开题报告

基于IPv6源地址验证的一种可信身份系统

周端奇　毕军　姚广

目录

1. 研究背景

- 传统的互联网缺乏广泛的可信基础
  - 缺乏身份认证机制，IP地址只是主机标识，而不是用户的身份标识
    - IP地址并不与用户真实社会身份对应
    - IP地址同时扮演主机标识和位置标识两个角色，位置改变会改变IP地址
  - 源地址缺乏可信性
    - 转发设备不检查源IP地址，无法保证源IP地址与发送者身份一致
    - 难以杜绝假冒攻击、重放攻击
  - 缺乏有效的身份验证回溯机制
    - IP地址按需分配，且可重用，无法查证攻击者
    - 目前各种认证系统独立运行，难以跨域回溯

1. 研究背景

- IP地址系统适合用作真实可信身份的载体
  - SAVA/uRPF等地址检查机制的存在，保证IP地址的基本可信
  - IP地址天然带有的主机标识含义与用户身份标识有一定的重叠，在不加入新层次的前提下，作为真实可信身份的载体成本最小。

2. 研究目的

- 建立真实可信身份通信系统，确保通信双方在具有真实可信身份的前提下完成通信。

- 满足三个设计原则：
  - 隐私性：用户的真实身份不会随意泄露。即在没有获得授权的情况下，无法通过报文确认报文发送者的真实身份
  - 可验证性：在获得授权的情况下，可以确认报文发送者的真实身份
  - 真实性：报文发送者难以伪造其身份，从而确保身份的真实性

3. 相关工作

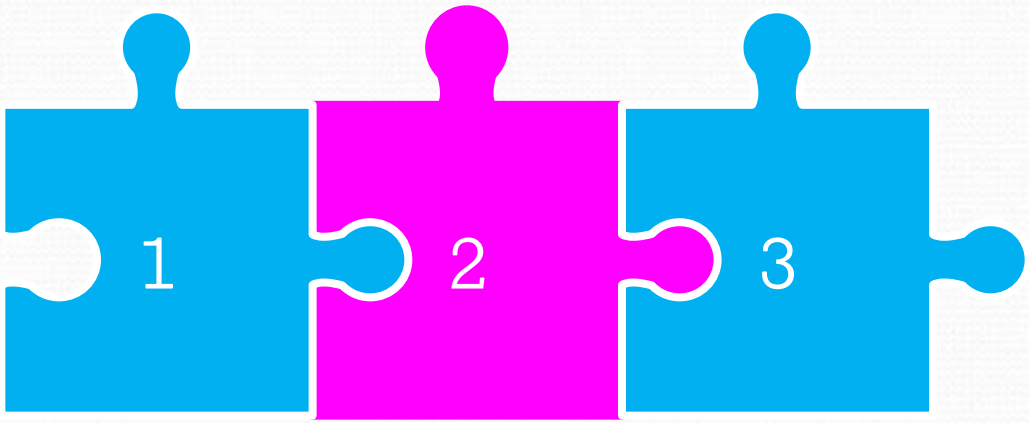
- 基于web认证的身份认证方案
  - 本地认证
  - 没有携带身份
    - 需要先获得IPv6地址再认证，IPv6地址不携带身份信息
  - 不支持跨域
    - 无法支持跨域的身份管理和溯源

4. 系统设计

真实可信身份系统设计

安全机制设计

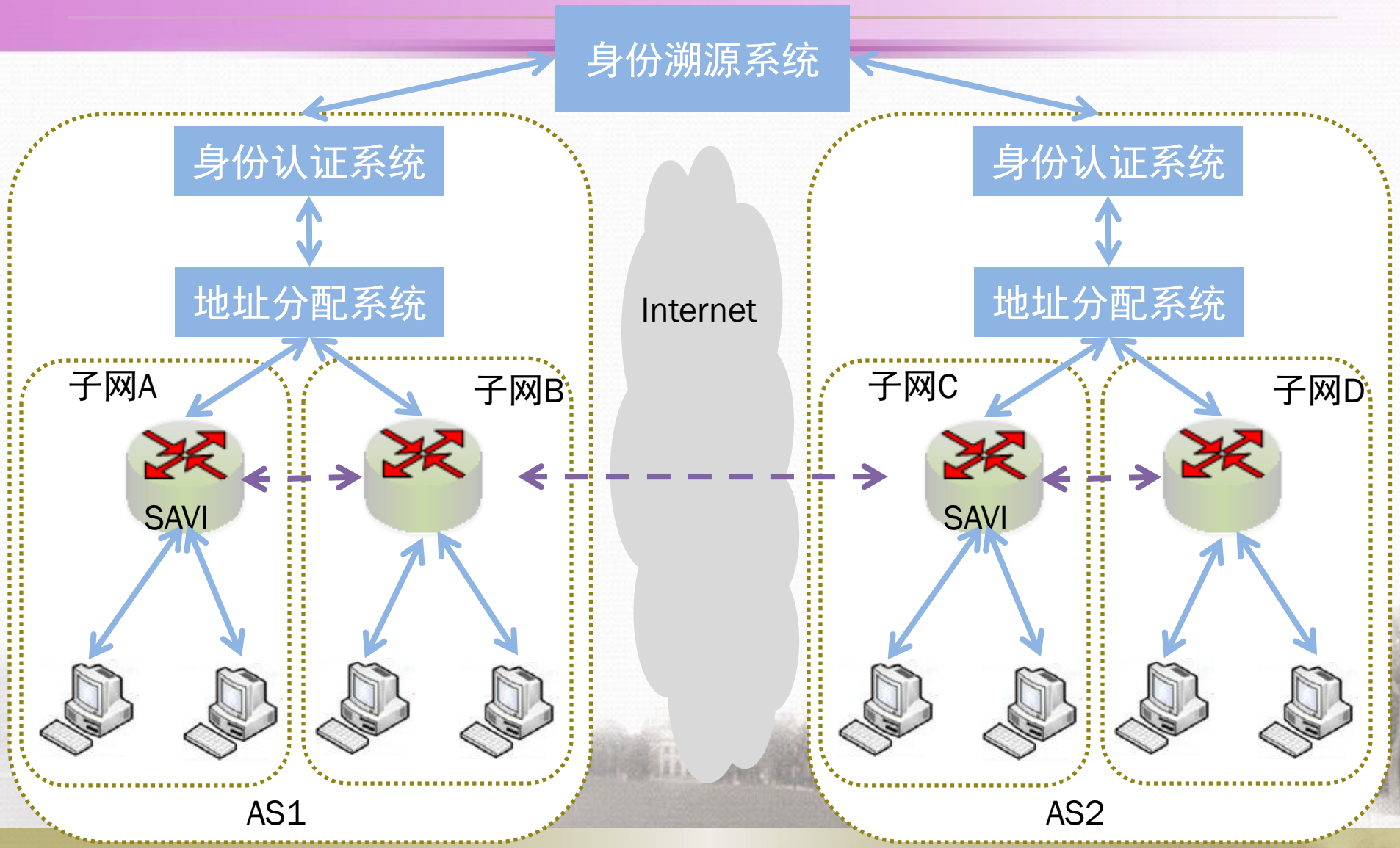
身份算法设计



4. 系统设计

- 名词定义：
  - NID(Network ID)：用户身份认证时的用户名；
  - EID(Encrypted ID)：使用加密算法对NID进行加密后的结果；
  - password：用户身份认证时的密码；
  - digest：加密后的密码；
  - GID(General ID)：IPv6地址的后64bit；

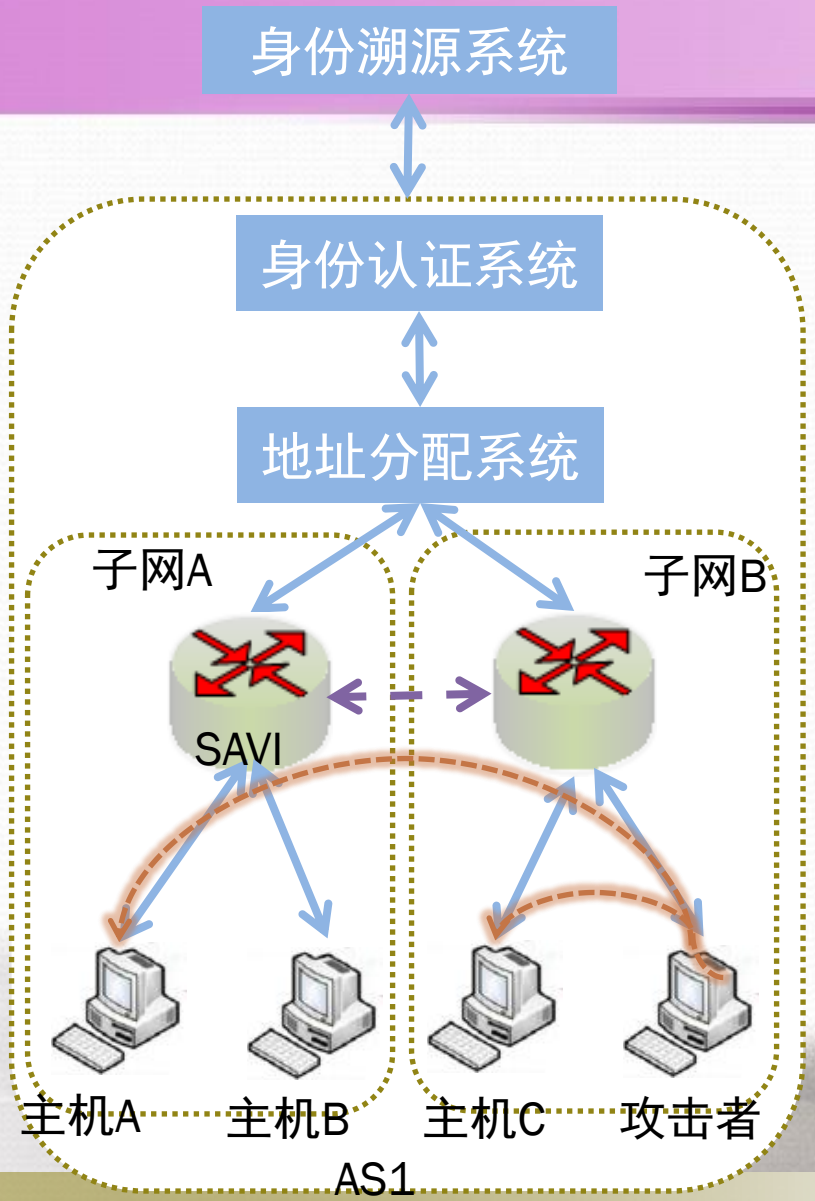
4. 系统设计：系统结构图


身份溯源系统
身份认证系统
地址分配系统
身份认证系统
地址分配系统
Internet
子网A
子网B
子网C
子网D
SAVI
SAVI
AS1
AS2

4. 系统设计：安全机制

- 安全机制设计主要是为了防假冒和防重放
- SAVI部署区：
  - SAVI有效地保证了源地址不可伪造，假冒报文和重放报文都会被SAVI过滤，从而防止了假冒攻击和重放攻击
- 域内源地址验证部署区（非SAVI部署区）：
  - 域内源地址验证部署区只能保证前缀粒度的源地址真实，可能存在假冒和重放攻击。

4. 系统设计：安全机制



- 不同子网：攻击者伪造主机A 地址
  - 由于子网前缀不同，攻击者的伪造报文会被SAVA系统过滤，攻击失效；
- 相同子网：攻击者伪造主机C地址
  - 攻击者只能在被伪造主机地址有效期内进行攻击，地址过期之后，攻击报文会被过滤系统过滤，无法继续实行攻击。

4. 系统设计：身份算法

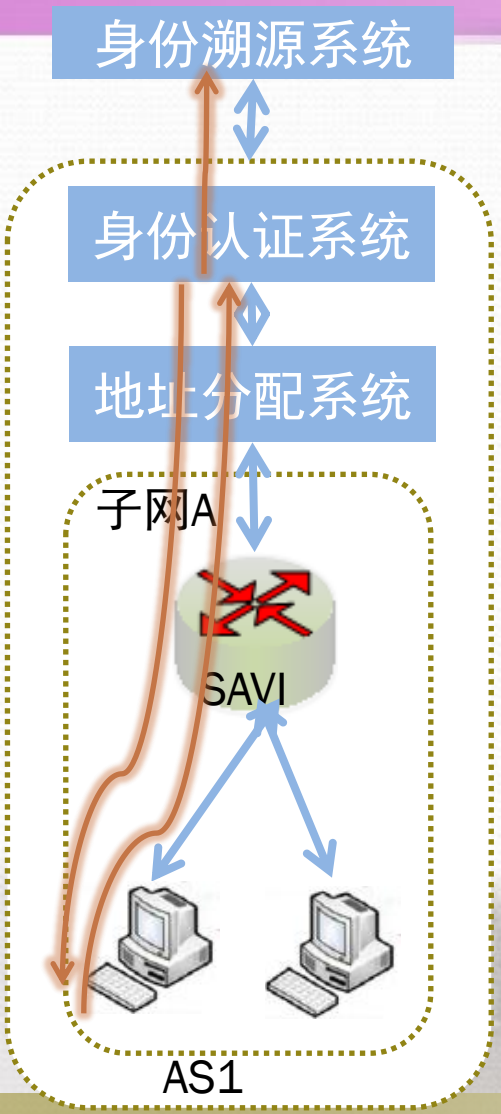
- 身份生成算法，将用户名NID加密为GID（64 bits），需要满足以下条件：
  - 隐私性：在没有密钥的情况下，难以通过GID解密获得NID；
  - 真实性：在没有密钥的情况下，可以验证GID的真实性；
  - 还原性：在有密钥的情况下，可以通过GID解密获得NID

- 算法：
  - 使用RSA-2048对NID进行加密，获得EID
  - 对EID使用MD5算法，获得GID

5. 系统实现

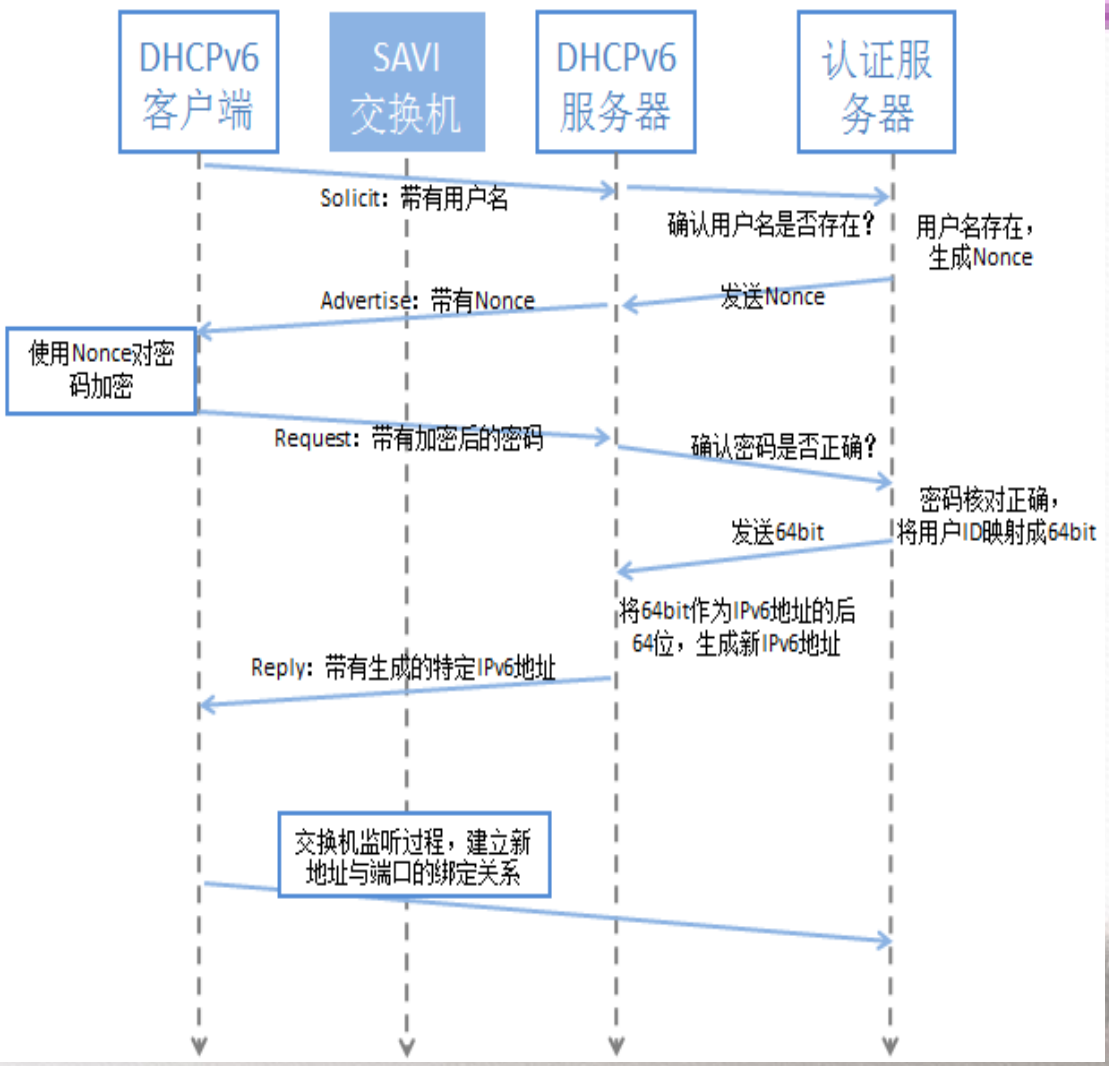
- 真实可信身份通信系统，包括：
  - 身份认证系统：对主机的身份进行认证，产生GID
  - 地址分配系统：根据GID，生成IPv6地址，分配给特定主机
  - 身份溯源系统：记录主机身份<NID, IPv6, time>
  - 报文过滤系统：双向过滤攻击报文

5. 系统实现：身份认证&地址分配



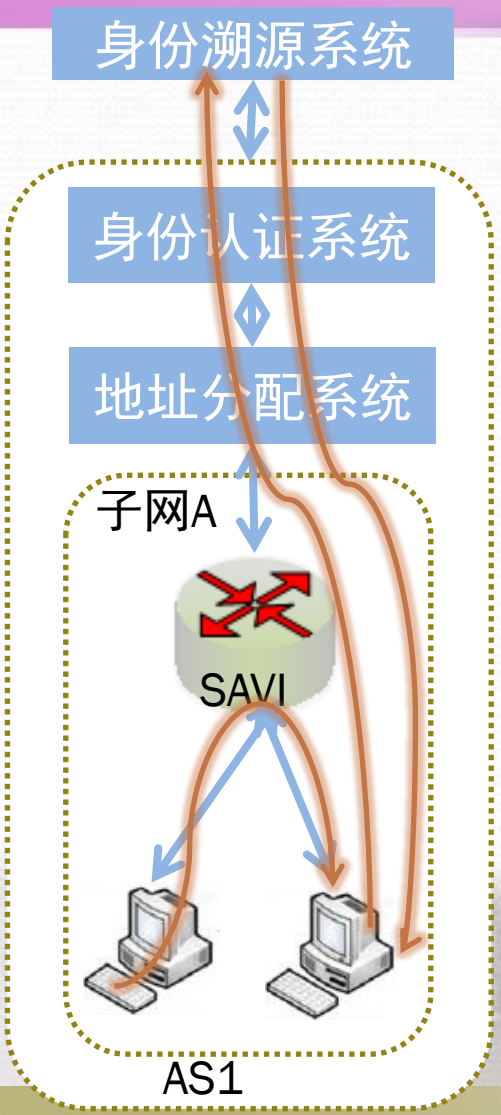
- 身份认证：
  - 基于DHCPv6协议进行扩展，使之支持用户身份认证流程；
  - 用户登录时，输入NID和password，进行认证；
  - 认证通过之后，身份认证系统向DHCPv6服务器发送GID；
- 地址分配：
  - DHCPv6服务器根据GID生成IPv6地址，发送给客户端
  - 客户端获取回复之后配置地址
  - 将<NID、IPv6、time>发送给身份溯源系统记录

5. 系统实现：身份认证&地址分配



- 交互流程：
  - 1，用户登录时输入用户名和密码；
  - 2，Solicit：NID
  - 3， 确认NID存在
  - 4，产生Nonce
  - 5，Advertise：Nonce
  - 6，Request：digest
  - 7，确认digest正确
  - 8，产生GID
  - 9，产生IPv6地址
  - 10，Reply：GID

5. 系统实现：身份溯源&报文过滤

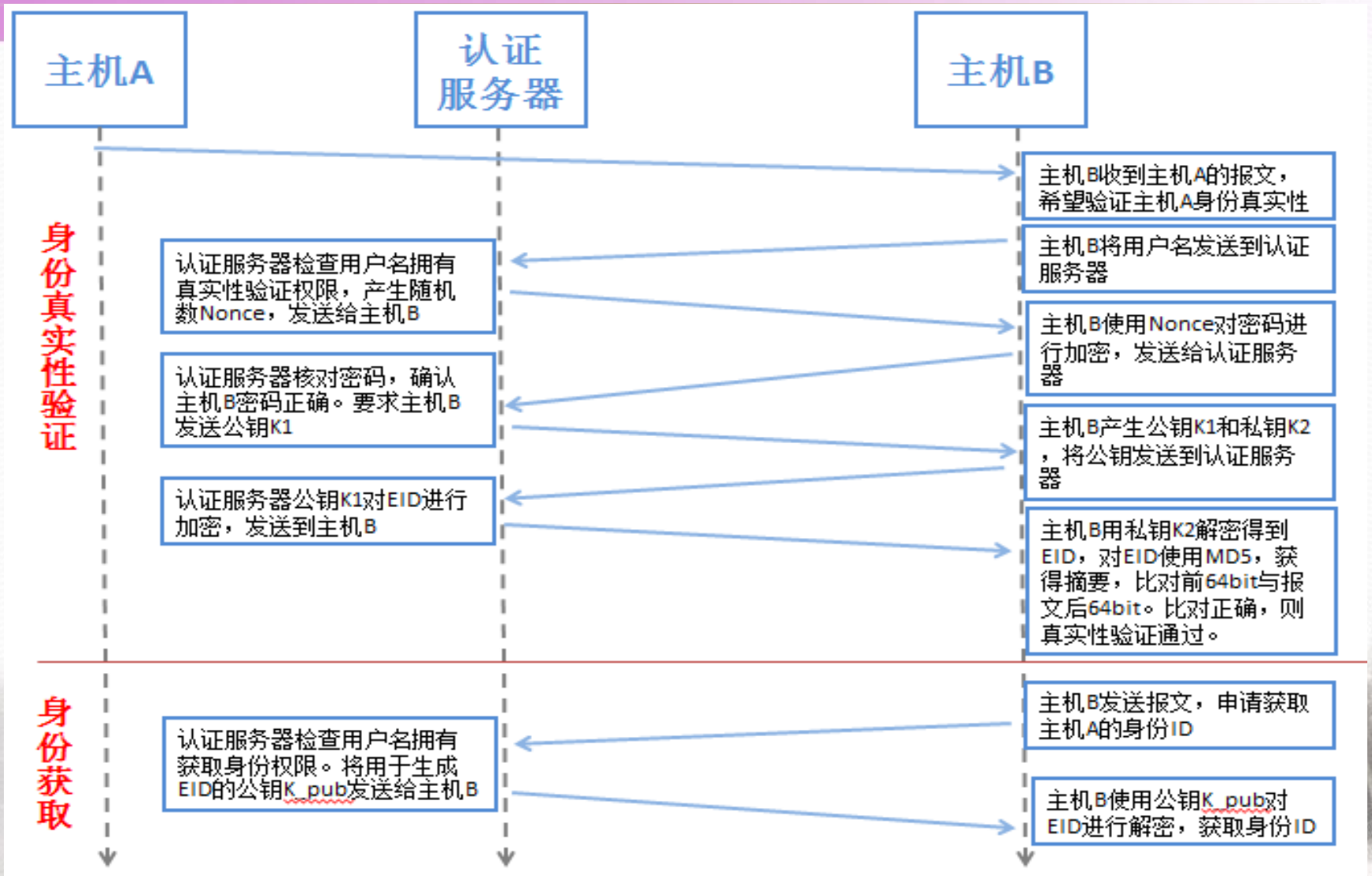


- 身份溯源：
  - 主机B在首次收到主机A的报文之后，可以通过身份溯源系统对主机A的身份进行验证。验证分为两个层次，分别需要对应的权限：
  - 真实性验证：验证主机A的身份是否真实可信；
  - 真实身份获取：可以获取主机A的真实身份，即NID；

- 报文过滤：
  - 主机B在确认主机A的身份是真实的之后，会将其<NID, IPv6, Time>加入到真实主机表中。
  - 当主机B再次收到报文时，会先检查该主机是否存在于真实主机表中。若存在，则可以正常通信；若不存在，则开始身份溯源过程。

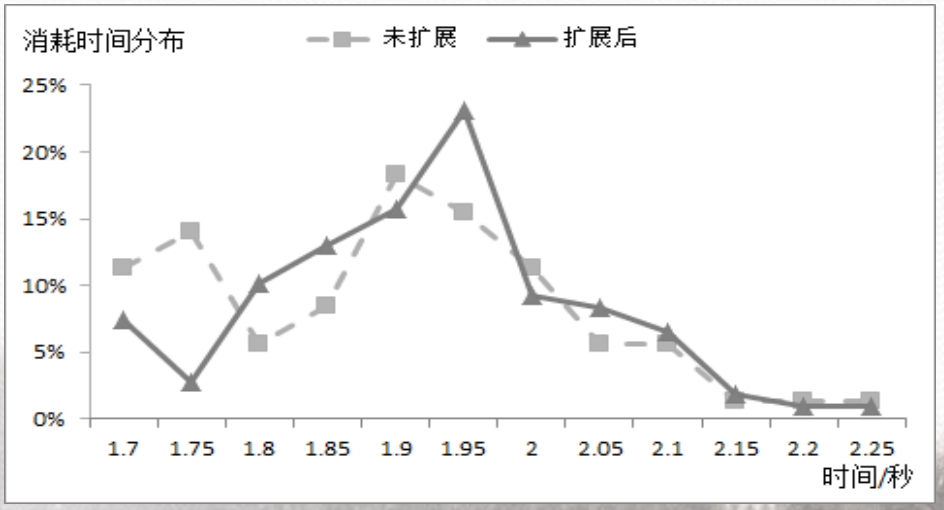
5. 系统实现：身份溯源&报文过滤

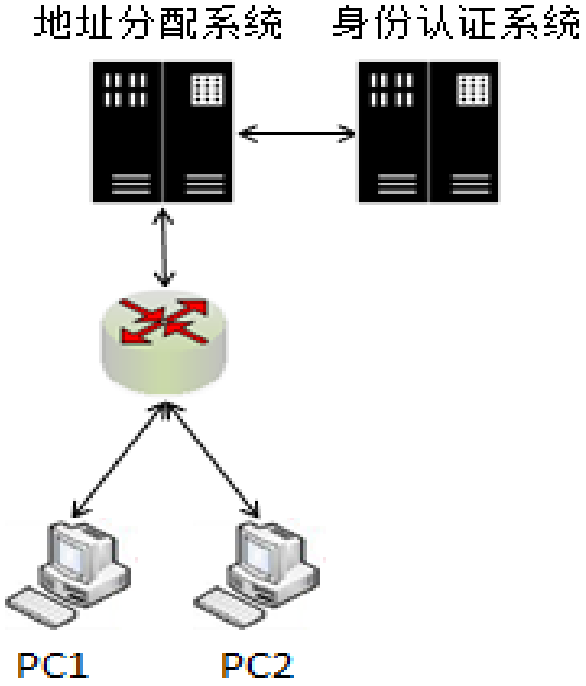
交互流程：



6. 系统评价

- 性能评估：
  - 可信身份系统中地址分配流程中添加了身份认证环节，带来了一定的延时。
  - PC1：对照组；PC2：实验组





6. 系统评价

- 性能评估：
  - 实验组平均比对照组需要多耗时0.047s，比对照组增加耗时2.63%，是身份认证系统所带来的延时效果。
  - 两次t检验结果说明：引入身份认证系统后，并没有显著增加地址分配流程的耗时，所引入耗时在统计上可以忽略不计。

统计指标	实验组	对照组
均值	1.831s	1.784s
方差	$0.099s^2$	$0.122s^2$
标准差	0.315s	0.349s
中位数	1.903s	1.870s
最大值	2.214s	2.207s
最小值	0.699s	0.663s

- 假设检验：
  - 双样本等方差t检验：

P-value=0.345 > 0.05，无法拒绝原假设。

  - 双样本异方差t检验：

P-value=0.356 > 0.05，无法拒绝原假设。

6. 系统评价

- 安全性：攻击者伪造GID
  - 假冒攻击：如果攻击者通过随机伪造密码，试图获取特定NID对应的GID。以每次地址分配耗时1.831s计算，则攻击者需要$4.7*10^{32}$年才能攻击成功一次。
  - 实验模拟攻击者进行假冒攻击。攻击者知道NID，通过随机产生密码希望获取GID。经过200次攻击，没有成功获取GID。
  - 重放攻击：会被源地址验证系统过滤
- 隐私性：攻击者通过GID或者EID获取用户身份NID
  - 主要依靠加密算法安全性来保证，本系统中采用RSA-2048

密钥长度n/bit	MIPS年
512	3*104
768	2*108
1024	3*1011
2048	3*1020

7. 总结

- 由于缺乏可信基础而常常发生伪造攻击，设计了真实可信身份通信系统，通过将用户身份嵌入到IPv6地址中，能够有效地防止用户身份被假冒。
- 保证了用户身份的隐私性、可验证性、真实性
- 设计了开放的用户身份映射接口，可以支持身份映射算法的自定义
- 实现了原型系统，并对系统进行了测试和评价

主要参考文献

[1] Droms, Ralph, et al. Dynamic host configuration protocol for IPv6 (DHCPv6)[EB/OL]. http://tools.ietf.org/html/rfc3315. 2003.

[2] Narten, Thomas, Susan Thomson, et al. IPv6 stateless address autoconfiguration[EB/OL]. http://tools.ietf.org/html/rfc3736. 2007.

[3] Bi, Jun, et al. A source address validation architecture (sava) testbed and deployment experience[EB/OL]. http://tools.ietf.org/html/rfc5210. 2008.

[4] Kumari, Warren, and Danny McPherson. Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)[EB/OL]. http://tools.ietf.org/html/rfc5635. 2009.

[5] Li, Jun, et al. SAVE: Source address validity enforcement protocol[A]. INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies[C]. Proceedings. IEEE. Vol. 3. IEEE, 2002.

[6] Bi, Jun, et al. Source Address Validation Improvement (SAVI) Framework. [EB/OL]. https://tools.ietf.org/html/rfc7039. 2013.

[7] Droms, Ralph, and William Arbaugh. Authentication for DHCP messages[EB/OL]. http://tools.ietf.org/html/rfc3118. 2001.

[8] Arbaugh, William, and Ralph Droms. Authentication for DHCP Messages[EB/OL]. http://tools.ietf.org/html/rfc3118. 2001.

清華大學
Tsinghua University

谢谢