计算机科学 2006Vol. 33№. 4

# 基于 AES 算法的移动 IPv6 绑定更新信息处理效率分析

李 峰 冯 永 周尚波
(重庆大学计算机学院 重庆 400044)

**摘 要** 移动 IPv6 中移动节点向家乡代理和通讯对端告知自己当前位置而传输的信息是通过绑定更新(Binding Update)来进行的,绑定更新的过程通过移动节点的注册来完成。家乡代理处理绑定更新信息的性能和效率对尽快定位移动节点的位置是一个比较关键的问题,尤其是在移动节点数量多、移动频繁及考虑信息加密的情况下,问题显得更为突出。IPv6 在这方面还需要做进一步的研究和改进。本文提出了移动 IPv6 中绑定更新信息数量统计的数学模型,并在该数学模型的基础上,首次提出将 AES 算法应用于该类信息的处理,并与其它处理方法做了比较。

**关键词** AES,移动 IPv6,绑定更新,效率

## The Efficiency Analysis of Disposing Binding Update/Acknowledgement Messages in Mobile IPv6 Based on AES Algorithm

LI Feng FENG Yong ZHOU Shang-Bo
(College of Computer Science, Chongqing University, Chongqing 400044)

**Abstract** In mobile IPv6, MN communicates with HA and correspondent nodes by Binding Update/Acknowledgement messages for locating its current position. The Binding Update/Acknowledgement proceeding is achieved by the MN registration. For quickly locating a MN, HA disposing efficiency is a key issue, especially under the condition that MN is excessive and it's moving is frequent. In mobile IPv6, it is necessary to improve the efficiency of HA disposing Binding Update/Acknowledgement messages. In this paper, the amount of Binding Update/Acknowledgement message mathematic model is proposed and AES algorithm is employed to encrypt/decrypt Binding Update/Acknowledgement messages firstly in mobile IPv6.

**Keywords** AES, Mobile IPv6, Binding update/acknowledgement, Efficiency

## 1 引言

移动 IP 技术中,当一个移动节点 MN(Mobile Node)从家乡链路进入外地链路时,移动节点检查接收到的广播中的网络前缀。如果没有一个前缀与移动节点家乡地址的网络前缀匹配,那么移动节点就是连接在外地链路上。这时,移动节点将启动注册过程,通过交互绑定更新信息,向家乡代理和通讯对端告之自己所处的当前位置。包含任何绑定更新信息的 IPv6 数据包,必须有 AH 扩展头或 ESP 扩展头[1],以此通过 AH 或 ESP 协议来保证绑定更新信息的安全。由于 AH 协议和 ESP 协议主要通过相应的加密、解密过程来完成对被保护对象的保密工作,相比其它 IPv6 数据包,对 AH 扩展报头或 ESP 扩展报头的处理占了整个数据包处理过程的很大比重。在移动 IPv6 的系统组件中,涉及对绑定更新信息处理的系统组件有家乡代理、通讯对端、移动节点。在这三个系统组件中,家乡代理承担了绝大部分绑定更新信息的处理。

AH 协议和 ESP 协议采用的加密和解密算法主要包括 RC5、DES、3DES[5,6],AES 算法将取代旧的数据加密标准(DES、3DES)而成为美国联邦信息处理标准(FIPS)。因为在大多数的分组密码中,密钥建立需要占用处理时间,在使用相同密钥加密大量数据的应用中,这个处理相对来说是无足轻重的。但是在密钥经常更换的应用系统中,如在 IPSEC 中,对 IP 分组进行加密,密钥建立所带来的开销将是非常关键的[2]。

## 2 绑定更新信息量数学模型的建立

移动 IP 的注册过程在以下几种情况下启动。一是当移动节点发现它的网络接入点从一条链路切换到另一条链路上;二是现有注册已过期。由于移动 IP 的注册存在着生存时间一定(有限)的问题,因此在并没有移动位置时,如果现有注册已过期,则移动节点重新进行绑定,以更新注册;三是移动节点在回到家乡链路后进行注销。

### 2.1 绑定更新信息数量的数学模型

#### 2.1.1 已配置家乡代理地址

移动节点知道家乡代理地址以及它的家乡地址、家乡地址前缀、DNS 服务器地址时,当移动节点检测到它已进入外地链路后,移动节点将向家乡代理发送绑定更新信息(Binding Update)。当家乡代理接到绑定更新信息后,经过验证并注册,向该移动节点发送绑定更新确认信息(Binding Acknowledgement),由此完成一次绑定更新过程(见图 1)。如果注册失败,移动节点需要再次注册。在协议规定的时间内,如果没有完成注册,则宣告失败。在一次成功注册的过程中,家乡代理需要处理的绑定更新数据包的个数为 2。$T_{con}$ 为协议规定的最长注册时间,如果注册时间超过它,则注册失败。设 $T_{avg}$ 为注册一次的平均时间,则在协议规定时间内,移动节点的最大注册次数为:

$$n=\lfloor \frac{T_{con}}{T_{avg}} \rfloor \quad (1)$$

假设某一个家乡代理管辖的 MN 数量为 $x$,每个 MN 的

移动次数是 $y$，一次注册成功的概率为 $p_1$，二次注册成功的概率为 $p_2$，依次类推，$n$ 次注册成功的概率为 $p_n$，在一段时间 $T$ 内，则家乡代理需要处理的绑定更新信息数量为：

$$F(x,y)=2p_1xy+4p_2xy+\cdots+np_nxy \quad (2)$$

2.1.2 *未配置家乡代理地址*

没有配置家乡代理地址的移动节点，也可以通过移动 IP 注册协议动态地得到家乡代理的地址。在这个过程中，移动节点将它的家乡地址的主机部分全置成 1，形成一个家乡链路上的 IP 广播地址，即网络前缀. 11…11。移动节点将这个家乡链路上的广播地址放入注册请求消息的家乡代理地址域中，移动节点就将这个家乡链路上的广播地址作为注册请求消息的目的 IP 地址。注册请求消息作为广播消息在家乡链路上发布，它将被家乡链路上的所有节点接收，当然也会被所有的家乡代理收到。然而，那台收到注册请求并愿意为该移动节点做家乡代理的设备，必须以特殊的方式回答一条注册应答并拒绝这次请求，同时在家乡代理地址域中给出自己的地址（不再是广播地址）。所有愿意为该移动节点作家乡代理的设备都以这种方式拒绝这次注册请求。移动节点收集所有表示拒绝的注册应答消息，并读出家乡代理地址域，这就是那些愿意为它做家乡代理的设备的 IP 地址。这时，移动节点可以将这些地址放入注册请求消息中，重新进行注册。可以看到，在这种情况下，家乡代理注册过程包含两个步骤：一步是请求家乡代理的有关信息的过程，另一步是向家乡代理的注册过程。

在请求家乡代理的有关信息过程中，家乡代理处理的绑定更新信息数量函数与直接向家乡代理注册时所需要处理的绑定更新信息数量函数类似，不同的只是发生概率的变化。假设在请求家乡代理的有关信息过程中，一次请求成功的概率为 $q_1$，二次请求成功的概率为 $q_2$，依次类推，$n$ 次成功的概率为 $q_n$，则在一段时间 $T$ 内，家乡代理需要处理这个过程中的绑定更新信息数量函数为：

$$A(x,y)=2q_1xy+4q_2xy+\cdots+2nq_nxy \quad (3)$$

结合移动节点不知道家乡代理地址时注册过程中的两个步骤，家乡代理需要处理的绑定更新数量函数为：

$$R(x,y)=A(x,y)+F(x,y) \quad (4)$$

2.1.3 *移动节点链路切换*

由于 2.1.1 和 2.1.2 两种情况是独立事件，假设移动节点知道家乡代理地址以及它的家乡地址、家乡地址前缀、DNS 服务器地址事件发生的概率是 $P$，则移动节点不知道家乡代理地址以及它的家乡地址、家乡地址前缀、DNS 服务器地址事件发生的概率就是 $1-P$。

所以，根据 2.1 节的分析，家乡代理处理绑定更新信息数量的数据模型为：

$$\phi(x,y)=pF(x,y)+(1-p)R(x,y) \quad (5)$$

其中 $x,y\in Int$

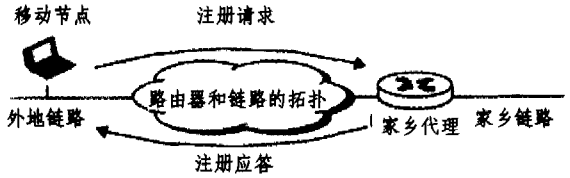


图 1 绑定更新注册过程

### 2.2 注册过期

绑定更新消息（Binding Update）中的生存时间域（Life Time）表示移动节点希望它的注册（即绑定表项）在失效前能存在多少秒。当移动节点检测到绑定表项快要失效之前，将重新注册。假设绑定更新消息中的生存时间域值为 $t$，则在一段特定的时间 $T$ 内，家乡代理需要处理的绑定更新信息数量为：

$$g(x)=\frac{T}{t}F(x,y),y=1 \quad x\in Int \quad (6)$$

### 2.3 移动节点在回到家乡链路后的注销

移动节点在回到家乡链路后进行注销（见图 2），其工作流程和注册时是一样的。因此，每一次注销，家乡代理处理的绑定更新信息数据包为 2 个，假设在时间 $T$ 内，注销的移动节点数为 $z$，则家乡代理需要处理的绑定更新信息数量为：

$$m(z)=F(z,y),y=1 \quad z\in Int \quad (7)$$

根据以上分析，在 IPv6 的移动环境下，家乡代理处理绑定更新信息数量的数据模型可用如下公式描述：

$$N(x,y,z)=\phi(x,y)+g(x)+m(z) \quad (8)$$

其中 $x,y,z\in Int$

从上式可见，家乡代理处理绑定更新的数据量与所管辖的移动节点及这些移动节点的移动频率呈同向变化；在应用规模和移动频率不断扩大的情况下，绑定更新的信息量将成倍增加。

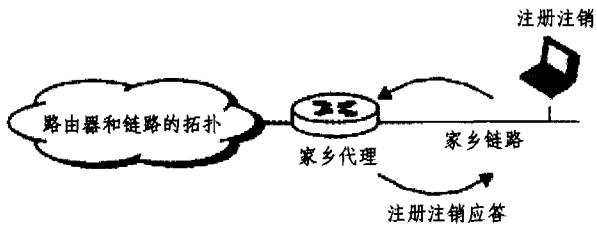


图 2 绑定更新注销过程

## 3 基于 AES 的块加密算法

AES 是一个密钥迭代分组密码算法，其加密过程包括一个初始密码加法，记作 AddRoundKey，接着进行 $N_r-1$ 次轮变换（Round），最后再使用一个轮变换 FinalRound。初始的密钥加法和每个轮变换均以状态（State）和一个轮密钥作为输入。第 $i$ 轮的轮密钥记为 ExpandedKey[$i$]，初始密钥加法的输入记为 ExpandedKey[0]。从 CipherKey 导出 ExpandedKey 的过程记为 KeyExpansion。AES 算法的高级语言伪 C 符号描述如下：

```
Function( state, CipherKey)
{
    KeyExpansion(CipherKey, ExpandedKey);
    AddRoundKey(state, ExpandedKey[0]);
    For (i=1;i< Nr ; i++) Round(State, Expand-
        edKey[i]);
    FinalRound(state, ExpandedKey[Nr]);
}
```

AES 的轮变换由 4 个步骤组成：SubBytes、ShiftRows、MixColumns、AddRoundKey。其中 SubBytes 是一个非线性变换，ShiftRows 是一个字节换位，MixColumns 的作用是在状态各列进行砖匠置换，AddRoundKey 是状态通过与一个轮

（下转第 102 页）

3)配置不灵活。针对每个网络环境需要进行不同的配置,并指定不同的策略,这需要耗费很多时间。

为了达到更大的欺骗性,将 Honeyweb 与 Honeyd 结合起来,利用后者提供的网络拓扑结构模拟功能[6]把 Honeyweb 安装到模拟网络图的一个节点上,实施从网络到主机、从主机到网络服务的多层次欺骗,能更有效地发挥 Honeyweb 的功能。

**展望** 蜜罐的出现为网络安全领域开辟了一个新的天地,它天生所具有的主动防御性克服了传统网络安全设备的缺陷和脆弱。将成熟的蜜罐或蜜网部署在现有的网络环境下,和防火墙、IDS 共同完成保护网络的任务将成为今后的趋势。

"道高一尺,魔高一丈"。随着蜜罐技术的发展,又出现了反蜜罐技术[7~9],它通过研究各种蜜罐的行为特征来发现蜜罐,甚至是攻破蜜罐。为了对付反蜜罐技术,蜜罐技术将继续从欺骗伪装、数据捕获、数据控制、数据分析等 4 个方向发展。对于欺骗伪装,难点还是在于如何设计一个逼真的陷阱系统而不被黑客发现;在数据捕获、数据控制方面,研究热点是如何在确保黑客无法以蜜罐为跳板去攻击其他系统的前提下尽可能地隐藏自己;对于数据分析,如何从大量日志记录中综合分析出黑客的行为意图和攻击技术以及如何还原攻击过程,将成为今后的挑战。作为一种低交互的蜜罐,Honeyweb 也将从欺骗伪装、数据捕获以及配置工作的简易性等方面作出更大贡献。

## 参 考 文 献


1 Spitzner L. The Value of Honeypots, Part One: Definitions and Values of Honeypots. http://www.securityfocus.com/infocus/1492, 2001
2 Baumann R. Honeyd - A low involvement Honeypot in Action. GCIA, GSEC, CCNA
3 Honeynet Project. Know Your Enemy: Honeynets. http://www.honeynet.org/papers/honeynet/ index.html, 2003
4 Honeynet Project. Know Your Enemy: GenII Honeynets. http://www.honeynet.org/papers/gen2/index.html,2003
5 Spitzner L. Honeytokens: The Other Honeypot. http:// www.securityfocus.com/infocus/1713,2003
6 Chandran R,Pakala S. Simulating Networks with Honeyd. http// www.paladion.net/papers/simulating_networks_with_honeyd.pdf
7 Spitzner L. Problems and Challenges with Honeypots. http://www.securityfocus.com/infocus/1757, 2004
8 Oudot L,Holz T. Defeating Honeypots: Network Issues Part1. http://www.securityfocus.com/infocus/1803, 2004
9 Oudot L,Holz T. Defeating Honeypots: Network Issues Part2. http://www.securityfocus.com/infocus/1805, 2004


(上接第 89 页)

密钥进行逐位异或而完成的状态调整。由此可见,AES 的大量运算集中在轮变换。轮变换的 4 个步骤可以在字节、状态行或状态列上并行进行,大部分的异或运算也可以并行进行。同时,并行处理器上的 AES 性能并不受到关键路径长度的限制[2,3]。

表 1 是 AES 算法和现有绑定更新消息中采用的 DES、3DES 等算法的性能比较[4],算法采用 ANSI C 实现。

表 1 AES、DES、3DES 等算法的性能比较

| Block size | speed (Mbits/Sec) |
|---|---|
| AES | 27.0 |
| DES | 16.9 |
| 3DES | 6.21 |
| RC5 | 13.9 |

## 4 不同的块加密算法的计算时间分析

根据前面的分析,IPv6 的移动环境下,在一段时间 $T$ 内,家乡代理处理绑定更新信息数量为(8)式的 $N(x,y,z)$,家乡代理处理这些信息量所需要的时间为:

$$t=T_r+T_c \tag{9}$$

其中 $T_c$ 为家乡代理在处理绑定更新信息过程中加/解密所消耗的时间,$T_r$ 为处理这些信息所消耗的其它时间。对于家乡代理在相同的环境、同样的平台下处理同样信息量的绑定更新信息,$T_r$ 是一个相同的量,$T_c$ 与采用的算法有关。

假设包含绑定更新信息的 IPv6 数据包的平均大小为 $S$ 字节,算法处理速度为 $M$,则家乡代理完成这些绑定更新信息的加/解密时间为:

表 2 绑定更新信息的块加密算法的时间函数

| 算法 | 时间(ms) |
|---|---|
| AES | 0.3N(x,y,z) S |
| DES | 0.5 N(x,y,z) S |
| 3DES | 1.3 N(x,y,z) S |
| RC5 | 0.6 N(x,y,z) S |

$$T_c=\frac{N(x,y,z)\times S\times 8}{M} \tag{10}$$

根据上述公式,则不同的块加密算法在加/解密这些绑定更新信息的时间函数见表 2。

**结论** 由上可知,采用不同的块加密算法,在同样的场景下,家乡代理处理绑定更新信息的效率不一样。其中,AES 算法占优。这对快速完成移动节点注册,快速定位移动节点的具体位置,有利于移动节点更加平滑地切换,同时也可以减少"三角路由"的存在时间。从另一个层面也可提高家乡代理的处理效率。尤其是在移动节点数量多、移动频繁的情况下,更具实际意义。本文在移动 IPv6 家乡代理处理绑定更新信息中引入了 AES 算法,并从理论分析与其他算法比较其效率,结果说明可缩短加密时间。下一步的工作是在 NS2 平台上完成仿真实验,进一步验证在移动 IPv6 的绑定更新信息处理过程中引入 AES 算法的优越性。

## 参 考 文 献


1 Arkko J,Devarapalli V,Dupont F. Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. rfc 3776, June 2004
2 Rijmen J D V. 高级加密标准(AES)算法—Rijndael 的设计. 谷大武,徐胜波译. 北京:清华大学出版社,2003
3 Rijmen J D V. The Design of Rijndael AES: The Advanced Encryption Standard. Springer-Verlag Berlin Heidelberg,2002
4 http://www.esat.kuleuven.ac.be/~bosselae/fast.html
5 Kent S,Atkinson R. IP Encapsulating Security Payload (ESP). rfc 2406, November 1998
6 Kent S,Atkinson R. IP Authentication Header. rfc 2402 , November 1998
7 Johnson D,Perkins C. Mobility support in ipv6. rfc 3775 , June 2004