

# 支持路径选择与快速切换的移动网络接入 路由器安全 Mesh

黄松华<sup>1)</sup> 孙玉星<sup>2)</sup> 黄 皓<sup>1)</sup> 陈贵海<sup>1)</sup>

<sup>1)</sup>(南京大学 计算机软件新技术国家重点实验室 南京 210093)

<sup>2)</sup>(南京审计学院信息科学学院 南京 211815)

**摘 要** 性能一直是网络移动投入实际运营的瓶颈所在,而现有认证机制产生的延时使之雪上加霜.文中为多穴嵌套移动网络的接入路由器 Mesh 引入一种高效的双向认证机制,基于此提出最优路径选择算法和接入失效快速恢复算法,以提高移动网络的整体性能,尤其是延时的降低.文中,基于固定 AAA 基础设施和动态可信邻居的安全关联转移被用于减少路由器 Mesh 的认证延时,其行为评估机制降低了路由器攻击或欺骗对路径评价的影响;基于顶层接入路由器网络前缀的移动路由器转交地址配置被用于消除嵌套接入环境下的多角路由和隧道嵌套问题,而必要时临时隧道和反向路由头可以替代随切换而来的绑定过程以缩短切换延时,最后通过接入路由器评价生成到达 Internet 的最优路径.定性分析与仿真分析表明,由于异域网络间建立安全关联的高效性,加上行为评估、路径评估和快速切换产生的性能优化作用,文中的安全 Mesh 在吞吐量、传输延时和切换延时方面较同类方案更加高效.

**关键词** 网络移动;信任转移;行为评估;最优路径选择;快速切换

中图法分类号 TP393 DOI 号: 10.3724/SP.J.1016.2009.00531

## A Secured Access Router Mesh of Mobile Networks with Path Selection and Fast Handover Support

HUANG Song-Hua<sup>1)</sup> SUN Yu-Xing<sup>2)</sup> HUANG Hao<sup>1)</sup> CHEN Gui-Hai<sup>1)</sup>

<sup>1)</sup>(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)

<sup>2)</sup>(School of Information Science, Nanjing Audit University, Nanjing 211815)

**Abstract** Performance is always the bottleneck for deploying network mobility (NEMO), and the delay resulting from existing authentication mechanism makes it even worse. This paper introduces an efficient authentication method for access router (AR) mesh of multihomed and nested mobile networks, with path selection and fast handover support to promote whole performance of mobile networks, especially to reduce the delay. First a mutual authentication method is presented based on fixed AAA infrastructure and dynamic trusted neighbors, integrated with a behavior evaluation mechanism. And based on this authentication method the algorithms for optimal path selection and recovery of access failure are proposed. In the solution, security association (SA) transfer is to cut down the authentication delay; multi-angular routing and tunnel-in-tunnel problem in nested situation can be eliminated through the Care-of-Address (CoA) configuration of mobile router based on top-level AR prefix; temporary tunnel and reverse routing header (RRH) may be borrowed to leave out the binding procedure in handover; AR evaluation will pro-

收稿日期:2008-09-17;最终修改稿收到日期:2009-01-06. 本课题得到国家“八六三”高技术研究发展计划项目基金(2007AA01Z409)、国家“九七三”重点基础研究发展规划项目基金(2006CB303004)、国家自然科学基金(60303023,60573131,60673154,60721002,60825205)和江苏省高技术研究项目基金(BG2007039)资助. 黄松华,男,1979年生,博士研究生,主要研究方向为网络移动与网络安全. E-mail: hsh@dislab.nju.edu.cn. 孙玉星,女,1977年生,博士研究生,讲师,主要研究方向为无线网络与网络安全. 黄 皓,男,1957年生,博士,教授,博士生导师,主要研究领域包括系统软件、信息安全. 陈贵海,男,1962年生,博士,教授,博士生导师,主要研究领域包括对等计算、传感器网络、并行计算.

duce an optimal path to the Internet. Analysis shows that, with efficient SA establishment between mobile networks and the foreign networks, expected node behavior evaluation, and optimized route, the solution in this paper is more efficient than the counterparts in terms of throughput, packet delay and handover delay.

**Keywords** network mobility; trust transfer; behavior evaluation; optimal path selection; fast handover

## 1 Introduction

Here is coming a new era for both communication and computation: May be one person with multi computers which are portable and need inter-connecting and moving as a personal mobile network<sup>[1]</sup>. Network mobility arises when a router connecting these mobile networks to the Internet dynamically changes its point of attaching to the Internet, thereby causing the reachability of the said network to be changed in relation to the fixed Internet topology<sup>[2]</sup>. IETF NEMO working group gave a proposal called network mobility basic support protocol (NBSP) to meet the requirements in 2005<sup>[3]</sup>.

Since the openness of mobile environment introduces more potential threats, several security issues, such as mutual authentication between nomadic terminals and foreign access networks, end-to-end confidentiality and integrity, credibility or reliability evaluation of access routers and so on, must be considered<sup>[4-5]</sup>. In addition, since traffic overload or handover delay in mobile environment brings new problems, fault tolerant mechanism is also an issue that cannot be ignored in mobile networks<sup>[6]</sup>.

Authentication, Authorization, and Accounting (AAA) is a useful solution for mutual authentication and authorized access. A secure deployment of NEMO into the real world cannot avoid the usage of AAA protocol<sup>[7]</sup>. Based on key management of AAA infrastructure, end-to-end confidentiality and integrity can be guaranteed through IPsec. Indeed, methods that integrate mobility and AAA for IPv4/v6 exist today. However, NEMO introduces far more complexity than host mobility and does challenge the authentication mechanisms by introducing new AAA issues because mobile network nodes may rely on multiple mobile routers to take care of their mobility management tasks in the nested topology, while it is not mentioned that how AAA issues are handled in NEMO environment in NBSP<sup>[8-9]</sup>. To address such a situation, AAA architecture adapted to nested-NEMO con-

figurations based on diameter protocol was proposed<sup>[10]</sup>.

Though AAA in Ref. [10] are a frame for identity authentication in nested NEMO, no detailed algorithm has been proposed. Benefits of multihoming such as reliable access point, optimized path, seamless handovers of the on-going sessions are not achieved<sup>[11]</sup>. Meanwhile, intentional or unconscious attack or deceit may happen in the dynamic and uncertainty environment where the access router's credibility varies with time, especially when the mobile networks are floating. Moreover, additional delay was introduced to the total handover delay, crucially affecting the prime objective towards seamless mobility, which adds fuel to the fire for real-time services or delay-sensitive traffic (e. g. VoIP or streaming multimedia services)<sup>[12]</sup>. Traditional mechanism based on AAA or public key infrastructure (PKI) can't adapt to these requirements<sup>[13]</sup>.

Fortunately, some other researches offered side benefits that alleviate the suffering mentioned above potentially. For example, there is a profusion of existing work aiming at offering trusted interaction among the mobile devices and their internal components, trust collaboration among mobile communication peers, and trust-intelligence support for the users at the mobile devices<sup>[14]</sup>. And Allard defined the IPsec context and then described a context transfer based solution to transfer IPsec context between two access routers in an IPv6 mobility environment to reduce time of establishing IPsec tunnel<sup>[15]</sup>. In addition, there are two ways closely related to reduce the handover delay caused by authentication procedures. First, optimization of reducing round trips between the foreign domain and the home domain can be achieved by encapsulating the binding information of Mobile IPv6 in the AAA exchange message<sup>[16-17]</sup>. Second, trust transfer solutions for security context were proposed to realize local authentication and seamless services over centralized cellular IP or WLAN architecture<sup>[18-19]</sup>. The handover procedures in the existing work however have to experience a trip to remote

home network for binding update or authentication, leading to long routing delay. Meanwhile, these solutions overlook the complex situation of NEMO, like nesting, being distributed etc. and do not support optimal path selection in data transmission and self-healing with less delay when handover bursts, which can be provided by multihoming. Still, NEMO are afflicted by poor performance in both handover and data transmission, and also security issues from dynamic environment.

To address these concerns, in this paper we propose an enhanced access router mesh, combining efficient identity authentication based on AAA infrastructure and trusted neighbors with behavior evaluation, optimal path selection, and self-healing of access failure, where security association transfer are introduced to avoid accessing AAA server in home network when identity authentication is needed every time and periodic identity authentication based on AAA may be trust-triggered when necessary. The proposed scheme can achieve the following advantages: 1) fault tolerance when access failure bursts; 2) high credibility between access routers from different domains; 3) high throughput and low delay in data transmission in nested and multihomed mobile networks. In addition, with little modification, our proposed scheme complies with the NBSP and the related security policies and recommendations.

The remainder of this paper is organized as follows. In Section 2, AAA infrastructure for NEMO and its enhanced solution with neighbor-based authentication and neighbors' behavior evaluation will be introduced. We give our secured algorithms for optimal path selection and fast handover based on enhanced AAA solution in Section 3. We discuss the performance and security in Section 4. Finally, this paper is concluded in Section 5.

2 Secured AR Mesh

AAA was proposed to meet the need for access control of all networks that allow an unknown user to connect to the network, and to identify itself to gain access to services and resources provided in the network. AAA protocols such as Diameter precisely enable mobile users to roam and obtain service in networks that may not necessarily be owned by their home service provider<sup>[12]</sup>. Nevertheless, a legal user may not always behave legally or properly, or in the way we expect. In this section, after multihomed and nested NEMO and its AAA infrastructure are introduced, behavior eval-

uation mechanism in mobile environment will be proposed to enhance AAA solution by reducing the negative impact of inharmonious act there. The following acronyms in Table 1 are used in this paper.

Table 1 Acronyms

acronym	full	acronym	full
RS	Router Solicitations	RA	Router Advertisement
MR	Mobile Router	FR	Fixed Router
AR	Access Router	NAS	Network Access Server
PaC	PANA Client	PAA	PANA Authentication Agent
MNP	Mobile Network Prefix	MNN	Mobile Network Node
HoA	Home-of-Address	CoA	Care-of-Address
HA	Home Agent	MN	Mobile Network
CN	Correspondent Node	SA	Security Association

2.1 NEMO Topology

The analysis detailed in this paper is based on a multihomed and nested NEMO scenario, where more than one network with more than one mobile router each exists. So one network has two mobile routers available at least and may use other networks to access the Internet. According to the deployment scenario, Fig. 1 gives the AR topology of multihomed and nested NEMO, with multi-HA and multi-MNP ignored for easy presentation. We give the formal description of NEMO topology as

$$\{MN_m, (MR_n, MNN_k, Dep_n, AR_{nj}, TLAR_{ni}, HA) | i \leq j\},$$

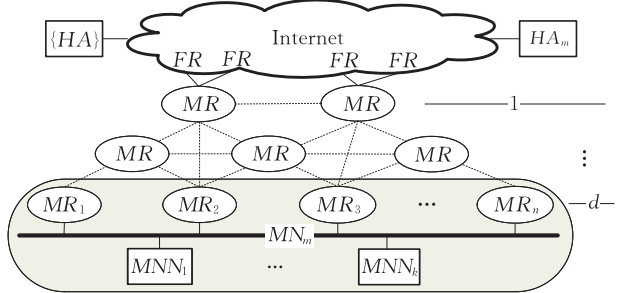


Fig. 1 AR Topology of NEMO

where, for one mobile network  $MN_m$ ,  $MR_n(n>1)$  denotes one of the mobile routers with  $Dep_n$  as its current nested depth,  $MNN_k(k>0)$  as one of the nodes it serves,  $HA_m$  as its home agent,  $AR_{nj}$  as one of the access routers it can reach, and  $TLAR_{ni}$  as its top-level AR; and  $d$  means the nested depth of  $MN_m$  (the least depth of its MRs); other  $MR$  here denotes the mobile network with one of the  $\{HA\}$  as its home agent. All MRs and FRs from the Internet infrastructure compose the AR mesh of NEMO, where we give related definitions as follows.

**Definition 1** AR Mesh is composed of multiple ARs, including MRs or FRs, which are inter-

connected.

**Definition 2** Fixed AR Mesh forms when at least one of ARs can connect current network with the Internet. Otherwise, it is called Floating AR Mesh.

**Definition 3** Top-level AR (TLAR) is the FR from the Internet infrastructure in Fixed AR Mesh or the MR with the least nested depth in Floating AR Mesh.

**Definition 4** When two ARs can access each other, one is the Neighbor AR (NAR) of the other.

**Definition 5** In two neighbor ARs that are authenticated each other, one with deeper nested depth (relative to the Internet) is called Sub AR (SAR), and the other Parent AR (PAR).

## 2.2 SA Transfer in Mobile Networks

For the safety of a multihomed and nested NEMO, it is necessary to secure every mobile router at every level by applying access control for any kind of service or network access, protecting against any unauthorized use and any type of impersonation. Here, AAA mechanism using Protocol for carrying Authentication Network Access (PANA), Diameter protocol and Extensible Authentication Protocol (EAP) is introduced to accomplish the task. And overall AAA architecture for the NEMO topology in Fig.1 is shown in Fig. 2.

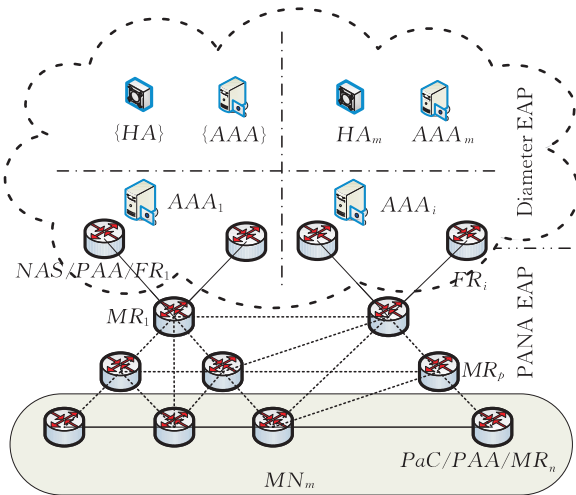


Fig. 2 Overall AAA Infrastructure

PANA is used as authentication protocol between MRs or MRs and FRs, with MRs as PaC or/and PAA and FRs as PAA; as AAA protocol, Diameter is used between AAA servers or FRs and AAA servers (AAA in Fig. 2 means both AAA server and EAP server), with FRs as NAS or AAA client; as authentication method, EAP is

running between MRs and AAA servers, where users' profiles are contained.

Also, we assume that SAs and safe passages are ready always between MRs and the AAA servers of home domain, between AAA servers of different domains, between AAA servers and PAAs in the same domain, and between ARs that have authenticated each other. Then, the way to implement mutual authentication when a MR (i. e.  $MR_n$  of  $MN_m$ ) switches to another AR (i. e.  $MR_p$ ) that can access the Internet can be realized with the help of its trusted neighbors (for example, one of its previous ARs), on condition that there exist trust relationship (like SAs) between its trusted neighbors and the AR to be accessed. If the current MR have no trusted neighbors, or its trusted neighbors have no trusted relationship with the AR to be access and this relationship establishment course (a recursive and breadth-first one similar to what the current MR is doing and will do) is beyond the time given, here comes the worst case shown in Fig. 3, where the mutual authentication will be done with help of its own AAA server in its home network, with one round trip.

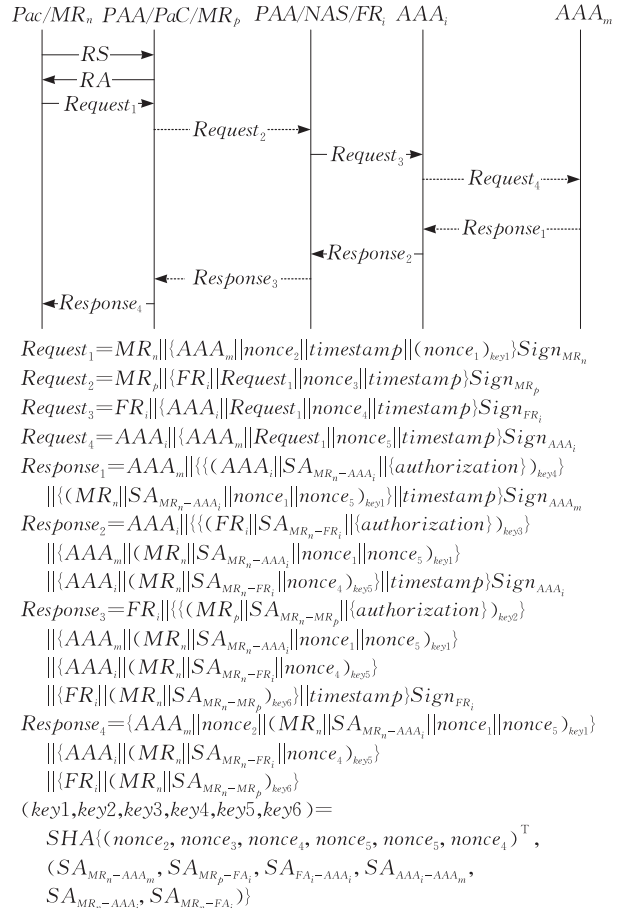


Fig. 3 Authentication Process

Here, the session key of the original passage will be updated according to the SA and the nonce received in authentication requests, and new-created SAs can be renewed through D-H method if ARs would like to keep them secret to their creators.

This architecture optimizes the mutual authentication of participating entities in a NEMO topology above by reducing the number of message exchange trips to one-round. Note that, currently, it is not necessary for MNNs and MRs in the same MN to be authenticated each other.

### 2.3 Behavior Evaluation Mechanism

Existing AAA schemes do not require additional mechanisms than those required for mutual authentication between ARs. As a result, the identity trust can be established before ARs access each other, but it does not protect network against intentional or unconscious attack or lying after identity authentication.

To address such a circumstance, we propose to use behavior trust as in our social lives. Trust here is established between two parties for a specific action. A trust value is some measure or quantity assigned by one party to its belief in the trustworthiness of other party.

Due to the high and frequent mobility of networks, limited-range and unreliability of wireless links, and sometimes lack of supports from AAA infrastructure, trust relations may have to be established using only on-line-available evidence, may be short-term and varies with time, and largely peer-to-peer, where the peers may not necessarily have a relevant “home domain” that can be placed into a recognizable trust hierarchy, and may be uncertain<sup>[17]</sup>. Here, we argue that in our NEMO topology: (1) Most ARs are honest and beneficent; (2) MRs are trusted by every MNNs from their own mobile network; (3) Trust between ARs is modified through direct evidence and relevant evaluation, with the help of existing detection model or behavior library<sup>[21-22]</sup>; (4) AR behavior is evaluated “on the fly” to substantiate dynamically formed trust relations; (5) Trust in period of validity can be transferred between ARs; (6) An AR may turn to another one for security or performance.

Different from the trust in MANETs, we do not calculate the trust for remote nodes but direct ones to form a credibility-aware environment with one link as its radius, and then the dependable path to the Internet by selecting the optimal nodes

in the next section. Evaluation’s goals in detail include: (1) to produce low credibility for negative nodes, and vice versa; (2) the corresponding trust values being decreased fast for negative reactions, being increased slowly for positive reactions, and being dropped faster for fluctuant reactions. The evaluation metric of one specific action  $B_i$  to determine whether or the extent to which  $A$  believes that  $C$  behaves properly is provided as follows:

$$Trust_{A \rightarrow C}(B_i, \alpha_i) = 1 - (1 - \alpha_i^{e^{f+o^2}})^{(s+1)}, o \leq \min(s, f) \quad (1)$$

Where,  $\alpha_i \in (0, 1]$ , is the trust threshold for  $B_i$ , which is initialized and can be adjusted according to related policies of  $A$ ;  $s, f, o$  are the number of  $C$ ’s positive responses, that of  $C$ ’s negatives responses, and time of  $C$ ’s swing responses<sup>①</sup>, observed by  $A$ .

And then the evaluation metric of  $C$ ’s general behavior for  $A$  is given here:

$$Trust_{A \rightarrow C} = \sum_{i=1}^I w_i \times trust_{A \rightarrow C}(B_i, \alpha_i) \quad (2)$$

Where,  $I$  is the number of behaviors that will be considered, and  $W_i$  is the corresponding weight.

Trust values calculated by Formula (2) will be used to modify the path availability in the next section, aiming at the high trustworthiness of the path selected after path evaluation according to the parameters of RAs from neighbor ARs.

## 3 Enhanced AR Mesh

Since mobile networks suffer from some inherent defects of wireless connection, taking advantage of multihoming to promote whole performance of NEMO is peremptorily needed. Meanwhile, AAA relies on frequently consulting the home network by sending back an authentication request when a mobile network roams to a foreign network or one of its MRs accesses a new AR. This procedure causes long handover delay and may not be feasible for real-time applications. Moreover, when mobile networks lose the Internet connectivity, AR handover and the following communication become impossible, since the AAA infrastructure on which authentication process relies or the HA to which binding update should be sent cannot be reached. To address these issues, in this section, for the multi-AR case of multihoming in nested mobile networks, the algorithms for optimal path

① Swing responses: negative or positive reactions, alternately.

selection and access failure healing based on AR identity authentication and behavior evaluation, path availability evaluation, and fast handover are proposed.

### 3.1 Optimal Path

In multihomed and nested mobile networks, MRs might receive RAs from some routers, including the MR of another mobile network or the FR of the Internet infrastructure. Here, a new path information options (PIO) to carry path-evaluation parameters and also TLAR prefix is extended to RA. Through the parameters in PIO of RAs and related metrics, the on-path nodes and then the path are evaluated. After that, AR is selected for every MNN or MR, and the optimal path based on AR load balance in mobile networks is built and maintained. Also, this solution can be extended easily to realize comprehensive load balance by selecting optimal MNP for MNNs, optimal HA for MRs and optimal MR for HAs<sup>[23]</sup>.

Different from existing solutions, ours has the following characteristics: hybrid identity authentication based on SA transfer or home AAA server; mutual authentication and behavior evaluations between ARs; low-trust-triggered home AAA re-authentication; TLAR prefix based CoA generation; dynamic path construction scheme based on MR selection for MNNs and AR selection for MRs. The algorithm in detail is shown as follows.

#### (1) Dynamic evaluation

ARs attain neighbors' trust values through dynamic evaluation in the way described in Section 2.3; ARs obtain neighbor's availability values by evaluating the capability of the paths from the ARs to the Internet through their RA parameters, which will be depicted in Section 3.2.

#### (2) Evidence collection

① MRs or MNNs receive RAs that are generated and broadcasted by TLAR at a certain interval or by request, and then updated and forwarded by the intermediate ARs.

② MRs receive the trust values and availability values of the ARs nearby from the PAR.

#### (3) Authentication and re-authentication

① If the RA received is from the AR whose information (i. e. trust value) has existed, the MR and AR will authenticate each other with the help of PAR in the same way pictured in Section 2.2, where ARs' mutual authentication is carried out with the help AAA<sub>m</sub>.

② Otherwise, PAR does not have SA with the AR neither, so MR has to turn to the AAA server

of home domain.

③ The re-authentication based on AAA infrastructure will run at a flexible interval or will be triggered when the trust value of AR is lower than the threshold.

#### (4) Path evaluation and selection

① MR admits the availability value and trust value of the AR according to its PAR's trust value, if the authentication is realized with the help of PAR.

② Otherwise, trust value and the availability value of the AR will be evaluated in the way described in Section 2.3 and Section 3.2 respectively.

③ According to the trust values and availability values calculated, the best AR for current MR will be selected, and when every MR has selected its AR, the optimal path to the Internet is created.

#### (5) CoA configuration and route update

① If the selected AR and the previously-selected AR are under the same TLAR, then the CoA configuration will be omitted.

② Otherwise, CoA of MR will be configured with the prefix of TLAR carried by PIO of RA.

③ MR sends the ICMPv6-Echo Reply Message to correspondent TLAR, building routes from the TLAR and on-path nodes towards the MR.

#### (6) MNN-CN communication

① If the MR's CoA is reconfigured, ordinary binding of NBSP will be triggered by sending binding update to HA, binding the MR HoA and the MNPs in charge to its new CoA.

② MR updates the availability information in the selected AR's RA, and broadcasts it to its MNNs, and every MNN will evaluate the MRs of current mobile network and choose the best one to send packets.

③ MR sends the packets from MNNs to CN directly if MR and CN have authenticated each other and the MNNs' addresses are bound to the MRs' CoAs at the CN; or through the MR-HA tunnel to protect location privacy.

Under security guarantee, optimal path selection enhances AR mesh with the load balance by selecting the strongest AR in a real-time way. Hence, in terms of ARs' local policy like high-bandwidth first or low-delay first and so on, benefits of multihoming in providing more powerful and more adaptive performance are achieved.

### 3.2 Path Availability Evaluation

To evaluate the path availability for each selection, AR metrics for MRs or MNNs based on PIO parameters are established in this section.

Availability evaluation is the extensions of behavior evaluation, including the best AR evaluation for MR and the best MR evaluation for MNN.

There are three steps to evaluate the path availability for a MR:

(1) Get it from PAR

If a MR has received the availability value of an AR from its PAR, then

$$A_{AR \rightarrow MR}^{vai} = A_{AR \rightarrow PAR}^{vai} \times Trust_{MR \rightarrow PAR} \quad (3)$$

Where,  $A_{A \rightarrow C}^{vai}$  means the availability value of A for C.

(2) Calculate it based on PIO parameters and trust value

If the AR is only authenticated without being selected, MR evaluates the AR behavior and calculates the  $trust_{MR \rightarrow AR}$  by Formula (2) while computing the availability value of the path from the AR to the Internet according to the PIO parameters.

Since load balance among multi-MR or multi-path is provided in terms of not only throughput and path delay, but workable link or stable topology, we define the best path as the one whose expected lifetime of MR-FR association is the longest, whose available throughput is the highest, whose transmission delay is the lowest. Thus, to select the best AR for MR, the availability value of the related path from the candidate AR to the Internet will be computed through three parameters plus one subjective preference and their corresponding weights, as shown below:

$$A_{AR \rightarrow MR}^{vai} = \left( x_0 \times \frac{1}{D} \sum_{d=0}^{D-1} P_{AR,d} + \sum_{i=1}^3 x_i \times V_i \right) \times Trust_{MR \rightarrow AR} \quad (4)$$

Where,  $P_{AR,d}$  represents the personal preference of on-path AR with  $d$  as its nested depth for its lower AR, and  $D$  is the nested depth of the candidate AR;  $V_1$  means the stable time of the path topology, which can be calculated according to the minimum interval after which a handover will happen to one of its upriver ARs,  $V_2$  means the path throughput, and  $V_3$  contains the information of the whole path delay.  $P_{AR}$  and  $V_1$  can be calculated, normalized and broadcasted by on-path MR easily through RA, while  $V_2$  and  $V_3$  will be computed as follows:

$$V_2^{(d)} = \min(V_2^{(d-1)}, a \times B_{1,d} \times F_{1,d} + b \times NC_{AR,d} \times RCM_{AR,d}) \quad (5)$$

$$V_3^{(d)} = \begin{cases} 1, & d=0 \\ c \times (V_3^{(d-1)} + V_{3,1,d})^{-1}, & 1 \leq d < D \end{cases} \quad (6)$$

Where,  $V_2^{(d)}$  and  $V_3^{(d)}$  denote the throughput and delay from the current node, through the candidate

AR with  $d$  as its nested depth, to the Internet respectively;  $B_{1,d}$  means the link bandwidth to the candidate AR;  $F_1$  means the free time proportion of the link;  $NC_{AR}$  means the number of connections that the candidate AR can provide;  $RCM_{AR}$  represents the free rate of CPU and memory of the candidate AR;  $V_{3,1,d}$  presents the link delay from current node to the candidate AR with  $d$  as its nested depth, while  $a, b, c$  play the role of normalization.

Through Formula (4), (5) and (6), the availability of every path to the Internet can be evaluated and the optimal path can be selected. To get the parameters requested, options such as  $NC_{AR}$  and  $RCM_{AR}$  will be appended to PIO. During the propagation of the RA down the AR Mesh, some parameters including Path ID, Sequence, and prefix of TLAR etc., are filled in by TLAR and do not change. The fields of the RA updated at each hop include AR Preference, Nested Depth, Path Digest, Stable Time, Path Bandwidth, Path Free Medium Time, Affordable Connections, and Path Delay etc.

(3) Revise it after being selected

If an AR or the related path is selected, the path availability value will be revised according to the past experience. The iterative process of the value revision is shown in Formula (7).

$$A_{AR \rightarrow MR}^{(t)} = \left( x_0 \times \frac{1}{D} \sum_{d=0}^{D-1} P_{AR,d} + \sum_{i=1}^3 x_i \times V_i^{(t)} \times \frac{V_i^{(t-1)}}{V_i^{(t-1)}} \right) \quad (7)$$

Where,  $t$  presents the sequence of iterative calculation;  $P_{AR}$ ,  $V_1$ ,  $V_2$  will be obtained as before, and  $V_3$  will be revised as Formula (8).

$$V_3^{(t)} = c \times (T_{RA}^{(t)} - T_{RA}^{(t-1)} - O_{RA}^{(t)})^{-1} \quad (8)$$

Where,  $T^{(t)}$  is the  $(t)$  th timestamp of the RA message from the TLAR and  $O^{(t)}$  is the offset between the  $t$ -th RA message and the  $(t-1)$ -th RA message.

Formula (7) and (8) help to modify the path availability when evaluating the path that has been selected for the moment, and otherwise, Formula (1), (2) and (3) will give a hand.

MNNs obtain the availability values of every path in the same way MRs do, except setting the trust threshold  $\alpha=1$ , since MRs take the factor of ARs' trust values into account, while MNNs will trust their MRs at discretion.

### 3.3 Recovery of Access Failure

Optimal path selection neglects the urgency when access failure happens suddenly. The authentication process when MRs never know the AR before and the binding procedure when the MR

CoA is reconfigured will introduce the unbearable delay, which may result in session or service interruption since handover cannot be finished in time. So, here a handover algorithm based on trust transfer and/or AR/MR-HA tunnel and reverse routing header (RRH) borrowing is proposed to heal the unexpected access failure<sup>[20]</sup>. The algorithm is described as below.

#### (1) AR discovery

If the MR loses its connection to Internet all of a sudden, it triggers an Internet-available AR discovery process.

#### (2) Authentication process

Instead of sending the authentication request to AAA server of home domain as in Section 2.2, MR sends this message to all ARs that have been authenticated to authenticate the ARs giving replies. If the AR to be authenticated does not have SA with all these ARs, they will also send the request to their own authenticated ARs to authenticate the ARs unknown to current MR, until the recursive process ends with the ARs that give replies authenticated or beyond the time given.

#### (3) Handover

The AR that be authenticated first will be selected. If the AR is under the same TLAR of the MR, MR will forward the packets to the AR selected directly, and then the routing to the MR will be updated at the on-path nodes; otherwise, the selected AR encapsulates the packet received from the MR and then sends it to the destination through its own AR/MR-HA tunnel. Here, IPv6 Reverse Routing Header (RRH) is borrowed to record the CoA of the selected AR to realize reverse routing to the current MR.

After handover successfully, the MR will return to the normal path selection procedure.

This algorithm also can practically accomplish the authentication process in floating AR mesh, where AAA infrastructure is unavailable due to the fact that authentication process can be completed with the help of local ARs.

## 4 Security Analysis

The AR mesh security for NEMO proposed in this paper will protect against the following major threats: replay attacks, tampering, masquerading and lying. In our solution, the AAA infrastructure based identity authentication is for the former three attacks, evidence based behavior evaluation and further path evaluation are for lying, and trust based context transfer for performance.

### 4.1 Identity Authentication

In this paper, we assume that, with AAA servers, NAS and their communication secured, an AAA infrastructure has been robustly established. Also, SA between every MR or FR/NAS and its AAA server in home network always exists.

Then, according to the authentication method in Section 2.2, any MR and its AR can establish their SA with mutual identity authentication fulfilled with the help of AAA infrastructure. Where, timestamp resists the replay attack;  $AAA_m$  helps to establish the SA between  $MR_n$  and  $AAA_i$ , and in the same way,  $AAA_i$  then helps to establish the SA between  $MR_n$  and  $AR_i$ , and then  $AR_i$  the SA between  $MR_n$  and  $MR_p$ . The confidentiality and integrity of SAs are protected by signatures and session keys;  $nonce_1$ ,  $nonce_5$ ,  $nonce_4$  make  $MR_n$  believe orderly that the  $SA_{MR_n-AAA_i}$ ,  $SA_{MR_n-FA_i}$ , and  $SA_{MR_n-MR_p}$  are legal; also,  $nonce_5$ ,  $nonce_4$ ,  $nonce_3$  orderly make  $AAA_i$ ,  $FR_i$  and  $MR_p$  believe that the  $SA_{MR_n-AAA_i}$ ,  $SA_{MR_n-FA_i}$ , and  $SA_{MR_n-MR_p}$  are legal.

**Definition 7**  $B$  is the SA Generator (SAG) of  $A$  and  $C$  when  $B$  helps to establish SA between  $A$  and  $C$ . Where,  $A$ ,  $B$ ,  $C$  are network entities, like routers or servers.

**Theorem 1** Transitivity of SA: SA between  $A$  and  $C$  can be established when both  $A$  and  $C$  have SA with the same network entity.

Theorem 1 can be easily proved through the triangular drawing, where two sides have been there. The problem is that, the SA is not a secret to SAG, which is not expected. Here, new SA will be regenerated according to nonce exchanged and the original SA to against such an issue. With the SA created, the mutual authentication against masquerading is carried out naturally. The transitivity of SA can be implemented in the way mentioned in Section 2.2.

Where there is a SA existing, where there is a fact that IPsec can be applied to protect the communication with confidentiality and integrity. Hence the tampering will be excluded.

### 4.2 Trust or Not

After identity authentication, whether to trust is left to behavior evaluation which is used in AR mesh to eliminate the negative influences of lying of legal users.

In this section, the effect of node behavior evaluation will be estimated. And further path evaluation will be analyzed in the next section with path selection.



Since  $MR_n$  has authenticated  $MR_p$ , evidences for behavior evaluation will be directly obtained by observing  $MR_p$ 's reaction to a certain action happened locally. Fig. 4 shows the evaluation result in the following situations: When the time of negative responses increases from 0 to 10 while trust threshold varies within 0 and 1; and then time of positive responses rises from 0 to 20; time of the two kinds of responses climbs alternatively, with fluctuating time from 0 to 10.

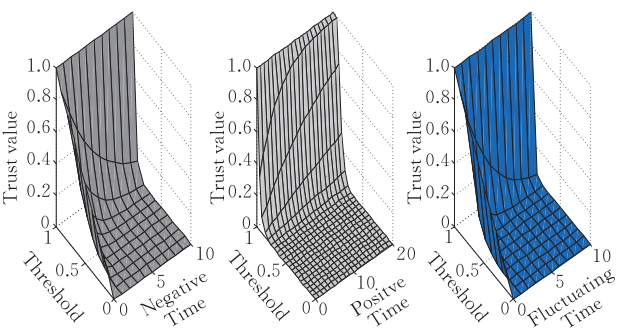


Fig. 4 Trust value surface

From Fig. 4, we can come to the conclusion

that trust value drops quickly when negative responses are observed, and drops more quickly with fluctuation while it ascends slowly when the positive reaction to the action takes place as what  $MR_n$  expected. Also,  $\alpha_i$  can be used to regulate the trust value; the larger trust threshold leads to the facts that trust value drops more slowly while rises more quickly.

5 Performance

In this section, after qualitative comparisons with the counterparts are made, throughput and delay from mobile networks to the Internet and handover delay of our secured AR mesh will be checked further by comparing with its counterparts by simulation. For the sake of convenience, the solutions in Ref. [10,17-18,20] are called NACA, NBAI, NACT, and RRH respectively, and that of this paper is called SARM.

SARM enhances NEMO security as well as performance with higher throughput or lower delay. Table 2 gives the overall qualitative comparisons of solutions mentioned before.

Table 2 Qualitative Comparisons

Criteria	Authentication		Nesting			Multihoming	
	AAA	Delay	Nesting	route optimized	data efficiency	path balance	handover delay
NACA	yes	high	yes	no	low	no	high
NBAI	yes	mid	no	no	low	no	mid
NACT	yes	low	no	no	low	no	mid
RRH	no	—	—	yes	mid	no	high
SARM	yes	low	yes	yes	high	yes	low

From the Table 2, we observe that NACA, NBAI and NACT support AAA, where AAA in NACA introduces high delay while that in NBAI or NACT does not work in nested environment. Meanwhile, NBAI has to carry out authentication through AAA server in home network and NACT is only favored in a closed environment. What's more, all these solutions overlook the complex situations of NEMO; do not eliminate great nesting tunnel overhead by providing route optimization and increasing data efficiency; have no balance among ARs and drop handover delay through multi-AR. Although RRH may eliminate the tunnel-in-tunnel overhead caused by nesting, more processing is needed at HA. Furthermore, security and merits resulting from multihoming are not achieved in RRH. Our solution takes all these problems into account, and gives the satisfactory results: (1) providing AAA authentication in nested mobile network while the delay introduced by AAA is resolved by SA transfer; (2) simplifying the route

and wiping off tunnel overhead in nested environment; (3) gaining potential performance (i.e. more throughput and lower delay through path balance, lower handover delay by turning to another AR and so on) provided by multihoming.

5.1 Throughput and Packet Delay

The throughput and packet delay is of importance to the mobile networks. Here, we compare our solution with NACA on throughput and packet delay from the mobile network with a nested depth of 3 to the Internet in a fixed AR mesh, with undependable wireless link and dynamic topology; the numbers of authenticated ARs for the on-path MR to select are random within 1 and 10; the trust values of these ARs are all random within 0.2 and 0.8; each link has a random bandwidth within 10 Mbps and has random propagation delay within 15 ms and with 5 ms discrepancy to the last one; for convenience,  $x_0 = x_1 = 0$  in path availability evaluation, and other parameters are listed in figures below (corresponding weight is regulated according

to the item that will be checked). We define  $T_{mi}$  and  $D_{mi}$  as the throughput and delay with fully-loaded data rate between MN and the Internet respectively and between one MNN and TLAR. Assuming that in the mobile network the number of MR increases from 1 to 10, and then after being measured 10 times the mathematical expectations of  $T_{mi}$  and  $D_{mi}$  are pictured in Fig. 5.

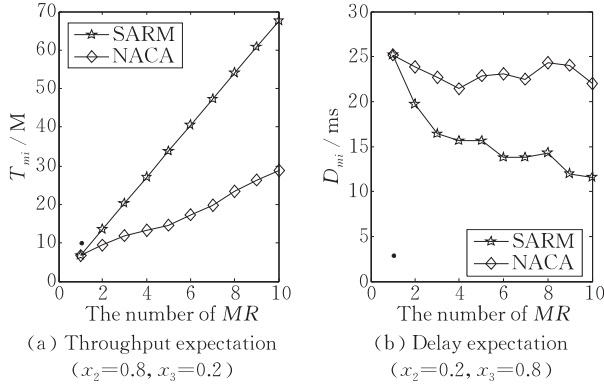


Fig. 5 Throughput and Delay

It can be seen from the Fig. 5 (a) that with the AR or MR load balance, the curve of the throughput from the mobile network to the Internet is improved remarkably with deepening of the curve gap. Fig. 5 (b) shows the delay curve of packet transmission from a MNN to a TLAR when the number of MRs increases. Evidently, compared with NACA, the latency is reduced significantly, and also more stable.

## 5.2 Handover Delay

As an important requirement to achieve seamless global roaming, small handover delay can significantly deduce packet loss rate and heal the access failure problem. But the fact is handover delay is a headache always for real-time applications in mobile networks. We compare our solution with NBAI and NACT when handover happens between ARs: (1) under the same TLAR; (2) from different TLARs of the same AAA domain; (3) from different AAA domain. Here, we define the handover delay as the period from when MR loses the link to its PAR to when MR has an authenticated AR that it can turn to.

NBAI integrates AAA messages and binding information of MIPv6, which reduces the time cost caused by the fact that authentication and binding procedure go one after another. While NACT proposes AAA context transfer based authentication to avoid the signal trip to home network every time mobile nodes access a foreign AR. However, visiting home network is necessary either for authenti-

cation in NBAI solution or for CoA binding in both solutions when inter-TLAR handover occurs.

We assume that the mutual authentication of nested ARs is extended in NBAI and NACT in the same way we do, and that a MR with  $D$  as its nested depth is visiting a foreign network under the TLAR whose AAA trip to the MR's home network experiences  $I$  domains, then we give the handover delay when the MR handovers in the following situations.

### (1) Inter-AR Under the same TLAR

$$D_{NBAI}^{ST} = 2 \left( \sum_{d=1}^D (D_{wl}^d + D_{ARP}^d) + \sum_{i=1}^I (D_{AAAP}^i + D_{idl}^i) + D_l \right) + 5D_{AP} \quad (9)$$

$$D_{NACT}^{ST} = \sum_{d=1}^D (z_d \cdot 4 \left( \sum_{n=1}^{D-d} (D_{wl}^n + D_{ARP}^n) + D_{AP} \right)), \quad \sum_{d=1}^D z_d = 1 \quad (10)$$

$$D_{SARM}^{ST} = y_1 \cdot \sum_{d=1}^D (D_{wl}^d + D_{ARP}^d) + y_2 \cdot D_{NACT}^{ST}, \quad y_1 + y_2 = 1 \quad (11)$$

### (2) Inter-AR under different TLARs of the same AAA domain

$$D_{NBAI}^{SD} = D_{NBAI}^{ST} + 2(D_l + D_{AAAP}) + D_{HAP} \quad (12)$$

$$D_{NACT}^{SD} = D_{NACT}^{ST} + \sum_{d=1}^D (D_{wl}^d + D_{ARP}^d + D_{TRHA}^d + D_{HAP}^d) \quad (13)$$

$$D_{SARM}^{SD} = D_{SARM}^{ST} + 2(D_{wl} + D_{ARP}) \quad (14)$$

### (3) Inter-AR of different domains

$$D_{NBAI}^{ID} = D_{NBAI}^{SD} \quad (15)$$

$$D_{NACT}^{ID} = D_{NACT}^{SD} + 2(D_{AAAP} + D_{idl}) + D_{AP} \quad (16)$$

$$D_{SARM}^{ID} = D_{SARM}^{SD} + 2y_2 \times ((D_{AAAP} + D_{idl}) + D_{AP}) \quad (17)$$

Where,  $d$  denotes the level of nesting and  $i$  is the domain id;  $D_{wl}$ ,  $D_l$  and  $D_{idl}$  denotes the delay of wireless link in mobile network, that of wired link in the same domain, and that of path between AAA servers of neighboring domains;  $D_{ARP}$ ,  $D_{HAP}$  and  $D_{AAAP}$  are the processing delays of AR, HA and AAA server respectively;  $D_{AP}$  means the processing delay for authentication;  $D_{TRHA}$  denotes the delay between HAs of on-path MRs or TLAR and these HAs;  $y_1$  and  $y_2$  mean the probability of MR handover for MNNs and that of AR handover for MRs, and  $z_d$  means the probability that a trusted AR with  $d$  as its nested depth helps to complete the authentication finally.

To analyze the performance differences among these solutions in detail, we give the concrete parameters as follows<sup>[24]</sup>:  $D_{wl} = D_{idl} = 4ms$ ,  $D_l = 2ms$ ;  $D_{ARP} = D_{HAP} = D_{AAAP} = 10ms$  if packet encapsulation

should be processed, else  $D_{ARP} = D_{HAP} = D_{AAAP} = 5\text{ms}$ ;  $D_{AP} = 5\text{ms}$ . In addition, since the hops between HAs of different MRs from different domain, between TLAR and these HAs, and between AAA server of foreign networks and that in home network are unpredictable,  $D_{TRHA}$  is assumed to be random, within 4 and 100ms, and  $I$  to be random within 10. Fig. 6 shows the results of handover delay according to the degree of nesting.

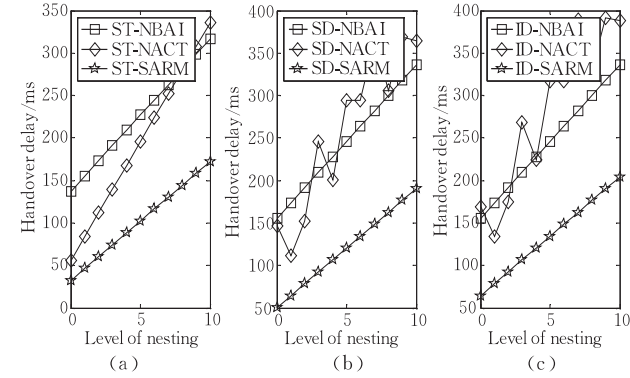


Fig. 6 Handover delay ( $y_1 = y_2 = 0.5$ ,  $z_d = 1/D$ )

From Fig. 6, it can be seen that with the increasing of the nested depth of MR, the gaps between other solutions and ours enlarge in all situations. And compared with the other two solutions, ours significantly reduces handover delay, which provides a better performance in handover for links recovery in multihomed and nested mobile network.

## 6 Conclusion

In order to address the performance bottleneck and related security issues in nested and multihomed mobile network, we present an AR mesh to promote the whole performance of mobile networks through balance and fast handover among multi-AR in a secured way. In the balance algorithm, traditional AAA identity authentication is replaced by the hybrid method combining direct SA transfer, traditional authentication, behavior and path availability evaluation, and optimal AR and path selection. While in the handover algorithm, original AAA scheme is replaced completely by the recursive SA transfer, to heal access failure by saving the precious time in handover. In AR mesh, periodical or policy-triggered traditional AAA authentication guarantees the identity authenticity further, and behavior and path availability evaluation determine the high reliability in entity behavior and path performance. Analysis indicates that since authentication is executed as locally as possible, and the most suitable AR and path is selected

with lying excluded, compared with the counterparts, our solution enhances NEMO with powerful performance, like higher throughput and lower communication delay and handover delay etc.

In addition, though our solution is for fixed AR mesh, it can be easily modified to support floating AR mesh. In the future, we are going to implement the prototype model with more detailed simulations in practical mobile environment to validate the analytical results.

## References

- [1] Lin Chung, Lei Lei. Research on next generation Internet Architecture. Chinese Journal of Computers, 2007, 30(5): 693-711(in Chinese)  
(林闯, 雷蕾. 下一代互联网体系结构研究. 计算机学报, 2007, 30(5): 693-711)
- [2] Ernst T, Lach H. Network mobility support terminology. RFC 4885, IETF, 2007
- [3] Devarapalli V, Wakikawa R, Petrescu A, Thubert P. Network mobility (NEMO) basic support protocol. RFC 3963, IETF, 2005
- [4] Tian Ye, Zhang Yu-Jun, Zhang Han-Wen, Li Zhong-Cheng. Identity-based hierarchical access authentication in mobile IPv6 network. Chinese Journal of Computers, 2007, 30(6): 905-915(in Chinese)  
(田野, 张玉军, 张翰文, 李忠诚. 移动 IPv6 网络基于身份的层次化接入认证机制. 计算机学报, 2007, 30(6): 905-915)
- [5] Jung S, Zhao F, Wu S F, Kim H. Threat analysis on network mobility (NEMO)//Proceedings of the ICICS. Lecture Notes in Computer Science. Malaga, Spain, 2004: 331-342
- [6] Kim W T, Jang J G, Park J M, Park Y J. Fault tolerant mechanism in dynamic multi-homed IPv6 mobile networks//Proceedings of the ACM/IEEE International Conference on Multimedia and Ubiquitous Engineering (MUE). Seoul, Korea, 2007: 401-406
- [7] Phang SY, Lee H, Lim H. A secure deployment framework of NEMO with firewall traversal and AAA server//Proceedings of the IEEE International Conference on Convergence Information Technology (ICCIT). Gyeongju, Korea, 2007: 352-357
- [8] Fathi H, Shin S, Kobara K, Chakraborty S S, Imai H, Prasad R. LR-AKE-based AAA for network mobility (NEMO) over wireless links. IEEE Journal on Selected Areas in Communication, 2006, 24(9): 1725-1737
- [9] Perera E, Sivaraman V, Seneviratne A. Survey on network mobility support. ACM Mobile Computing and Communications Review, 2004, 8(2): 7-19
- [10] Zrelli S, Ernst T, Bournell J, Valadon G, Binet D. Access control architecture for nested mobile environments in IPv6//Proceedings of the Conference on Security and Network Architecture (SAR). Batz sur Mer, France, 2005: 115-126
- [11] Ernst T, Montavont N, Wakikawa R, Paik E. Motivations and scenarios for using multiple interfaces and global addresses. Internet draft, IETF, 2007
- [12] Faccin S M, Le F, Perkins C E, Patil B, Dupont F, Laurent-Maknavicius M, Bournelle J. Mobile IPv6 authentication, authorization and accounting requirements. Internet draft, IETF, 2004
- [13] Li Xiao-Yong, Gui Xiao-Lin. Research on dynamic trust model for large scale distributed environment. Journal of

- Software, 2007, 18(6): 1510-1521 (in Chinese)  
(李小勇, 桂小林. 大规模分布式环境下动态信任模型研究. 软件学报, 2007, 18(6): 1510-1521)
- [14] Yan Z. A conceptual architecture of a trusted mobile environment//Proceedings of the IEEE International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU). Lyon, France, 2006: 75-81
- [15] Allard F, Bonnin J. An application of the context transfer protocol: IPsec in a IPv6 mobility environment. International Journal of Communication Networks and Distributed Systems, 2008, 1(1): 110-126
- [16] Li Jun. Research on handover performance of MIPv6 with AAA [Ph. D. dissertation]. Institute of Computing Technology, Chinese Academy of Sciences, Beijing, 2006 (in Chinese)  
(李军. 支持 AAA 的移动 IPv6 网络切换性能研究 [博士学位论文]. 中国科学院计算技术研究所, 北京, 2006)
- [17] Ahn Y, Lee T, Choo H, Lee S. DNA: Diameter NEMO applications based on binding update integration//Proceedings of the IEEE International Symposium on Parallel and Distributed Processing and Applications (ISPA). Sorrento, Italy, 2006: 1-10
- [18] Politis C, Chew K A, Akhtar N, Georgiades M. Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks. IEEE Wireless Communications, 2004, 11(4): 76-88
- [19] Huang C, Li J. A context transfer mechanism for IEEE 802.11r in the centralized wireless LAN architecture//Proceedings of the ACM/IEEE International Conference on Advanced Information Networking and Applications (AINA). Okinawa, Japan, 2008: 257-263
- [20] Thubert P, Molteni M. Ipv6 reverse routing header and its application to mobile networks. Internet Draft, IETF, 2007
- [21] Liu F, Cheng X, Chen D. Insider attacker detection in wireless sensor networks//Proceedings of the IEEE Conference on Computer Communications (INFOCOM). Anchorage, USA, 2007: 1937-1945
- [22] Yan Fen, Huang Hao, Yin Xin-Chun. A detection algorithm for multi-step attack based on CTPN. Chinese Journal of Computers, 2006, 29(8): 1383-1391 (in Chinese)  
(严芬, 黄皓, 殷新春. 基于 CTPN 的复合攻击检测方法研究. 计算机学报, 2006, 29(8): 1383-1391)
- [23] Huang Song-Hua, Wu Xiao-Bing, Lu Yin, Huang Hao, Chen Gui-Hai. SMART: A strengthened model of access router tree for multihoming in nested mobile network. Chinese Journal of Electronics, 2009, 18(1): 125-131
- [24] Kuo G, Ji K. Novel hierarchical network mobility support protocol with bidirectional end-to-end route optimization solution for nested mobile networks//Proceedings of the IEEE Global Communications Conference (GlobeCom). San Francisco, USA, 2006: 1-6



**HUANG Song-Hua**, born in 1979, Ph. D. candidate. His current research interests include network mobility and network security.

**SUN Yu-Xing**, born in 1977, Ph. D. candidate, lecturer. Her current research interests include wireless network

and network security.

**HUANG Hao**, born in 1957, professor, Ph. D. supervisor. He has long been engaged in the research of the information system security of computer, and the network and information security.

**CHEN Gui-Hai**, born in 1962, professor, Ph. D. supervisor, CCF senior member. His current research areas cover peer-to-peer computing, sensor networks and parallel computing.

## Background

With the prevalence of portable terminal and IP network, the potential demand for network mobility (NEMO) in military, public traffic, health care etc. is stimulated, and NEMO become a hot topic in the next generation Internet in recent years. NEMO support is concerned with managing the mobility of an entire network, viewed as a single unit that changes its point of attachment to the Internet and thus its reachability in the Internet topology. At present, poor performance, including low throughput, high packet delay, session interruption in handover etc. still stands in the way to NEMO's application in practice. Meanwhile, lack of appropriate security mechanism makes the situation even worse.

Due to multihoming and nesting, and the changeability of topology, the key factor that guarantees reliable and efficient running of NEMO is trust, including whether the access points can be trusted, in which degree they can be trusted, and vice versa. Thus, researches on how to establish and then evaluate the trust relationship dynamically and quickly in identity, availability, and performance have great significance.

This research work is mainly supported by the National High-Tech Research and Development Program of China (863) under grant No. 2007AA01Z409 named "Research on Distributed Trust Computing System". How to evaluate the terminal efficiently for the trusted network connection is one of the important parts of the 863 program. In the past year, the research groups have done a lot of related work including terminal reliability evaluation based on distributed network service, trust transfer between mobile devices or platforms based on trust chain or attestation and so on. In the future, a whole prototype of Trusted Operating System and Trusted Network Connect, combined with AAA infrastructure, will be implemented to test all the techniques proposed by the authors. Also the work is supported in part by the National Basic Research Program of China (973) under grant No. 2006CB303004, Jiangsu High-Tech Research Program of China (BG2007039), and the Natural Science Foundation of China (NSF) under grant Nos. 60303023, 60573131, 60673154, 60721002, 60825205.