社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2005－DPS－122 (33)
2005－CSEC－ 28 (33)
2005／3／23

自律分散型公衆無線インターネットアクセスサービスのセキュリティに関する考察

黄 穎 大平 健司 藤川 賢治 岡部 寿男

自律分散型公衆無線インターネットでは、ブロードバンドアクセスラインとアクセスポイントを持つ人ならだれでもインターネット接続サービスを提供でき、モバイルノードはインターネット上の認証機構のアカウントを所有し、アクセスポイントや通信相手がその認証機構に問い合わせることでモバイルノードの認証を行う。

しかし、インターネットやセキュリティに関する知識のないアクセスポイント所有者にとってノード認証や通信記録の保存といった管理業務は負担が高い。一方、従来のISP型公衆無線インターネットと異なりアクセスポイントが悪意を持って運用されている場合もある。モバイルノードの通信が盗聴、改ざん、成りすましなどを受ける可能性がある。

本研究ではモバイルノード、アクセスポイント、通信相手のセキュリティを保障しながらアクセスポイントの管理コストを最小限にするような方式を提案する。

提案する方式はアクセスポイントで認証を行う方式と行わない方式の二種類に大別される。まずアクセスポイントで認証を行わない方式として、PPTPトンネリング技術を利用してすべての通信がモバイルノードのホームゲートウェイを経由する実装とHIPプロトコルによるモバイルノードと通信相手のエンドツーエンドのセキュリティを保障する実装を提案する。アクセスポイントで認証を行う方式ではモバイルノードがインターネット上の認証機構のアカウントを所有し、アクセスポイントが当該認証機構に問い合わせることでモバイルノードを認証する。その手法として、MIPv6+IPsecAH拡張技術による認証を得た上モバイルノードと通信相手ダイレクト通信するような実装を提案する。

Secure Models of Autonomous Distributed Public Wireless Internet Access

YING HUANG , KENJI OHIRA , KENJI FUJIKAWA
and YASUO OKABE

In autonomous distributed public wireless internet access services, access points are managed by anyone with broadband internet access lines and access points. Users with accounts to any authentication infrastructure in the Internet can enjoy the access service through any of these access points.

However, as the owners have little knowledge about the Internet and security, management costs such as authenticating users and saving their communication records are too high. On the other hand, as anyone can set up access points, users are exposed to the threat of their communication being eavesdropped, manipulated or spoofed by malicious access points.

In this paper, we propose secure models of the autonomous distributed internet access services using the conbinations of two approaches: authentication at access point and tunnelling features.

In the approach with authentication at access points, mobile nodes own accounts to some authentication infrastructure. Once authentications at access points are successful, the mobile nodes and their correspondent nodes can setup a direct communication. In implementation, we use the LIN6 and the MIPv6+IPsecAH protocols.

In the approach without authentication at access points, we suggest mechanisms either forwarding all the traffic to a tunneling server or using an end-to-end security protocol. In implementation. we use the PPTP protocol for forwarding and the HIP protocol to ensure end-to-end security between the mobile nodes and correspondent nodes.

† 京都大学
Kyoto University

1. Introduction

In this paper, we clarify the requirements and propose secure models for autonomous distributed public wireless internet access services.

In the past few years, rapid growth has been seen in public wireless internet access service. Today, mobile users tend to access the Internet at a variety of locations, including restaurants, hotels, shopping malls, libraries and airports, for email, web and other internet applications. IEEE802.11a/b/g wireless LAN provides a high speed internet connectivity to meet their requirements. Coverage, management cost and pricing challenges have been addressed[1]. As most of the single ISPs lack widespread coverage, two approaches have been taken —increasing the number of access points and roaming among multiple ISPs[2] with a centralized authentication server and exclusive lines to it. However, both solutions cost too much. As a result, the business model is not profitable for the ISPs because they cannot recover their investments.

Recently, some self-managed hotspot wireless services have appeared. They are provided by the owners of some commercial facilities as added services to attract more customers. Some of these access points do not authenticate users at all. The unidentified mobile nodes are threats to other nodes in the Internet. To improve this situation, features to restrict limited applications are adopted. IMAP and SSH are relatively high security applications because the communication is secured and users are required to authenticate for each application. SMTP or HTTP is much less secure. As in most of the current implementation, the access points do not save the SMTP or HTTP records; they are vulnerable to SPAM email or slander in BBS from a malicious mobile node in the visiting hotspot. HTTP proxy or SMTP gateway could be deployed to save the communication record, however their running costs are expensive. For mobile nodes, the access points in self-managed hotspot are less reliable than that of ISP type. Without mutual authentication between the mobile nodes and the access points, mobile users are exposed to the threat of their communication being eavesdropped, manipulated or spoofed by malicious access points.

In this paper, we first clarify definition of the autonomous distributed internet access services — access points are managed by anyone with a broadband internet access line; users with accounts to any authentication infrastructure in the Internet can enjoy the access service through any of these access points. We then propose our secure models of the autonomous distributed internet access services using two approaches: one with authentication at the access point, and the other without such authentication. Finally we analyze and evaluate the security level achieved in our proposed models.

We are motivated by the desire of building secure autonomous distributed public wireless Internet access models with minimum operation cost, large scalability and optimal routing. Autonomous distributed type is less reliable compared to the ISP type, however the increasing trend and demand of autonomous distributed type urge us to provide security features for it. If we clear the security problems, people can have more opportunities to enjoy the public WLAN service, and they can have more chances to provide the services to others as well. The effect is synergistic.

This paper will be organized as follows: in Chapter 2, we defines three types of public wireless Internet access services. In Chapter 3, we clarify the security requirements. In Chapter 4, we propose four models using two approaches — authentication at access point and tunneling mechanisum. In Chapter 5, discuss three implementations based on the PPTP, the HIP and the IPsecAH protocols. Finally, in Chapter 7, we make some notes on our conclusion and the future work.

2. Types and Properties

In this chapter, we break down public wireless Internet into three types — ISP type, self-managed type and autonomous distributed type.

2.1 ISP type

In the ISP type public wireless Internet, ISPs are in charge of the access points and the access line to the authentication server. They are responsible to manage user accounts, save authentication records and ensure the authentication process secure. Mobile users trust their facilities, including the access points, authentication servers and access lines provided by the ISPs. They sign contracts and obtain their accounts before using the connectivity services provided by the ISPs. Currently security problems of the ISP type public wireless Internet are caused by the wireless propertity. Mobile nodes run the risk of their messages being eaversdropped, spoofed and manipulated by malicious nodes or fake access points[3] in the wireless area. Coverage, management cost and pricing challenges have been addressed. As most of the single ISPs lack widespread coverage, two approaches have been taken —increasing the number of access points and roaming among multiple ISPs[2] with a centralized authentication server and exclusive lines to it. However, both solutions cost too much. As a result, the business model is not profitable for the ISPs because they cannot

recover their investments.

2.2 Self-managed Type

Nowadays the owners of restaurants, shops, hotels are beginning to provide wireless Internet access as an added services to attract more customers. The access points are owned and managed by the owners of these commercial facilities. In this paper, the services is referred to as self-managed type.

Some of the services use initial setting of access point — no user authentication, WEP only or even none.

Some hand out scratch-off cards containing a one-time login and password when mobile users have shown their identification such as passport, or driving license. As it requires someone to check the IDs, the operation cost is expensive.

Some use cell phone for authentication. Mobile Users enters email addresses of their cell phone and receive one-time accounts in replies. It is based on the idea that those cell phone users have registered their personal identification information to the cell phone carrier. Even illicit uses are detected, the carriers can provider the email record when requested. The method is automatic, real-time however it usually requires a 802.1x infrastructure for authentication.

Others add extra features to restrict a limited application to pass through: IMAP, SSH and HTTPS are relatively high security level applications, because the communication is protected and mobile users should have account for these services; POP is less secure because its account and password could be eavesdropped by any node in the wireless area; SMTP or HTTP is much less secure because it is vulnerable to SPAM email or slander in BBS from a malicious mobile are detected from those access points. The filtering features also prevent the mobile nodes from sending virus to infect other nodes in the Internet. The owners of those access points are responsible to identify the illicit user when requested, or he will be sued and punished according to the ISP Law[4]. As the access points do not save the communication record, it is difficult for the owners to tell which mobile node did the illicit user accurately.

Different from the ISP type, access points in self-managed type public wireless Internet access services can be malicious. In conventional self-managed public wireless internet access services, mobile nodes are exposed to the threat that their communication being eavesdropped, manipulated or spoofed by some malicious access points. Only the 802.1x authentication can mitigate the risk, however it is expensive to deploy.

In overall, the self-managed type has some weaknesses: they are run with different security policies; users have to obtain accounts repeatedly each time they visit a new hotspot; all the network components, including the mobile nodes, access points and correspondent nodes, are exposed to attacks.

2.3 Autonomous Distribyted Type

In this paper, we propose autonomous distributed internet access services — access points are managed by anyone with a broadband internet access line; mobile nodes with accounts to any authentication infrastructure in the Internet can enjoy the access service through any of these access points.

As the owners are not required to prepare authentication facilities, the management cost is very low. This encourages more people to provide this type of services. As the services in our proposed type is independent to any ISPs, anyone in the wireless coverage can obtain the internet connectivity.

Figure.1 shows the comparisons of coverage and management cost with the other two types. Our proposed type will have a wider coverage than that of the rest two types and lower managament cost than the ISP type.

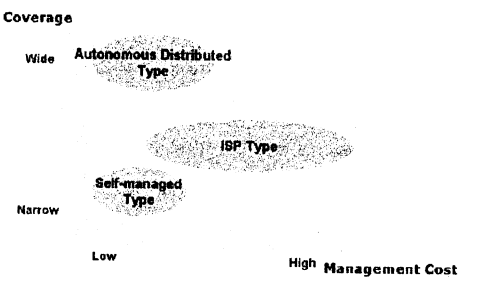

Fig. 1 Comparisons among Different Types

3. Security Requirements

In autonomous distributed public wireless Internet access service, security is a challenge. Without authenticaiton and encryption, security problem will be crucial. Mobile nodes' messages could be eavesdropped, manipulated and spoofed by malicious nodes in the wireless area or access points. On the contratry, owners of access points have to take legal reseponsiblities if illict uses are found from malicious nodes visiting the wireless areas. In this chapter, we first analyze vulnerabilities and threats. Then we discuss some conventional security approaches and explain why these features are not applicable to the autonomous distributed public wireless Internet access services.

3.1 Vulnerabilities

Security problems may get worse because of the wireless, mobile, public properties in public wireless Internet access service.

Wireless The last hop is unsecured and exposed to attacks in the wireless coverage area. It is easier to eavesdrop, manipulate or spoof those messages than wired Internet.

Mobile When node obtains a new address from its visiting network, it updates the address information with its correspondent node. A false address update message could cause DoS attack to any arbitrary nodes in the Internet.

Public A mobile node may connect to access points which belong to ISPs it has not contracted with. It is more difficult to identify the nodes when some attacks are detected.

Autonomous Distributed The access points are less reliable as they are mostly owned by personal or small group rather than well-known ISPs. Malicious access points are threat to both the mobile node and its correspond node.

3.2 Threats

Because of one or more vulnerabilities above, we list up the possible threats as follows.

- **To Wireless Mobile Nodes**
  i) Message eavesdropping by a malicious wireless node or access point. ii)Message manipulating and spoofing by a malicious wireless node or access point.
- **To Correspondent Nodes**
  False address update message by a malicious mobile node.
- **To the Internet**
  DoS Attack, SPAM/Virus distribution by a malicious wireless mobile node.
- **To Access Points**
  Legal responsibility when some attacks with the source IP address access points assigned are detected. The attacks, including DoS, SPAM and Virus, are caused by malicious nodes in the wireless coverage of access points.

3.3 Conventional Approaches

MAC, WEP and 802.1x are used for authentication and data encryption. However, none of the three solutions is adequate for security and authentication purpose for public wireless Internet access. A MAC address can be masqueraded through address spoofing, while the 40-bit WEP key can be broken in time[5),6)]. The MAC and the WEP mechanisms do not scale large number of users — it is impossible to register the MAC addresses to all the access point that the mobile node may visit; it is also impossible to share the secret key between the destination access point and the mobile node ahead of time. The 802.1x is more secure but the centralized authenticate mechanism makes it more cumbersome and more expensive to implement.

4. Design Principle and Proposed Models

In this chapter, we first demonstrate our design principle. Then we propose four secure models of autonomous distributed public wireless Internet access services.

4.1 Design Principle

We design our secure models using two approaches — authentication at access point and tunneling features.

- **Authentication**
  Authentication at Access Point Authentication processes at access points can reduce the chances of DoS attacks from malicious nodes, because if a mobile node has been successfully authenticated before, at least the mobile node is verified by some components. A public authentication facility or a home gateway is required for this feature.
  No Authentication at Access Point No authentication at access points can reduce the management cost to minimum. All what the access points have to do is to permit some specific tunneling procols, such as the PPTP and the SSH, to pass through.
- **Tunneling Feature**
  In related researches, one approach using VPN tunneling technologies has been taken. Mobile users obtain accounts from the tunneling server and establish end-to-end secure channels with it. The tunneling server can be either a PPTP/SSH server or a home gateway. The home gateway is based on the concept that people with broad band internet access own home servers to control their appliances when they are away from their home network. If tunneling feature is added to the home gateways, mobile users can use them as their own VPN server. Access points are configured to block all traffic except several specific VPN protocols. In this way, a security level that is no worse than the regular internet can be maintained.
  Tunneling Tunneling feature has two advantages: i)It release the leagle responsiblity of the access points. Mobile nodes obtains IP addresses from their tunneling server, if any illicit use with the source IP address is detected, it is the tunneling server while not the access point to take the responsiblity. ii)The feature can also prevent the mobile node's location information from being exposed to the correspondent node because it uses the IP address

obtained from the tunneling server, while not the access point the mobile node visits.

Native Native communication between mobile nodes and their correspondent nodes enables optimal routing, which is more efficient.

By conbining the two approaches with two options each, we classified the proposed models in Table1

Table 1 Proposed Models

	Tunneling	Native
w/o Authentication	Unverified Tunneling	Unverified Nati
w/ Authentication	Verified Tunneling	Verified Native

5. Proposed Implementations

In this chapter, we discuss three possible implementations for our proposed models.

5.1 Unverified Tunneling Model

We propose to implement this model using PPTP technology. All the traffic is forwarded to mobile nodes' tunneling servers. In this way, a security level which is no worse than the regular Internet can be maintained.

The MS-CHAP version2 is preferable for mutul authenticaion to mitigate the risk of a bogus PPTP server.

Figure2 shows how we apply PPTP to the Unverified Tunneling Model.

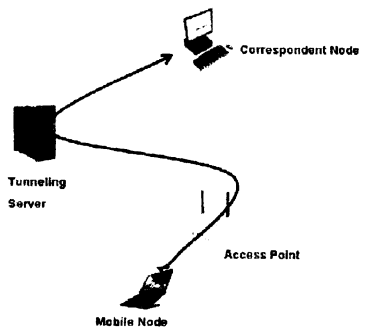

Fig. 2 Unverified Tunneling Implementation

5.2 Unverified Native Model

For unverified native model, we propose to use HIP, a proposed protocol in IETF. The protocol seperates the end point identifier and the locator nodes of IP addresses. An HI(Host Identity) is a public key which directly represents the host identity. A HIT(Host Identity Tag) is a hash of the HI. It is 128 bits long and is included in HIP payloads.

The HIP basic exchange mechanism — a mechanism to exchange four HIP packets with puzzles and solutions — establishes a trusted relationship between the mobile node and its correspondent node.

Both the mobile node and the correspondent node should obtain the HIs from a public key infrastructure to verify each other.

Figure3 shows how we apply HIP to the unverified native model.

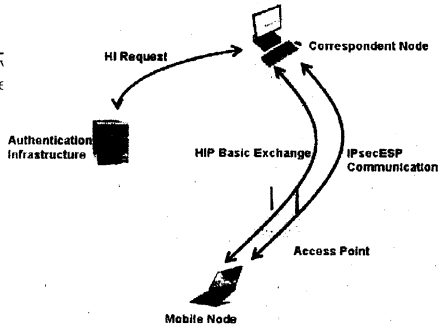

Fig. 3 Unverified Native Implementation

5.3 Verified Native Model

For verified native model, we propose to use MIPv6 and IPsecAH extension. MIPv6 is a standard IETF protocol. It is designed to maintain exisiting connections over location changes and to ensure that the mobile node can be reached at a new location. The 128-bit IPv6 address is made up of a 64-bit routing prefix and a 64-bit interface address.

An home address option is included in the MIPv6 extension header to indicate mobile node's home address when it is in a visiting network. The home address can be used as a node identifier. IPsecAH is required to protect the authenticity of the home address portion. The IPsecAH protocol should be extended to support public key cryptography. Verifiers including the access point and the correspondent node are required to query the authentication infrastructure when necessary.

Once the authentication is successful, the mobile node and the correspondent node establish a native communitation with IPsecAH protocol.

Figure4 shows how we apply MIPv6+IPsecAH extension to the verified native model.

6. Conclusion and Future Work

The rapid global diffusion of wireless public Internet is accelerated by the demand of ubiquitous Internet. Current ISP types are expensive to run and do not scale while conventional autonomous distributed type is not secure enough.

In this paper, we have analyzed security problems that are specific or more crucial in public

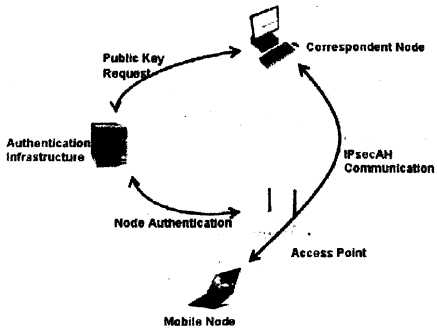

Fig. 4 Unverified Native Implementation

wireless Internet. Then we have discussed some secure models to meet the security requirement. Then we proposed three possible implementations based on these models.

The proposed secure models and their implementations can provide value for all the components in the autonomous distributed public wireless Internet. Mobile nodes and their correspondent nodes will benefit from the secure communication. Owner of the access points will benefit from providing public Internet access with low operation cost and minimum legal responsibility. The Internet will benifit from shifting to a secure ubiquitous communication environment with few DoS, Virus and SPAM emails attacks.

Future work on our proposed models contains implenetation and more detailed evaluation. We want to deploy and check our proposed secure models in pratice.

References

1) Anand Balachandran, Geoffrey M.Voelker and Paramvir Bahl:Wireless hotspots: current challenges and future cirections, *Proc. of WMASH 2003*, (2003).
2) Yasuhiko Matsunaga, Ana Sanz Merino, Takashi suzuki and Randy H.Katz: Secure Authentication System for Public WLAN Roaming, *Proc. of WMASH 2003*, (2003).
3) 清水 渉, 小林 稔幸: 無線ホットスポットサービスのセキュリティ, **研究報告「マルチメディア通信と分散処理」** *No.2001-DPS-107*, (2002).
4) 総務省:特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律, 平成十三年十一月三十日法律第百三十七号.
5) David Golombek: Single computer breaks 40-bit RC4, (1996).
6) Nikita Borisov, Ian Goldberg and David Wagner: *(In)Security of the WEP algorithm*, http://www.isaac.cs.berkeley.edu/isaac/wepfaq.html.