Topologically-Aware AAA Overlay Network in Mobile IPv6 Environment*

Jun Li[1,2,3], Xin-ming Ye[2], and Ye Tian[1,3]

[1] Institute of Computing Technology, Chinese Academy of Sciences,
No. 6 Kexueyuan South Avenue, Beijing, 100080, China
[2] Department of Computer Science, Inner Mongolia University,
No. 235 Daxue Avenue, Hohhot, 010021, China
[3] Graduate University of Chinese Academy of Sciences
No. 19 Yuquan Avenue, Beijing, 010021, China
{lijun,jack_ty}@ict.ac.cn xmy@imu.edu.cn

Abstract. In mobile IPv6 network, AAA mechanism is necessary for administration and security because roaming nodes are permitted and become majority. However, disharmonies are exposed when MIPv6 meets AAA. On one hand, AAA procedures increase the latency of MIPv6 handover by inserting several message round trips before mobile registration. Thus the handover performance is reduced. On the other hand, AAA does nothing to help MIPv6 with its security problem. The fact is that MIPv6 has to struggle with those problems by itself. The result is that MIPv6 become complicated and inefficient. The crux of the matter is that AAA and MIPv6 are separately designed from their own viewpoints without mutual reinforcement. In this study, a Topologically-Aware AAA Overlay Network (TA^{4}ON) is used for compatibly combining together resources and capacities from both sides. All connected AAA participators construct an overlay network which is naturally topology-aware. MIPv6 security issues, for example key generating and peer identifying, are handled by AAA. Secret materials and even MIPv6 signals can be delivered through TA^{4}ON. As shown in this paper, at little additional cost all things serve their proper purposes and finally performance and security of MIPv6 are improved.

Keywords. Mobile IPv6, AAA, Overlay Network, Performance, Security

1 Introduction

At the beginning of defining Mobility support in IPv6 (MIPv6) [1] , researchers came to an agreement that performance and security are very important for it. Almost at the same time when MIPv6 specification was a draft, several enhancement solutions were discussed constructively. Among them, some enhancements were to improve the handover performance. The most famous of them are FMIPv6 [2] and HMIPv6 [3], they became experimental standards recently.

Enhancements for security were proposed, too. IPSec [4][5] was used to protect the communication between Mobile Node (MN) and Home Agent (HA) [6]. Also, that proposal became a standard and was released with MIPv6. Several other proposals are under discussed, for an instant, [7] is for authenticating MN while it is away from home. However, In MIPv6, only internal security problems are cared. Some problems are resolved locally without an overall consideration.

From the viewpoint of administration and security, Authentication, Authorization and Accounting (AAA) mechanism is foundational infrastructure for the entire network.

* This work was supported by NSFC grant No. 60263002.

Almost all the operators have deployed AAA in their networks, and it will be the same situation in the future mobile Internet. AAA infrastructures are connected with each other. Communications between them are protected by pre-shared Security Association (SA). AAA infrastructures that belong to different administrative domains or different operators can be connected to provide service to subscribers of other domains [8]. Of course, in this case administrators involved must have reached an agreement in advance.

Here comes the problem. On one hand, AAA delays MIPv6 handover by inserting the access control before mobile registration procedure.

See figure 1. MN has to perform home registration (step 2 in figure 1) and correspondent registration (step 3 in figure 1) only after it has been authenticated and authorized to access network by back end AAA server (step 1 in figure 1). Authentication procedure may be very time-consuming according to network topology. Particularly, when MN is in a foreign administrative domain, authentication messages may have to pass through several administrative networks and AAA servers to get to its destination.

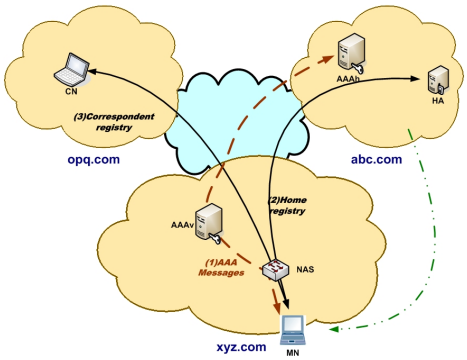

Fig. 1. AAA mechanism and MIPv6 handover

Abc.com is the home domain of MN and AAAh is its registry AAA server. Xyz.com is the current domain where MN is located. In domain xyz.com, NAS is a Network Access Server and AAAv is the designated AAA server for that NAS.

Because the total handover latency is nearly doubled comparing to the situation without access control, time sensitive applications will not work well. This is a real challenge for MIPv6. HMIPv6 can't keep away from this difficulty either. FMIPv6 gets even worse in that it can't be "fast" and just works as standard MIPv6. To address such issue, a good idea is to combine two procedures together, ie. integrats home registration messages into AAA messages and let home AAA server communicate with HA [9][10]. However, it is not enough only to care the home registration procedure. Correspondent registration should be taken into account, too. Some other solutions [11][12] were proposed just to give architecture for MIPv6 and AAA to work together but handover performance was not considered.

On the other hand, security is another focal point of MIPv6 handover. However, AAA does nothing for it though AAA is good at this.

MIPv6 is trying hard to resolve all problems by itself, including security issues. For example, [7] is trying to authenticating MN by carrying authentication data in packet header. At the same time, instead of resolving all the security issues listed in [1] and [13], this will make MIPv6 so complicated, unoperationable and inefficient. Return Routability (RR) procedure is used in [1] to protect correspondent registration, however, there are still many flaws in it as listed in [1]. [14] is trying to secure the route optimization between MN and CN by static key, however there are still some limits to use its mechanism, such as MN and CN must be in the same domain and so on. This is not flexible enough for future global mobility.

[15] gave a solution to protect all traffic for MIPv6, but HA is its bottleneck. It's already a heavy burden for HA to record the positions and forward messages for all roaming MNs. That solution can make HA overworked. Under this situation, HA becomes a vulnerable link of the entire chain.

On the contrary, we know that AAA infrastructures have powerful computing capacity and are natively good at security concerns. In addition, AAA servers can be connected to construct an overlay network, so they know easily the topology of network in a large scale. They should do more good to MIPv6 rather than just carry home registration messages. So far, we see few studies focusing on this point.

AAA and MIPv6 have been developed separately. Both of them have their own purposes, protocols, mechanisms, application field and so on. It's not easy to combine them together and work harmoniously. We are trying to resolve this issue in a novel way. From the point of view of our study, AAA infrastructures are the "virtual backbone" of inter-networks at application layer, and they are core layer for administration and security.

In light of those situations mentioned above, this research is carried out to achieve three goals below,

- *Compatibly merge AAA mechanism and Mobile IPv6;*
- *Speed up signal delivery for Mobile IPv6;*
- *Provide security service for Mobile IPv6.*

The main contribution of this study is (1) TA^{4}ON is used to enhance MIPv6. Performance and security level are both improved; (2) Only little additional costs are added to AAA infrastructures and MIPv6 remains specialized and efficient.

The rest of this paper is organized as follows. Section 2 introduces the background of this study. Section 3 describes the framework of TA^{4}ON. Section 4 shows in detail how TA^{4}ON enhances MIPv6. Section 5 gives a analysis and evaluation. Section 6 ends this paper with conclusion and future work.

2 Preliminary

In this section, Mobile IPv6 and Diameter base protocol (the newest and typical version of AAA protocol) are described as background of this research respectively. The significance of performance and security for MIPv6 is highlighted. The topologically-aware inter-connection on application layer is described as the feature of Diameter.

2.1 Mobility Support in IPv6 (MIPv6)

IPv6[16], above all, has a huge address space which is believed never to be exhausted. MIPv6 is fresh blood to IPv6 family. It adds feature of host mobility to IPv6.

In figure 2, a MIPv6-enabled Node (MN) has a permanent address at its registry network. That address is called Home Address (HoA) and the registry network is *home network*. Networks except home network are all called *foreign networks*. Each time MN handovers to or boots at a foreign network, it will get a Core-of Address (CoA) by stateful or stateless address auto-configuration① [17]. The subnet prefix of CoA is same as that foreign network's.

There is at least one important fixed node, called Home Agent (HA), at home network. Every time MN gets a new CoA (the new one is called Current CoA, CCoA. The old one is called Previous CoA, PCoA.), it must register that CCoA with its HoA to HA by exchanging binding messages②. That procedure is called Home Registration (HR). HA's functionality is to impersonate MN by proxy neighbor discovery when MN

is away from its home network. It receives packets destined MN's HoA③, then forward them to the CCoA of MN via a pre-established tunnel④ and reversely. All communications between HA and MN are protected by IPSec with a pre-shared Security Association (SA) [6]. At this point, MN can be reached again after changing its point of attachment.

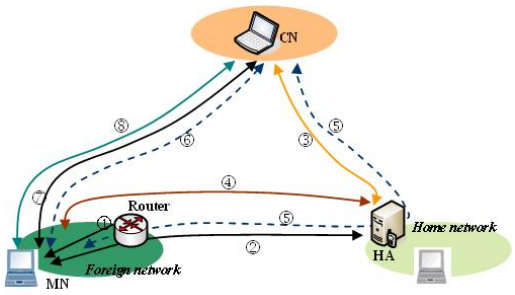

Fig. 2. Communications while MN moves to a foreign link

MN may optionally send binding update message⑦ to the source of those packets, called Correspondent Node (CN), to eliminate triangle routes, MN-HA-CN. That procedure is called Correspondent Registration (CR). Those binding messages are protected by a leading Return Routability (RR) procedure ⑤⑥ (dashed line in figure 2). Then CN and MN can send message directly to each other⑧ without detour via HA. Usually this is called route optimization.

Procedure HR, RR and CR are performed one after the other. Messages exchanged during HR, RR and CR are called *handover signal messages*. HR messages are prerequisite for handover and it must be the first step among them. CR is carried out only for the purpose of route optimizing after HR is completed successfully. RR is the leading security procedure for CR.

So as far as performance is concerned, HR is the first step to recover the reachability. However, HR is not enough in most cases because reachability is not really recovered immediately after HR. Usually CN insists to send packets to MN's PCoA before CR is finished. If CR is late or somehow aborted, then CN has to sent packets to MN's home network. At this time, reachability is really restored. Even so, too many packets have been lost and HA may become the bottle neck of route. Again if somehow HR is late, then the situation becomes worse because even HA does not know at all where MN is. Granting that everything goes as our wishes, "optimized route" may be the worse one because it is not always the truth in a Internet route triangle that the sum cost of two lines is greater than the cost of the third one [18]. Usually applications require low latency time and small rate of packet lose on handover, so handover performance is a challenge for MIPv6.

Security is another coin side for MIPv6. To protect communication between MN and HA, including HR messages, IPSec with pre-shared SA is used[6]. But pre-shared SA is not flexible enough for MIPv6, for example, to support Dynamic Home Agent Address Discovery (DHAAD) and Mobile Prefix Discovery (MPD). DHAAD and MPD in MIPv6 may leak information about network topology and make MN to be tricked into believing false information about prefixes. Although CR is protected by a leading RR procedure, threads still exist because RR is not flawless. Security problems of MIPv6 are listed in [1]. Nevertheless, no applicable solution is given.

In some place, security procedures conflict with handover performance. For example, RR procedure defers CR procedure at least 1.5 round trips. If IKE[19] is used for generating dynamic SA, then SA has to be regenerated on each time handover, which

must detain HR for a few round trips. MIPv6 is facing a dilemma of emphasizing performance or security.

2.2 Diameter based AAA mechanism

MIPv6-capable mobile nodes can roam among networks that belong to their home Service Provider as well as others. This is a result of the service level agreements that exist between operators. One of the key AAA protocols that allow this kind of roam mechanism is Diameter [8]. [9] is an Internet Draft specifies a new application to Diameter that supports Mobile IPv6.

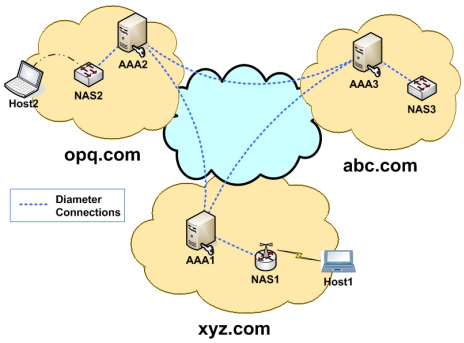

Fig. 3. Diameter based AAA mechanism

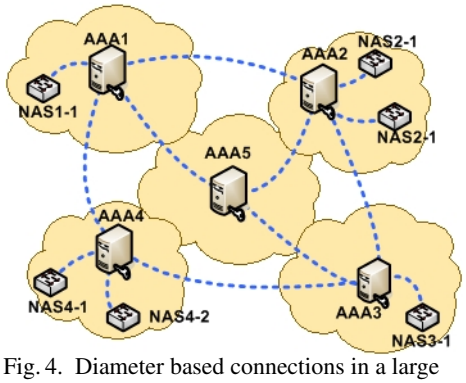

Fig. 4. Diameter based connections in a large scale

According to Diameter base protocol, Diameter connections are established between each two adjacent AAA servers as well as between AAA servers and their own subordinate NASs as soon as they begin to serve. Communications are protected by pre-shared SA. Connections will be kept until service stops. *So we can believe that connections are always secure and stable.* The methods for connection setup and communication protection are beyond the scope of this paper.

In figure 3, there are three administrative domains which may belong to different operators. Among those operators roaming agreements exist. In each domain there may be several networks or sub-networks, and at least one AAA server. AAA1, AAA2 and AAA3 are Diameter AAA servers located at different domains and serve their own subscribers respectively. For example, AAA1 is the registry server of host1 at its home domain, “xyz.com”. And AAA2 is the registry server of host2 at its home domain, “opq.com”. Network Access Server (NAS) is the command executor for the designated AAA server. It is the nearest AAA infrastructure to hosts which need to access network.

Next we will describe a typical occasion of AAA message flow. If, sometime NAS1 has to authenticate a host registered at a foreign domain, say abc.com, a request message originated from that host is forwarded to a designated AAA server, AAA1. And then some messages are exchanged between AAA1 and AAA3. If necessary, messages may pass an inter-mediate domain, and then an AAA server in that domain is responsible for forwarding the messages forth and back. When a result message eventually arrives at NAS1, it will know how to do with that host.

Figure 4 shows a bigger inter-network. There are five connected Diameter AAA servers and their own five subordinate administrative domains. There are immediate connections among some of them. AAA4 and AAA5 can be bridges for AAA1 and AAA3, AAA1 and AAA3 can be bridges for AAA2 and AAA4. However, those candidates may not become real bridges. Whether a AAA server is a bridge for others is decides by administrators of involved domains. They must take necessity, cost, security

and performance into consideration. A real AAA bridge server must be the result of agreeing on those factors.

3 Topologically-Aware AAA Overlay Network

In our opinion, AAA infrastructures connected together via Diameter protocol are switch nodes of an overlay network. Let's take a new look at figure 3. If only AAA messages are considered, then an overlay network can be observed. AAA servers are switch nodes and AAA connections are links between two adjacent switch nodes. If a domain is big enough then AAA servers in it can be connected hierarchically to obtain high efficiency of management.

Furthermore, this AAA overlay network is born topologically-aware. Usually AAA servers and NASs are deployed along the topology of networks. Administration domain is composed of several physical networks (or subnetworks), each of which there is at least one NAS working for a designated AAA server which is in charge of businesses of this domain. Diameter connections between different domain are setup between two AAA servers located in top level of each domain respectively.

If we think about this overlay network in a much larger scale, then it becomes "virtual backbone" for the whole inter-network. Top level AAA servers are core switch nodes and NASs become the edge switch nodes of this overlay network (See figure 4). Again if we make AAA infrastructures to shoulder much more responsibility, then they will be the "core layer" of administration for the whole inter-network. This is exactly what we are doing and the object is called Topologically-Aware AAA Overlay Network (TA^4ON).

3.1 Basic Assumptions

Before going on the discussion, we have following basic assumptions. Some of them were mentioned above, but we reorganize them below for clearly understanding.

1) The scope of operation may cover several administrative domains which may belong to different operators. There are agreements among them to grant AAA servers to be connected together using AAA protocol like Diameter.
2) There is at least one AAA server in an administrative domain. AAA servers and Network Access Servers in a same domain are connected to be a hierarchical structure.
3) At least one AAA server (usually the one at top level) in each domain is the Gateway Server (GS). GSs are interconnected for exchanging and forwarding AAA messages according to agreements between operators.
4) The communication between each two connected AAA servers and between AAA servers and NASs is protected in some way. It is believed secure to communicate through those connection. However, how to do so is out of the scope of this paper.
5) Administration factors described in subsection 2.2 are ignored. A Diameter AAA server is a bridge server for others only if necessary and possible.

3.2 Framework

To achieve the objectives listed in section 1, we want the AAA overlay network to delivery as many as MIPv6 signals. And it must get much more information about the inter-network, such as topology and status.

Figure 5 is a diagram for our framework of TA^4ON. To simplify our discussion, there is only one AAA server in each of those three administrative domains. So they are

all GSs and are interconnected to be an AAA overlay network. Not only MN but also HA and CN are connected to this overlay network. They all trust the nearest AAA infrastructures (AAA server and NAS) in their registry domain, then indirectly the AAA infrastructures in other domains. Each node has a unique identity for living in this overlay network. Usually Network Access Identity (NAI) [20] or Mobile Node Identity (MNI) [21] is used. NAI looks like someone@somedomain.com, where somedomain.com is the name of registry domain.

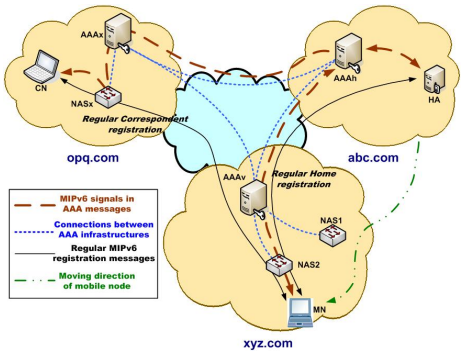

Fig. 5. Framework of TA[4]ON

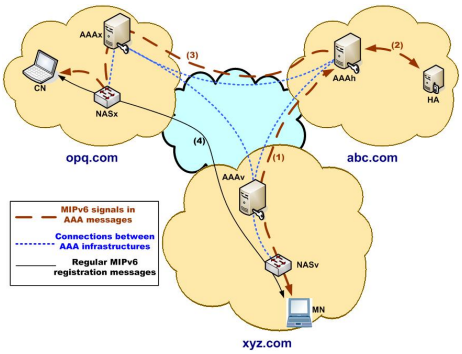

Fig. 6. Signals delivering and key materials distributing

MN, CN and HA need to establish trust relationships with AAA infrastructures in their registry domain. They are also required to understand new type of AAA messages and the MIPv6 signals inside.

Note that only AAA messages run on the AAA overlay network, including original and new created types. Other messages, such as MIPv6 regular signals and normal data stream, are transported as usual.

3.3 Definition of TA[4]ON Messages

MIPv6 signals are not only carried piggyback in some primitive AAA messages, but also delivered in some new types of message specially defined for MIPv6. Following is a list of primary types of new defined messages.

Type 1 (T1): handover registration. It is defined for delivering Binding Update (BU) and Binding Acknowledgment (BA) on handover registration, including home registration and correspondent registration. Note this type of message is not for the regular registration message sent between MN and HA/CN periodically.

Type 2 (T2): key material. It is defined for delivering security related data, such as secret key, lifetime and initial parameters and so on. Usually, key material is delivered to two peers, MN and HA or MN and CN, which need to initialize and protect their subsequent communication.

Type 3 (T3): dynamic home. It is defined for delivering Dynamic Home Agent Address Discovery (DHAAD) messages and Mobile Prefix Discovery (MPD) messages between MN and HA.

Type 4 (T4): network status. It is defined for delivering status information about involved network. AAA servers need to send probe packet to be aware of the network status. And if necessary, right current information about the network is delivered to some node which requires them.

Note, each type of message has options which can be used to differentiate subtypes.

Connections between any two AAA infrastructures are believed to be secure and stable, so we can use them to deliver some security sensitive messages. And any other

signals of MIPv6 can be transmitted on this overlay network, too. Of course, if unnecessary, MIPv6 signals can be transmitted as usual.

3.4 Network Status Table

Every AAA server must maintain a Network Status Table (NST) to keep the current status of its domain and its neighbor domains. NST is used for interconnected AAA servers to find the way to other domain or sub-domain. In TA^{4}ON NST is a "virtual topology table" for the overlay network. We believe that it must to some degree be a mirror of the real inter-network. So NST is necessary for TA^{4}ON to be "Topologically-Aware".

Table 1 is an sample of NST on AAAv in domain xyz.com. In Table 1, "Domain Name" is the destination domain. "Next Peer" is the valid way to that destination. Actually "Next Peer" is a AAA server. It is similar to the next hop in IP routing table. Entries in Table 1 must be symmetric, that is if AAAv has an entry for AAAx, then AAAx must has an entry for AAAv.

In addition, besides information in NST AAA server must know which MN is connecting to some NAS and which MN is registered at some HA. To do so, it must know information in its domain not only about NASs but also about HAs. AAA server must know which HA is in its domain and what its link prefix is. There is pre-established secure tunnel between AAA server and HA.

Table 1. Network Status Table on AAAv

Sn	Domain Name	Next Peer
1	abc.com	aaav.abc.com
2	opq.com	aaax.opq.com
3	other.com	aaax.opq.com

AAA servers send T4 messages with probe option to all its peers periodically to make sure that peer is alive and by the way get other status information about them. Probe T4 is sent not only to immediate peers but also to all other peers in NST because AAA servers must be "Topologically-Aware". AAA overlay network is setup by manual configuration because of administration and security, no dynamic routing algorithm is used. And so AAA overlay network is usually limited in a moderate scale.

4 Methodology

In this section, three typical usages of TA^{4}ON are described to show how TA^{4}ON enhances MIPv6.

4.1 Handover Signals Delivery

There are several solutions [9][22] for integrating MIPv6 home registration messages into AAA authentication messages in one round trip. This is supported by our proposal, too. See figure 6, following describes the procedure for delivering handover signals.

Step 1, when MN moves into a foreign network, it constructs authentication request message M_1 with its NAI and authentication data inside and with signal of MIPv6 home registration piggybacked.

$$M_1 = NAI_{mn}|Auth\_data_{mn}|MIPv6\_HR(HoA, CCoA) \quad (1)$$

Step 2, MN sends M_1 to NASv. NASv forwards M_1 to designated AAA server, AAAv. And then AAAv forwards M_1 to AAAh, the registry AAA server of MN (up

direction of message flow 1 in figure 6). Before forwarding M_1, NASv and AAAv may store information and set soft states for M_1.

Step 3, on receiving M_1, AAAh authenticates MN with data inside. If successfully, AAAh exchanges T1 messages with HA to perform home registration in the name of MN (message flow 2 in figure 6).

Step 4, AAAh puts a successful BA into the authentication answer message and sends it back to MN (down direction of message flow 1 in figure 6).

Step 5, when MN receives a successfully authentication answer message from NASv, it knows that a) it is granted to access the network, b) home registration has been completed.

Above procedure has been used in other proposals [9][10][22]. However, in those proposals only HR was considered, CR was neglected. To speed up CR, besides operations described above, following additional operations are added.

At step 1, MN appends request message of CR to M_1, including HoA and CCoA of MN, NAI of CN. HoA and CCoA is for CN used to update binding list. NAIs is used for AAAh to identify CN's registry AAA server. At step 4, AAAh sends T1 message with HoA and CCoA to AAAx. AAAx checks whether this messages is valid. If so, AAAx forwards this message to NASx, NASx then forwards it to CN (flow 3 in figure 6). Usually at step 5, MN receives the answer from AAAh, CN almost at the same time receives this T1 message. Then in only one round trip authentication, HR and CR are all finished.

4.2 Key material distribution

In addition, in our proposal secret materials can be distributed over TA^{4}ON. There are at least two types of secret materials, one is between MN and HA, the other is between MN and CN.

Key materials between MN and HA can be used to setup dynamic SA between them. HA won't have to save SA for each MN registered at HA. MN won't save SA with its HA either. At MN only secret key with AAAh is remembered. When necessary, MN sends T2 request to AAAh, then AAAh generates a key material randomly [23] and sends T2 message over TA^{4}ON to MN and HA, respectively. Thus MN and HA can setup their SA with their secret material.

Key materials between MN and CN can be generated and distributed similarly. If AAAh receives a T2 request for this kind of key material, on sending key materials to MN, AAAh must identifies CN's registry AAA server and sends key materials to it. While MN and CN finally receive key material from their own registry AAA server respectively, they can work out a common Short-Term Static Key (STSK) according certain arrangement. After that, each time MN handover to new foreign link, RR is not necessary any more because they already have a short-term static key. CN can also send T2 request to its registry AAA server firstly, then key materials are generated and distributed by this AAA server.

STSK differs from the method described in subsection 4.1. They are used in different situation. The latter is used for CR on handover. STSK is used for BU sent periodically (flow 4 in figure 6).

To reduce the unnecessary workload of MN, CN and TA^{4}ON, T2 request for STSK can be sent as appendix of M_1 described in subsection 4.1 and it is feasible for MN and CN to use a STSK a few times until they believe that it should be replaced.

4.3 Dynamic Discovery of Mobile Prefix and Home Agent

In MIPv6 specification [1], it is allowed for home agent to change its address and even the topology of home network is allowed to change. The dynamic home agent discovery

function could be used to learn addresses of home agents in the home network. But this is also an easy way for attacker to find target. Mobility prefix discovery is useful for MN to learn new topology of its home network. However, this must be done before the topology changes.

Here we use T3 messages to deal with this kind of problem. The prerequisite is that the address of AAAh will never change. Usually, it is truth in the real world.

When the address of home agent is changed or the topology of home network is changed, AAAh will be firstly informed in some manual way. So there are two cases for mobile node to learn about that. One is solicited mode. Mobile node send a T3 message with request option to AAAh, AAAh reply a T3 message with current information of home agents and home network to mobile node. The other is unsolicited mode. AAAh send T3 messages actively with new information about home agent and network to all involved mobile nodes as soon as anything changes in home network.

At the same time, secret materials are sent in T2 to related peers. Namely, if home agent is involved in above procedure, the new key material for IPSec SA_{mn-ha} is generated and sent by AAAh to mobile node and designated home agent respectively.

5 Analysis and evaluation

5.1 Security Analysis

Above all, the security of TA^{4}ON is guaranteed by AAA protocol, so it is believed that TA^{4}ON is secure and stable. Communication between MN/CN and NASs is protected by key setup with the materials from AAA server during authentication procedure. Next, we discuss the security of MIPv6 when TA^{4}ON is used.

As far as HR and CR is concerned, signals are delivered over TA^{4}ON, so no security problem need worrying about. Communication between AAAh and HA is protected by preestablished secure tunnel. Communication between MN/CN and NASs is protected by key setup with the materials from AAA server during authentication procedure. So no vulnerability is introduced as long as TA^{4}ON is secure enough.

Key material distribution is secure, too. Most hops are in the TA^{4}ON. The final hop is between MN/CN and NASs. They are all under protection. Key material can be protected by additional encryption: registry AAA server encrypts key material by preshared SA before sending it to MN/CN; MN/CN decrypts it and generates STSK from it. Only MN and CN have the STSK, others, even NASs, have no idea about STSK. To determine how many times MN and CN use their STSK is not discussed in this paper.

MIPv6 signals between MN and CN are protected either by TA^{4}ON or by STSK, so RR procedure is canceled. Vulnerability introduced by RR is wiped out.

The security of DHAAD and MPD is also guaranteed by TA^{4}ON because all related signals are delivered on TA^{4}ON as well as key materials between peers.

5.2 Performance Analysis

TA^{4}ON is topologically-aware. Signals delivered on it can be thought to pass though a optimized route.

Similar with [22][10], HR over TA^{4}ON is performed in one trip. However, CR was not mentioned in [22][10]. CR over TA^{4}ON is finished in only one round trip, too. Usually, handover time can be derived out by following equation,

$$T = T_{IPv6} + T_{auth} + T_{hr} + T_{rr} + T_{cr} \tag{2}$$

where T is the total time of handover, T_{IPv6} is time latency for IP address configuration and Duplicate Address Detection (DAD, if stateless auto-configuration is used).

This is same in all solutions. T_{auth} is the time latency for authentication. T_{hr} is time latency for home registration. T_{rr} is time latency for RR procedure and T_{cr} is time latency for correspondent registration. To simple our discussion, T_{IPv6} is ignored. Also comparing to delivery latency, processing is too small, so it is ignored, too. If we compute T with message round time, then we get following results.

$$T = T_{auth} + T_{hr} + T_{rr} + T_{cr} \tag{3}$$

In solution without optimization, T_{auth}=1, T_{hr}=1, T_{rr}=1.5 (path detouring HA is 1.5) and T_{cr}=1.

$$T_{no-opt} = 1 + 1 + 1.5 + 1 = 4.5 \tag{4}$$

In solution with half optimization, T_{auth} + T_{hr}=1.1 (Latency between AAAh and HA is 0.1 because they in the same domain). Thus

$$T_{half-opt} = 1.1 + 1.5 + 1 = 3.6 \tag{5}$$

In our solution, T_{auth} + T_{hr} + T_{cr} = 1.1, T_{rr} = 0. Thus

$$T_{full-opt} = 1.1 + 0 = 1.1 \tag{6}$$

Comparing those results, we can say that our solution outperforms others.

If dynamic key is used between HA and MN, IKE is very time-consuming because there must be two phases and a few round trip in each phase. However, it is very easy and fast to implement dynamic key in our solution. AAAh can send dynamic key to HA and MN separately after a successful authentication. No extra count of round trip is introduced. Dynamic key distribution and authentication answer returning is finished simultaneously.

5.3 Additional Cost

Though security and performance of MIPv6 is improved, additional cost is added. Firstly, we have to take some cost to setup and maintain TA^{4}ON. This may be a demanding task. Secondly, protocols involved must be extended to support new operations. Finally, additional process and bandwidth occupation is inevitable.

However, TA^{4}ON maintenance is not conducted frequently. Protocol extension is done only once and only a little work is needed. Extra resource consumption is inevitable, but its benefit is noteworthy.

6 Conclusions and Future Work

A Topologically-Aware AAA Overlay Network (TA^{4}ON) is proposed for merging AAA mechanism and MIPv6. TA^{4}ON is aware of network topology and capable of security business. MIPv6's mobile signals and secret material can be delivered fast and securely through TA^{4}ON. Dynamic discovery of mobile prefix and home agent can be easily completed with the help of TA^{4}ON. So performance and security of MIPv6 handover are improved. Comparing to existing MIPv6-AAA methods, TA^{4}ON is not a partial but a total solution.

There still are a lot of work to do to make TA^{4}ON much more useful. TA^{4}ON may gain better performance if cooperates with HMIPv6. It may be helpful for MN and CN to optimize their routes, up stream and down stream separately. And TA^{4}ON may be used not only in MIPv6 environment but in any place where AAA mechanism is used.

References

1. D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", *IETF RFC3 775*, June 2004
2. R. Koodli, Ed., "Fast Handovers for Mobile IPv6", *IETF RFC 4068*, July 2005
3. H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", *IETF RFC 4110*, August 2005
4. S. Kent, R. Atkinson, "IP Authentication Header (AH)", *IETF RFC 2402*, November 1998
5. S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", *IETF RFC 2406*, November 1998
6. J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", *IETF RFC 3776*, June 2004
7. A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, "Authentication Protocol for Mobile IPv6", *IETF-ID*, working in progress.
8. P. Calhoun, J. Loughney, E. Guttman, et al., "Diameter Base Protocol", *IETF RFC 3588*, June 2003
9. Franck Le, Basavaraj Patil, Charles E. Perkins, Stefano Faccin "Diameter Mobile IPv6 Application", *IETF-ID*, working in progress.
10. Kim C., Kim Y.S., et al., "Performance Improvement in Mobile IPv6 Using AAA and Fast Handoff", *Proc. of 2nd International Conference on Computer Science and its Applications (ICCSA'04)*, June 2004
11. Wang R.C., Chen R.Y., Chao H.C., AAA architecture for mobile IPv6 based on WLAN, *International Journal of Network Management*, Volume 14 , Issue 5, Pages: 305 C 313 ISSN:1099-1190, September 2004
12. R.I. C., Reen-Cheng, W., Han-Chieh, C., "Mobile IPv6 and AAA Architecture Based on WLAN", *Proc. of International Symposium on Applications and the Internet Workshops (SAINTW'04)*, January 2004
13. J. Kempf, J. Arkko, Nikander P., "Mobile IPv6 security", *ACM Wireless Personal Communications*, v29, n 3-4 SPEC.ISS., June, 2004, p 389-414
14. Charles E. Perkins, "Securing Mobile IPv6 Route Optimization Using a Static Shared Key", *IETF-ID*, working in progress.
15. Ying Qiu, Jianying Zhou, Feng Bao, "Protecting All Traffic Channels in Mobile IPv6 Network", *Proc. of IEEE Wirelsss Communications & Networking Conferance (WCNC'04)*, March 2004
16. S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", *IETF RFC 2460*, December 1998
17. Narten, T., Nordmark, E., Simpson, W. "Neighbor Discovery for IP Version 6 (IPv6)", *IETF RFC 2461*, December 1998
18. A.D. Pramil, S. Antoine, A.H.Aghvami, TCP performance enhancement over mobile IPv6: innovative fragmentation avoidance and adaptive routing techniques,*IEE Proc.-Commun.*, Vol. 151, No. 4, August 2004
19. Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", *IETF-ID*, working in progress
20. Aboba, B. and M. Beadles, "The Network Access Identifier", *IETF RFC2486*, January 1999
21. A. Patel, K. Leung,M. Khalil, *et al.*, "Mobile Node Identifier Option for MIPv6", *IETF-ID*, working in progress
22. Jun Li, Xin-ming Ye, Jing-lin Shi, Miao Wang, "Authenticated Stateful Auto-Configuration for Mobile IPv6 based on pre-IP Access Control", *Proc. of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'05)*August 2005
23. D. Eastlake, 3rd, J. Schiller,S. Crocker, Randomness Requirements for Security, *IETF RFC 4086*, June 2005
24. Gabriel Montenegro, Claude Castelluccia, "Crypto-based identifiers (CBIDs): Concepts and applications", *ACM Transactions on Information and System Security (TISSEC)*, Volume 7 Issue 1, Pages: 97 - 127,ISSN:1094-9224, February 2004
25. T. Aura, "Cryptographically Generated Addresses (CGA)", *IETF RFC 3972*, March 2005