协议抗拒绝服务攻击性自动化证明

孟博，黄伟，王德军，邵飞

（中南民族大学 计算机科学学院，湖北 武汉 430074）

摘 要：首先从攻击者上下文与进程表达式 2 个方面对标准应用 PI 演算进行扩展，然后从协议状态的角度，应用扩展后的应用 PI 演算对协议抗拒绝服务攻击性进行建模，提出一个基于定理证明支持一阶定理证明器 ProVerif 的抗拒绝服务攻击性自动化证明方法，最后应用 ProVerif 分析与验证了 JFK 协议与 IEEE 802.11 四步握手协议抗拒绝服务攻击性，发现 IEEE 802.11 四步握手协议存在一个新的拒绝服务攻击，并且针对 IEEE 802.11 四步握手协议存在的拒绝服务攻击提出了改进方法。

关键词：拒绝服务攻击；形式化；自动化证明；协议状态

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)03-0112-10

Automatic proof of resistance of denial of service attacks in protocols

MENG Bo, HUANG Wei, WAND De-jun, SHAO Fei

(School of Computer, South-Center University for Nationalities, Wuhan 430074, China)

Abstract: First, the applied PI calculus was extended from two aspects: attacker contexts and process expression, then from the view of protocol state, the protocols were modeled with the extended applied PI calculus and a automatic method of proof of resistance of denial of service attacks based on theorem proof with first order theorem prover ProVerif was presented, finally resistance of denial of service attacks in JFK protocol and IEEE 802.11 four-way handshake protocol were analyzed. The results obtained are that JFK protocol is resistance of denial of service attack and IEEE 802.11 four-way handshake protocol is not. At the same time a new al of service attack in IEEE 802.11 four-way handshake protocol was found. The methods to prevent resistance of denial of service attacks in IEEE 802.11 four-way handshake protocol were proposed.

Key words: denial of service attacks; formal method; automatic proof; protocol state

1 引言

拒绝服务攻击具有威害巨大及难以有效防御的特点，越来越受到网络安全专家与用户的关注。拒绝服务攻击是通过各种手段使提供服务的主机无法提供服务的一种攻击，本质是对分布式系统的可用性进行攻击。按照攻击方式可以分为：资源消耗型、服务中止型和物理破坏型。这种攻击简单有效，如攻击者可以发送大量垃圾信息给服务器，造成服务器处理大量无效的数据，从而无法向合法用户提供正常的服务，而产生拒绝服务攻击；此外拒绝服务攻击很难甚至无法确定攻击者，并且能够通

收稿日期：2011-04-06；**修回日期**：2011-12-13

基金项目：国家民委基金资助项目（10ZN09）；国家自然科学基金资助项目（60603008）；中南民族大学自然科学基金资助项目（YZZ09008）；武汉市科技型中小企业技术创新基金资助项目（SZY11008）

Foundation Items: The Foundation of State Ethnic Affairs Commission of China (10ZN09); The National Natural Science Foundation of China (60603008); The Natural Science Foundation of South-Center University for Nationalities(YZZ09008); The Technology Innovation Foundation of SME in Wuhan (SZY11008)

过这种攻击产生其他攻击，例如，中间人攻击，会话拦截攻击等。目前的 TCP/IP 协议架构从链路层到应用层都存在拒绝服务攻击，例如，链路层的 ARP Flooding 攻击、ARP poisoning 攻击，网络层的 ICMP 攻击，传输层的 SYN Floods 攻击，应用层的 session flooding 攻击、buffer overflow 攻击等。

对拒绝服务攻击的形式化建模，目前有 2 类主要方法，一类是以用户合约为基础的 Yu-Gligor 形式化建模方法[1]，另一类是以代价为基础的 Meadows 形式化建模方法[2]，后者受到了人们的重点关注。

安全协议的形式化分析与验证方法主要有定理证明、模型检测、逻辑推理、类型检测等。代表性的定理证明方法有 Paulson 的归纳证明法和 Thayer 等学者提出的串空间模型。基于定理证明的方法在自动化工具支持方面虽然无法与模型检测方法比拟，但是它克服了模型检测固有的缺陷——状态空间爆炸的问题，能够处理无穷状态系统。定理证明可以通过自动化的定理证明器协助完成证明过程。主要的定理证明器有 ProVerif、Isabelle、HOL、ACL2、PVS 等，其中 ProVerif 是 Blanchet[3]开发的基于 Dolev-Yao 模型的一阶定理证明器，它可以分析和验证使用 Horn 子句或应用 PI 演算描述的安全协议的秘密性、强秘密性、认证性等。ProVerif 已经成功分析了很多复杂的协议，如电子商务协议[4]、网络投票协议[5,6]、JFK 协议[7]等。

在拒绝服务攻击中非常重要的一类攻击就是利用了协议状态而产生的，例如，利用协议状态的保持来耗尽系统资源，产生资源消耗型拒绝服务攻击；修改协议状态，使其前后状态不一致而产生协议中止型拒绝服务攻击。因此，本文脱离以用户合约为基础的 Yu-Gligor 形式化建模方法与以代价为基础的 Meadows 形式化建模方法，从协议状态的角度，对协议抗拒绝服务攻击性进行建模，分析与验证协议抗拒绝服务攻击性。由于标准应用 PI 演算[8]不能够对协议状态进行建模，为了能够使用基于应用 PI 演算 ProVerif 来自动化分析与验证协议抗拒绝服务攻击性，必须对标准应用 PI 演算进行扩展。首先从 2 个方面：一个是攻击者上下文，另外一个是进程表达式对标准应用 PI 演算进行扩展，然后应用扩展后的应用 PI 演算对协议抗拒绝服务攻击性进行建模，提出一个基于定理证明支持一阶定理证明器 ProVerif 的抗拒绝服务攻击性自动化证明方法，最后应用 ProVerif 来分析与验证协议的抗拒绝服务攻击性。

2　相关的工作

目前，协议拒绝服务攻击形式化建模主要有 2 类方法。

Yu 和 Gligor 基于时态逻辑，引入用户合约，提出了一个对共享服务拒绝服务攻击的形式化规范和验证方法。他们把拒绝服务攻击归结为新鲜性与安全性问题。Yu-Gligor 形式化建模方法的核心思想是以访问控制策略为基础对拒绝服务攻击进行形式化建模，因此不能够处理在认证发生之前产生的拒绝服务攻击，如 SYN Floods 攻击。此外 Yu-Gligor 形式化建模方法不支持自动化工具。Millen[9]通过对时间逝去的明确度量对 Yu-Gligor 形式化建模方法进行了扩展，使得它可以处理最大等待时间策略。Cuppens 与 Saurel[10]应用模态逻辑和道义逻辑也对 Yu 和 Gligor 框架的可用性策略进行了形式化建模。

Meadows 提出了基于代价的拒绝服务攻击形式化建模方法，该形式化建模方法通过设置容忍关系灵活的判断协议是否会产生拒绝服务攻击，适合对协议的资源消耗型拒绝服务攻击进行建模。Meadows 声明其框架支持 NRL 协议分析器，但是没有给出具体例子。基于代价的形式化建模方法存在一个问题：在任何时候产生一个伪造的数据比验证它要花费的代价要小，按照 Meadows 形式化建模方法，那么所有的协议都不能够抵抗拒绝服务攻击。Ramachandran[11]应用 Meadows 形式化建模方法分析并指出 JFK 协议具有抗拒绝服务攻击性。Smith[12]等应用 Meadows 形式化建模方法分析了 JFK 协议，声称在允许攻击者 IP 地址保密或者协议双方的 DH 协议的公钥可以重用的情况下，JFK 协议存在 2 个拒绝服务攻击，但是我们认为他们的结论是值得商榷的。基于 Meadows 形式化建模方法，Groza 与 Minea[13]应用支持 ASLan 规范语言的 AVANTSSAR 自动化工具对资源消耗型的拒绝服务攻击进行了建模，分析 STS 与 JFK 协议，指出 STS 协议不能抵抗拒绝服务攻击，JFK 协议具有抗拒绝服务攻击性；Abadi 和 Blanchet[7]应用观察等价关系对抗拒绝服务攻击性进行建模，且应用 PI 演算分析并证明 JFKr 协议具有抗拒绝服务攻击性；Lafrance 和 Mullins[14]应用安全进程代数 SPPA 与容许干扰

来对安全协议中的拒绝服务攻击进行建模，具体是通过引入“Impassivity”来描述攻击者通过利用低代价的行为来产生对协议另外一方的高代价行为的干扰，适合对资源消耗型拒绝服务攻击进行建模，并且分析证明 1KP 支付协议不能够抵抗拒绝服务攻击；周世健等学者[15]对串空间模型进行了扩展，分析了 IEEE 802．11i 四步握手协议抗拒绝服务攻击性，发现其存在拒绝服务攻击；Tritilanunt 等[16,17]指出 Meadows 基于代价的形式化建模方法存在 2 个主要的问题：1) 仅仅考虑到诚实的协议参加方；2) 代价的分类方式太粗糙而不具有实用性。故他们应用着色 Petri 网提出了一个基于时间和代价的形式化拒绝服务形式化建模方法，分析了 HIP 协议，指出在攻击者为类型 3（攻击者选择正确的客户端难题答案（client puzzle solution））和类型 4（攻击者伪造客户端难题答案（client puzzle solution））情况下，存在拒绝服务攻击。

除了上述 2 类主要的形式化建模方法之外，Agha 等[18]应用概率重写理论 PMAUDE 对拒绝服务攻击进行了形式化建模，应用 CSL 逻辑形式化描述拒绝服务攻击成功的概率，并且应用基于统计的模型检查器 VESTA 对 TCP 三步握手协议进行了分析，指出 TCP 三步握手协议不具有抗拒绝服务攻击性。Mahimkar 和 Shmatikov[19]基于博弈的 ATL 逻辑，对资源消耗与带宽消耗抗拒绝服务攻击性进行了建模，应用 MOCHA 模型检查器分析并证明 JFKr 协议具有抗拒绝服务攻击性。

3　扩展的应用 PI 演算

为了对协议状态及抗拒绝服务攻击性进行建模，从 2 个方面对标准应用 PI 演算进行扩展：一个是攻击者上下文，另外一个是进程表达式。扩展应用 PI 演算语义与标准应用 PI 演算相同。

3.1　攻击者上下文

按照攻击者对消息的攻击能力将攻击者所处的上下文分为现实上下文和理想上下文。

现实上下文形式化表示为

$$n\,\mathbb{N}.C\left[C\left[\overline{c}\langle u\rangle\right]\overline{u}\langle N\rangle.P\right],\quad n\,\mathbb{N}.C\left[C\left[c(u)\right]u(x).P\right]$$

其中，$u\in\mathbb{N},c\notin\mathbb{N}$，也就是说，在现实上下文中，消息发送方要发送消息 N，先在公开通道 c 上发布通道名 u，然后通过通道 u 发送消息 N；消息接收方要接受消息 N，必须先从公开通道 c 上获取通道 u，然后在通道 u 上接受消息 N。现实上下文即存在 Dolev-Yao 攻击者的不安全环境，攻击者拥有拦截、读取、修改和发送消息的能力。

理想上下文形式化表示为 $n\,\mathbb{N}.C\left[\overline{u}\langle N\rangle.P\right]$，$n\,\mathbb{N}.C\left[u(x).P\right]$，其中，$u\in\mathbb{N}$，也就是说，在理想上下文中，消息发送方要发送消息 N，直接通过通道 u 发送消息 N；消息接收方要接受消息 N，直接在通道 u 上接受消息 N。消息 N 的安全性取决于通道 u 的安全性。由于在每次通信的时候，通道 u 都会随机生成或是通信双方事先共享的安全通道，因此在理想上下文中，攻击者不能对消息拦截、读取、修改和发送，理想上下文即安全上下文。

3.2　项

应用 PI 演算[5]是一个用来描述并发进程的语言。它继承了 PI 演算的通信与并发结构，增加了函数和等价理论。消息不仅是原子名，还可以是通过名字和函数构成的项。

项的定义如图 1 所示。用 a、b、c、m、n 等标识符及其组合表示名字，用 x、y、z 表示变量；也使用原语言变量 u、v、w 表示名字和变量；用 f、g、h 表示函数项，每个函数项都带有固定元数的参数，例如，$encrypt(m,k)$ 表示函数 $encrypt$ 有参数 m 和 k。函数项是用来构造项的。因此，项 M、N、T、V 是变量，名字和函数项。

M,N,T,V ::=		项
	x,y,z	变量
	a,b,c,L,m,n	名
	$f(M_1,\mathrm{L},M_l)$	函数

图 1　项的定义

如果项 $M=f(M_1,\mathrm{L},M_n)$，则项 M 有子项 $M_i,i\in[1,n]$。项 $M_i,i\in[1,n]$ 也可能包含子项，不包含任何子项的项叫作原子项。项 M 用来描述协议中参与者之间相互交换的消息。变量可以描述任何消息或值，名字用来描述原子值，函数项用来描述从已知消息和值构造新的消息和值。

3.3　扩展后的进程

扩展后的进程如图 2 所示，空进程 0 不做任何操作；并行复合进程 $P|Q$ 同时运行进程 P 和 Q；复制进程 $!P$ 并发执行无数个 P 进程；受限进程 $n\,n.P$ 首先产生一个新的私有名字 n，然后执行 P 进程；条件进程分为 2 种：理想上下文中的条件进程

if $M=N$ then P else $C\left[\overline{c}\langle S\rangle\right].Q$ 和现实上下文中的条件进程if $M=N$ then P else Q。理想上下文中的条件进程 if $M=N$ then P else $C\left[\overline{c}\langle S\rangle\right].Q$ 首先判断条件 $M=N$ 是否为真，如果为真，则执行 P 进程，否则执行 $C\left[\overline{c}\langle S\rangle\right].Q$ 进程；现实上下文中的条件进程 if $M=N$ then P else Q 首先判断条件 $M=N$ 是否为真，如果为真，则执行 P 进程，否则执行 Q 进程；消息输入进程 $u(x).P$ 准备从通道 u 接受消息，并将接收到的消息与 P 中的 x 绑定，然后执行 P 进程；消息输出进程 $\overline{u}\langle N\rangle.P$ 准备从通道 u 输出消息 N，然后执行 P 进程。闭进程 P 从通道 c 输出消息 M，当且仅当存在进程 P' 和 P''，使得 $P\left(\rightarrow\cup\equiv\right)^{*}\overline{c}\langle M\rangle.P'\mid P''$。

$P,Q,R::=$	进程
0	空进程
$P\mid Q$	并行进程
$!P$	复制进程
$vn.P$	限制名
if $M=N$ then P else Q	现实上下文中的条件进程
if $M=N$ then P else $C\left[\overline{c}\langle S\rangle\right].Q$	理想上下文中的条件进程
$u(x).P$	消息输入
$\overline{u}\langle N\rangle.P$	消息输出

图 2　扩展后的进程

3.4　进程上下文

进程上下文 C 是带洞([_])的进程表达式，如图 3 所示。if $M=N$ then C else Q 表示如果项 M 与项 N 匹配，那么执行进程上下文 C，则 C 是可验证上下文。if $M=N$ then P else C 表示如果项 M 与项 N 不匹配，那么执行进程上下文 C，则 C 是不可验证上下文。

$C::=$
- $[\,]$
- $P\mid C$
- $C\mid Q$
- $!C$
- $un.C$
- if $M=N$ then C else Q
- if $M=N$ then P else C
- $u(x).C$
- $\overline{u}\langle N\rangle.C$

图 3　进程上下文

4　定义和符号说明

定义 1　带注解 Alice-and-Bob 规范描述。

n 个形如 $A\rightarrow B:R_1^i,\mathrm{L},R_m^i\,\|\,M_i\,\|\,O_1^i,\mathrm{L},O_k^i$ 的申明组成协议的带注解 Alice-and-Bob 规范描述。协议由 n 条消息组成，一个申明对应着一条消息的产生与发送。其中，$i\in[1,n]$，A，B 是协议的参与者，M_i 是协议的第 i 个消息，R_1^i,L,R_m^i 是 A 执行的产生消息 M_i 的操作；O_1^i,L,O_k^i 是 B 收到消息 M_i 后执行的处理消息的操作。此定义借鉴了 Meadows[2]的思想。

令 $l=A\rightarrow B:R_1^l,\mathrm{L},R_m^l\,\|\,M_l\,\|\,O_1^l,\mathrm{L},O_k^l$ 为协议的带注解 Alice-and-Bob 规范描述的一个申明，$act_l(A)$ 为 A 在 l 上的操作集合，$act_l(A)\left[R_1^l,\mathrm{L},R_m^l,M_l\right]$ 表示 A 执行操作 R_1^l,L,R_m^l，并且在操作成功后发送消息 M_l 给 B。$act_l(B)\left[M_l,O_1^l,\mathrm{L},O_k^l\right]$ 表示 B 在收到消息 M_l 后，对 M_l 执行一系列操作 O_1^l,L,O_k^l，如果任何验证操作失败，则停止操作。

定义 2　消息 M_l 认证性。

如果 $l=A\rightarrow B:R_1^l,\mathrm{L},R_m^l\,\|\,M_l\,\|\,O_1^l,\mathrm{L},O_k^l$ 成功执行，则认为 B 收到了 A 发送的消息 M_l。如果 B 收到了消息 M_l，但是 A 没有执行 $act_l(A)\left[R_1^l,\mathrm{L},R_m^l,M_l\right]$ 操作，则认为 B 收到的消息 M_l 被篡改了。如果 B 收到的消息 M_l 被篡改并且 B 能够发现，则认为 B 收到的消息 M_l 是可认证的。

定义 3　操作一致性。

a 和 $ß$ 是一致的当且仅当 $act_i(A)\left[R_1^i,\mathrm{L},R_m^i,M_i\right]$ 中的 M_i 和 $act_j(B)\left[M_j,O_1^j,\mathrm{L},O_k^j\right]$ 中的 M_j 是完全相等的。其中，$i,j\in[1,n]$，$a\in act_i(A)\left[R_1^i,\mathrm{L},R_m^i,M_i\right]$，$b\in act_j(B)\left[M_j,O_1^j,\mathrm{L},O_k^j\right]$，$act_i(A)\left[R_1^i,\mathrm{L},R_m^i,M_i\right]$ 是 A 产生消息的操作集合，$act_j(B)\left[M_j,O_1^j,\mathrm{L},O_k^j\right]$ 是 B 处理消息的操作集合。

定义 4　g_1 逻辑先于 g_2。

R 为协议带注解 Alice-and-Bob 规范描述，S 为 R 中操作的集合。对于 S 中的任意操作 g_1 和 g_2，g_1 逻辑先于 g_2 当且仅当：

1) 如果 $g_1,g_2\in act_i(A)\left[R_1^i,\mathrm{L},R_m^i,M_i\right]$ 或者 $g_1,g_2\in act_j(B)\left[M_j,O_1^j,\mathrm{L},O_k^j\right]$，$i,j\in[1,n]$，并且 g_1 先于 g_2 发生；

2) 如果 $g_1 \in act_i(A)\left[R_1^i, \mathrm{L}, R_m^i, M_i\right]$，$g_2 \in act_j(B)\left[M_j, O_1^j, \mathrm{L}, O_k^j\right]$，$i, j \in [1,n]$，并且$g_1$与$g_2$是一致的；

3) 存在操作g_3，使得g_3逻辑先于g_2，g_1逻辑先于g_3。

定义 5　关联集合。

协议中的任意消息M_i和M_j的关联集合 ? 为$act_j(B)\left[M_j, O_1^j, \mathrm{L}, O_k^j\right]$中验证操作 v 的数据项集合 J 和 M_i 的数据项的集合 Y 的交集，即 ? =J n Y 。其中$i, j \in [1,n]$且$i < j$。

关联集合 ? 反映了消息之间互相影响的程度：? 为空集，消息之间互不影响，是独立的，关联度为零；? 包含的数据项越多，消息之间互相影响的程度就越高，关联度越高。

定义 6　抗拒绝服务攻击性。

P 为协议带注解 Alice-and-Bob 规范描述，B 具有抗拒绝服务攻击性，当且仅当 $Recv(B)$ 中的任意一对消息M_i和M_j的关联集合 ? 满足：

1) ? 是空集∅；

2) ? 中的每一个元素都是可认证的。

其中，$Recv(B)$ 为协议 P 中参与者 B 所有处理消息的操作按逻辑先于组成的集合，$i, j \in [1,n]$ 且 $i < j$。

如果协议 P 中任意一对消息M_i和M_j之间互不关联，那么处理这两条消息的下文是互相独立的，则 B 具有抗拒绝服务攻击性；如果消息M_i和M_j相关联，则对消息M_j的处理依赖于对消息M_i的处理，那么处理这 2 条消息的上下文是状态关联的，则消息M_i和M_j关联集合 ? 必须是可认证的才使 B 具有抗拒绝服务攻击性。

5　自动化证明抗拒绝服务攻击性方法

首先，应用扩展后的应用 PI 演算对协议带注解 Alice-and-Bob 规范描述进行精确的形式化建模。假设协议由 $2n$ 条消息组成，协议参加者为 Alice 和 Bob，Alice 分别发送消息$M_i \ i \in [1,n]$和接收消息$M_i' \ i \in [1,n]$，Bob 分别接收消息$M_i \ i \in [1,n]$和发送接收消息$M_i' \ i \in [1,n]$。协议进程 $PP \equiv n\hbar.(!Alice|!Bob)$ 是封闭进程，由任意的发起者进程 $Alice$ 和响应者进程 Bob 并行复合组成。根据扩展后的应用 PI 演算，进程 $Alice$ 和 Bob 可以经过一系列的规约到达如图 4 所示某一个进程。

$Alice, Bob(\to \cup \equiv)^* 0$	$Alice, Bob(\to \cup \equiv)^* !P$
$Alice, Bob(\to \cup \equiv)^* n\,n.P$	$Alice, Bob(\to \cup \equiv)^* P \mid P'$
$Alice, Bob(\to \cup \equiv)^* c(x).P$	$Alice, Bob(\to \cup \equiv)^* \overline{c}\langle N \rangle.P$
$Alice, Bob(\to \cup \equiv)^*$ if $M = N$ then P else Q	
$Alice, Bob(\to \cup \equiv)^*$ if $M = N$ then P else $C\left[\overline{c}\langle S \rangle\right].Q \quad c \notin \hbar$	

图 4　可达进程

为了应用 ProVerif 对 Bob 的抗拒绝服务攻击性进行形式化分析，需要对 Bob 收到的消息$M_i \ i \in [1,n-1]$进行形式化建模，如果攻击者能够从公开信道 c 上获得秘密 S，则攻击者可以通过对消息M_i进行攻击使协议产生拒绝服务攻击。

首先对消息M_1进行建模。如图 5 所示。在现实上下文中交换和处理消息M_1，在理想上下文中交换和处理消息$M_1', M_2, \mathrm{L}, M_n, M_n'$。协议进程 PP 为 $PP \equiv n\hbar.(!Alice_1 | !Bob_1)$，其中，$c_1, c$ 是公开信道，$c_i, i \in [2,n]$ 是 Bob 接收消息M_i的隐私通道，$Alice_1(\to \cup \equiv)^* C\left[\overline{c}\langle c_1 \rangle\right]\overline{c_1}\langle M_1 \rangle.Alice_2 \quad c \notin \hbar, c_1 \in \hbar$，$Bob_1(\to \cup \equiv)^* C\left[c(x)\right]x(m_1).Bob_2 \quad c \notin \hbar$，$Alice_i(\to \cup \equiv)^* C\left[\overline{c_i}\langle M_i \rangle\right]Alice_{i+1}, c_i \in \hbar, i \in [2,n-1]$，$Bob_i(\to \cup \equiv)^* C\left[c_i(m_i)\right]Bob_{i+1}, c_i \in \hbar, i \in [2,n-1]$。如果攻击者能够从公开信道 c 上获得秘密 S，则攻击者可以通过对消息M_1进行攻击使协议产生拒绝服务攻击。

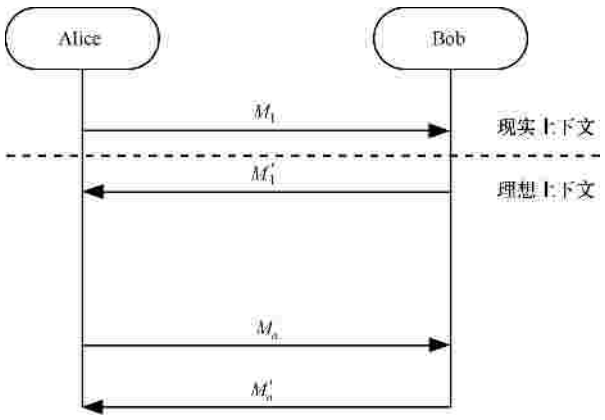

图 5　消息 M_1 的形式化模型

采用类似的方法对消息$M_i, i \in [2,n-1]$分别建立如图 6 所示的模型。在现实上下文中交换和处理消息M_i，在理想上下文中交换和处理消息$M_1, M_1', \mathrm{L}, M_{i-1}, M_{i-1}', M_i, M_{i+1}, M_{i+1}', \mathrm{L}, M_n, M_n'$。协议进程 PP

为 $PP \equiv n\hbar.(!Alice_i \mid !Bob_i)$，其中，$c_i, i \in [2, n-1]$，$c$ 是公开信道，$c_j, j \in [2, n-1] \cap j \neq i$ 是 Bob 接收消息 M_i 的隐私通道，$Alice_i\ (\to \cup \equiv)^* C[\overline{c}\langle c_i \rangle]\overline{c}_i\langle M_i \rangle.Alice_{i+1}$　$c \notin \hbar, c_i \in \hbar$，$Bob_i\ (\to \cup \equiv)^* C[c(x)]x(m_i).Bob_{i+1}$　$c \notin \hbar$　$Alice_j\ (\to \cup \equiv)^* C[\overline{c}_j\langle M_j \rangle]Alice_{j+1}$，$c_j \in \hbar$，$j \in [1, n-1] \mid j \neq i$，$Bob_j\ (\to \cup \equiv)^* C[c_j(m_j)]Bob_{j+1}, c_j \in \hbar, j \in [1, n-1] \mid j \neq i$。如果攻击者能够从公开信道 c 上获得秘密 S，则攻击者可以通过对消息 M_i 进行攻击使协议产生拒绝服务攻击。

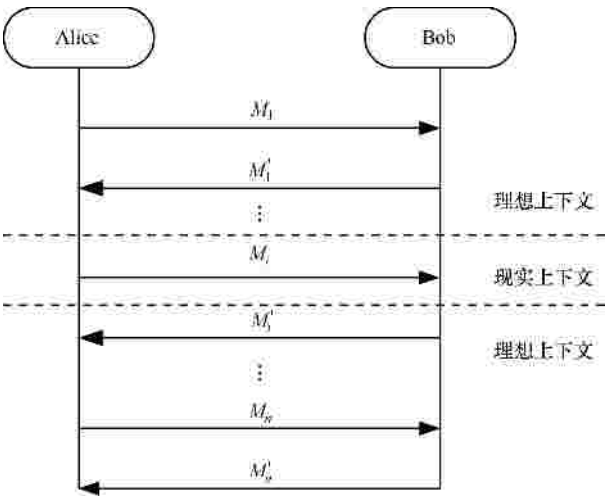

图 6　消息 M_i 的形式化模型

定理　抗拒绝服务攻击性。协议进程 PP 的响应者 Bob 具有抗拒绝服务攻击性当且仅当对 Bob 收到的所有消息 $M_i, i \in [1, n]$ 的形式化模型，PP 都不能从公共通道 c 输出秘密消息 S，即不存在进程 P'，P'' 和攻击者进程 $Attacker$，使得 $(PP \mid Attacker)(\to \cup \equiv)^* \overline{c}\langle S \rangle.P' \mid P'', c \notin \hbar, S \in \hbar$。

证明

Bob 具有抗拒绝服务攻击性，依据定义 6，$\forall M_i, M_j \in Recv(Bob)$，$i, j \in [1, n]$，$M_i$ 逻辑先于 M_j，验证操作 v 是进程 if $M = N$ then P else $C[\overline{c}\langle S \rangle].Q \in act(Bob)[M_j]$，则对消息 M_i 的形式化模型：

1) $w = \varnothing$ 即在协议规范描述中 $M = N$ 的值与消息 M_i 无关，那么不论在理想上下文还是现实上下文中交换 M_i，$M = N$ 的值恒为真，协议进程 $PP\ (\to \cup \equiv)^* P$；

2) $w = \{\hbar\}$，其中，$\hbar$ 是可认证项，即攻击者无法成功篡改 $\hbar$ 的值，那么不论在理想上下文还是现实上下文中交换 M_i，$M = N$ 的值恒为真，协议进程 $PP\ (\to \cup \equiv)^* P$。

所以，对响应者 Bob 收到的所有消息 $M_i, i \in [1, n]$ 的形式化模型，PP 都不能从公共通道 c 输出秘密消息 S。

如果对于响应者 Bob 收到的消息 $M_i, i \in [1, n]$ 的形式化模型，PP 能从公共通道 c 输出秘密消息 S，即存在进程 P'，P'' 和攻击者进程 $Attacker$，使得 $(PP \mid Attacker)(\to \cup \equiv)^* \overline{c}\langle S \rangle.P' \mid P'', c \notin \hbar$，则攻击者 $Attacker$ 可以通过篡改与 v 关联的逻辑先于 M_j 的消息，使 $M = N$ 的值为假。那么关联集合 w 存在不可认证项 $\hbar'$，所以协议进程 PP 的响应者 Bob 不具备防止拒绝服务攻击性。　　证毕。

由定理可知如果攻击者能够获得秘密消息 S，那么它能够构造一个拒绝服务攻击：在不影响其他消息正常交互的情况下，篡改消息 M_i 的内容并使其不被接收者察觉，产生拒绝服务攻击。

至此，可以使用扩展后的应用 PI 演算对抗拒绝服务攻击进行形式化描述，基于给出的定理，应用 ProVeif 自动化证明协议的抗拒绝服务攻击性。

6　一阶定理证明器 ProVerif

ProVerif[3]是 Blanchet 开发的基于重写逼近的一阶定理证明器。它基于 Prolog 语言，能够分析与验证使用 Horn 子句、应用 PI 演算及本文提出的扩展的应用 PI 演算描述的安全协议的安全性。同时，它克服了模型检测方法固有的缺陷－状态空间爆炸问题，能够处理无穷状态系统。ProVerif 已经成功分析了很多复杂的安全协议，如电子商务协议[4]、网络投票协议[5,6]等。

ProVerif 的体系结构如图 7 所示，由协议输入、处理和输出 3 部分组成。协议输入部分主要包括安全协议形式化描述和安全属性的形式化定义。ProVerif 对输入的协议形式化描述进行初始处理，主要是语法检查。输入语言为应用 PI 演算、Horn 子句或者本文提出的扩展的应用 PI 演算。

处理部分负责根据安全协议的形式化描述对要证明的安全属性进行逻辑推导证明。它包括自动翻译模块和逻辑推导模块。当输入语言为应用 PI 演算或本文提出的扩展的应用 PI 演算时，自动翻译模块主要负责实现安全协议的应用 PI 演算或本文

提出的扩展的应用 PI 演算形式化描述到一阶逻辑规则的转换，逻辑推导模块则基于一阶逻辑规则对要证明的安全属性进行推理和验证。当输入语言为 Horn 子句时，处理部分为逻辑推导模块，不需要自动翻译模块。

结果输出部分主要负责输出处理结果。从输出结果可以得知该协议是否满足相应的安全属性，供用户进一步分析，但是 ProVerif 不输出详细的证明过程。如果不满足某安全属性，则 ProVerif 会给出详细的攻击方式。

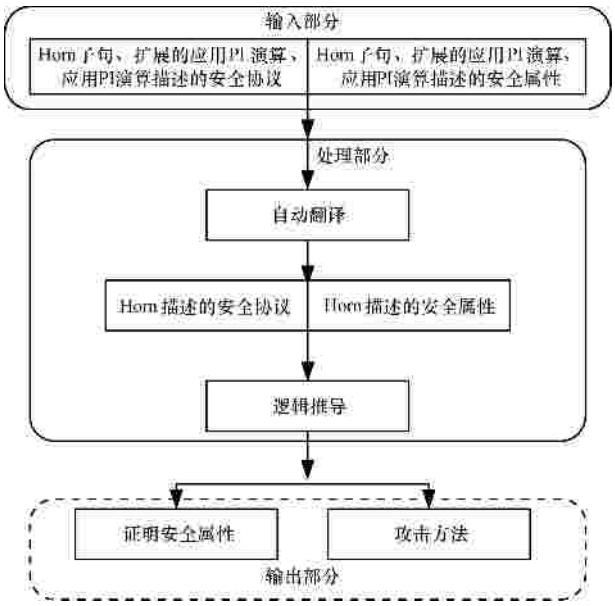

图 7 ProVerif 结构

7 JFK 与 IEEE 802.11 四步握手协议抗拒绝服务攻击性

7.1 JFK 协议

JFK(just fast keying)协议是一个密钥交换协议，主要有 JFKr 和 JFKi 2 个版本，主要区别是对协议双方提供不同的身份保护。JFKr 基于 Sign-and-MAC 协议[20]，能够在有主动攻击者的环境中保护响应者的身份，在被动攻击者的环境中保护发起者的身份。JFKi 基于 ISO 9798-3 密钥交换协议[21]，能够在有主动攻击者的环境中保护发起者的身份。Abadi 和 Blanchet[7]应用应用 PI 演算分析了对 JFKr 协议的秘密性、认证性、可否认性，同时用手工的方式分析了 JFKr 抗拒绝服务攻击性，指出 JFKr 协议可以抵抗拒绝服务攻击。Aiello 等学者[22,23]采用非形式化的方法分析了 JFK 协议的安全性。这里主要应用提出的自动化抗拒绝服务攻击方法分析 JFKr 协议的抗拒绝服务攻击性。

JFKr 协议涉及 2 个角色：协议的发起者 Alice 和协议的响应者 Bob。攻击者建模为 Dolev-Yao 模型中的攻击者，既可以在公开信道上监听、拦截、修改，删除和插入消息，又可以伪装成诚实的参与者。

JFKr 协议的 Alice-and-Bob 规范描述如图 8 所示，符号说明见文献[17]。

消息1： $Alice \rightarrow Bob : N_{\text{Alice}}, x_{\text{Alice}}$

消息2： $Bob \rightarrow Alice : N_{\text{Alice}}, N_{\text{Bob}}, x_{\text{Bob}}, g_{\text{Bob}}, t_{\text{Bob}}$

消息3： $Alice \rightarrow Bob : N_{\text{Alice}}, N_{\text{Bob}}, x_{\text{Alice}}, x_{\text{Bob}}, t_{\text{Bob}}, e_{\text{Alice}}, h_{\text{Alice}}$

消息4： $Bob \rightarrow Alice : e_{\text{Bob}}, h_{\text{Bob}}$

图 8 JFKr 协议的 Alice-and-Bob 规范描述

JFKr 协议有 4 条消息组成，消息 1 和消息 2 通过 Diffie-Hellman 密钥交换协议建立共享密钥。首先 Alice 生成公钥 x_{Alice} 和随机数 N_{Alice}，发送给 Bob。Bob 生成公钥 x_{Bob}、随机数 N_{Bob}，认证 cookie t_{Bob}。t_{Bob} 是状态信息 $(x_{\text{Bob}}, N_{\text{Bob}}, N_{\text{Alice}})$ 的 MAC 值。$(x_{\text{Bob}}, N_{\text{Bob}}, N_{\text{Alice}})$ 是 Bob 成功收到消息 1 准备发送消息 2 时的自己环境状态。消息 3 和消息 4 提供认证性。消息 3 和消息 4 包含加密随机数、Diffie-Hellman 指数及其他信息的签名。Alice 生成消息 3 发送给 Bob，Bob 验证消息 3 中状态信息的 MAC 值 t_{Bob} 的正确性。如果验证成功，Bob 用 $(ID_{\text{Bob}}, sa_{\text{Bob}}, s_{\text{Bob}})$ 及 K_e 生成加密后的身份标识 e_{Bob} 及其 MAC 值 h_{Bob} 组成消息 4 发送给 Alice。

基于提出的抗拒绝服务攻击性自动化证明方法，应用扩展的应用 PI 演算对 JFKr 协议响应者 Bob 收到的消息 1 进行建模，然后转换成 ProVerif 的输入语言，最后应用 ProVerif 对 JFKr 协议进行分析。由于空间的限制，只给出了 ProVerif 的分析结果，如图 9 所示。图 9 表明公开通道 c 没有输出秘密信息 dos。

图 9 JFKr 的 ProVerif 输出结果

根据消息 1 形式化模型，得知 Bob 处理收到的消息 1 和消息 3 的操作是 $Recv(Bob)\{act(Bob)\left[M_1, O_1^1, \text{L}, O_i^1, \text{L}, O_n^1\right], act(Bob)\left[M_3, R_1^3, \text{L}, R_i^3, \text{L}, R_k^3\right]\}$。验证操作 v 是对 $t_{\text{Bob}} = H\{K_{\text{Bob}}\}(x_{\text{Bob}}, N_{\text{Bob}}, N_{\text{Alice}})$ 的验证，其中，$(x_{\text{Bob}}, N_{\text{Bob}}, N_{\text{Alice}}) \notin M_1$。所以消息 1

和消息 3 的关联集合 ? 为空集。这和 ProVerif 在公开通道 c 的输出是一致的。由定义 6 可知 JFKr 中的响应者 Bob 能够防止拒绝服务攻击。

7.2　IEEE 802.11 i 四步握手协议

IEEE 802.11 标准是无线局域网中广泛采用的标准。由于 IEEE 802.11 标准被证明在实体认证和有线等价保密方面是不安全的，IEEE 802.11i 标准[21]被提出来增强 IEEE 802.11 的安全性。IEEE 802.11i 除了引入了新的密钥管理和生成算法，还改进了加密和认证算法。它定义了一个基于 IEEE 802.1X 认证和 4 步握手的强安全网络关联。Bicakcia 与 Tavli[24]对 IEEE 802.11 的拒绝服务攻击与防范措施进行了深入研究。

四步握手协议简化了的 Alice-and-Bob 规范描述如图 10 所示。

消息M_1：	$Alice \to Bob: Anonce, m_1$
消息M_2：	$Bob \to Alice: Snonce, m_2, MIC_2$
消息M_3：	$Alice \to Bob: Anonce, m_3, MIC_3$
消息M_4：	$Bob \to Alice: m_4, MIC_4$

图 10　四步握手协议的 Alice-and-Bob 规范描述

其中， $Anonce$ 和 $Snonce$ 分别为认证者 Alice 和请求者 Bob 生成的随机数，它用来生成 PTK（Pairwise Transient Key）。m_1、m_2、m_3、m_4 分别为不同的消息，其中，m_1、m_2、m_3、m_4 都包含有重放计数值 $Replay\_Counter$ 。$MIC_2 = MIC(Snonce, m_2)$，$MIC_3 = MIC(Anonce, m_3)$，$MIC_4 = MIC(m_4)$， MIC（message integrity code）值为消息完整性码。

四步握手协议运行过程如下：首先认证者 Alice 首先发送消息 M_1 给请求者 Bob，请求者 Bob 收到消息 M_1 后，首先验证重放计数值 $Replay\_Counter$ 的有效性，验证通过则产生一个随机数 $Snonce$，然后应用伪随机函数 PRF(pseudo random functions)生成临时密钥 PTK。伪随机函数 PRF 输入为 $Anonce$、$Snonce$ 与其他信息。请求者 Bob 生成 MIC 值，把消息 M_2 发送给认证者 Alice。认证者 Alice 收到消息 M_2 后，计算临时密钥 PTK 值，验证 M_2 中的 MIC 值，生成消息 M_3 给请求者 Bob。请求者 Bob 收到消息 M_3 对 MIC 值进行验证，如果成功，生成并发送消息 M_4 给认证者 Alice，安装 PTK。认证者 Alice 在收到 M_4 后对 MIC 值进行验证，如果验证成功，安装 PTK。至此四步握手结束，产生并安装 PTK。

应用提出的自动化抗拒绝服务攻击性证明方法，ProVerif 给出了两个拒绝服务攻击：拒绝服务攻击 1，如图 11 和图 12 所示。拒绝服务攻击 2，如图 13 和图 14 所示。其中拒绝服务攻击 2 是应用我们提出的方法发现的。。

根据四步握手协议规范，由于请求者 Bob 对消息 M_3 的验证依赖于临时密钥 PTK，而临时密钥 PTK 的生成取决于 $Anonce$ 和 $Snonce$， $Snonce$ 的产生又依赖于对消息 M_1 的重放计数值 $Replay\_Counter$ 的有效性验证，所以攻击者只要成功篡改或重放 $Anonce$ 与计数值 $Replay\_Counter$，就可以使请求者 Bob 对合法的消息 M_3 的验证失败，从而产生拒绝服务攻击。

根据消息 M_1 形式化模型，请求者 Bob 处理消息 M_1 和消息 M_3 的操作 $Recv(Bob)\{act(Bob)[M_1, O_1^1, \text{L}, O_i^1, \text{L}, O_n^1], act(Bob)[M_3, R_1^3, \text{L}, R_i^3, \text{L}, R_k^3]\}$。其中，$v$ 是 $MIC_3 = H\{KCK\}(Anonce^3, m_3)$ 验证操作，$KCK = \{Anonce^1, Snonce, MSK\}$， $M_1 = \{Anonce^1, m_1\}$，$M_3 = \{Anonce^3, m_3, MIC_3\}$。所以 M_1 和 M_3 的关联集合 $w = \{Anonce^1\}$。由于四步握手协议没有对 $Anonce^1$ 进行验证，$Anonce^1$ 是不可认证的，由定义 6 可知四步握手协议中的请求者 Bob 不能防止拒绝服务攻击。

拒绝服务攻击 1，如图 11 和图 12 所示。图 11 表明公开通道 c 输出秘密信息 S 。ProVerif 构造的拒绝服务攻击 1 如图 12 所示：在协议的一次运行中，请求者 Bob 收到消息 M_3 前，攻击者伪造一个随机数 $Anonce'$ 和重放计数值 $Replay\_Counter'$（使 $Replay\_Counter'$ 的值为有效值），并生成消息 M_1 发送给请求者 Bob，根据四步握手协议规范，请求者 Bob 重新生成 PTK，此时 Bob 收到合法的消息 M_3，

```
Could not find a trace corresponding to this derivation.
RESULT not attacker:dos[] cannot be proved.
```

图 11　针对拒绝服务攻击 1 的 ProVerif 输出

消息M_1：　$Alice \to Bob: Anonce, m_1$

消息M_2：　$Bob \to Alice: Snonce, m_2, MIC_2$

消息M'_1：$adversary \to Bob: \{Anonce', m'_1\}$

消息M_3：　$Alice \to Bob: Anonce, m_3, MIC_3$

$MIC(Anonce, m_3) \neq MIC_3$

消息M_4：　$Bob \to Alice: m_4, MIC_4$

图 12　ProVerif 输出的拒绝服务攻击 1

将不能通过对 MIC 值验证。根据四步握手协议规范，认证者 Alice 在将重新发送 M_3，但仍然不能通过验证，n 次这样的验证后，认证者 Alice 将和请求者 Bob 重新开始认证。从而产生拒绝服务攻击。

拒绝服务攻击 2，如图 13 和图 14 所示。图 13 表明公开通道 c 输出秘密信息 S。ProVerif 构造的拒绝服务攻击 2 如图 14 所示。拒绝服务攻击 2 与拒绝服务攻击 1 基本上是相同的，区别是攻击者只伪造重放计数值 $Replay\_Counter'$，使 $Replay_Counter'$的值为有效值。

```
Could not find a trace corresponding to this derivation.
RESULT not attacker:dos[] cannot be proved.
```

图 13　针对拒绝服务攻击 2 的 ProVerif 输出

消息M_1：　$Alice \rightarrow Bob : Anonce, m_1$

消息M_2：　$Bob \rightarrow Alice : Snonce, m_2, MIC_2$

消息M'_1：$adversary \rightarrow Bob : \{Anonce, m'_1\}$

消息M_3：　$Alice \rightarrow Bob : Anonce, m_3, MIC_3$

$MIC(Anonce, m_3) \neq MIC_3$

消息M_4：　$Bob \rightarrow Alice : m_4, MIC_4$

图 14　ProVerif 输出的拒绝服务攻击 2

针对拒绝服务攻击 1，He[25]提出请求者 Bob 除了存储 PTK，另外为每一个消息 M_1 存储一个 TPTK(temporary PTK)，在收到消息 M_1 时，仅更新 TPTK，在收到正确的消息 M_3 时才更新 PTK。但是，当攻击者大量发送伪造的消息 M_1 时，Bob 就会存储大量的 TPTK，产生存储资源消耗型的拒绝服务攻击。

基于以上分析，为了防止拒绝服务攻击 1 和 2，我们认为使消息 M_1 可认证即可。具体方案是应用认证者 Alice 的签名密钥对 M_1 进行签名或使用 MSK 对 M_1 进行加密。这样就使消息 1 是可认证的，来防止拒绝服务攻击 1 和 2。在通过认证以后再分配资源。

如果只防止拒绝服务攻击 2，那么请求者 Bob 可以存储其在一定时间内收到的 *Anonce*，并且在进行下一步处理前，检查 *Anonce* 是否是在一定时间内是重放的，则可以防止这种攻击。

8　结束语

拒绝服务攻击具有威害巨大及难以有效防御的特点，受到网络安全专家与用户的重点关注。形式化方法是分析协议安全性强有力的工具。本文没有遵循 Yu-Gligor 形式化建模方法和 Meadows 形式化建模方法，而是从协议状态的角度，应用形式化方法对拒绝服务攻击性进行建模。首先从攻击者上下文与进程表达式 2 个方面对标准应用 PI 演算进行扩展，然后应用扩展后的应用 PI 演算对协议的抗拒绝服务攻击性进行建模，提出了一个基于定理证明的支持一阶定理证明器 ProVerif 的抗拒绝服务攻击性自动化证明方法，最后应用 ProVerif 分析与验证了 JFK 协议与 IEEE 802.11 四步握手协议抗拒绝服务攻击性，证明 JFK 协议能够抵抗拒绝服务攻击，而 IEEE 802.11 四步握手协议的确存在拒绝服务攻击，同时也发现了 IEEE 802.11 四步握手协议的一个新的拒绝服务攻击。针对 IEEE 802.11 四步握手协议存在的攻击提出了 2 种改进方法。由于提出的抗拒绝服务攻击性自动化证明方法主要从协议状态来分析协议抗拒绝服务攻击性，因此既可以分析利用协议状态的保持产生的资源消耗型拒绝服务攻击，又可以分析协议中止型拒绝服务攻击，但是在分析由其他原因产生的存储资源消耗型的拒绝服务攻击方面还有欠缺，可以作为下一步的工作方向。同时在未来的工作中，计划应用提出的基于定理证明的支持一阶定理证明器 ProVerif 的抗拒绝服务攻击性自动化证明方法对复杂的电子商务、电子投票协议的抗拒绝服务攻击性进行深入的研究，验证其抗拒绝服务攻击性。

参考文献：

[1] YU C，GLIGOR V. A formal specification and verification method for the prevention of denial of service[J]. IEEE Transactions on Software Engineering, 1990, 16(6):581-592.

[2] MEADOWS C. A cost-based framework for analysis of denial of service networks[J]. Journal of Computer Security, 2001, 9(1/2):143-164.

[3] BLANCHET B. An efficient cryptographic protocol verifier based on prolog rules[A]. Proc of the 14th IEEE Workshop on Computer Security Foundations Workshop (CSFW)[C]. Cape Breton, Nova Scotia, Canada, 2001.82-96.

[4] 郭云川, 丁丽, 周渊等. 基于 ProVerif 的电子商务协议分析[J]. 通信学报,2009,30(3):125-129.
GUO Y C, DING L, ZHOU Y, *et al*. E-commerce protocol analysis based on ProVerif[J]. Journal on Communications, 2009, 30(3): 125-129.

[5] MENG B, HUANG W, LI Z M, *et al*. Automatic verification of security properties in remote Internet voting protocol with applied pi cal-

culus[J]. International Journal of Digital Content Technology and its Applications, 2010, 4(7):88-107.

[6] MENG B. Refinement of mechanized proof of security properties of remote Internet voting protocol in applied PI calculus with ProVerif[J]. Information Technology Journal, 2011, 10(2):293-334.

[7] ABADI M, BLANCHET B, FOURNET C. Just fast keying in the pi calculus[J]. ACM Transactions on Information and System Security, 2007, 10(3):1-59.

[8] ABADI M, FOURNET C. Mobile values, new names, and secure communication[A]. Proc of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)[C]. London, UK, 2001.104-115.

[9] MILLEN J K. A resource allocation model for denial of service protection[J]. Journal of Computer Security, 1993, 2(2-3):89-106.

[10] CUPPENS F, SAUREL C. Towards a formalization of availability and denial of service[A]. Proc of Information Systems Technology Panel Symposium on Protecting Nato Information Systems in the 21st Century[C]. Washington, 1999.

[11] RAMACHANDRAN V. Analyzing DoS-Resistance of Protocols Using a Cost-based Framework[R]. Technical Report DCS/TR-1239, Yale University, 2002.

[12] SMITH J,GONZALEZ-NIETO J M,BOYD C. Modelling denial of service attacks on JFK with Meadows's cost-based framework[A]. Proc of the 2006 Australasian Workshops on Grid Computing and E-Research (ACSW Frontiers)[C]. Darlinghurst, Australia, 2006. 125-134.

[13] GROZA B, MINEA M. Formal modelling and automatic detection of resource exhaustion attacks[A]. Proc of 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS)[C]. HongKong,China, 2011.

[14] LAFRANCE S, MULLINS J. Using admissible interference to detect denial of service vulnerabilities[A]. Proc of the Sixth International Workshop in Formal Methods (IWFM)[C]. Ireland, 2003.

[15] 周世健, 蒋睿, 杨晓辉. 安全协议DoS 攻击的形式化分析方法研究[J].中国电子科学研究院学报.2008, 3(6):592-598.
ZHOU S J, JING R, YANG X H. DoS attacks on security protocols of the formal analysis[J]. Journal of Research Institute of China Electronics, 2008, 3(6):592-598.

[16] TRITILANUNT S,BOYD C,FOO E, *et al*. Cost-based and time-based analysis of DoS-resistance in HIP[A]. Proc of the Thirtieth Australasian Conference on Computer Science (ACSC '07)[C]. Darlinghurst, Australia, 2007.191-200.

[17] TRITILANUNT S. Protocol Engineering for Protection Against Denial of Service Attacks[D]. Brisbane Australia, Queensland University of Technology, 2009.

[18] AGHA G, GREENW ALD M, GUNTER C A, *et al*. Formal modeling and analysis of DoS using probabilistic rewrite theories[A]. Proc of International Workshop on Foundations of Computer Security (FCS)[C].Chicago IL,2005.

[19] MAHIMKAR A, SHMATIKOV V. Game-based analysis of denial-of-service prevention protocols[A]. Proc of the 18th IEEE workshop on Computer Security Foundations (CSFW)[C]. Aix-en-Provence, France, 2005.287-301.

[20] KRAWCZYK H. Invited talk, SIGMA: the SIGn-and-MAc approach to authenticated diffie Hellman and its use in the IKE protocols[A]. Proc of the 23rd Annual International Cryptology Conference (CRYPTO)[C]. Santa Barbara, California, USA, 2003.400-425.

[21] CANETTI R , KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[A]. Proc of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT)[C]. Innsbruck, Austria, 2001.453-474.

[22] AIELLO W, BELLOVIN S M, BLAZE M, *et al*. Efficient, DoS-resistant, secure key exchange for Internet protocols[A]. Proc of the 9th ACM Conference on Computer and Communications Security (CCS)[C]. Washington, DC, USA, 2002.48-58.

[23] AIELLO W, BELLOVIN S M, BLAZE M, *et al*. Just fast keying: key agreement in a hostile internet[J]. ACM Transactions on Information and System Security, 2004, 7(2):242-273.

[24] BICAKCIA K, TAVLI B. Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks[J].Computer Standards & Interfaces, 2009, 31(5):931-941.

[25] HE C, MITCHELL J C. Analysis of the 802.11i 4-way handshake[A]. Proc of the 3rd ACM Workshop on Wireless Security (WiSe '04)[C]. ACM, New York, NY, USA, 2004.43-50.

作者简介：

孟博（1974-），男，河北行唐人，中南民族大学副教授、硕士生导师，主要研究方向为安全体系结构与协议、软件验证。

黄伟（1983-），男，湖北咸宁人，硕士，中南民族大学助教，主要研究方向为安全体系结构与协议、软件验证。

王德军（1974-），男，湖北钟祥人，博士，中南民族大学讲师，主要研究方向为安全体系结构与协议、网络安全、容灾备份和分布式系统。

邵飞（1986-），男，山东济宁人，中南民族大学博士生，主要研究方向为安全体系结构与协议、软件工程。