doi:10.3969/j.issn.1000-436x.2012.z1.024

基于 AAA 认证的仓储移动网络安全关联转移方案

张永晖[1,2]，林漳希[3]，刘建华[1]，梁泉[1]

(1.福建工程学院 福建省汽车电子与电驱动技术重点实验室，福建 福州 350108;
2.中南大学 信息科学与工程学院，湖南 长沙 410083; 3.德克萨斯理工大学 商学院，Lubbock, TX 79409-2101 美国)

摘 要：提出基于 AAA 认证的移动网络(NEMO)安全预接入通告方案，由无线传感器定位信息预判切换，触发安全关联等上下文转移，并告知对端节点或对端服务器的数据处理中心，提前实现安全验证。用π演算建模以保证与现有 NEMO 安全机制兼容。理论分析知其减少的不当路由开销可达一半，模拟显示延时和资源占用大为降低。

关键词：仓储物联网；资源预留；安全关联转移；网络移动协议；预先地址簿告知；信任转移

中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2012)Z1-0186-06

Warehouse mobile access network security associate pre-anticipated notification scheme based on AAA authentication

ZHANG Yong-hui[1,2], LIN Zhang-xi[3], LIU Jian-hua[1], LIANG Quan[1]

(1. The Key Lab. for Automotive Electronics and Electric Drive of Fujian Prov. Fujian University of Tech., Fuzhou 350108, China;
2. School of Info. Science & Eng., Central-South University, Changsha 410083, China;
3. The Rawls College of Business Admin, Texas Tech University, TX 79409-2101, USA)

Abstract: A security pre-anticipated notification scheme was proposed for network mobility, based on AAA authentication. Pre-judged handover by wireless sensor network locating, security association information context was triggered to forward to data processing center in corresponding node router, in order to achieve trust authentication in advance. The scheme models on Pi calculus proved its compatibility with NEMO basic protocol. Analysis results display that costs become the half and simulations results show delay and resource occupied reduces significantly.

Key words: warehouse Internet of things; RSVP; security association transfer; (network mobility) NEMO; address book informing; trust transfer

1 引言

在仓储物联网络中，为满足出入库、盘点数据等实时性需求[1]，以及海量数据传输和苛刻的时限要求，必须使用资源预留协议。而目前移动 IPv6 方案有较大时延[2]，切换过程的 AAA 服务器尤其繁复，导致雪上加霜。同时 MRSVP、MIPRSVP 等 RSVP 技术，没有考虑传输过程中的数据加密[3]，如 Dynamic RSVP 缓冲数据分组通过隧道转发，更加剧安全认证阶段的延迟[4]。

收稿日期：2012-07-29

基金项目：福建省自然科学基金资助项目（2012J01243, 2012J01244）；福建省科技厅 K 类基金资助项目（JK2011035）；福建省工商发展资金企业技术创新专项省属基金资助项目（闽经贸计财[2011]704 号四（一）52）；福建工程学院基金资助项目（GY-Z10067, GY-Z11065）

Foundation Items: The Natural Science Foundation of Fujian Province (2012J01243, 2012J01244); Fujian Sci.& Tech. Department k-Project(JK2011035); Fujian Province Industrial and Commercial Development Fund on Enterprises Technical Innovation Provincial Project(Fujina Economic and Trade Planning Finance([2011]704. Four One 52); Fujian U. of Tech. Funds (GY-Z10067, GY-Z11065)

黄松华等[5]设计的最优路径选择和接入失效快速恢复算法，可降低安全关联转移的延时，但是算法基于固定 AAA 基础设施，也并非常见的默认信任机制，无法兼容。利用网关为中心控制 RSVP 服务[6]，会形成较多的 IP-in-IP 隧道，不利于安全验证。利用缓冲数据分组可平滑 RSVP 切换[7]，却也引入了更多的延迟，还加剧了隧道中保证 QoS 的困难。

解决之道有：一是升级网络[8]，直接支持大数据资源预留的实时要求，但是成本较高。二是改进现有互联网安全协议，如以集群、安全智能体和同步技术[9] 可加快延时，或学习节点移动模式[10]，以辅助路由和缓冲资源分配。以上两者对现有协议所作修改较大，而且没有考虑安全方面的影响。本文在第 2 种方式的基础上借助于无线传感器网络提供精确预测，将未来位置通知地址薄中所有可能的对端通信中心，称地址本通告方案(ABI, address-book inform)，从而提前传输安全机制的上下文关联。将安全机制分成切换前后，将部分 AAA 认证过程提前到切换前进行，并尽可能实现并行，从而缩短延迟。为保持与现有体系兼容，详细步骤以π演算语言进行描述，以保证方案内在的一致性及与 MIPv6 的兼容性。并将修改范围缩小到物联网支持网络内部。

2　基于地址簿通告的 AAA 切换时序优化

现有授权过程中，如增强 802.16e 安全机制[11]建立 AAA 需要 16 步；Diameter 移动 IPv6[12]需要 18 步，难以在移动环境下实施。借助 ABI 上下文信息，可以简化 AAA 过程，如图 1 所示。切换前过程仅有 3 步，切换后仅有 4 步，大大缩短了 AAA 步骤。

假定 AAA 服务器之间总是存在安全关联，MR 与家乡 AAA 服务器(AAAH)之间存在必要的授权密钥和外地授权所需的 Diffie-Hellman 密钥分配参数(KDP，key distribution parameters)。定义 C=E(K，M)表示明文 M 使用密钥 K 加密为密文 C。为简化起见，E($K_{A\text{-}B}$，M)表示为 E(M)，当且仅当 $K_{A\text{-}B}$ 是 A 和 B 之间随机产生的对称式加密密钥。

模型构成有:移动路由器(MR, mobile router)、家乡代理(HA, home agent)、接入路由器(PAR, previous access router)、下一接入路由器(NAR, new access router)、家乡认证机构(AAAH, authentication authorization accounting server of home)和外地认证机构(AAAF, authentication authorization accounting server of foreign)。方案采用 802.1x，客户端到认证

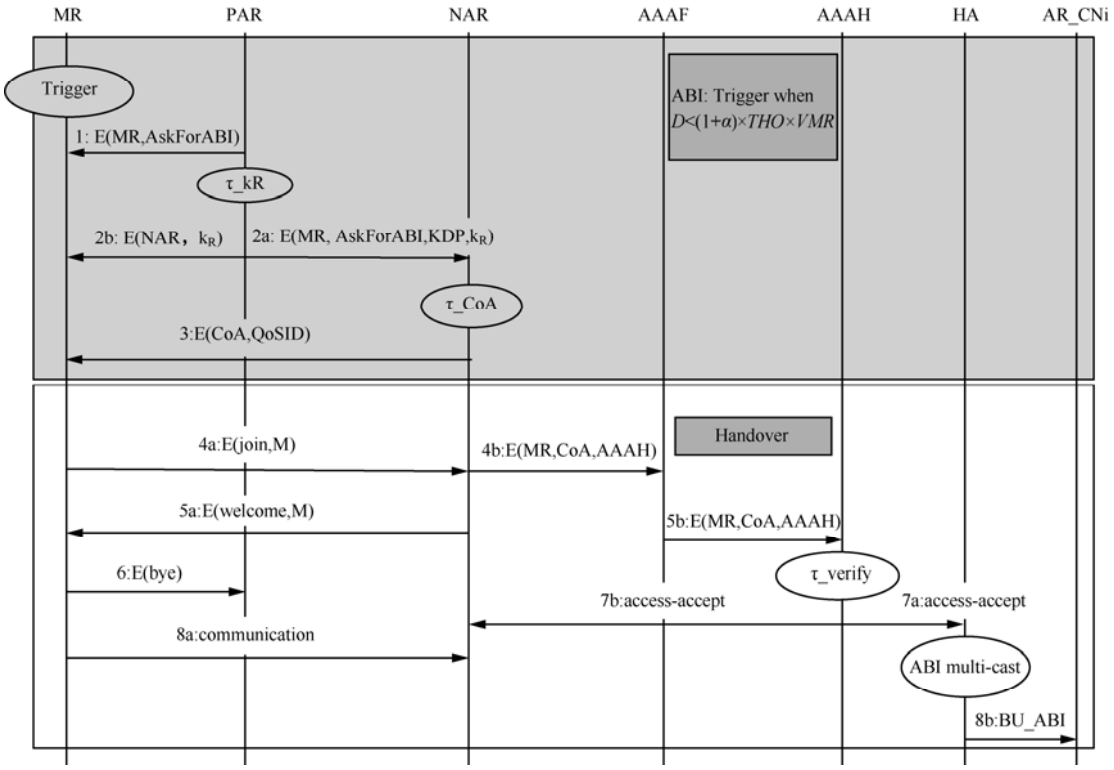


图 1　基于 ABI 的 AAA 切换优化时序

端采用 EAP over LAN 协议，认证端到认证服务器采用 EAP over RADIUS 协议。NAR 为中转 AAA 认证端，PAR 作用为 Kerberos 分发中心。MR 用作 client 客户端，PAR、NAR 作为 AAA 服务器的认证端。具体过程描述如下(a 与 b 表示同时进行)。

1) MR 向 PAR 传递消息 E(MR, AskForABI)。PAR 内部进程τ_k_R 生成随机密钥 k_R。

2) a.PAR→NAR:PAR 作为中间转发服务器转发 MR 的外地认证的密钥分配参数 KDP，作为 MR 和 NAR 未来通信的密钥，使用先前通过数字证书建立的和 NAR 共有的 session 密钥 k_{PAR_NAR} 加密转发请求，将 E(MR, AskForABI, KDP, k_R)转发到 NAR。b.PAR→MR: 同时以 k_{MR_NAR} 加密 E(NAR，k_R)并返回给 MR。NAR 内部进程τ_CoA 分配新的转交地址 CoA。

3) NAR→MR: E(CoA, QoSID)通知 MR 新的 CoA，使用 k_R 作为缺省的 $k_{MR\to NAR}$。QoSID 是可选参数。NAR 内部进程τ_RSVP 在局部地区建立新的 QoS 保证，本方案采用移动资源预留协议(MRSVP, mobile resource reservation protocol)的资源预留方式。当 MRSVP 路径建立请求接触到原有 RSVP 节点时，新的 QoS 保证路径建立成功。如果新的 QoS 保证路径建立不成功，则降低 QoS 等级之后再试图进行 MRSVP 路径建立。如果路径建立成功，返回新的 QoS 等级 ID。通知原有路径降低 QoS 等级，更新 QoSID。这一步也可以推迟到 AAA 验证成功之后由 AAA 发起。好处是不会为欠费的 MR 分配资源，坏处是切换延时增加。

预处理过程完毕，之后进行切换过程。

4) a. MR→NAR: E(join，M). MR 使用 k_R 作为缺省的 $k_{MR\to NAR}$ 请求加入 NAR。b. NAR→AAAF: 绑定更新过程 BU，也就是 E(MR，CoA，AAAH)这一步也可能与 5)同时进行。NAR 将 CoA 与 KDP 一起通过其当地 AAAF 服务器向 AAAH 转交，如果在本地，则直接向 AAAH 提交。其目的不是验证 AAA 的 KDP 验证信息(这点之前的 PAR 已经做过了)，而是检验计费条件是否满足，保证未欠费。这一步的优先级别很低，可以推迟到切换各阶段完成之后进行。从而优先保障 MR 的切换实时性和 QoS。

5) a. NAR→MR: 发送 E(welocome，M). NAR 批准 MR 加入。b. AAAF 向 AAAH 转交绑定更新信息 E(MR，CoA，AAAH)。

6) MR 通知 PAR 断开。AAAH 内部进程τ_verify 检验计费情况，只有 MR 的权限没到期或欠费，才进行下一步。

7)a 与 b 是由 AAAH 通知家乡代理 HA 和 NAR 允许接入(access-accept)。

8) a .MR→NAR：通信开始。

至于 b.HA→AR_n:BU_ABI。发送 ABI 绑定更新信息实际上可以与 2)~8)步同时进行，只要 PAR 或 NAR 有空闲。ABI 中规定，凡是与 MR 中节点通信的对端节点 CN 会记入地址簿，根据最新最多的原则进行筛选。一旦生成，这些 CN 的接入路由器 AR 就会转发给 MR 的 HA。HA 将之加入 MR 的 ABI 多播地址中，接到 BU，HA 就向 ABI 多播地址中各个 AR_n，以多播的形式通告 MR 新的 CoA，也就是 BU 信息。

由于切换预过程中进行了大部分步骤，这样同一时刻对于任意一点就减少了接入等待时间，从而缩短传输延迟。上下文信息不断发向所有，提请准备。接到相关信息，不管当前是否能维持通信或者是处于容迟网络所许可的中断，相关的 AAA 认证服务器都可以向下一组外地路由器提前发起托管传送，并开始重建 QoS 路径，不当避免大多数基于 IP-in-IP 隧道的资源预留，加速初始化进程，同时由于节点到达之前已经预先传输了 QoS 路径建立的指令，就部分解决切换过程中的 QoS 问题。

AAA 认证服务器在中心服务器上保存自己的地址簿，此后在更改地址簿名单时，自动通知家乡通信中心服务器更新地址簿，而最近联系的 AAA 认证服务器名单则定期更新。作为渡轮，当移动到外地网络时，必须向 AAA 认证服务器通知自己的关照地址，新的关照地址由家乡通信中心服务器通知地址簿上所有其他的对应家乡通信中心。每个 AAA 认证服务器 也会定时和家乡通信中心地址服务器联系，以获得最新的地址簿上关照地址信息。这类信息传递不需要实时传送，可以安排在网络比较空闲的时候传输，因此不会较多地影响网络的性能。

3 切换时序优化方案的π演算模型

新的安全方案最重要的是与现有 NEMO 方案兼容，否则就没有现实意义。

π演算能形式化描述结构不断变化地并发系统和交互系统，1991 年 Robin Milner 以此获得 ACM 图灵奖。现广泛用于各种通信协议、移动代理系统的建模与验证。π演算基本概念如下。P::= 0：空进

程；P|Q：并发(并行)；P+Q：选择；[x=y]P：匹配；τ.P：内部前缀；x<y>.P：输出前缀；X(y).P：输入前缀；*v*.P：限制；A(x1, x2,…, xn)：代理。

定义 m1 为 MR 的公有通道，m2’为 NAR 的公有通道，m2 为 MR 与 NAR 之间的私有通道，m3 为 PAR 与 NAR 的公有通道，m4 为 NAR 与 AAAF 的公有通道，m5 为 AAAF 与 AAAH 的公有通道，m6 为 AAAH 与 HA 公有通道。

MR 模型：MR(m, m1, m2, m2’)= ([Trigger= true]m1<E(MR, AskForABI)>.m1<E(NAR, k_R)>.

m2'<E(CoA, QoSID)>.(m2<E(join, M)>. m2 (E(welcome，M). m1<bye>)+MR(fail)

如满足触发条件，MR 通过信道 m1 发送自己的消息和 ABI 请求，等候从信道 m1 收到 PAR 发来的 NAR 消息和与 NAR 会话的随机密钥。从与 NAR 的公有信道 m2’收到 NAR 发来的转交地址及服务质量 ID 后，通过与 NAR 的私有通道发送加入请求，并附带删自己的信息，接着收到 NAR 批准 MR 加入的消息。于是 MR 发送中断消息给 PAR，否则返回失败消息。

PAR 模型：PAR(m1, m3)=m1(E(MR，AskForABI)). τ_k_R.(m1<E(NAR, k_R)>|

m3<E(MR, AskForABI, KDP, kR)>). m1(E(bye)) +PAR<fail>

当 PAR 通过信道 m1 收到 MR 的消息及 ABI 请求后，便生成随机密钥 k_R，于是通过信道 m1 发送 NAR 的相关信息，及其与 NAR 会话的随机密钥。接着 PAR 作为中间转发服务器转发 MR 的外地认证的密钥分配参数 KDP，作为 MR 和 NAR 未来通信的密钥，使用先前通过数字证书建立的和 NAR 共有的 session 密钥 k_{PAR_NAR} 加密转发请求，将 E(MR，AskForABI, KDP, k_R)传发到 NAR。否则返回失败消息。

NAR 模型：NAR(m2, m2’m3)=m3(E(MR，AskForABI, KDP, kR)).τ_CoA.(m2(E(join, M))|

m4< E(MR, CoA, AAAH)>).(m2< E(welcome，M)>|m4< E(MR, CoA, AAAH)>)+NAR<fail>

NAR 收到信道 m3 发送过来的消息后，于是内部分配新的转交地址。从信道 m2 收到请求加入消息的同时也向外部的 AAA 服务器发送 MR、CoA、及 AAAH 的绑定请求的相关信息。通过信道 m2 发送批准加入消息的同时也收到了 AAAF 发回来的绑定确认消息，否则失败。

AAAF 模型：AAAF(m4)=m4(E(MR, CoA, AAAH)) .m4< E(MR, CoA, AAAH)>+AAAF<fail>

收到 NAR 通过信道 m4 发来的绑定更新消息及返回的确认的消息。

AAAH 模型：AAAH(m5, m6)=m5(E(MR, CoA, AAAH)). τ_verify.m6<access-accept>+AAAH<fail>

从信道 m5 收到绑定更新时，通过信道 m6 通知 MR 的家乡代理准入，否则返回失败消息。

HA 模型：HA(m6, m7)=m6(access-accept). m7 <BU_ABI>+HA<fail>

当通过信道 m6 收到 MR 有权访问的消息时，通过信道 m7 发送 ABI 绑定更新消息。

ARn 模型：ARn(m7)=m7(BU_ABI)+AR<fail>

其通过信道 m7 收到 ABI 绑定更新消息。使用系统模型：System2≡MR(m, m1, m2, m2’)|PAR(m1, m3)|NAR(m2, m2', m3)|AAA(m4)|

AAAH(m5, m6)|HA(m6, m7)|ARn(m7)　　(1)

综合以上各组成部分，得到整个系统模型 System2。

一致性证明是输入系统模型，观察其在各种常见模式下的约简是否存在矛盾。使用 UppSala 大学开发的机器自动化验证工具 MWB (www.it.uu.Se/reSearch/group/mobility/mwb)，最终实现了 system2 的一致性证明。

弱模拟证明是观测系统外在表现，从而讨论不同协议之间交流的可能性。本文只讨论观察弱模拟，即对不可观察的活动序列进行抽象，只考虑通道处定义的接收或发送活动，仅在外部跟踪，其他活动都被视作内部活动。此时 2 个系统可以具有不同的内部结构和不同的内部行为，因此可以讨论 2 个系统的接口兼容。

取相应的 NEMO 方案，将其π演算模型表示为 System1[13]，设系统 A 和 B 的行为被形式化为进程 P_a，如果可以表示为 $\text{system2} \xrightarrow{a} \text{system1}$，则 system2 对于进程 P_a 可以弱模拟 system1 的功能。使用 MWB 可以验证各进程下弱模拟 system1 成立。因此，在单纯的 NEMO 环境中，ABI 模型也可以工作。

4　开销分析

4.1　路由开销分析

本节先比较 ABI 方案与 NEMO 基本支持方案（BSP）的效率。BSP 在通信初始化时，对于对端通信中心 CN 来说发起呼叫的开销为

$$C_{CN\_launch}=C_{CN\to HA}+C_{HA\to CN}+C_{CN\to MS} \quad (2)$$

C_{CN_launch}为对端通信中心发起 ABI 所经路径的开销。式(2)描述了对端通信中心向 HA 获得关照地址后再向 MS 呼叫的过程。如果采用 HA 直接将呼叫请求转交给 MS 的方案，则有

$$C_{CN\_launch}=C_{CN\to HA}+C_{HA\to MS}+C_{MS\to CN} \quad (3)$$

ABI 方案显著缩短了中转时间。有如下定理。

定理 1 发起呼叫的平均时间恒有

$$C_{CN\_launch\_ABI}<C_{CN\_launch}$$

证明 设任意两点 A，B 来回时间相等，即$C_{A\to B}=C_{A\to B}$。

对于式(2)的情况，$C_{CN\_launch}=2C_{CN\to HA}+C_{CN\to MS}$

为方便比较，ABI 采用 $_{CN\to HA}$ 往返的形式。根据 ABI 策略，有

$$C_{CN\_launch\_ABI}=\gamma C_{CN\to MS}+(1-\gamma)\,C_{CN\_launch}$$

于是 $C_{CN\_launch\_ABI}-C_{CN\_launch}=\gamma C_{CN\to MS}+(-\gamma)C_{CN\_launch}=-2\gamma C_{CN\to HA}$

对于式(3)的情况，ABI 采用 CN→HA→MS 的方式。在(1−γ)的概率下，先走直线距离，如果没有获取到 ABI 信息，则回转家乡通信中心获得信息，此时实际上全部三边都经过了。于是有 $C_{CN\_launch\_ABI}-C_{CN\_launch}=\gamma C_{CN\to MS}+(-\gamma)C_{CN\_launch}=-\gamma(C_{CN\to HA}+C_{HA\to MS})$

综合 2 种情况，有 $C_{CN\_launch\_ABI}-C_{CN\_launch}<0$ 即 $C_{CN\_launch\_ABI}<C_{CN\_launch}$。证毕。

如 ABI 方案维持对端通信中心的命中率为 95%，此时对端通信中心的开销是 $C_{CN\to MS}$，仅有 5%的概率是式(2)所描述的 C_{CN_launch}。于是发起呼叫的平均时间为

$$C_{CN\_launch\_ABI}=C_{CN\_launch}-2\times 95\%(C_{CN\to FR})$$

即一般会少走 1.9 倍对端通信中心→FR 路径($C_{CN\to FR}$)。对于 MS 或者 MR 在切换过程的分析与之类似。三角路由其任意两边υ与第三边γ之比的相对值在文献[14]已经计算出 E(υ/γ) =0.532 481 683 54，如γ=0.9 左右，即大约节省一半的开销。

4.2 ABI 方案的信令开销分析

渡轮中心的位置信息只需要在对端通信中心之间传递，无需扩散到整个骨干路由域上，ABI 信息并不进入路由表，而是根据家乡代理中节点数据库传送。设移动站 MS 到家乡通信中心的信令包含自身转交地址关照地址长度为 b_{CoA} 和家乡地址 b_{HA}，节点可能的最高速为 V_{max}，覆盖范围做最保守估计，不基于分层切换，每 cell 切换一次，cell 取最小覆盖范围 D_{min}，则必须发送 ABI 位置信息时间间隔 $t_{ABI}>D_{min}/V_{max}$，于是 ABI 信息所占通信量为 $B=(b_{CoA}+b_{HA}+b_{Other})/\ t_{ABI}<(b_{CoA}+b_{HA})\ V_{max}/D_{min}$。

ABI 的额外信令$(b_{CoA}+b_{HA}+b_{Other})$一般不大于 40B(320bit)，仓储物联网节点可能的最高速为动车(394km/h)，取 V_{max}=394km/h≈109.4m/s；Wi-Fi 的覆盖范围在 3~5km，WiMAX 最大在 30~50km；取 D_{min} =3km；则所占用的带宽为 B<11.68bit/s。选播发送数据分组$(b_{CoA}+b_{HA}+b_{Other})n$，$n$ 为对端数据中心个数，开销不大于 3.2kbit，只相当于一次传输。

对比常见的带宽，语音通信为 56kbit/s，压缩语音通信为 8~8.5kbit/s，为一般压缩语音通信的 0.001 374，即千分之一。GPRS 平均网速为：移动 57.6kbit/s，CDMA 为 156kbit/s，则为万分之零点七到万分之零点二。Wi-Fi 网络网速最低的 802.11b 的带宽是 11Mbit/s，为其百万分之一。由此可知，ABI 的信令开销较小，传送时还可以进行捎带处理，不必专门传输。可以忽略。

5 仿真结果及分析

取 DTNrg 在 dtnrg.org 提供的 DTN2 和 LTP 代码，植入 NS2，得到本次试验的平台。传感器共 64 个点，分 8 组，用星形连接到 8 个 sink 上，8 个 sink 以环形联入虚拟网络，虚拟 8 个渡轮为根据调度灵活运动，虚拟圆环直径 100km，沿途用 Wi-Fi 小区不完全覆盖，直径为 1km，站点数 k=20，40，80，160，320(完全覆盖)。渡轮速度 50km/h，逆时针运动。设 Wi-Fi 网络带宽 54Mbit/s，蜂窝网络带宽 3.84Mbit/s，各类业务的到达时间服从泊松分布，用户的到达相互独立，sink 的业务 t_p 精确到 0.1s。业务组合如下：从 0 到 4 类分别为 50%，15%，15%，18%，2%；时长服从负指数分布，均值 1/μ分别为 3 000s，100s，200s，100s，200s；业务量为 1kbit/s，2^2kbit/s，2^4kbit/s，2^6kbit/s，2^8kbit/s。每次实验延续时间 2 000s。资源预取，设命中率为 0.85。在无线传感器网络部署 NEMO 方案，采用 diameter 安全验证[12]进行对比实验。均重复 30 次，取平均值。其结果如表 1 和图 2 所示。

按文件的平均延迟 t_A，本方案整体优于 NEMO 方案，中间站点数 k=40、80、160(对应于覆盖率约在 0.125、0.25、0.5)时，本方案尤为突出。而在 k=320(对应站点全面普遍覆盖的情况

下)，因为传输速度较快而负载没饱和，2 种方案相差无几。在 k=20 时(对应覆盖率为 0.062，站点极少)，由于预先准备赢得时间相对总体传输时间的相对值较小，因此 2 种方案也相差不大。此外本方案标准偏差普遍偏高，这应该是由于本方案上下文如果预取成功则比 info 方案延迟小，如果预取不成功，则比 NEMO 方案要大，因此总体波动比较大。

表 1　　与 NEMO 对比实验结果

站点数 k	平均延迟 t_A (s/file)		对比偏差	相对标准偏差	
	ME	NEMO		ME	NEMO
320	2.56687	2.54418	0.88%	19.89%	17.04%
160	6.21035	7.79316	−25.49%	12.00%	13.17%
80	11.4478	15.6488	−36.70%	25.59%	18.32%
40	24.9654	28.676	−14.86%	36.02%	24.74%
20	52.6936	60.045	−13.95%	19.15%	16.01%

实验还探讨了方案的最小延时与资源预留集数 MSPEC 的关系。当最小延时 t_d 增加，MSPEC 的平均数也增加，如图 2 所示。当 t_d<0.3s 时，MSPEC 剧增，这是因为方案采用提前量进行 ABI 信息移交，增加了 MSPEC 的不确定性所致。在 t_d=1.1s 之后，该不确定性达到饱和，MSPEC 变化不大。由于最小延时 t_d 与平均延时 t_A 存在正线性相关关系，因此本方案有效地节省了资源预留所占用的资源。

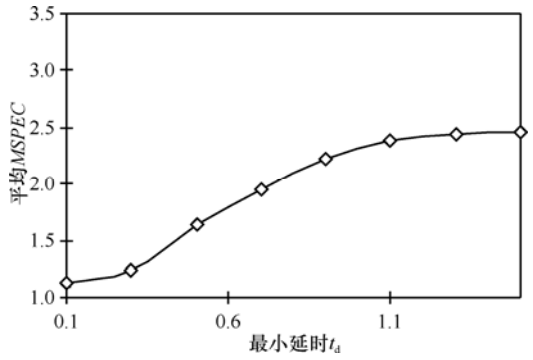


图 2　最小延时 t_d 对平均 MSPEC 数的影响

6　结束语

本文提出支持实时大数据量传输的移动网络安全预接入方案。通过将 AAA 安全认证和安全关联消息分段转移；从而明显降低了网络延迟，信令增加极小，也可用于实时大数据量传输的其他移动网络场景。方案使用π演算建模，能够保证与 MIPv6 的接入安全机制兼容。下一步工作是当众多节点竞争预接入方案的上下文转移服务时，设计效用函数，由其决定安全关联转移的先后顺序。

参考文献：

[1] LIU X, SUN Y. Information flow management of vendor-managed inventory system in automobile parts inbound logistics based on internet of things[J]. Journal of Software, 2011, 6(7): 1374-1380.

[2] MIRAZ G M, RUIZ I L, GÓMEZ-NIETO M. University of things: applications of near field communication technology in university environments[J]. Journal of E-working, 2009, 3(1): 52-64.

[3] MALEKIAN R, ABDULLAH A H, SAEED R A. A cross-layer scheme for resource reservation based on multi-protocol label switching over mobile IP version6[J]. International Journal of the Physical Sciences, 2011, 6(11): 2710-2717.

[4] XIE D L, WANG F H. A self-adjustment QoS architecture for wireless sensor networks[J]. The Journal of China Universities of Posts and Telecommunications. 2010, 17(32): 79-83.

[5] AYUB Q, RASHID S, ZAHID M S M. Optimization of epidemic router by new forwarding queue mode TSMF[J]. International Journal of Computer Applications IJCA, 2010, 7(11): 5-8.

[6] CHEN J L. A survey of trust management in WSNS, internet of things and future internet[J]. KSII Transactions on Internet and Information Systems (TIIS), 2012, 6(1): 5-23.

[7] ASGHAR J, HOOD I, LE Faucheur F. Preserving video quality in IPTV networks[J]. IEEE Transactions on Broadcasting. 2009, 22(12): 15-27.

[8] 周灵, 王建新. 无线多媒体传感器网络路由协议研究[J]. 电子学报. 2011,39 (1): 149-156
ZHOU L,WANG J X. Research on routing protocol in wireless multimedia sensor network[J] Acta Electronica Sinica, 2011, 39 (1): 149-156.

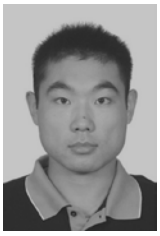
[9] LÓpez T S, BRINTRUP A, ISENBERG M A. *et al*. Resource management in the internet of things: clustering, synchronisation and software agents[A]. In: Architecting the Internet of Things [M]. Verlag New York Inc: Springer: 2011.

[10] MATRON M, CANTINAS M. Car: context-aware adaptive routing for delay tolerant mobile networks[J]. IEEE Trans. on Mobile Computing, 2009, 8(2): 246-260.

[11] JANG H J, HAN Y H, JEE J, *et al*. Mobile IPv6 Fast Handovers over IEEE 802.16 e Networks[S]. IEEE RFC5270. 2008.

[12] BOURNELLE J, GIARETTA G, NAKHJIRI M, *et al*. Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction[S]. IETF RFC 5778: 2010.1

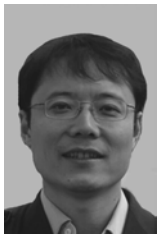
（下转第 200 页）



张菁（1987-），男，山东济南人，国防科学技术大学博士生，主要研究方向为系统软件、数据存储和云计算技术。

陈红（1987-），男，湖南益阳人，国防科学技术大学硕士生，主要研究方向为云环境中的资源管理和计费机制。

吴庆波（1969-），男，浙江宁波人，博士，国防科学技术大学研究员，主要研究方向为系统软件、高性能计算和嵌入式系统。



孔金珠（1974-），男，山西闻喜人，硕士，国防科学技术大学副研究员，主要研究方向为系统软件、虚拟化和高性能计算。

戴华东（1975-），男，湖北随州人，博士，国防科学技术大学研究员，主要研究方向为系统软件和高性能计算。

管刚（1982-），男，湖北蕲春人，硕士，腾讯研究院副总监，主要研究方向为面向公众服务的网络操作系统技术。

（上接第 191 页）

[13] ROSA-VELARDO F, MARROQUIN-ALONSO O, DE FRUTOS-ESCRIG D. Mobile synchronizing petri nets: a choreographic approach for coordination in ubiquitous systems[J]. Electronic Notes in Theoretical Computer Science, 2006, 150(1): 103-126.

[14] 张永晖. 基于用户行为的下一代移动互联网络若干关键问题的研究[D].长沙: 中南大学, 2010.
ZHANG Y H. Key Technologies Research of Next Generation Mobile Internet Based on User Behavior[D]. Changsha: Central- South U., 2010.

作者简介：

张永晖（1973-），男，湖南长沙人，博士，福建工程学院讲师，主要研究方向为移动互联网接入和容迟网络。

林漳希（1953-），男，福建漳州人，德克萨斯理工大学博士生导师，主要研究方向为 QoS 路由和网络安全。

刘建华（1967-），男，江西南昌人，博士，福建工程学院副教授，主要研究方向为路由和高性能算法。

梁泉（1972-），男，湖南洞口人，博士，福建工程学院副教授，主要研究方向为移动网络和机会网络。