인증 메시지의 평균 개수가 감소할 수 있는, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법을 제공하는 데에 있다.

과제의 해결 수단

[0008] 상기의 목적을 달성하기 위해 본 발명의 실시형태에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법은 분산 위치 서버에서 K[이동노드(MN)의 고유 아이디(ID_{MN})의 해시]-V[MN의 현재 IP 어드레스] 쌍의 메인 복사본을 추가 또는 업데이트하는 단계; 상기 분산 위치 서버에서 K-V 쌍의 백업 복사본을 추가 또는 업데이트하는 단계; 및 TALM(ticket-based authentication mechanism) 프로토콜을 수행하는 단계를 포함하는 것을 특징으로 한다.

[0009] 상기 실시형태에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, 상기 K-V 쌍의 메인 복사본을 추가 또는 업데이트 단계는, 상기 이동 노드가 그 위치를 등록 또는 업데이트하기 위해 코드 서클 내에서 선으로 연결되어 있는 액세스 노드에 연결하는 단계; 상기 액세스 노드가 그것의 위치 레지스터로 상기 이동 노드 위치의 등록 또는 업데이트를 요청하는 단계; 상기 액세스 노드가 핑거 테이블을 확인하여 코드 서클상의 가장 가까운 K의 후속자를 검색하는 단계; 상기 액세스 노드가 위치의 등록 쿼리 또는 업데이트 쿼리를 상기 후속자에게 전송하는 단계; 상기 후속자)의 위치 레지스터가 상기 이동 노드의 위치 바인딩 정보를 저장 또는 업데이트하는 단계; 및 상기 후속자의 위치 레지스터가 역 쿼리 경로에서 등록 응답을 상기 이동 노드에 회신하는 단계를 포함할 수 있다.

[0010] 상기 실시형태에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, 상기 K-V 쌍의 백업 복사본을 추가 또는 업데이트하는 단계는 상기 K-V 쌍의 메인 복사본을 추가 또는 업데이트 단계와 동일할 수 있다.

[0011] 상기 실시형태에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, 상기

TALM 프로토콜을 수행하는 단계는 티켓의 생성 및 만료 단계와 이전의 액세스 라우터에서 티켓을 수집하는 단계를 포함할 수 있다.

[0012] 상기 실시형태에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, 상기 티켓의 생성 및 만료 단계는, 상기 이동 노드가 온 된 직후 액세스 라우터를 등록 할 필요가 있을 때, 상기 이동 노드에서 상기 액세스 라우터에 초기 메시지를 송신하는 단계; 상기 액세스 라우터가 상기 초기 메시지를 수신하면 자신의 난수를 추가하여 메시지를 생성하여 인증 서버에 송신하는 단계: 상기 인증 서버가 키에 의해 암호화된 티켓을 생성하는 단계; 상기 인증 서버가 상기 액세스 라우터에 이동 노드와 액세스 라우터가 공유하는 키를 전송할 메시지를 송부하는 단계; 상기 액세스 라우터가 메시지를 사용하여 K와 이동 노드가 통신하게 하는 단계; 및 상기 이동 노드가 위치 업데이트 메시지와 함께 마지막 메시지를 상기 액세스 라우터로 전송하는 단계를 포함할 수 있다.

[0013] 상기 실시형태에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, 상기 티켓 수집 단계는, 상기 이동 노드가 nAR[이동 노드의 새롭게 첨부된 액세스 라우터]에 메시지를 전송하는 단계; 상기 nAR이 상기 메시지를 수신하고 pAR[이전에 첨부된 이동 노드의 액세스 라우터]에 메시지를 전송하는 단계; 및 상기 pAR이 티켓 유효 시간 및 키에 대한 정보를 추가하여 메시지 를 nAR에게 전송하는 단계를 포함할 수 있다.

발명의 효과

[0014] 본 발명의 실시형태에 의한, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 의하면, 분산 위치 서버에서 K[이동노드(MN)의 고유 아이디(ID_{MN})의 해시]-V[MN의 현재 IP 어드레스] 쌍의 메인 복사본을 추가 또는 업데이트하는 단계; 상기 분산 위치 서버에서 K-V 쌍의 백업 복사본을 추가 또는 업데이트하는 단계; 및 TALM(ticket-based authentication mechanism) 프로토콜을 수행하는 단계;를 포함하여 구성됨으로써, 평균 인증 대기 시간이 적고, 위치 업데이트당 인증 메시지의 평균 개수가 감소할 수 있다는 뛰어난 효과가 있다.

[0015] 좀 더 상세하게는,

[0016] 첫째, TALM에서 인증 티켓의 재사용을 하므로 평균 인증 대기 시간이 종래의 EAP-TLS 프로토콜에 비해 현저히 적다.

[0017] 둘째, 액세스 노드(AN)의 에리어(Area) 증가에 따라 이동 노드(MN)가 더 적은 수의 핸드 오버 인증을 수행하고 그 결과 인증 메시지의 평균 개수가 감소한다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, K-V 쌍의 메인 복사본을 추가 또는 업데이트 단계를 설명하기 위한 플로우챠트이다.

도 2는 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, TALM 프로토콜을 수행하는 단계 중 티켓의 생성 및 만료 단계를 설명하기 위한 플로우챠트이다.

도 3은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, TALM 프로토콜을 수행하는 단계 중 티켓수집 단계를 설명하기 위한 플로우챠트이다.

도 4는 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 적용되는 6-비트 코드 식별자 공간을 나타내는 도면이다.

도 5는 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 적용되는 분산 위치 관리에 있어서의 내결함성을 설명하는 도면이다.

도 6은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, K-V 쌍의 메인 복사본의 추가/업데이트를 설명하는 도면이다.

도 7은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, TALM 프로토콜을 수행하는 단계 중 티켓의 생성 및 만료 단계를 설명하기 위한 메시지 흐름도이다.

도 8은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, TALM 프로토콜을 수행하는 단계 중 티켓수집 단계를 설명하기 위한 메시지 흐름도이다.

도 9는 본 발명의 실시 예의 시뮬레이션에 사용되는 셀 네트워크 토포로지이다.

도 10은 본 발명의 실시 예에 의한 TALM 프로토콜과 종래의 EAP-TLS 프로토콜의 평균 인증 대기 시간을 나타내는 도면이다.

도 11은 티켓의 유효 기간이 변경 될 때마다 본 발명의 실시 예에 의한 TALM 프로토콜의 위치 업데이트 당 인증 메시지의 평균수를 나타내는 도면이다.

도 12는 이동 노드(MN)의 속도가 변화하는 경우 본 발명의 실시 예에 의한 TALM 프로토콜의 위치 업데이트 당 인증 메시지의 평균수를 나타내는 도면이다.

도 13은 AN 지역이 변경되었을 경우 본 발명의 실시 예에 의한 TALM 프로토콜의 위치 업데이트 당 인증 메시지의 평균수를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 본 발명의 실시 예를 도면을 참조하여 상세히 설명하기로 한다.

[0020] 도 1은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, K-V 쌍의 메인 복사본을 추가 또는 업데이트 단계를 설명하기 위한 플로우챠트이고, 도 2는 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, TALM 프로토콜을 수행하는 단계 중 티켓의 생성 및 만료 단계를 설명하기 위한 플로우챠트이며, 도 3은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, TALM 프로토콜을 수행하는 단계 중 티켓수집 단계를 설명하기 위한 플로우챠트이며, 도 4는 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 적용되는 6-비트 코드 식별자 공간을 나타내는 도면이며, 도 5는 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 적용되는 분산 위치 관리에 있어서의 내결함성을 설명하는 도면이며, 도 6은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, K-V 쌍의 메인 복사본의 추가/업데이트를 설명하는 도면이며, 도 7은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, TALM 프로토콜을 수행하는 단계 중 티켓의 생성 및 만료 단계를 설명하기 위한 메시지 흐름도이며, 도 8은 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 있어서, TALM 프로토콜을 수행하는 단계 중 티켓수집 단계를 설명하기 위한 메시지 흐름도이다.

[0021] 먼저, 본 발명의 실시 예와 관련된 작업에 대해 설명하기로 한다.

[0022] [이동성 관리 및 핸드오버 인증]

[0023] [비특허문헌 9]에서 제안 된 분산 및 동적 위치 관리 방식은 IETF Mobile IP와 비교하여 신호 트래픽과 신호 지연을 줄인다. 저자는 각 이동 노드(MN)의 최신 이동성과 트래픽 부하에 따라 지역의 네트워크 경계를 동적으로 조정하여 신호 부하를 분산시키는 방식을 제안했다.

[0024] DHT 기반 메커니즘은 무선 네트워크에서 다른 문제를 해결하기 위해 광범위하게 제안되었다. [비특허문헌 10]에서는 DHT를 기반으로 한 개량형 핸드오버 관리 메커니즘이 제안되었다. [비특허문헌 11]에서는 무선 메쉬 네트워크를 위한 DHT 기반의 분산 현지화 서비스도 제안되었다. IP 핸드 오버에 의한 패킷 손실을 줄이기 위해 향상된 전송을 위한 모바일 스트림 제어 전송 프로토콜(mSCTP) 및 위치 관리를 위한 코드(Chord) DHT [비특허문헌 12에서 제안됨]를 이용한 메커니즘이 [비특허 문헌 13]에 제안되었다. [비특허문헌 14]에서는 위치 서버로서 높은 계산 능력과 안정성을 가진 노드를 사용하는 분산 위치 관리를 위한 2층 코드 DHT가 도입되었다.

[0025] EAP-TLS [비특허문헌 15에서 제안됨]은 기존의 무선 모바일 네트워크에서 널리 사용되는 일반적인 인증 방식이다. 그것은 이동 노드(MN)에 대한 초기 및 핸드오버 인증을 위한 완전 EAP 교환을 수행한다. 기본 인증 방식으로 EAP-TLS가 도입되어 분석되었으나, 이 방식에서는 성능 최적화는 이루어지지 않았다. 예를 들어, 이동 노드(MN)가 그 연결 지점을 변경할 때, 이동 노드(MN)는 긴 대기 시간을 유발하는 완전 EAP 교환을 수행해야하기 때문에 유저 경험의 질은 저하된다. 이러한 문제를 해결하기 위해 핸드 오버 인증의 성능 최적화에 관한 연구가 이루어 졌다. 예를 들어, 이동 노드(MN)가 PMIPv6 환경에서 다른 액세스 라우터와의 핸드 오버 인증을 할 경우 [비특허문헌 16]에서 제시된 인증 방식은 액세스 라우터, 즉 PMIPv6의 모바일 액세스 게이트웨이(MAG)로부터 얻은 로컬 증명서를 이용한다. [비특허문헌 17]에서는 이동 노드(MN)가 PMIPv6 환경에서 인증 서버에서 발급 한

자격 증명을 재사용하여 다른 액세스 네트워크에서 핸드오버 인증을 안전하게 할 HOTA(Handover Optimized Ticket-based Authentication)이 제안되었다.

[0026] 그 제안 방식은 고정 크기의 액세스 네트워크 영역(즉, 액세스 라우터가 커버하는 영역)을 고려하고 있기 때문에, [비특허문허 9]의 분산 및 동적 관리 방식과 비교할 때 본 논문의 작업은 다르다. 또한 제안 된 방식은 DHT를 기반으로 분산 된 안전한 위치 관리를 위한 복제 전략을 도입하였다. 우리의 연구는 제안 된 방식이 모든 액세스 라우터가 위치 레지스터를 갖는 것으로 간주되고 위치 관리의 내결함성을 제공하기 위해 DHT를 확장하기 때문에, 이전 DHT 기반 메커니즘 [비특허문헌 10], [비특허문헌 11], [비특허문헌 13], 및 [비특허문헌 14]와 비교할 때 다르다. 기존의 인증 방식과 비교할 때, DMM을 위해 개발 되고 응용 프로그램 수준의 보안을 제공하는 데 초점을 맞추고 있다

[0027] [코드(Chord) DHT]

[0028] 코드는 피어 투 피어(peer-to-peer) DHT에 대한 프로토콜과 알고리즘이다. DHT의 중심 기둥은 [0, 2n-1]의 범위에 있는 n비트의 식별자이다. 노드의 식별자는 그것의 ID이다. 데이터 항목의 식별자가 그것의 키(key)이다. 노드와 데이터 항목 모두 동일한 n비트의 코드 식별자 공간에 매핑된다. 키 및 값의 쌍 (K, V)은 ID가 K 이상인 노드에서 호스트 된다. 코드 서클내 노드는 이전 노드 까지 시계 반대 방향으로 앞에 있는 모든 키에 대해 담당한다[비특허문헌 18에서 제안됨].

[0029] 도 4는 10개의 노드와 7개의 데이터 항목을 갖는 6비트 코드 식별자 서클을 도시한다. N8이 K5의 시계 방향으로의 다음 노드인 후속 노드(Successor)임을 나타내며, K43의 후속 노드는 그 식별자가 동일한 N43이다. 모든 노드는 식별자 서클에서 다른 노드를 가리키는 핑거 테이블이라는 라우팅 테이블을 유지한다. 핑거 테이블은 n비트의 식별자를 갖는 원형 안에 n개의 엔트리(entry)가 있다. 노드 p에서 행 i의 핑거 테이블 엔트리는 적어도 2^{i-1}만큼 p에 후속하는 제 1 노드, 즉 후속 노드 ($p + 2^{i-1}$)를 식별한다. 여기서 $1 \leq i \leq n$이다. 예를 들어, 제 3 핑거($8 + 2^2 = 12$)는 N15이다. 핑거 테이블 내의 노드의 i 번째 핑거는 식별자 서클에서 항상 직후의 노드이다. 라우팅 목적을 위해 각 핑거 엔트리는 노드 ID와, IP 주소 및 포트의 쌍으로 구성된다. p와 p의 핑거 테이블에서 수적으로 가장 가까운 후속값 사이에 K가 놓이는 식으로 쿼리가 노드 p에 도달하면, 노드 p는 쿼리에 대한 응답으로서 후속자에게 보고한다.

[0030] 이하, 본 발명의 실시 예에 의한, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 대해 설명하기로 한다.

[0031] 내결함성 분산 위치 관리를 구현하기 위해 핑커 테이블 기반 코드 DHT를 선택한다. 코드(Chord)는 O(logm) 시간에 MN의 위치 바인딩을 저장, 업데이트 및 검색하기 위한 단순하고 효율적인 프로토콜이기 때문에 바람직하다. 여기서, m은 셀룰러 네트워크에서 액세스 네트워크의 총수이다.

[0032] 본 발명의 실시 예에서 모든 이동 노드(MN)는 ID(식별자)(예를 들어, SIP와 같은 URI SIP : MNO@abc.com) 또는 MN의 고정 IP 어드레스에 의해 고유하게 식별된다. 이 ID는 변경되지 않는다. 모바일 네트워크는 AN(액세스 노드)로 구성된다. 집중형 네트워크에서, LR(위치 레지스터)은 독립적인 엔티티이다. 모든 AN에 LR 평션들을 분배할 수 있다. 즉, AN은 AR(액세스 라우터) 평션과 LR 평션을 모두 가진다. MN은 AN의 AR을 통해 인터넷에 액세스할 수 있다. IP 접두사는 AR에 연결된다. 즉, MN이 AN j에 의해 관리되는 경우, MN은 접두사가 AN j의 AR에 연결된 IP 어드레스를 얻는다. MN의 위치는 LR에 의해 관리되고, LR은 MN의 ID와 접두사 사이의 관계를 알고 있다. 따라서 MN의 위치를 아는 것은 그 IP 어드레스를 아는 것과 같다.

[0033] 데이터 항목은 MN의 ID이고, 노드는 모바일 네트워크의 AN이다. MN의 ID와 AN의 네트워크 접두사에 의해 생성된 해시 값을 사용하여 키와 AN을 코드 서클에 매핑한다. 각 MN은 K를 생성하는 데 사용되는 고유 ID인 ID_{MN}을 갖는다. AN 네트워크 접두사의 해시 값과 MN ID의 해시 값은 동일한 주소 공간에 매핑된다. LR은 셀룰러 네트워크에서 MN의 위치 바인딩 정보를 유지한다. LR의 각 엔트리는 K-V 쌍을 유지한다. 제안된 시나리오에서, K는 ID_{MN}의 해시이며, V는 MN의 현재 IP 어드레스이다

[0034] 본 발명의 실시 예에 의한 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법은, 분산 위치 서버에서 K[이동노드(MN)의 고유 아이디(ID_{MN})의 해시]-V[MN의 현재 IP 어드레스] 쌍의 메인 복사본을 추가 또는 업데이트하는 단계; 상기 분산 위치 서버에서 K-V 쌍의 백업 복사본을 추가 또는 업데이트하는 단계; 및 TALM(ticket-based authentication mechanism) 프로토콜을 수행하는 단계를 포함한다.

[0035] **[분산 위치 서버에서 K-V 쌍의 추가 또는 업데이트 단계]**

[0036] 본 발명의 실시예에서는 내결함성 분산 위치 서버를 제안했다. 이동 노드(MN)의 위치 바인딩의 단일 수준의 복제를 통해 내결함성을 달성한다. 이동 노드(MN)의 위치 바인딩의 메인 및 백업 복사본을 유지하는 두 피어[즉, 액세스 노드(AN)]가 동시에 다운 될 가능성은 제로에 가깝다. 따라서 도 5에 도시된 바와 같이 단일 수준의 복제만을 고려하는 것이 타당하다. 도 5는 8개의 액세스 노드(AN)가 매핑된 코드 서클을 보여준다. 이 도면은 AN7에 유지되는 K-V 쌍의 백업 복사본이 AN3에서 유지되는 메인 복사본의 실패인 경우 CN(Correspondent Node)에 의해 액세스 되는 것을 보여준다.

[0037] 분산 위치 서버에서 K-V 쌍의 추가 또는 업데이트 단계를 K-V 쌍의 메인 복사본을 추가 또는 업데이트 단계와, K-V 쌍의 백업 복사본을 추가 또는 업데이트하는 단계를 구분하여 설명하기로 한다.

[0038] <u>K-V 쌍의 메인 복사본을 추가 또는 업데이트 단계</u>

[0039] K-V 쌍의 메인 복사본의 추가 또는 업데이트의 단계별 절차를 도 1 및 6을 참조하여 설명하기로 한다.

[0040] K-V 쌍의 메인 복사본의 추가 또는 업데이트시 그 쌍은 코드 서클에서 K = 해시(ID_{MN})의 첫 번째 후속자인 피어(peer)에 할당된다.

[0041] 현재 연결되어 있는 AN(즉, 피어)를 통해, 이동 노드(MN)는 위치의 등록 또는 업데이트를 그 기본 LR로 전송한다. 키와 함께 저장되는 위치 정보는 MN의 현재 IP 주소이다.

[0042] 피어는 이동 노드(MN)에서 위치의 등록 쿼리 또는 업데이트 쿼리를 받으면 자신이 관리하는 어드레스 공간에 K가 포함되어 있는지 여부를 확인한다. K가 포함되어 있는 경우 위치를 등록 또는 업데이트하고, 확인응답을 이동 노드(MN)에 통지한다. K가 포함되어 있지 않은 경우 그것의 핑거 테이블을 확인하여 코드 서클에서 K의 가장 가까운 후속자를 찾아 그 후속 노드에 쿼리를 전송한다. 이 과정은 관련 K를 관리하는 타켓 노드를 찾을 때까지 계속된다. 10개의 AN이 6비트 코드 서클에 매핑되는 간단한 예제의 도움으로, 본 발명의 실시예의 분산 위치 서버에서 K-V 쌍을 추가 또는 업데이트하는 프로세스를 설명한다. 도 6은 K-V 쌍의 추가 또는 업데이트 프로세스를 나타낸다.

[0043] 먼저, 이동 노드(MN)가 그 위치를 등록 또는 업데이트하기 위해 코드 서클 내에서 현재 선으로 연결되어있는 액세스 노드(AN)(도 6에서는 AN8임)에 연결한다(S110).

[0044] 이어서, 스텝(S120)에서는 액세스 노드(AN8)가 그것의 위치 레지스터(LR)로 이동 노드(MN)의 위치 등록 또는 업데이트를 요청한다.

[0045] 스텝(S130)에서는 액세스 노드(AN8)가 핑거 테이블을 확인하여 코드 서클상의 가장 가까운 K의 후속자(AN43)를 검색한다.

[0046] 좀 더 상세하게 설명하면, 액세스 노드(AN8)의 위치 레지스터(LR)는 K = 해시(ID_{MN})를 계산한다. 기본 위치 레지스터(AN8의 LR)는 그것에 의해 관리되는 주소 공간이 K를 포함하는 지의 여부를 확인한다. LR는 K를 찾아 내지 못한다. 따라서 액세스 노드(AN8)는 코드 서클상의 가장 가까운 K의 후속자를 검색하기 위해 핑거 테이블을 확인한다. 도 6에 도시된 바와 같이, K에 가장 가까운 후속은 AN43이다.

[0047] 스텝(S140)에서는 액세스 노드(AN8)가 위치의 등록 쿼리 또는 업데이트 쿼리를 후속자(AN43)에게 전송한다.

[0048] 스텝(S150)에서는 액세스 노드(AN43)의 위치 레지스터(LR)가 이동 노드(MN)의 위치 바인딩 정보를 저장 / 업데이트한다.

[0049] 스텝(S160)에서는 후속자(AN43)의 위치 레지스터(LR)가 역 쿼리 경로에서 등록 응답을 이동 노드(MN)에 회신한다.

[0050] CN(Correspondent Node)으로부터의 위치 검색 쿼리는 위와 같은 방법으로 처리된다. 위치 쿼리의 결과로서 CN은 ID_{MN}를 제공 할 때 이동 노드(MN)의 현재 IP 어드레스를 얻는다.

[0051] <u>K-V 쌍의 백업 복사본을 추가 또는 업데이트 단계</u>

[0052] K - V 쌍의 백업 복사본의 추가 또는 업데이트시, 그 쌍은 코드 서클상의 K' = 후속자(해시(ID_{MN})) + (2^n / 2)의 첫 번째 후속자인 피어에 할당된다. K-V 쌍의 백업 복사본 추가 또는 업데이트 단계는 메인 복사본의 추가 또는

업데이트에 대해 설명한 것과 동일하다. 제안된 메커니즘 내의 AN(피어)의 실패는 전형적인 P2P 시스템과는 대조적인 드문 경우임을 강조한다.

[0053] **[TALM(ticket-based authentication mechanism) 프로토콜 수행 단계]**

[0054] 본 발명의 실시예에서는 분산 위치 관리 방식에 보안을 제공하는 TALM 프로토콜을 제안한다. 인증 프로세스는 다음의 두 부분으로 나눌 수 있다.

[0055] 첫째, 이동 노드(MN)의 보안 인증서(인증을 수행함)가 만료 된 시점 또는 이동 노드(MN)가 처음 온되었을 때의 인증(티켓 생성 및 만료).

[0056] 둘째, 이동 노드(MN)가 이전 액세스 라우터(AR)에서 필요한 보안 인증서를 획득해야 하는 이동 노드(MN)의 IP 핸드오버시 인증(이전 AR에서 티켓 수집).

[0057] AN = AR + LR로 정의된다. 즉, 액세스 노드(AN)는 AR(액세스 라우터)와 LR(위치 레지스터) 기능을 모두 가진다.

[0058] 프로토콜에서 광범위하게 사용되는 기호는 다음의 [표 1]에 열거되어 있다.

표 1

[0059]

심벌	의미
MN을 위해 사용된 심벌들	
X	메시지
AS	인증 서버
MN	이동 노드
A ‖ B	메시지 A 및 B의 결합
K_{A-B}	A와 B사이에 공유된 키
E(K, X)	키 K를 사용하여 암호화된 메시지 X
N_A	A에 의해 생성된 난수(랜덤한 넘버)
ID_{MN}	MN의 고유 ID
AR	액세스 라우터
ID_{AR}	AR의 고유 ID
TK	티켓
TT	시작 타임과 종료 타임

[0060]

[0061] 인증 서버(AS)와 이동 노드(MN) 사이에서 공유되는 키인 K_{AS-MN} 및 AR과 AS 사이에서 공유되는 키인 K_{AS-AR}이 이미 존재한다고 가정한다. 인증 서버(AS)는 이동 노드(MN) 및 액세스 라우터(AR)와 공유하는 세션 키(K_{MN-AR})를 제공하기만 하면 된다.

[0062] **<u>티켓 생성과 만료</u>**

[0063] 티켓 생성과 만료를 위한 TALM 단계를 도 2 및 도 7을 참조하여 설명하기로 한다.

[0064] 먼저, 이동 노드(MN)가 온(On) 된 직후 액세스 라우터(AR)를 등록 할 필요가 있을 때, 이동 노드(MN)에서 액세스 라우터(AR)에 초기 메시지(MN_{Reg})를 송신하거나, 이동 노드(MN)가 이전 티켓의 만료 때문에 새로운 티켓을 생성한다(S210).

[0065] MN -> AR : $MN_{Reg}(ID_{MN} \| ID_{AR} \| N_{MN})$

[0066] N_{MN}은 이동 노드(MN)에 의해 생성되는 보수(난수)이다.

[0067] 이어서, 스텝(S220)에서는 액세스 라우터(AR)가 초기 메시지(MN_{Reg})를 수신하면 자신의 난수를 추가하여 메시지($MN_{Reg}AS_{Msg}$)를 생성하여 인증 서버(AS)에 송신한다.

[0068] AR-> AS : $MN_{Reg}AS_{Msg}(E(K_{AR-AS}, ID_{MN} \| ID_{AR} \| N_{MN} \| N_{AR}))$

[0069] 액세스 라우터(AR)는 인증 서버(AS)와 공유하는 키를 사용하여 AS에 보내기 전에 이 메시지를 암호화한다.

[0070] 스텝(S230)에서는 인증 서버(AS)가 다음의 티켓을 생성한다.

[0071] $TK = E(K_{TK}, K_{MN-AR} \| ID_{MN} \| TT)$

[0072] 이 티켓은 다른 키(K_{TK})를 사용하여 암호화된다. 이 티켓 내에는 K_{MN-AR}(MN과 AR 사이에서 공유됨)과 이 티켓이 유효한 시간(TT)이 있다. 인증 서버(AS)는 K_{MN-AR}를 이동 노드(MN)및 액세스 라우터(AR) 모두에 전송하길 원한다.

[0073] 스텝(S240)에서는 인증 서버(AS)가 액세스 라우터(AR)에 이동 노드(MN)와 액세스 라우터(AR)가 공유하는 키(K_{MN-AR})를 전송할 메시지(AS_{Res})를 송부한다.

[0074] $AS \rightarrow AR : AS_{Res}(ID_{MN} \| TK \| E(K_{MN-AS}, K_{MN-AR} \| ID_{AR} \| TT \| N_{MN})$

[0075] $E(K_{AR-AS}; K_{TK} \| TT \| N_{AR}))$

[0076] 액세스 라우터(AR)는 메시지의 $E(K_{AR-AS}, K_{TK} \| TT \| N_{AR})$ 부분만을 추출 할 수 있다. AR이 K_{TK}을 취득하면 TK를 복호화하여 K_{MN-AR}을 추출 할 수 있다.

[0077] 스텝(S250)에서는 액세스 라우터(AR)가 메시지(RegRes)를 사용하여 K와 이동 노드(MN)가 통신하게 한다.

[0078] $AR \rightarrow MN : RegRes(ID_{MN} \| TK \| E(K_{MN-AS}, K_{MN-AR} \| ID_{AR} \| TT \| N_{MN})$

[0079] AS와 그 키를 이용할 때, MN은 K_{MN-AR}을 추출 할 수 있다.

[0080] 스텝(S260)에서는 이동 노드(MN)가 위치 업데이트 메시지와 함께 마지막 메시지(AuthMsg)를 액세스 라우터(AR)로 전송하여 자신을 인증한다.

[0081] 액세스 라우터(AR)와 이동 노드(MN) 모두가 K_{MN-AR}을 가지고, 티켓의 만료를 알고 있다.

[0082] $MN \rightarrow AR : AuthMsg\ (ID_{AR} \| TK \| E\ (K_{MN-AR}; ID_{MN} \| IP\text{-}Addr \| \ (N + 1)\ MN))$

[0083] 액세스 라우터(AR)가 메시지를 성공적으로 해독하면 이동 노드(MN)는 자신을 성공적으로 인증한 것이다. IP-Addr은 안전하게 전송된 이동 노드(MN)의 현재 IP 어드레스이다. 메시지에서 난수가 사용되어 man-in-the-middle 재생 공격을 방지한다. 메시지의 흐름을 도 7에 도시한다.

[0084] **이전 액세스 라우터(AR)에서의 티켓 수집**

[0085] 이전 액세스 라우터(AR)에서의 티켓 수집 단계를 도 3 및 도 8을 참조하여 설명하기로 한다.

[0086] 먼저, 이동 노드(MN)가 K_{MN-AR}에 대해서 알지 못하는 nAR[이동 노드(MN)의 새롭게 첨부 된 액세스 라우터(AR)]에 메시지(nAR_{Reg})를 전송한다(S310).

[0087] $MN \rightarrow nAR : nAR_{Reg}(TK \| ID_{MN} \| N_{MN} + 1)$

[0088] 여기서, N_{MN}은 MN에 의해 생성된 난수이다.

[0089] 이어서, 스텝(S320)에서는 nAR이 메시지(nAR_{Reg})를 수신하고 K_{MN-AR}을 갖는 pAR (이전에 첨부된 MN의 AR)에 메시지($MN_{Reg-pAR}$)를 전송한다.

[0090] $nAR \rightarrow pAR : MN_{\ Reg-pAR}\ (E(K_{pAR-nAR}, ID_{MN} \| NMN + 1))$

[0091] 스텝(S330)에서는 pAR이 티켓 유효 시간 및 키(K_{TK})에 대한 정보를 추가하여 메시지(MN_{RegRes})을 nAR에게 다시 전송한다. pAR은 nAR와 공유하는 키를 사용하여 이 것을 암호화한다.

[0092] $pAR \rightarrow nAR : MN_{RegRes}(E(K_{pAR-nAR}, ID_{MN} \| TT \| K_{TK}))$

[0093] nAR은 pAR와 공유하는 키를 사용하여 티켓을 얻기 위해 메시지(MN_{RegRes})를 해독한다. K_{TK}을 취득하면 TK를 해독하

고 K_{MN-AR}을 추출한다. 도 8에 메시지의 흐름이 도시된다.

[0094] 본 섹션에서는 제안된 위치 관리를 안전하게 만드는 프로토콜(TALM)을 제안했다. 이동 노드(MN)가 액세스 라우터(AR)와 어떻게 상호 작용하는지, 그리고 유저 세션을 위해 인증 서버(AS)에 의해 티켓이 어떻게 생성되는지를 설명했다. 또한 인증 대기 시간을 단축하기 위해 티켓을 재사용하는 방법에 대해 설명했다.

[0095] 다음 섹션에서는 TALM의 성능을 평가한다.

[0096] [성능 평가]

[0097] TALM과 EAP-TLS를 비교한다. EAP-TLS 기반 인증은 이동 노드(MN)와 그것의 인증 서버(AS) 간의 EAP 교환을 수행한다; EAP TLS에서 티켓 재사용이라는 개념은 없다. 일반적으로 성공적인 EAP-TLS 인증은 인증 프로세스의 네 단계를 가진다[비특허문헌 17에 개시됨].

[0098] **성능 메트릭**

[0099] 성능 메트릭을 계산함으로써 본 발명의 실시예에 의한 프로토콜을 평가하고, 그 결과를 EAP-TLS의 결과와 비교한다. 시뮬레이션 프로그램은 C ++로 작성된다. 시뮬레이션 시간은 1 년이다.

[0100] 인증 대기 시간 : 인증 대기 시간은 티켓을 생성하거나[처음으로 액세스 라우터(AR)에 자신을 인증하는 이동 노드(MN)에 의해 생성], 만료 될 때 티켓을 갱신하거나, 또는 IP의 핸드오버의 경우 티켓을 이전의 AR로부터 다시 얻기 위한 대기 시간이다. IP 핸드오버는 이동 노드(MN)가 그 네트워크 액세스 포인트를 변경할 경우 발생한다. 평균 인증 대기 시간은 일정 기간의 누적된 인증 대기 시간을 그 기간 내의 위치 업데이트 메시지의 총수로 나눔으로써 산출된다.

[0101] 위치 업데이트 메시지 당 인증 메시지의 수: TALM 프로토콜 단계를 필요로 하는 경우에 일정 기간의 인증 메시지 수는 그 기간 내에 이전의 액세스 라우터(AR)로부터의 티켓 생성, 티켓 갱신 및 티켓 수집의 경우 이동 노드(MN)가 AR에 대해 자신이 인증하는 횟수이다. 위치 업데이트 메시지 당 인증 메시지의 수는 이동 노드(MN)에 의해 실행되는 총 인증 수를 일정 기간 내에 MN에 의해 전송되는 위치 업데이트 메시지의 총수로 나눠 계산된다.

[0102] **TALM 인증 대기 시간의 계산**

[0103] 액세스 라우터(AR)와 인증 서버(AS) 사이의 홉(hops) 수를 nhops로 하고, 1 홉에서의 메시지 전송 지연을 T_{MN-AR}로 하며, 이동 노드(MN)에서 인증 서버(AS)로의 메시지 전송 지연을 T_{MN-AS}하자.

[0104] [비특허문헌 17]에서 정의된 것과 동일한 파라미터 설정을 사용한다. 구간 [5,9](즉, T_{MN-AR} = 20ms)에서 nhops 값을 선택하고, 구간 [10, 40] m/s에서 MN의 속도가 취해지고, 구간 [100, 200] m에서 MN에 대한 AR-에리어(area)의 반경이 취해진다.

[0105] 액세스 라우터(AR)과 인증 서버(AS) 사이에는 n 홉이 있을 수 있다. 따라서 액세스 라우터(AR)에서 인증 서버(AS)까지의 메시지 전송 지연은 T_{AR-AS} = nhops∽T_{MN-AR}이다.

[0106] 이동 노드(MN)에서 인증 서버(AS)로의 메시지 전송에 있어서, 지연은 두 부분으로 분할된다. 첫째, 메시지가 이동 노드(MN)에서 액세스 라우터(AR)로 전송되고, 두 번째, 메시지가 액세스 라우터(AR)에서 인증 서버(AS)에 보내어질 때이다. 이 전송 지연은 $T_{MN-AS} = T_{MN-AR} + T_{AR-AS}$ = 20ms + (nhops × T_{MN-AR})이다.

[0107] 티켓 생성 메시지의 순서는 다음과 같다.

[0108] 1) MN-> AR; 1 홉, 0.02s

[0109] 2) AR-> AS; n 홉, n×0.02s

[0110] 3) AS-> AR; n 홉, n×0.02s

[0111] 4) AR-> MN; 1 홉, 0.02s

[0112] 5) MN-> AR; 1 홉, 0.02s

[0113] 홉 당 메시지 전송 지연이 0.02s이기 때문에, 이동 노드(MN)과 액세스 라우터(AR) 사이의 홉 수는 1이며, 액세스 라우터(AR)와 인증 서버(AS) 사이의 홉 수는 nhops이기 때문에, 전체 인증 프로세스 시간 = T(MN → AR)+T(AR → AS) + T(AS → AR) + T(AR → MN) + T(MN → AR) = 0.02 + (nhops×0.02) + (nhops×0.02) +

0.02 + 0.02s 이다.

[0114] 티켓 생성 메시지의 순서는 다음과 같습니다.

[0115] 1) MN-> nAR; 1 홉, 0.02s

[0116] 2) nAR-> pAR; 1 홉, 0.02s

[0117] 3) pAR-> nAR; 1 홉, 0.02s

[0118] (이전 AR에서의) 티켓 수집 시간 = T(MN-> nAR) + T(nAR-> pAR) + T(pAR-> nAR) = 0.02 + 0.02 + 0.02s.

[0119] **EAP-TLS의 인증 대기 시간의 계산**

[0120] 초기 인증 지연은 이동 노드(MN)가 그것의 만료시에 티켓을 만들거나 업데이트 할 때의 인증 지연이다. [비특허문헌 17]에서 계산된 바와 같이, 그것은 $3T_{MN-AR} + T_{AR-AS} + T(m, T_{MN-AS})$이며, 여기에서 T_{MN-AR}는 MN과 AR 간의 전송 지연이며, T_{AR-AS}는 AR과 AS 간의 전송 지연이며, $T(m, T_{MN-AS})$는 m=4일 때의 T의 함수이며, MN과 AS 사이의 전송 지연은 $T_{MN-AR} + T_{AR-AS}$이다.

[0121] [비특허문헌 17]에서 계산된 바와 같이, EAP-TLS에서의 핸드오버 인증 지연= L_{12} + 초기 인증 지연 + D_{SA} + D_{RS} + D_{REG} + D_{PLMA}이다. 여기서 L_{12} = 0.04535, $D_{SA} = 4T_{MN-AR}$, D_{RS}는 MN과 AR 사이의 전송 지연이며, $D_{REG} = 2T_{AR-LMA}$, $D_{PLMA} = T_{AR-AS} + T_{MN-AR}$이다.

[0122] **결과와 논의**

[0123] 이하, 네트워크 토폴로지, 파라미터 셋팅, 시뮬레이션 결과, 및 결과 논의를 제공한다.

[0124] 도 9에 도시된 바와 같은 상황에서 19의 육각형 AN의 랩-어라운드 셀 네트워크 토포로지가 사용되었다.

[0125] 시뮬레이션을 위해, [비특허문헌 7], [비특허문헌 19] - [비특허문헌 21]에서 선택된 지수 분포의 확률 변수가 될 AN-영역의 체류 시간 α을 선택한다. [표 2]의 7개의 시나리오 결과는 다음 섹션에 주어져 논의된다.

표 2

[0126]

S. #	성능 메트릭	가변 파라미터	파라미터 값
1	인증 대기시간	nhops	티켓 수명 = 24 hrs, nhops ∈ {5,6,7,8,9}, 속도 = 1 m/s, AN-에리어 = 10^4 km^2
2	위치 업데이트당 인증 메시지 수	티켓 수명	티켓 수명 ∈{12,24,48,72} hrs, nhops =랜덤{5,9}, 속도 = 1 m/s, AN-에리어 = 10^4 km^2
3	위치 업데이트당 인증 메시지 수	MN의 평균 속도	티켓 수명= 24hr, nhops =랜덤{5,9}, 속도 ∈ 1,5,10 m/s, AN-에리어 = 10^4 km^2
4	위치 업데이트당 인증 메시지 수	AN-에리어	티켓 수명= 24hr, nhops =랜덤{5,9}, 속도 = 1 m/s, AN-에리어 ∈ 10^4,10^3,10^2,10,1 km^2

[0127] **평균 인증 대기 시간**

[0128] TALM의 평균 인증 대기 시간과 EAP-TLS 시간을 비교한다. 이 실험의 가변 매개 변수는 nhops이다. 이 실험 결과

를 도 10에 나타낸다. nhop가 증가하면 두 프로토콜의 평균 인증 대기 시간이 증가한다. 결과는 TALM이 EAP-TLS보다 뛰어난 성능을 보여준다. 도 10에 나타낸 바와 같이 95 % 신뢰 구간에서 TALM의 시뮬레이션 결과를 계산한다. TALM에 의한 인증 대기 시간 감소율은 99%에 거의 가깝다. 이것은 주로 TALM에서의 인증 티켓의 재사용에 의한 것이다.

[0129] **TALM의 위치 업데이트 당 인증 메시지의 평균 수**

[0130] 도 11은 티켓의 유효 기간이 변경 될 때마다 위치 업데이트 당 인증 메시지의 평균 개수를 보여준다. 티켓의 유효 기간의 증가에 따라 위치 업데이트 당 인증 메시지의 평균 개수가 감소한다. 티켓의 더 긴 수명을 위해, MN은 수명이 더 짧은 경우 만료 횟수보다 적은 횟수의 인증 티켓 만료에 직면한다.

[0131] 도 12는 이동 노드(MN)의 속도가 변화하는 경우 위치 업데이트 당 평균 인증 메시지 수에 미치는 영향을 보여준다. 속도의 증가에 따라 인증 메시지의 평균수가 증가하는 것을 알 수 있다. 이것은 속도의 증가에 따라 이동 노드(MN)는 더 많은 IP 핸드 오버를 경험하는 이유 때문이다. 따라서 이동 노드(MN)는 더 많은 핸드 오버 인증을 수행하고 그 결과 인증 메시지의 평균 개수가 증가한다.

[0132] 도 13은 액세스 AN-에리어가 변경되었을 경우 위치 업데이트 당 평균 인증 메시지 수에 미치는 영향을 보여준다. AN-에리어의 증가에 따라 인증 메시지의 평균 개수가 감소하는 것을 알 수 있다. 이것은 AN-에리어의 증가에 따라 이동 노드(MN)가 IP 핸드 오버를 덜 받기 때문이다. 따라서 이동 노드(MN)는 더 적은 수의 핸드 오버 인증을 수행하고, 그 결과 인증 메시지의 평균 개수가 감소한다

[0133] 본 발명의 실시예에 의한, 지능형 5G 무선 네트워크를 위한 보안 및 내결함성 분산 위치 관리 방법에 의하면, 분산 위치 서버에서 K[이동노드(MN)의 고유 아이디(ID_{MN})의 해시]-V[MN의 현재 IP 어드레스] 쌍의 메인 복사본을 추가 또는 업데이트하는 단계; 상기 분산 위치 서버에서 K-V 쌍의 백업 복사본을 추가 또는 업데이트하는 단계; 및 TALM(ticket-based authentication mechanism) 프로토콜을 수행하는 단계;를 포함하여 구성됨으로써, 평균 인증 대기 시간이 적고, 위치 업데이트당 인증 메시지의 평균 개수가 감소할 수 있다.

[0134] 좀 더 상세하게는,

[0135] 첫째, TALM에서 인증 티켓의 재사용을 하므로 평균 인증 대기 시간이 종래의 EAP-TLS 프로토콜에 비해 현저히 적다.

[0136] 둘째, 액세스 노드(AN)의 에리어(Area) 증가에 따라 이동 노드(MN)가 더 적은 수의 핸드 오버 인증을 수행하고 그 결과 인증 메시지의 평균 개수가 감소한다.

[0137] 도면과 명세서에는 최적의 실시 예가 개시되었으며, 특정한 용어들이 사용되었으나 이는 단지 본 발명의 실시형태를 설명하기 위한 목적으로 사용된 것이지 의미를 한정하거나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 수 있을 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0138] MN: 이동 노드

AS: 인증 서버

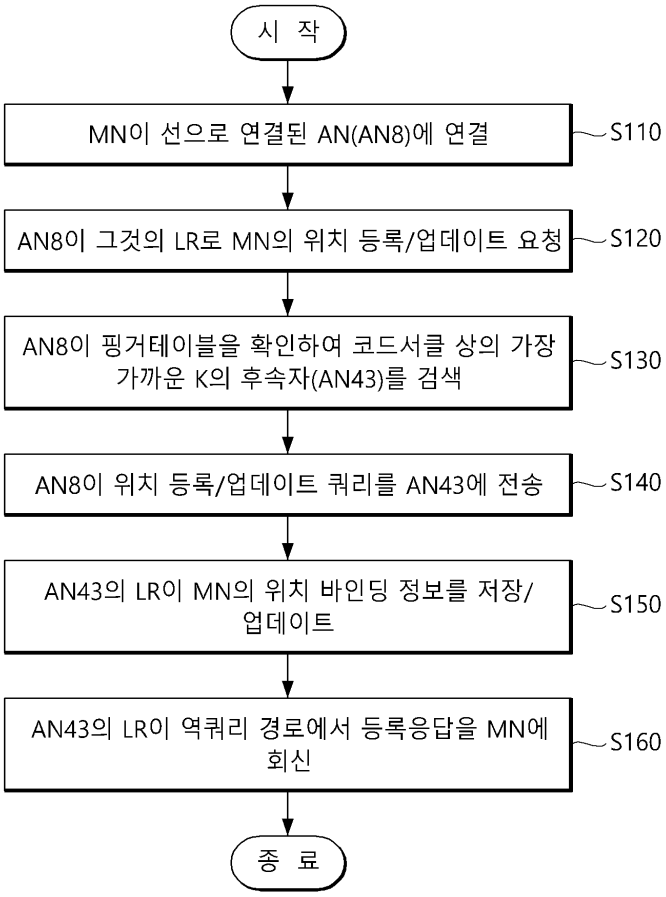
AR: 액세스 라우터

AN: 액세스 노드

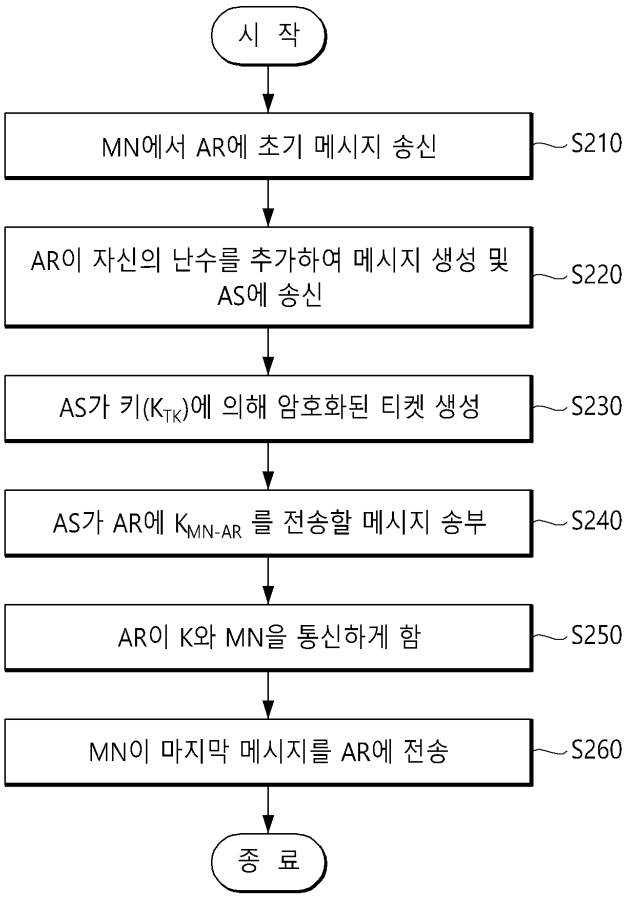
LR: 위치 레지스터

도면

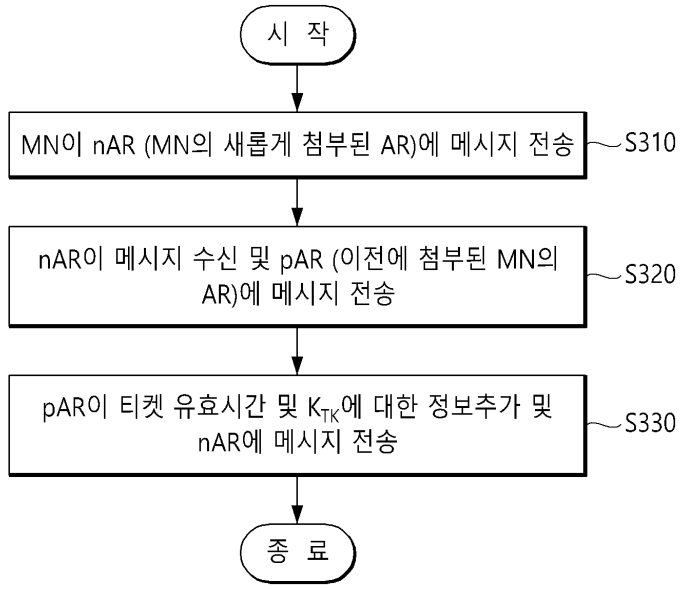
도면1


시 작
MN이 선으로 연결된 AN(AN8)에 연결
S110
AN8이 그것의 LR로 MN의 위치 등록/업데이트 요청
S120
AN8이 핑거테이블을 확인하여 코드서클 상의 가장 가까운 K의 후속자(AN43)를 검색
S130
AN8이 위치 등록/업데이트 쿼리를 AN43에 전송
S140
AN43의 LR이 MN의 위치 바인딩 정보를 저장/업데이트
S150
AN43의 LR이 역쿼리 경로에서 등록응답을 MN에 회신
S160
종 료

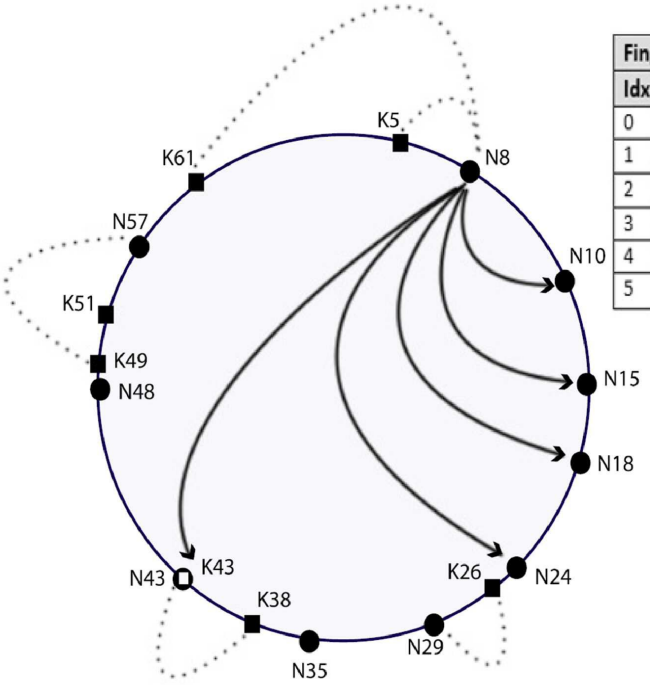
도면2


시 작
MN에서 AR에 초기 메시지 송신
S210
AR이 자신의 난수를 추가하여 메시지 생성 및 AS에 송신
S220
AS가 키(K_{TK})에 의해 암호화된 티켓 생성
S230
AS가 AR에 K_{MN-AR} 를 전송할 메시지 송부
S240
AR이 K와 MN을 통신하게 함
S250
MN이 마지막 메시지를 AR에 전송
S260
종 료

도면3

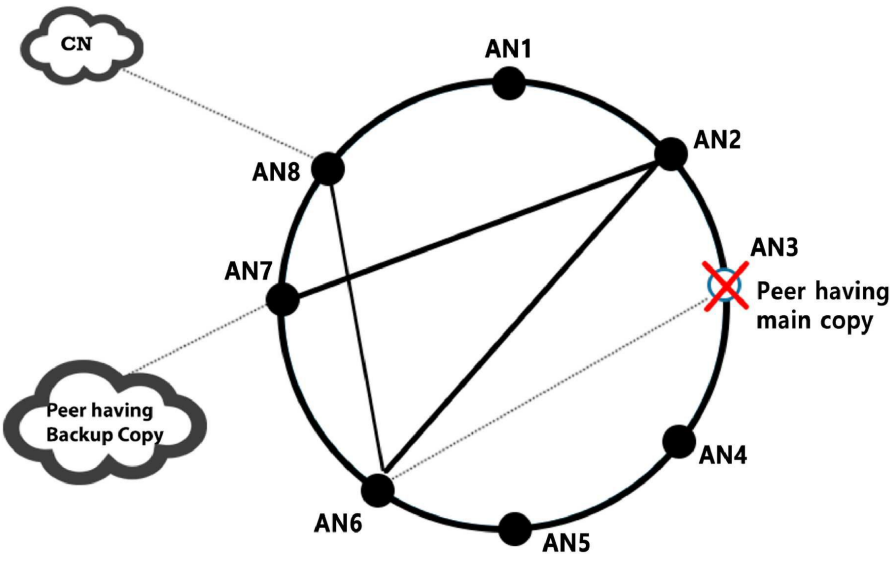

시 작
MN이 nAR (MN의 새롭게 첨부된 AR)에 메시지 전송
S310
nAR이 메시지 수신 및 pAR (이전에 첨부된 MN의 AR)에 메시지 전송
S320
pAR이 티켓 유효시간 및 K_{TK}에 대한 정보추가 및 nAR에 메시지 전송
S330
종 료

도면4

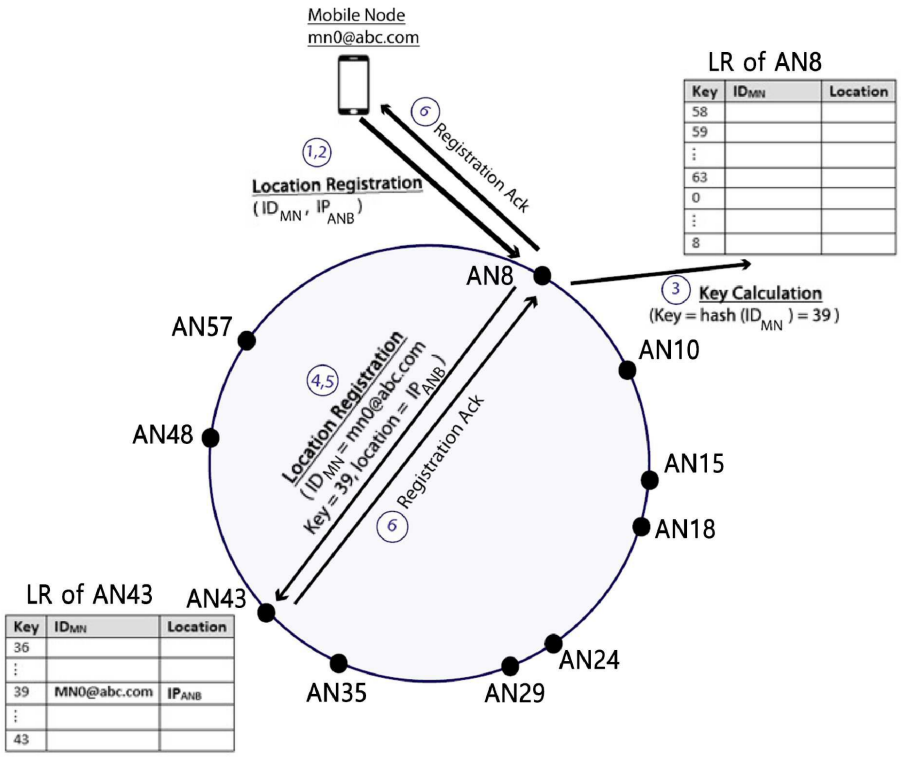


Finger Table of N8		
Idx	Target ID	Successor
0	N8 + 1	N10
1	N8 + 2	N10
2	N8 + 4	N15
3	N8 + 8	N18
4	N8 + 16	N24
5	N8 + 32	N43

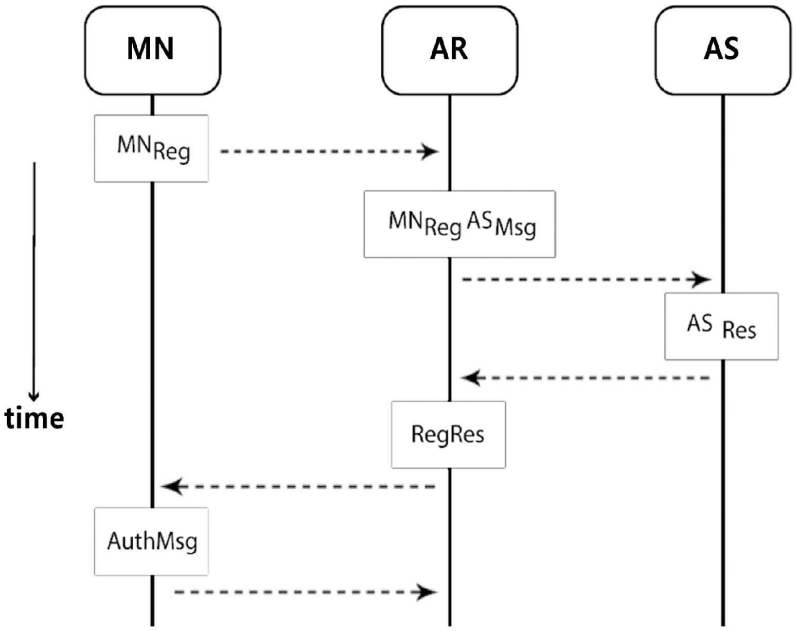
도면5



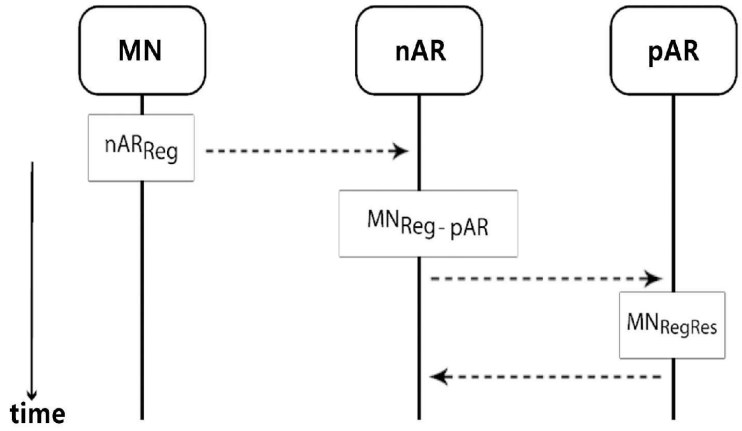
도면6


Mobile Node
mn0@abc.com
(1,2)
Location Registration
(IDMN, IPANB)
(6) Registration Ack
LR of AN8
Key | IDMN | Location
58
59
63
0
8
AN8
(3) Key Calculation
(Key = hash (IDMN) = 39)
AN57
AN10
AN48
AN15
AN18
AN43
AN24
AN35
AN29
(4,5) Location Registration
(IDMN = mn0@abc.com, Key = 39, location = IPANB)
(6) Registration Ack
LR of AN43
Key | IDMN | Location
36
39 | MN0@abc.com | IPANB
43

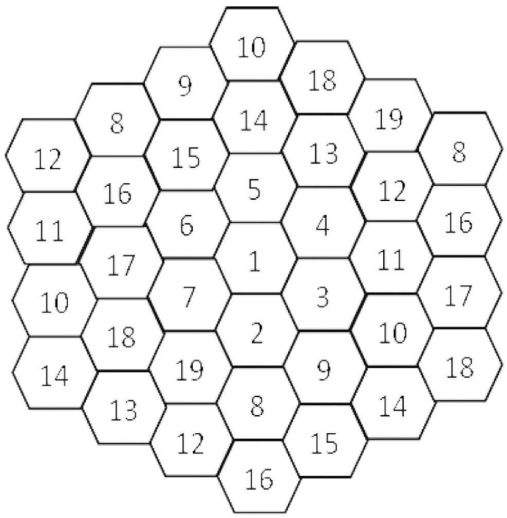
도면7


MN
AR
AS
MNReg
MNReg ASMsg
AS Res
RegRes
AuthMsg
time

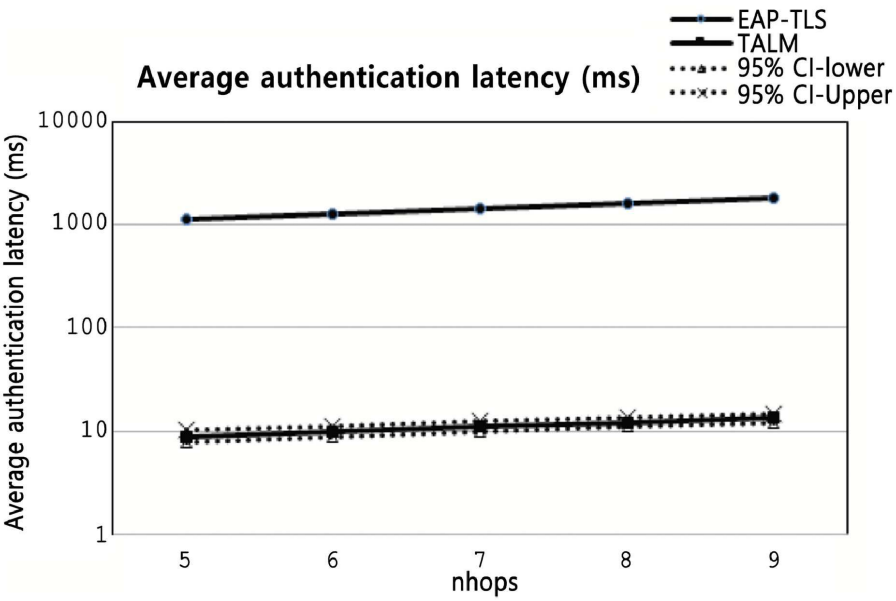
도면8


MN
nAR
pAR
nAR_Reg
MN_Reg - pAR
MN_RegRes
time

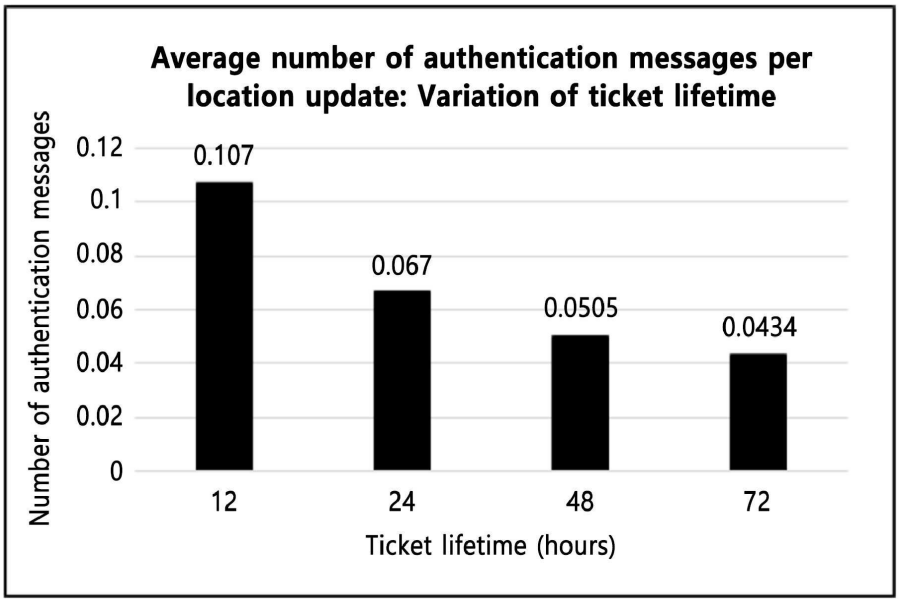
도면9


10
9
18
8
14
19
12
15
13
8
16
5
12
11
6
4
16
17
1
11
10
7
3
17
18
2
10
14
19
9
18
13
8
14
12
15
16

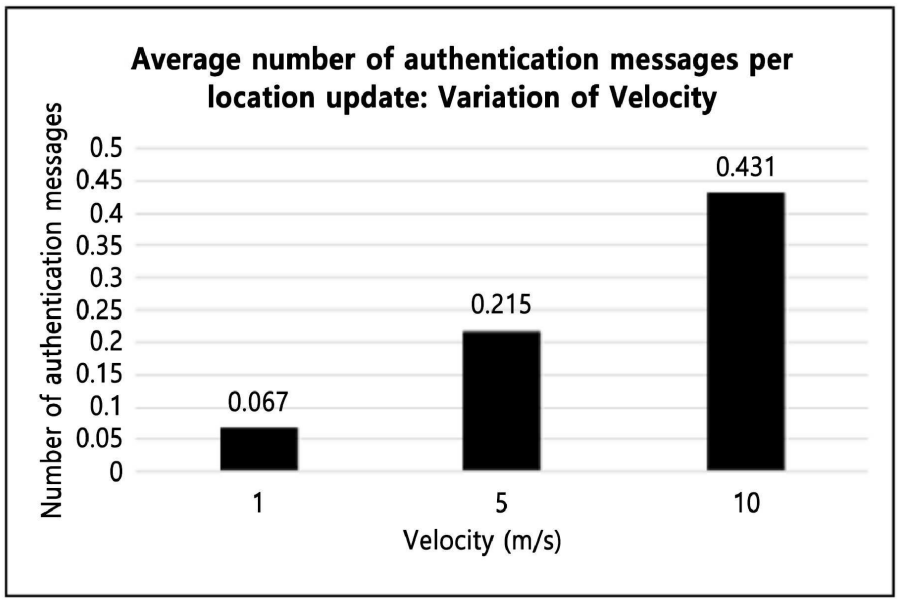
도면10


Average authentication latency (ms)
EAP-TLS
TALM
95% CI-lower
95% CI-Upper
Average authentication latency (ms)
10000
1000
100
10
1
5
6
7
8
9
nhops

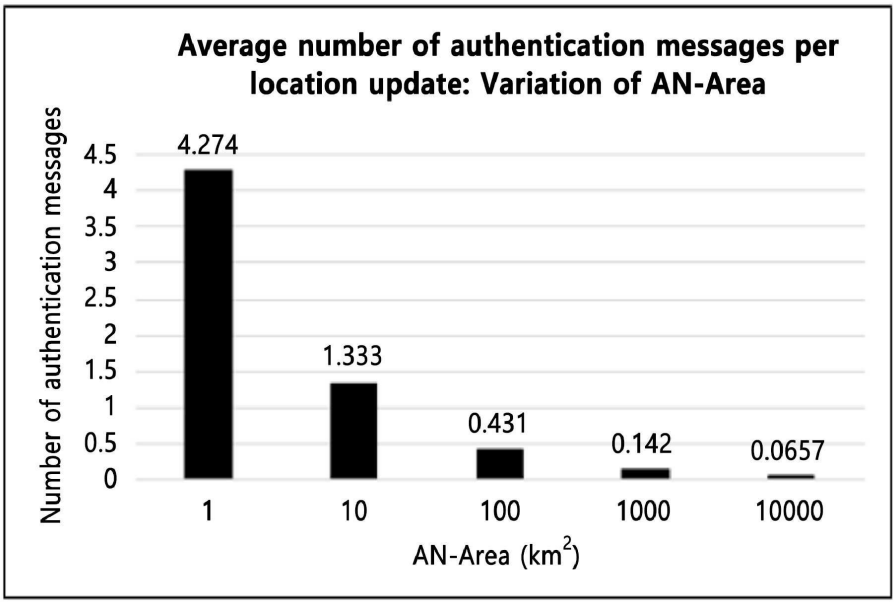
도면11


Average number of authentication messages per location update: Variation of ticket lifetime
Number of authentication messages
0.12
0.1
0.08
0.06
0.04
0.02
0
0.107
0.067
0.0505
0.0434
12
24
48
72
Ticket lifetime (hours)

도면12


Average number of authentication messages per location update: Variation of Velocity
Number of authentication messages
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0.067
0.215
0.431
1
5
10
Velocity (m/s)

도면13



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제6항

【변경전】

상기 티켓 수집 단계는

【변경후】

상기 티켓을 수집하는 단계는