Ad Hoc망의 사용자 인증 메커니즘

이철승* · 박도준* · 신명숙* · 이준**
*조선대학교 대학원 컴퓨터공학과
**조선대학교 전자정보공과대학 컴퓨터공학과

User Authentication Mechanism of Ad-hoc Network

Cheol-seung Lee* · Do-jun Park* · Myung-suk Shin* · Joon Lee**
*Dept. of Computer Engineering Graduate School. Chosun University
**Dept. of Computer Engineering. Chosun University
E-mail : cheolseung@hotmail.com

요 약

본 논문은 Ad-hoc망 환경에서 Kerberos V5 인증 프로토콜을 이용한 사용자 인증 문제를 해결하려고 한다. Ad-hoc망은 기존의 무선망과는 달리 고정 노드가 없이 랜드 자체가 이동 무선 노드들로 구성된 맵이며, DSR 라우팅 프로토콜을 이용하여 경로 설정 문제를 해결한다.

무선망에서 정의한 보안 구조 및 요소, 기존 인증 시스템과 관련된 각종 암호 기술을 살펴본 후, Ad-hoc 기반 구조와 전송 경로 보안등을 이용하여 응용 계층에서의 사용자 인증을 위해 서버 클라 이언트가 지니는 실제 상의 문제점과 이동 노드간의 보안상 취약점을 찾아 대안을 제공한다.

ABSTRACT

In this paper we challenge the user Authentication using Kerberos V5 authentication protocol in Ad-hoc network environment. Ad-hoc network is a collection of wireless mobile nodes without the support of a stationary infrastructure, and DSR routing protocol, which is one of famous mobile ad-hoc routing protocols, has the following network path problem.

this paper is the security structure that defined in a mobile network and security and watches all kinds of password related technology related to the existing authentication system. It looks up weakness point on security with a problem on the design that uses Ad-hoc based structure and transmission hierarchical security back of a mobile network, and a server-client holds for user authentication of an application level all and all, and it provides one counterproposal.

키워드

Ad-hoc, Authentication, Kerberos, Routing

1. 서 론

인터넷의 급속한 성장으로 무선망 사용에 대한 요구가 다양해 채었으며, 시간과 공간의 제한을 받지 않는 새로운 자원의 인터넷 기술인 Ad-hoc망이 필요하게 되었다. Ad-hoc망은 기지국 중심의 통신을 하지 않으며, 망에 포함된 각 노드들이 서로 중계국 역할을 하여 통신한다.

본 논문은 Ad-hoc망에서 신뢰성 있고, 적합한 사용자 인증 문제를 해결하기 위해, 기존의 무선망과는 달리 DSR 라우팅 프로토콜을 이용하여 경로 설정 및 경로 유지를 하며, 무선망의 보안 구조 및 요소, 인증 시스템과 관련된 각종 암호 관련 기술을 살펴본 후, Ad-hoc망과 KerberosV5 인증 프로토콜을 이용하여 이동 노드 사이의 관리 문제점을 해소하고, 응용 레벨의 무선 단말기에서 암호화 알고리즘 실험 결과를 이용하여 성능 분석을 한다.

II. 인증 시스템 기반 기술

2.1 Ad-hoc

Ad-hoc망은 데이터전송에 필요한 고정된 네트워크 기반 시설이나, 중앙 통제 요소가 없이 동적
으로 구성된 노드들이 라우팅에서의 기능을 제공하는 네트워크를 말한다.

우선 말하는 Link-State, Distance-Vector와 같은 효율적인 라우팅 프로토콜을 많이 사용하지만, 변화할 경우를 적응하기가 쉽다. 또한 노드의 제한된 대역폭과 저 전력을 효율적으로 사용하기 위해서 라우팅 오피저울을 줄여야 하는 제약 조건을 가지며, Ad-hoc망에서는 라우팅 프로토콜은 크게 Table-driven방식과 On-demand 방식으로 분류할 수 있다. 전자는 각각의 노드가 링크체 노드에 대한 라우팅 정보를 유지하고 이용해 라우팅을 수행하며, 후자는 망의 모든 노드에 대한 전체 경로를 항상 유지하는 것이 아니라 전송할 데이터가 발생했을 때에 경로를 확
득하고 실제 경로에 대한 정보만을 유지하는 방식
이다[1].

2.2 DSR(Dynamic source Routing)는 Ad-hoc망의 
노드들 사이의 다중 흐름을 지원하는 간단하고 효율 
적인 프로토콜로서, 실제 네트워크 관리나 어떤 기 
반시설에 대한 요구 없이도 스스로 조정되며,
경로 발견과 경로 유지는 완전한 On-demand에 의 
해서 구성되어 질 수 있다. 그러나 라우팅 정보 
교환으로 인해 발생한 불필요한 네트워크 대역
폭 내의 부하를 줄일 수 있고, 노드 자체의 전력에 
관한 문제, 네트워크 내에서 다양한 패킷의 충돌로 
발생되는 문제 등을 감소 시킬 수 있다. 따라서 빠 
르게 변화하는 이동 네트워크의 적응을 원활히 할 
수 있는 여러 장점을 가질 수 있다.

2.3 Kerberos
Kerberos는 중앙집중식으로 하나의 안전한 인증 
서비스를 두어 사용자들을 인증화 할 수 있도록 한 인증
서비스이다. Kerberos v4 가 가장 널리 사용되고 있으며, 
보안 규범을 몇 가지 수정하여 v5 가 Internet draft 표준(RFC1510)으로 발표되었다[5]. Kerberos v5에서는 영역(realm)이라는 개념을 도 
입하여 Kerberos 서버와 여러 개의 클라이언트, 그
리여러 개의 운영 시스템으로 구성된 완전한 서비스의 
Kerberos환경을 구성하였고 다음과 같은 조건
을 필요로 한다.

a. Kerberos 서버는 사용자 ID와 해시된 페스와 
드를 데이터베이스에 가지고 있어야 한다.
b. Kerberos 서버는 각 서버를 제공하는 서버의 
비밀키를 공유하여야 한다.
c. 외부 영역과 상호 인증을 지원하기 위해 각 상호 
운영 영역에는 있는 Kerberos서버는 비밀키를 
다른 영역에 있는 서버와 공유한다.

<table>
<thead>
<tr>
<th>1. Kerberos 인증 절차</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Request Ticket - Granting Ticket</td>
</tr>
<tr>
<td>2. Ticket + Session Key</td>
</tr>
<tr>
<td>3. Request Service - Granting Ticket</td>
</tr>
<tr>
<td>4. Ticket + Session Key</td>
</tr>
<tr>
<td>5. Request Service</td>
</tr>
<tr>
<td>6. Provide Server, Authentication</td>
</tr>
</tbody>
</table>

24 인증 시스템 문제점
무선 인터넷 환경에서 대부분의 인증 프로토콜은 
비밀키 기반 인증 작업을 위해 사전에 비밀에 일치하는 
네트워크를 필요로 하며, 무선 인터넷 환경의 동적으로 변화하는 대역 
폭과, 높은 전송률 무선 단말기의 임약성 때문에 
공개키 암호화 기법은 무선 환경에 맞지 않으며, 
또한 Ad-hoc망의 경로 설정 요청에 네트워크 부하 
및 프로토콜 변환을 위한 라우팅 기법이 불가피 하 
는 문제점이 발생하였다[1]. 또한 신속한 재요청 설 
정을 위한 다중 경로를 고려해야 하며, 이중 단말 
간의 호환성과, 신뢰할 수 있는 보안 및 적법한 인 
증 문제를 사급한 실정이다.

3.1 Ad-hoc망의 인증 메커니즘
본 장에서는 Kerberos 인증 프로토콜을 이용하 
여 Ad-hoc망의 노드간 인증 메커니즘을 설계한다. 
기존 인증 기술 및 인증 시스템의 문제점과 제안 
한 인증 메커니즘의 요구 사항과 구성 요소들을 고 
려한 후, Ad-hoc망의 적합성 여부를 평가 및 분석
하여 Ad-hoc망의 보안 인프라를 구축한다.
본 인증 메커니즘은 CA에서 인증한 사용자 정보를 
羌 Ad-hoc망에서 유효기간 내에 적절 인증이 
가능하도록 해주며, 각 노드의 라우팅 캐시에 내 
부 테이터, 암호화 등을 안전하게 저장할 수 있 
어 보안성 및 투명성에 유의하게 하였다.

Ad-hoc망의 DSR 프로토콜은 이용하여 경로 
설정 과정 및 경로 유지를 하며 Kerberos 프로토 
콜 절차를 융동하여 소스 노드가 접근하려는 목 
적지노드에 보안성을 강화하였다.

3.2 DSR의 경로 설정
DSR 프로토콜은 어떤 소스 노드가 목적지노드로 
패킷을 보내려고 할 때 모든 라우팅에 대한 정보를 알고 있지 않은 관계로 소스노드에서 목적지노드의 경로에 대한 정보를 알아내야 한다.
소스노드는 패킷 전송을 위한 경로가 필요할 때 경 
로 요구(RREQ : Route Request) 패킷을 인접한 노
드로 보드캐스트하여, 중간노드에서 목적지노드 
까지의 경로를 얻거나, 목적지노드를 찾을 때까지 
계속 보드캐스트 된다[2].
목적지노드나 목적지노드까지의 경로를 가지고 
중간노드들이 RREP 패킷을 소스노드로 응답하여
경로 발견 과정을 마치게 된다. 목적지 노드에서는 경로에러가 발견되었을 때 사용하기 위한 다중 경로를 응답한다. 소스노드에서는 응답 받은 다중경로 중 최선의 경로를 선택하여 패킷 전송을 시작하고, 다른 경로들은 라우트 캐쉬에 저장해 둔다.

그림 1. 다중 경로의 응답

그림 1은 소스노드(X)에서 목적지노드(Y)로의 다중경로를 응답 받는 경우를 보여주고 있다. X는 경로 발견을 위해 RREP패킷을 생성하여 브로드캐스트한 후, 일정 시간 동안 RREP의 응답을 기다린다. X는 일정 시간 동안 도착한 RREP중 최적의 경로를 선택하고 2개의 후보 경로를 더 선택한다. X에서 최적 경로 선택 후, 다른 RREP가 도착할 경우, 다시 경로 선택을 수행한다. X는 경로의 흐름을 계산하여 현재 사용 중인 경로보다, 최적이지 않으면 사용 가능한 경로를 후보 경로로 만들고, 도착한 경로를 사용한다. 만약 현재 사용 경로보다 최적의 경로는 아니지만 보관하고 있는 후보 경로보다 최적이면 후보 경로를 대체하여 도착한 경로를 사용한다. 결국 X는 경로의 최적 경로에 따라 3개의 다중 경로를 보관한다. 이때, 보관할 필요가 없는 경로는 라우트 캐쉬의 라이브러리 동체에 의해 자동으로 삭제된다.

3.3 DSR의 경로 유지

경로 유지 단계(Route Maintenance)는 앞에서 획득한 정보를 보관/유지하는 알고리즘이다. 소스 경로 상에 있는 어떤 연결이 실패하면 목적지노드(Y)가 경로 정보를 다시 요청하기 때문에, 소스 노드(X)는 경로 에러(RERR: Route Error)패킷을 발생시키며 X의 캐쉬로부터 실패한 경로를 삭제하게 된다. 만약 X의 라우트 캐쉬에 다른 후보 경로가 존재하 면, 경로를 전송하고, 이러한 경로가 없을 때에는 다시 경로 설정 단계를 시작하게 된다.

그림 2는 소스노드(X)에서 목적지노드(Y)로 패킷을 전송할 때 패킷에는 A,B,C 노드로 거쳐서 전송되는 경로에 대한 정보가 포함되어 있다. 최초 X에서 A로 패킷이 전달되면, A는 X에게 응답 신호를 보내며, B,C 노드들도 같은 방법으로 응답 신호를 보낸다. 그러면 그룹 경로가 파손되었을 경우 C는 B에게 응답 신호를 보내지 못하게 되고, B가 경로 파손을 감지하여 경로 유지 알고리즘을 사용한다. B가 C로부터 응답 신호를 받지 못하거나 제한 시간이 지나서 패킷을 재 전송할 경우 B는 Y로 가는 다른 경로로 라우트 캐쉬에 검색한다. 단일 B에 Y로 가는 다른 경로가 있으면 노드는 전달해야 할 데이터 패킷의 헤더를 지우고 라우트 캐쉬에서 검색된 새로운 경로를 라우트 헤더로 바绿色通道。그러나 B가 Y로 가는 다른 경로를 라우트 캐쉬에 가지고 있지 않으면 B는 데이터 패킷을 버린다. 또한 Y로의 RREQ도 생성하지 않는다. 대신에 B는 Y로 Route Error 메시지를 보낸다. Y가 노드 B로부터 Route Error 메시지를 받으면 Y의 라우트 캐쉬에 저장되어 있는 D로 가는 경로를 지우고 Route Error 메시지를 이웃 노드에게 전파하여 패킷이 전달되지 않았음을 알린다.

이와같이 라우트프로토콜을 이용하여 X에서 Y로 연결이 이루어지면 X는 Kerberos 인증 서버(AS)에 접속하여 인증 과정을 거친다.

그림 2. 경로 유지

3.4 접속 및 사용자 인증

먼저 소스노드(X)는 KerberosAS에게 인증을 받아야 한다. 이는 공격자로부터 네트워크 자원 사용, 메시지 가로채기, 사용자 위장, 재전송, 공격을 막는 데 필요하기 때문이다. X는 KerberosAS에게 원하는 터켓승인서버(TGS)에 인증 메시지를 전송한다.

KerberosAS는 사용자 데이터베이스(UserDB)에서 각 노드들의 정보를 검색한 후, 정상적인 노드라면 요청한 TGS가 해당 서버(DirServer)에 있는지 검색하게 된다. 만약 정상적인 TGS가 존재한다면 X는 정상적인 노드로 인증을 한다.

3.5 소스노드와 목적지노드의 연결

DSR프로토콜을 통해 소스노드(X)와 목적지노드(Y)의 경로 설정이 되면, X는 Y의 공개키(PKY)를 알고자 할 경우 DirServer에 존재하는 Y의 TGS를 사용하여 인증 계체를 생성한다. 이와 반대로 Y에서 X의 공개키(PKx)를 알고자 할 경우는 후방인증 계체를 생성한다. 그 후 X와 Y간의 직접적인 연결이 이루어지며, PKy를 X에서 알게 되었으므로, X는 PKy로 X의 ID, 원하는 TGS 등을 암호화하여 전송하게 된다.4)

3.6 소스노드와 목적지노드간의 키교환

소스노드(X)와 목적지노드(Y)간의 직접적인 연결이 이루어졌을 때, X와 Y간의 인증 절차는 그림 3과 같다. X는 KerberosAS의 DirServer에서 얻은 PKy로 X

- 715 -
인증 정보를 암호화하여 전송한다. AS는 Y의 비밀키로 수신된 메시지를 복호화한 다음 X에게 PK로 X와 TGS간 공유하는 세션키 \( K_{s,TGS} \)을 암호화하여 전송한다. 이때 Y의 티켓승인서버 (TGS) 접근승인키(Ticket  \( t_{TGS} \))도 함께 보내는데, 역시 여기에도 세션키 \( K_{s,TGS} \)가 포함되어 있다. 이는 X와 Y의 TGS에게 은밀한 방법으로 세션 키를 분배하는 방법으로, 이후부터 X,Y간의 공격을 사용하지 않고, 비밀키로 메시지 인증 뿐만 아니라, 비밀키로 메시지 인증 단계를 하게 된다. 나머지 과정은 Kerberos V5의 메시지 인증 절차와 같다.

![그림 3. 소스노드와 목적지노드간의 키교환](image)

**IV. 제안 메커니즘**

1. Source \( \rightarrow \) AS
2. \( M((\text{Option}, \text{ID}_x, \text{ID}_T, t_{TGS}, \text{Time}, \text{Nonce})) \)
3. AS \( \rightarrow \) Source
4. \( M((\text{PK}_x, \text{t}_{TGS}, \text{Authentication}_{x,T}, \text{ID}_T)) \)
5. Source \( \rightarrow \) AS
6. \( M((\text{EPK}_x, (\text{Option}, \text{ID}_x, \text{ID}_T, t_{TGS}, \text{Time}, \text{Nonce}))) \)
7. AS \( \rightarrow \) Source
8. \( M((\text{ID}_T, \text{Ticket}_{TGS}, \text{EPK}_x, (K_{s,TGS}, \text{Time}, \text{Nonce}))) \)
9. Source \( \rightarrow \) TGS
10. \( M((\text{Option}, \text{Ticket}_{TGS}, \text{Authentication}_{x,T}, \text{ID}_x, \text{ID}_T)) \)
11. Authentication \( \rightarrow \) \( EK_{x,TGS}, (K_{s,TGS}, \text{ID}_T) \)
12. \( TGS \rightarrow \) Source
13. \( M((\text{ID}_T, \text{Ticket}_{TGS}, \text{EPK}_x, (K_{s,TGS}, \text{Time}, \text{Nonce}, \text{ID}_x)) \)
14. \( \text{Ticket}_{TGS}, (\text{Flags}, K_{s,TGS}, \text{ID}_x, \text{AD}, \text{t}_{TGS}) \)
15. Source \( \rightarrow \) Server
16. \( M((\text{Option}, \text{Ticket}_{TGS}, \text{Authentication}_{x,T}, \text{ID}_x, \text{ID}_T, \text{TGS}) \)
17. Authentication \( \rightarrow \) \( EK_{x,TGS}, (K_{s,TGS}, \text{Time}, \text{Subkey}, \text{seq}) \)
18. Source \( \rightarrow \) Source

![그림 4. 제안 인증 메커니즘](image)

제안한 인증 메커니즘은 DSR라우팅 프로토콜과 Kerberos 프로토콜을 이용한 노드간 인증 서비스를 하는 메커니즘이다. 즉, Kerberos V5의 단단한 인증 서비스 장점을 활용하였으며, Kerberos의 DirServer가 노드의 Realm의 역할을 대신하여 노드간의 상호 연결을 한다. 인증 서비스 교환 단계에서 페이스워드의 명문 전송 없이 목적지노드의 공개키로 암호화 전송하여, AS로부터 도청 및 가로세기 위험이 없는 소스노드와 목적지노드간의 인증을 받을 수 있도록 하였다. 제안한 인증 메커니즘은 Kerberos V5 인증 프로토콜, Ad-hoc망의 DSR라우팅 프로토콜을 기본으로 하고 있으며, 소스노드와 Kerberos AS 사이에서 인증 정보가 교환되는 알고리즘은 그림 4와 같다.

**V. 결론 및 향후 연구 과제**

최근 몇 년 동안 Ad-hoc망에서의 다양한 라우팅 프로토콜 및 무선 네트워크의 보안, 인증 방면에 대한 연구가 활발히 진행중에 있지만, 무선인터넷 및 Ad-hoc망에서의 보안, 인증은 미비한 상태이다. 본 논문에서는 Kerberos와 DSR 라우팅 프로토콜을 이용하여 이동 단말 노드간의 사용자 인증 메커니즘을 제안하였다. 초기 세션은 공개키 방식에 기반을 두었고 소스노드와 TGS사이부터 세션은 이전 세션에 포함되어 있는 세션 키를 이용하는 공통 키 방식을 사용하여 공개키 방식과 공통키 방식의 상호 혼용성을 해준 브로젝트의 설계로 보았다.

DSR라우팅 프로토콜을 사용하여 Ad-hoc망의 인증 문제는 제안해 보았지만 다른 라우팅 프로토콜을 이용한 인증 및 Ad-hoc망의 보안은 아직 미비한 실정이며 향후 무선 인터넷망의 성장을 감안하여 좀 더 안전하고, 효율적인 무선 인터넷 환경을 위해 보안성 및 효율성을 강화한 강력한 무선 인터넷 환경을 위해 지속적인 연구 및 논문이 필요할 것이다.

참고문헌