Enhancing Security for Vertical Handoff in SARAH under the Heterogeneous Networks

Kyusuk Han, Youngjoon Seo, Sungjune Yoon, and Kwangjo Kim*

*International Research center for Information Security, ICU

Abstract

SARAH (Selective Advance Reservations and resource-Aware Handoff direction) [1] was designed to increase the efficiency of handoff in both L2 and L3 communications. However, the design was not considered to operate under the heterogeneous environments.

In this paper, we discuss the security problems of SARAH such as privacy, authentication, key management, *etc.*. We propose a solution by separating the neighbor mapping table from the base station and suggest a concept of the neighbor mapping server which binds IP address and MAC address and manages security policies and secure parameters. Finally, we show the implementation results of our design to verify the practical aspects of our idea. We claim that our idea shows the secure solution for SARAH to be used under the heterogeneous environments.

I. Introduction

In the wireless environment, the handoff process plays one of the most important roles for the seamless communication. When a mobile node is watching the movie, the mobile node wants the seamless connection during roaming. SARAH (the selective advance reservations and resource-aware handoff direction) is designed for this purpose[1].

In the design of SARAH, the mobile node receives a L2 beacon message from a foreign agent (*FA*) and passes the message to the home agent (*HA)*. L2 beacon message contains MAC address of *FA*. Then, *HA* searches the stored neighbor-mapping table (*NMT*) to find the IP address bound to the MAC address. After that *HA* builds the pseudo reservation path (*PRP*) to the *FA*. Using both L2 and L3 communications significantly reduces the connection latency during roaming, which it is the most important characteristic of .SARAH.

However, it is difficult to expect that the *NMT* of SARAH operates well in real environments, since the home agent has to store *NMT* to know the neighbor *FA*s. For example, there are two major wireless Internet service providers in Korea; Netspot from Korea Telecom and Anyway from Hanaro Telecom. Even though they build sufficient wireless hot spots in every accessible place, there can be no available wireless network in some place. They need to negotiate for the sharing of wireless network. It means that Netspot's user can use Anyway's wireless network if there is no Netspot's hot spot or weak one.

Since, SARAH depends on the NMT, a base station needs to have the information of neighbor base station. With SARAH, a base station of Netspot should have the information of the nearest base station of Anyway. However, it is difficult to expect that a base station stores the other company's or other group's information

Therefore, we suggest a new model that the base stations do not have NMT and can know other IP address without having NMT. In the model, we design the neighbor mapping server which plays a role like NMT, which manages the neighbor mapping and the securities.

The paper is organized as follows; Chapter 2 describes the overview of SARAH and discusses

security issues on SARAH in the heterogeneous networks. Chapter 3 describes the security architecture of Mobile IP which inspired our motivation to this research. Our security design is shown in Chapter 4. Chapter 5 shows the implementation result. Chapters 6 describes the further work and conclusion.

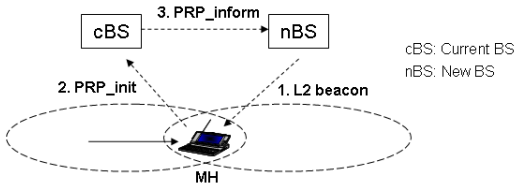


Figure 1 Host Movement Detection

II. Neighbor Detection in Heterogeneous Network

1. Vertical Handoff

Vertical handoff (handover) is the handoff between heterogeneous networks, such as between UMTS and WLAN. These heterogeneous networks can be Cellular Networks (UMTS, CDMA2000, and GSM), WiMAX, WLAN, and WPAN. With this concept, the handoff within the same network domain is called horizontal handoff. In the last decade, many new wireless communication systems have been proposed and developed. These communication systems have different network coverage and form a hierarchical overlay network. A vertical handoff is thus occurred when moving between these different communications systems.

Vertical handoff between WLAN and UMTS (CDMA2000) attracts extreme attentions in all the research areas of the 4G wireless network, due to the benefit of utilizing the higher bandwidth and lower cost of WLAN as well as better mobility supports and larger coverage of UMTS.[2] Therefore, many researches are focused on the vertical handof f[3] for this aspect.

2. Host movement detection scheme of SARAH

To detect the most available neighbor base station, mobile node detects L2 beacon frames from multiple reachable BSs. SARAH assumes the underlying networks to be generic wireless networks. In [1], they implemented their design with IEEE 802.11 network.

In the communication for the pseudo reservation path generation, there are two control messages as following.

- PRP_init: notification of movement
- PRP_inform: initiation of PRP establishment

Individual base stations continually broadcast their own L2 beacon message for their advertisement. In those messages, only MAC address of the base station is known. Assume a mobile host exists, who has the link with a base station and moving around. The mobile host receives the advertising L2 beacon message. The mobile host transfers the MAC address in the message to the current base station as PRP_init message. The base station searches the IP address from the neighbor mapping table. The base station finds the IP address and sends PRP_inform message for the initiation of PRP to that IP address (a foreign agent). Figure 1 describes the process.

Using the neighbor mapping table, the number of pseudo reservation paths (PRPs) are reduced.

Neighbor Mapping Table of SARAH binds between neighboring BS's MAC address and IP address. It is referred for host movement detection. Table 1 shows an example of a neighbor mapping table.

BS ID	MAC Address (Wireless)	Network ID	IP Address (Wired)	R	S
1	00:20:A6:4C:99:BE	220.69.186.0/24	220.69.186.145	1	1
2	00:02:2D:0B:6F:E5	192.168.1.0/24	192.168.1.2	1	0
3	00:20:A6:4C:99:95	220.69.187.0/24	220.69.187.128	1	1
...	...	...	...	...	...

Table 2 Example of a Neighbor Mapping Table

3. Security issues of SARAH in Heterogeneous Network

In SARAH, each base station has a neighbor mapping table. In the neighbor mapping table, MAC addresses and IP addresses are bounded. When the identification request from mobile nodes occurs, the base station searches the corresponding IP address in the table. When the IP address is found, the base station (the home agent) sends the pseudo reservation path information (PRP_inform) to the foreign agent of the IP address. It will work well if there are not any changes in the network.

However, storing neighbor mapping table inside of base station requires the update of list when new base stations join the network. Even only one base station joins, every neighbor base station has to update their tables.

In case of Wi-Fi services, ISPs (Internet Service Providers) negotiate on the sharing their wireless networks to minimize the duplicated infrastructure. Even they agreed the sharing wireless networks, none knows all information where other company's wireless access points are installed. For any cases, it is trivial that the building infrastructure would be done individually. It makes the case that there is no information of IP addresses in the neighbor mapping table even several access points actually exist.

Moreover, when the current base station tries to connect to the neighbor base station which belongs to the different ISPs, several security issues are raised with the current SARAH architecture. The first issue is how to authenticate the mobile node and base stations, since it is more reasonable that there is no shared secret between the base stations with different ISPs. The second issue is the key management. Key agreement between the current base station and the foreign base station, and between the mobile node and the foreign base station should be considered. The third is the privacy. For the secure communication, the message should be encrypted.

Therefore, we introduce the neighbor mapping server which roles neighbor mapping with known MAC addresses for base station's request, also manages the security policies like handling the user access controlling. In this case, we can easily manage the frequent update of the base station's state also achieve the security. Since all wireless network owners know about the neighbor mapping server, they send the updated information of the base stations to the server. Each base station can know the up-to date neighbor's states with the communication between the server and the base station, and then make the secure communications.

III. Related Work

In this chapter, we show the basic security architectures of Mobile IP, which was the motivation for our design.

The requirements for Mobile IP[4] are defined that a mobile node share a static security association (SA) with its home agent, allowing the mobile node to share an SA with foreign agents, which in turn can share SAs with home agents.

Also, the requirements for implementing Mobile IP with *AAA* (Authentication, Authorization, and Accounting) features are defined that each agent has authority that *AAAH* for a home agent and *AAAL* for a local agent (a foreign agent).[5]

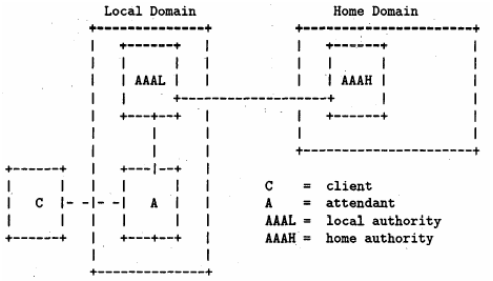


Figure 2 AAA Servers in Local and Home Domain

And, security Association requirements exist between the mobile node and AAAH (same domain), *AAAL* and *AAAH* (for reliability of data transfer), and attendant foreign agents (for knowledge of available resources). Also, other requirements exist; the client's credentials should not be duplicated by *AAAL* or the attendant foreign agent, the ability of a client to provide complete but unforgeable credentials, the ability of attendant to manage requests from multiple clients belonging to different domains, simultaneously, and inexpensive attendant equipments to handle more clients.

Figure 2 describes the basic model of mobile IP.

In the model, a client requests a service from foreign domain, the attendant serves the client. In that case, the attendant demands credentials. There is no direct access to data for verification and therefore, it consults a local authority. The local authority gets the required data for verification of client's credentials from the *AAA* server in the home domain. After the client's credential is authorized, the attendant provides the requested service to the client.

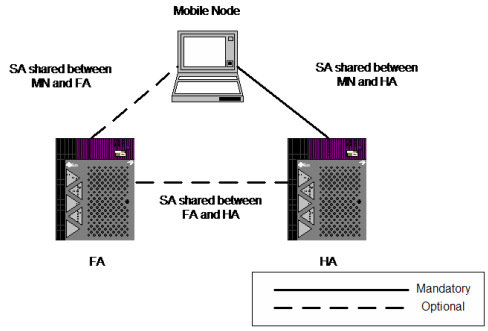


Figure 3 Secure Association in the Mobile IP

Figure 3 shows secure associations in the mobile IP. When all three entities use authentication, a $N \times N$ number of security associations is required. This problem becomes much more important in inter-domain mobility scenarios. Using Mobile IP trust model, we can let the strong security be guaranteed.

Therefore, we can adopt the AAA server model to our design. Since the higher layer communication is operated under IP layer, we can assume the secure communications with the neighbor mapping server, which we describe in the next chapter, are available.

IV. Our Design

1. Assumption

The home agent (HA) and the mobile node (MN) have the secure association. They share a key for a secure communication, which is used for the encryption of messages and the authentication of the entitiy. The neighbor mapping server (NMS) roles the neighbor mapping to generate the pseudo reservation path in SARAH.

2. Neighbor Mapping Server

We suggest the neighbor mapping server for the Neighbor Mapping. Initially the role of NMS is binding IP address to known MAC address. Also, to adopt the neighbor mapping server for the vertical handoff, we need to consider the potential security risks and define the security requirements. For example, FA should be able to authenticate HA whether FA accept the traffic transmission.

In the design, *NMS* has two tables, the neighbor mapping table (*NMT*, table 1) and the user policy table (*UPT*, table 2). MAC addresses and bound IPs, shared keys between *NMS* and base stations, and Group IDs are stored in *NMT*. User ID, the information of service levels and other policies are stored in *UPT*.

The *Service Level* is used to decide whether the service is available for the user. In table 2, the service level of a user *MN1* is '1', while the service level of a user *MN2* is '2'. For our implementation, we defines that service level '1' means vertical handoff is available, and '2' means unavailable.

MAC_Addr	IP	UniKey	Group
MAC_BS1	210.107.248.161	Key_BS1	1
MAC_BS2	210.107.248.201	Key_BS2	2
....	...	...	...

Table 3 Neighbor Mapping Table of NMS

User ID	Service Level	Other Policies	...
MN1	1	...	...
MN2	2	...	...
....	...	...	...

Table 4 User Policy Table

The division of service level is necessary since the ISPs can measure different costs for each level. If vertical handoff happens and a user uses other company's network, the subscribed company has to pay the fee for that case. It is a bit of managing considerations that disabling the vertical handoff can

reduce the overall cost.

3. Authentication

We assume that the secure associations between *MN* and *HA*, also between *HA* and *NMS* already exist. We show the process of authentication with step a)—f).

a) *HA* sends MAC address of *BS2* to *NMS*.

b) *NMS* finds IP address and a shared key KEY_{BS_2} of *BS2*.

c) *NMS* generates a random number r, and a message authentication code $H_{KEY_{BS_2}}(r)$.

d) *NMS* sends $(r, H_{KEY_{BS_2}}(r))$ to *HA*.

e) *HA* sends $(r, H_{KEY_{BS_2}}(r))$ to *FA*.

f) *FA* can verify with own key KEY_{BS_2} with checking if $received = H_{KEY_{BS_2}}(r)$.

Since only *FA* and *NMS* have the key KEY_{BS_2}, *HA* and other attackers cannot forge it. Of course, the communication to *NMS* should be encrypted, since anybody can capture the communication and try to impersonate as *HA* without encryption.

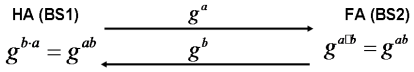
And then, we also need to build the secure channel between *HA* and *FA*. Therefore, we have to have a key exchange process to enable the encryption.

At first, we note that we can consider *FA* is authenticated with the information from *NMS*.

In other way, we can use $(r, ID_{BS_1}, H_{KEY_{BS_2}}(r))$ rather than $(r, H_{KEY_{BS_2}}(r))$. In that case, we can omit the key exchange process shown in the next section. Since *BS2* can verify with the ID of *BS1*, no other entity can forge it. However, every entity can know the communication, which occurs the privacy problem. We have to choose one of them in certain circumstances.

4. Key Exchange Requirement

Now, we modify the generic key exchange process in our design. In general cases, key exchanging should be done after the entities are authenticated. For key exchanging, several protocols are proposed. For example, Diffie-Hellman key exchange protocol (DHKEP), a public key cryptosystem based protocol, is well-known and implemented in many cryptographic libraries like IPsec and SSL. Following shows the DHKEP process.



From Diffie-Hellman problem, a mathematical hard problem, even g^a and g^b is known, knowing g^{ab} is difficult. 'Hard' means the computational cost is impossibly expensive to solve the problem. Of course the above process has the risk of man-in-the-middle attack, and we can consider more advanced methods. However we can keep on using that method in practice. Since even the attack on the method occurs, the adversary can not impersonates *FA* or leaks the key.

In our design, as we mentioned, we modify the sequences of authentication and key exchange. *FA*s do not have to authenticate themselves to the mobile node or *HA*. A bogus foreign agent can impersonate a real foreign agent simply by following protocol and offering agent advertisements to the mobile node. The bogus agent can, for instance, then refuse to forward decapsulated packets to the mobile node when they were received. However, the result is no worse than if any node were tricked into using the wrong default router, which is possible using unauthenticated router advertisements as specified in RFC 1256[6].

Since only one way authentication is necessary in the mobile IP, authenticating *FA* by *HA* is not necessary. And message authentication code can do the role of authentication of the entity. For example, in the movie theater, we only show the ticket to authenticate when we enter in.

5. Overall Process

In this section, we describe the processes of pseudo reservation path generation with our modification of SARAH.

- *FA* broadcasts L2 beacon message. *MN* receives the message and sends it to *HA*, as shown in Figure 5.

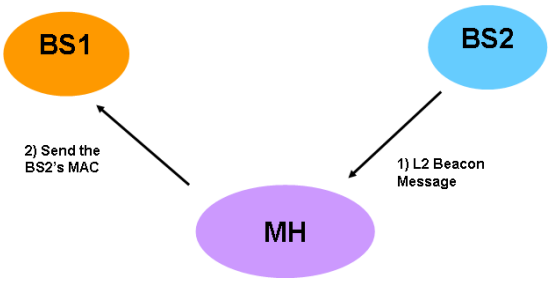


Figure 5 MH receive L2 Beacon Message

- *BS1* already has the secure communication with *NMS*. *BS1* sends *MH*'s ID, *BS2*'s MAC address to *NMS*. *NMS* searches his *NMT* and finds *BS2*'s Group and IP address binding the MAC address. If *BS1* and *BS2* are in the same group, *MNS* generates $T=(T_L,T_R)=(r,H_{KEY_{BS2}}(ID_{BS1},r))$. In other case, *MNS* find *MH*'s service level with ID in the *UPT*. If *MH*'s level is '1', *NMS* generates *T*. If not, *NMS* rejects the communication.

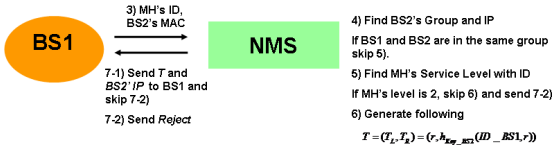


Figure 6 BS1 receive IP address of BS2

After that, *NMS* sends *T* and *BS2*'s IP to *BS1* (*HA*). Figure 6 shows the process.

- *BS1* then sends *PRP_Inform* with Key exchange request to *BS2*. In this stage, *BS2* doesn't authenticate *BS1*. Therefore, the confidentiality of the communication holds, but the authentication does not yet. The process is shown in figure 7.

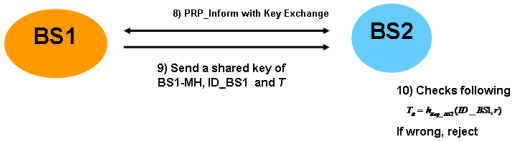


Figure 7 BS2 authenticate BS1

With the key establishment, *BS1* sends *T* to *BS2*. *BS2* then checks $T_R=H_{KEY_{BS2}}(ID_{BS1},r)$. If *BS2* authenticates *BS1*, *BS1* sends a shared key between *BS1* and *MH*. We consider if *BS2* trusts *BS1*, *BS2* also trusts *MN*, which is linked to *BS1*.

- After the authentication of *BS1* (*HA*) is done, *BS1* and *BS2* begin generating the pseudo reservation path. The last part is the same as SARAH, as shown in figure 8, that RSVP path and RSVP resv message transmission process are continued.

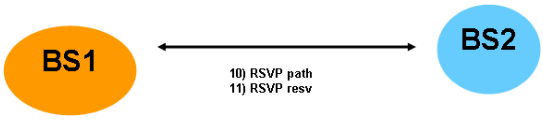


Figure 8 BS1-BS2 transmit RSVP path and RSVP resv message

V. Implementation Results

1. Environments

We implemented our design using RSVP and mobile IP with SARAH.

At first, we modified *sarahd*. When we execute *sarahd*, SARAH daemon configuration file is set up through *sarahd_config.c*. In our implementation, when NMS (Neighbor Mapping Server) considers the foreign agent as an authorized one, the same procedure of *sarahd* follows. In other case, we use our implementation that there is no neighbor address in configuration file. So, when the handoff occurs, no service is provided, and it can reduce the computation cost during the communication with NMS.

And then, we implemented our design that is the process of authentication before the pseudo reservation path generation process. For the process, we implemented following two authentication server

- *NMS*, authenticates whether *MN* can handoff to other networks .

- *AuthBS*, authenticates the other *BS*

NMS contains the neighbor mapping table of all authorized base stations. Also the user policy table is also built in *NMS*. *AuthBS* is built in each base station. For example, when the foreign agent authenticates the home agent, AuthBS of foreign agent begins the authentication process. Figure 9 and

10 shows the *AuthBS* and the neighbor mapping server, *NMS* in our implementation. For our implementation, we minimized the availability of the server just to checking the MAC address and providing the authentication resource for the *BS2*. With that *BS2* can trust *BS1*. More detailed implementation remains and it's our further work.

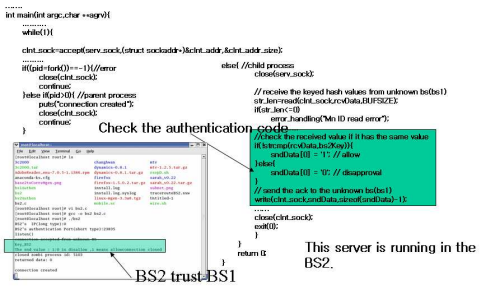


Figure 9 AuthBS of BS2

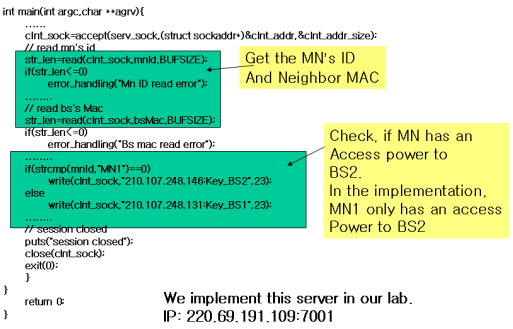


Figure 10 Neighbor Mapping Server

Figure 11 shows checking MAC address by *NMS*, which is received from *BS1*.

2. Scenarios

With the implementation, we show two scenarios that the service levels of the mobile node are '1' and '2'. Service level '1' means the mobile node can access the foreign agent in the different group, while service level '2' means the mobile node cannot. *BS1* and *BS2* are in the different groups.

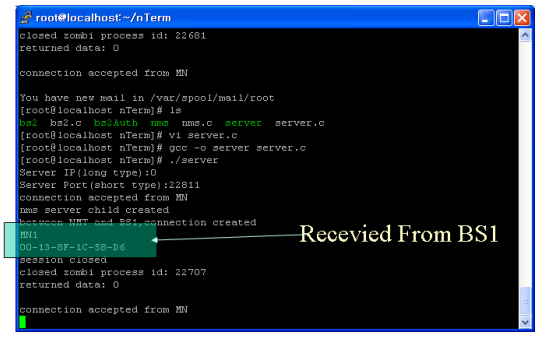


Figure 11 MAC address checking

VI. Conclusion and Further Work

In this paper, we argued the security problems of SARAH for adapting in the heterogeneous networks. Storing the neighbor mapping table inside the base station occurs the hardness of maintenance of base stations. In the real environments, a number of problems makes hardwares been disabled, like the out of order, superannuation, *etc.*. It is difficult that base stations update their neighbor mapping tables in each case. And, the communication under heterogeneous networks requires strong security considerations like authentication, key management *etc.*.

Therefore, we argued the separation of neighbor mapping table from the base stations, and proposed the neighbor mapping server which binds the MAC address and IP address and manages the several security policies and keys required for participants.

And then, we showed the security requirements in the procedure that the foreign agent should be able to authenticate the home agent. Since the base stations stores no neighbor mapping table for themselves, they have to ask to the neighbor mapping server. It makes the significant obstacle for the performance, and it is better to let the authentication be available between the home agent and the foreign agent. We also claimed that the authentication of the foreign agent is unnecessary, because the home agent gets the information of the foreign agent from the neighbor mapping server, and the strong security is unnecessary in the phase of the pseudo reservation path.

Finally, we implemented our design to verify the practical aspects of our idea. With maintaining the

whole design the implementation in the phase 1, we added the neighbor mapping server.

Our design and implementation showed that the modification of the model of the neighbor mapping table enables the vertical handoff in SARAH. Currently, we implemented our design in the heterogeneous environment with the different domain of the same Wi-Fi networks. Evaluating the overall performances with comparison to original SARAH is the remaining work. Also, extending the real heterogeneous environment with the different network, like GPRS, CDMA, and so on, is our further work.

We believe that our idea is the meaningful solution for the use of SARAH in the heterogeneous environment.

References

[1] Kyounghee Lee, Myungchul Kim, Chansu Yu, Ben Lee, Seungphil Hong, "Selective advance reservations based on host movement detection and resource-aware handoff", International Journal of Communication Systems, Volume 19, Issue 2, p 163-184

[2] http://en.wikipedia.org/wiki/Vertical_handoff, Wikipedia.org

[3] Rong-Jyh Kang, Hsung-Pin Chang, Ruei-Chuan Chang, "A Seamless Vertical Handoff Scheme," wicon, pp. 64-71, First International Conference on Wireless Internet (WICON'05), 2005.

[4] Mobile IP, RFC 2002, 1996

[5] Mobile IP Authentication, Authorization, and Accounting Requirements, RFC 2977, 2000

[6] Charles E. Perkins, "Mobile Networking Through Mobile IP", Sun Microsystems

.