doi: 10.3969/j.issn.0490-6756.2018.05.013

安全协议抗 DoS 攻击的形式化分析研究

高 强[1], 林星辰[1], 林宏刚[2], 金大鹏[2]
(1. 国家计算机网络应急技术处理协调中心,北京 100029; 2. 成都信息工程大学信息安全工程学院,成都 610225)

摘 要: 随着拒绝服务攻击给协议的可用性带来的危害越来越大,需要行之有效的方法对安全协议的抗 DoS 性进行分析. 但是目前对安全协议的抗 DoS 性进行分析的方法模型都存在一些缺陷,有的只能分析部分的 DoS 攻击,有的只关注协议各方计算资源的消耗,而忽略了存储资源消耗. 针对以上不足,本文对基本的串空间模型进行扩展,引入消息相关度集合和代价函数,提出了一种分析安全协议抗 DoS 性的新方法,并利用该方法,对 JFK 协议的抗 DoS 性进行了详细分析.

关键词: 安全协议; 拒绝服务攻击; 扩展串空间模型
中图分类号: TP393.08 **文献标识码**: A **文章编号**: 0490-6756(2018)06-1211-08

A formal analysis for security protocol against DoS attacks

GAO Qiang[1], *LIN Xing-Chen*[1], *LIN Hong-Gang*[2], *JIN Da-Peng*[2]
(1. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China;
2. College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: As DoS attacks lead to an increasing risk to the availability of protocol, Some effective methods are required to analyze the anti-DoS performance of security protocols. However, the current proposed methods for analyzing the anti-DoS performance of security protocols have some shortcomings, some can only analyze a part of DoS attacks, and some only focus on the agreement of computing resources consumption, while ignoring the consumption of storage resources. In view of the above deficiencies, this paper extends the strand space model with introducing the message correlation set and the cost function, and proposes a new method to analyze the anti-DoS performance of the security protocol. Detailed anti-DoS performance analysis is presented for the JFK protocol by the new proposed method in the paper.

Keywords: Security protocols; Denial of Service Attacks; Extended strand space model

1 引 言

拒绝服务(Denial of Service, DoS)攻击是一种常见的网络攻击方式,是通过各种手段,达到使得提供服务的主机不能提供正常服务的目的. 随着 DoS 攻击带来的危害越来越大,因此,如何实时检测和有效减轻 DoS 攻击成为近年来重要的研究领域之一. 在实时检测方面,Saied[1] 等用不断更新学习样本方式提高对未知类型的 DoS 攻击检测率. 杨可心等[2] 提出基于 BP 神经网络的方法能有效提高 DDoS(Distributed Denial of Service, DDoS)攻击检测率;在有效减轻 DoS 攻击方面,刘江等[3]

收稿日期: 2017-04-12
基金项目: 四川省科技厅重点研发项目(2017GZ0319)
作者简介: 高强(1984—), 男, 工程师, 研究方向为信息安全. E-mail: gaoqiang@cert.org.cn
通讯作者: 林宏刚. E-mail: linhg@cuit.edu.cn

提出一种基于改进 DHCP 协议的地址跳变方法，增加了攻击者进行拒绝服务攻击的难度；Meadows[4-6]提出的基于代价的形式化分析方法，适合对资源消耗型 DoS 攻击进行建模，该建模方法通过设置容忍关系，比较产生一个数据和验证这个数据所要花费的代价大小，判断协议是否存在 DoS 攻击；基于 Meadows 的形式化分析模型，Minea 与 Groza 分析了 JFK 与 STS 协议[7]，指出 JFK 协议能够抵抗 DoS 攻击，而 STS 协议不具有抗 DoS 攻击能力；基于时态逻辑，Yu 和 Gligor 引入用户合约，提出一种对共享服务 DoS 攻击的形式化规范与验证方法[8]，该方法的核心思想是以访问控制策略为基础，对 DoS 攻击进行建模，所以不能够处理发生在认证之前的 DoS 攻击；周世健等学者[9]，在基本串空间的基础上[10-12]，进行了扩展，提出了判断安全协议 DoS 攻击分析的两条检验规则，并利用这两条规则，分析了 IEEE802.11i 四步握手协议，发现其存在的 DoS 攻击，并针对此提出了改进办法，这些规则是基于代价，能够较好的分析资源消耗型 DoS 攻击，但是对服务中止型 DoS 攻击却无能为力. 孟博等学者[13]，从进程表达式和攻击者上下文两个方面扩展了标准应用 PI 演算，并且从协议状态的角度，建立安全协议抗 DoS 攻击分析模型，并验证了模型的有效性. 由于该方法主要是从协议状态的角度来分析抗 DoS 攻击性，因此可以分析由于协议的状态保持而产生的资源消耗型 DoS 攻击，以及服务中止型 DoS 攻击，但是在分析其他原因产生的资源消耗型 DoS 攻击时还存在不足. 常静等[14]利用改进的 Meadows 模型方法，对 JFKi 协议的抗 DoS 攻击能力进行了分析，但分析过程中，仅仅对协议双方的资源代价进行了比较，是对资消耗型 DoS 攻击的分析，并未提及服务中止型 DoS 攻击. 本文提出的基于扩展串空间模型的协议抗 DoS 攻击的形式化分析方法，不仅分析了 JFKi 协议抗资源消耗型 DoS 攻击的能力，而且分析了抗服务中止型 DoS 攻击的能力，比其他分析方法更加准确与全面.

2 安全协议抗 DoS 攻击的形式化分析模型

2.1 串空间模型简介

串指的是协议运行到某个时刻，某个主体所产生行为的一个消息序列，包含发送和接收的消息序列，串可以用来表示代表安全协议中合法主体以及非法的攻击者的行为. 串空间是协议运行当中所有可能出现的诚实参与者以及攻击者的串的集合. 串空间模型中，各种事件之间的关系可以用图结构来表示，具有简洁，直观的特点. 在串空间模型中，可以用各个串之间的连接关系来表示协议的正确性. 接下来首先介绍串空间模型的基本概念.

设集合 A 中的元素为参与协议的主体之间交换的消息，则称 A 是项集合，称 A 的元素为项. 集合 A 是由两个原子项集合 T 和 K 进行连接、加密、求逆三种运算得到的，其中 T 是原子消息集合，K 是密钥集合. 由 T 和 K 构造集合 A 的三种运算定义如下.

join：$A\times A\rightarrow A, t_1\in A, t_2\in A$，则 $t_1t_2\in A$.

encr：$K\times A\rightarrow A, t\in A, k\in K$，则 $\{t\}_k\in A$.

inv：$K\rightarrow K, k\in K$，则 $inv(k)=k^{-1}\in K$.

在安全协议的串空间模型证明中，经常用到下面的自由假设.

假设 $m_1, m_2, m_3, m_4\in A, k_1, k_2\in K$，则有：

(1) 自由连接：$m_1m_2=m_3m_4$，则有：$m_1=m_3\wedge m_2=m_4$.

(2) 自由加密：如果 $\{m_1\}_{k_1}=\{m_2\}_{k_2}$，则有：$m_1=m_2\wedge k_1=k_2$.

(3) 连接加密互斥：$m_1m_2\neq\{m_3\}_{k_1}$.

(4) 原子不可分割：$m_1m_2\notin \mathrm{T}\cup\mathrm{K}$，$\{m_1\}_{k_1}\notin \mathrm{T}\cup\mathrm{K}$.

子项是项的概念中最重要的关系，子项记为符号 $\sqsubset$. $t_0\sqsubset t_1$ 表示 t_0 是 t_1 的子项.

定义 1 子项的递归定义：

(1) $a\sqsubset a$；

(2) $a\sqsubset\{g\}_K$，如果 $a\sqsubset g$；

(3) $a\sqsubset gh$，如果 $a\sqsubset g\vee a\sqsubset h$；

在安全协议中，项既可以被主体接收，也可以由主体发送.

定义 2 集合 $\{+,-\}$ 是串空间的动作集，其中发送消息用“+”表示，接收消息用“-”表示.

定义 3 二元组 $\langle\sigma,a\rangle$ 表示一个事件，其中 $\sigma\in\{+,-\}$，$a\in A$. 用 $+a$ 和 $-a$ 代表一个事件，$+a$ 和 $-a$ 称为带符号的消息. $(\pm A)^*$ 为带符号项的有限序列集合.

定义 4 串是协议参与者所执行事件的序列，令 $\sum$ 表示串的集合，定义迹映射 tr：$\sum\rightarrow(\pm A)^*$，将一个串映射到有限消息序列的集合.

定义 5 串空间的其他基本概念：

(1) 结点,假设串 $s \in \sum$,s 中的每个事件称为串s的一个结点,用$n=\langle s,i\rangle$表示,其中i是结点n在串中序号. 结点 n 属于串 s,记为 $n \in s$,结点的集合记为 N.

(2) 结点 $n=\langle s,i\rangle \in s$,定义 $\mathrm{index}(n)=i$,$\mathrm{strand}(n)=s$,若结点 n 代表的实体动作为$(tr(s))_i=\sigma a$,定义 $\mathrm{term}(n)=\sigma a$,$\mathrm{uns\_term}(n)=((tr(s))_i)_2=a$,$\mathrm{sign}(n)=\sigma$,称 term 为结点事件函数,uns_term 为结点消息函数,sign 为结点符号函数.

(3) 结点 $n_1,n_2 \in N$,存在一个边 $n_1 \rightarrow n_2$,当且仅当 $\mathrm{term}(n_1)=+a$,$\mathrm{term}(n_2)=-a$,称 n_1 发送消息 a 给 n_2,或者 n_2 从 n_1 接收了消息 a.

(4) 若 $n_1=\langle s,i\rangle$,$n_2=\langle s,i+1\rangle$,则存在边 $n_1 \Rightarrow n_2$,称作事件相继发生,表示事件 n_2 在事件 n_1 之后发生,称 n_1 是 n_2 在同一个串上的因果前驱.

(5) 集合 N 以及两类边 $n_1 \rightarrow n_2$ 和 $n_1 \Rightarrow n_2$ 的集合构成一个有向图$\langle N,(\rightarrow \cup \Rightarrow)\rangle$.

(6) 丛的定义如下:假设$\rightarrow_c$属于$\rightarrow$,$=>_c$属于$=>$,且 $C=\lceil N_c,(\rightarrow_c \cup =>_c)\rceil$是$\lceil N,(\rightarrow \cup =>)\rceil$的一个子图,$C$ 丛当且仅当满足:① C 是有限的无环图;② 若 n_2属于 N_c,且 $\mathrm{term}(n_2)$为负,则存在唯一的一个结点 n_1,使得$n_1 \rightarrow n_2$;③ 若 n_2属于 N_c,且 $n_1 \Rightarrow n_2$,则 $n_1 =>_c n_2$.

2.2　对基本串空间模型的扩展

基本的串空间模型,将关注点集中在安全协议的秘密性与认证性,并未重视安全协议的可用性. 针对安全协议中引起 DoS 的原因,本小节从消息相关度集合与代价函数两方面对基本串空间模型进行扩展. 其中,消息相关度集合针对服务中止型 DoS 提出,代价函数针对资源消耗型 DoS 提出.

2.2.1　消息相关度集合

定义 6　消息相关度集合. 若结点 n_i,n_j 属于 N,M_i 为 $\mathrm{term}(n_i)$的所有子项构成的集合,M_j 为 $\mathrm{term}(n_j)$的所有子项构成的集合,则结点 n_i,n_j 的消息相关度集合定义为集合 M_i 与集合 M_j 的交集 O,集合 O 反应了结点 n_i 和 n_j 的消息相关程度,若 O 为空集,表明 n_i 和 n_j 是不相关的,反之,若集合 O 中包含的元素越多,表明结点 n_i 和 n_j 的消息相关程度越高.

2.2.2　代价函数

计算机在运行安全协议时,消耗的主要是 CPU 的计算资源和保存运行数据的存储资源,在先前的安全协议抗 dos 研究方法中,往往只关注 CPU 的计算资源,只考虑计算机能够处理的用户请求数与计算机的 CPU 运算速度之间的关系,或者将计算机所付出的资源代价做模糊处理,不加区分,例如在 Meadows 框架中,对参与者行为付出的代价简单的处理为"cheap","medium","expensive",这样的处理方式,在协议的具体运行环境中,显然是不够精确的,不同的应用环境下,参与者所具有的能力是不同的,应当具体问题具体分析.

影响参与者同一时间内能处理的用户请求数量的因素,除了 CPU 的计算能力,另一个重要的因素是参与者所具有的存储资源. 任何协议的运行,或多或少都要保存协议当前的运行状态,用户名等信息,必然要消耗一定的存储资源,因此,在分析安全协议的抗 DoS 性时,应当考虑存储资源代价. 接下来,以串空间模型为基础,引入 CPU 计算资源与存储资源双重代价,如图 1 所示.

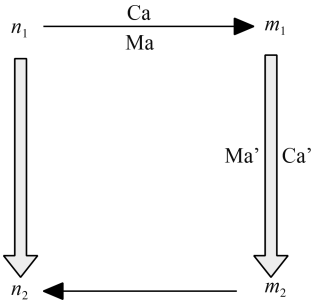

图 1　代价函数串空间模型

Fig. 1　Strand space model of cost function

定义 7　计算资源代价函数 C_a,C'_a. 其中 C_a 为边 $n_1 \rightarrow m_1$ 到非负实数 R 的映射,表示节点 n_1 产生消息 a 时付出的 CPU 计算资源,C'_a 为边 $m_1 \Rightarrow m_2$ 到非负实数 R 的映射,表示节点 m_1 接收并验证消息 a 时付出的 CPU 计算资源代价,单位为秒(s).

定义 8　存储资源代价函数 M_a,M'_a. 其中 M_a 为边 $n_1 \rightarrow m_1$ 到非负实数 R 的映射,表示节点 n_1 产生消息 a 时付出的存储资源,M'_a 为边 $m_1 \Rightarrow m_2$ 到非负实数 R 的映射,表示节点 m_1 接收并验证消息 a 时付出的存储资源代价,单位为比特(bit).

定义 9　分析安全协议的抗资源消耗型 DoS 时,需要知道参与者在生成每一条消息时付出的 CPU 计算资源代价以及存储资源代价. 存储资源代价容易得到,因为每一条消息的格式是已知的,容易计算出消息的字节数,然后根据系统的总存储资源,便可计算出系统最多可同存储的消息数. 然而不同的参与者的 CPU 计算能力是不同的,即使是同一个操作,消耗的时间也各不相同,因此不能

将参与者生成一条消息时付出的 CPU 计算资源代价设为固定值. 较为合理的方法是,根据每一个算法操作需要的时钟周期数来估算 CPU 计算资源代价,因为成熟的精简的算法,每一步消耗的时钟周期是相似的,根据 CPU 的主频以及算法操作的时钟周期数,便可计算出生成每一条消息需要的 CPU 计算资源代价. 表 1 给出了常见密码算法操作在执行过程中需要的 CPU 时钟周期数[15].

表 1 常用算法 CPU 消耗

Tab. 1 The CPU consumption of commonly algorithm

算法	每比特时钟周期数
AES	21.7
HMAC(SHA1)	11.9
SHA-521	17.7
操作	时钟周期数
DH 1024	$8.2*10^5$
RSA 1024 Signature	$2.71*10^6$
RSA 1024 Verification	$1.3*10^5$

2.2.3 *代价函数与处理消息数关系* (1) 发起者端. 假设发起者生成并发送一条消息,消耗 CPU 的计算资源代价为 C_a,则单位时间内发起者能生成的消息数为

$$N_c=1/C_a;$$

假设发起者存储一条消息的状态信息需要占用存储资源代价为 M_a,发起者具有的总存储资源为 M_i,则发起者同时能存储的消息数量为

$$N_m=M_i/M_a;$$

因为收 CPU 计算资源和存储资源的双重限制,则单位时间内,发起者能生成并发送的消息数

$$N_i=\min(N_c,N_m);$$

通常的服务中,有多个发起者同时向响应者申请服务,假设有 j 个发起者,则单位时间内发送到响应者的消息数

$$N_i=N_1+N_2+\cdots+N_j;$$

其中,N_j 表示第 j 个发起者向响应者发送的消息个数.

(2) 响应者端. 同发起者端类似的,假设响应者接收并处理一条消息所付出的 CPU 计算代价是 C_a',具有的存储资源为 M_r,处理一条消息占用存储资源为 M_a',则单位时间内响应者 CPU 能够处理的消息数最多为

$$N_c'=1/C_a';$$

响应者同时最多能存储的消息数为

$$N_m'=M_r/M_a';$$

响应者同一时间内最多能够响应发起者的消息数为

$$N_r=\min(N_c',N_m');$$

2.3 基于扩展串空间模型的协议抗 DoS 攻击形式化分析方法

利用上文提出的消息相关度集合和代价函数,提出两条检验规则,分别用于分析安全协议的抗服务中止型 DoS 和资源消耗型 DoS 的能力.

服务中止型 DoS 攻击产生的原因是协议本身存在缺陷,当攻击者篡改请求者数据,或者发送伪造的虚假数据时,响应者却不能及时发现,仍然当作正常的数据处理,使其前后状态不一致,导致认证失败,协议不能继续向下执行,造成 DoS. 基于此,提出如下规则 1.

规则 1 设 s 是协议的响应者串,n_i,n_j 是 s 中满足 $\mathrm{sign}(n_i)=-,\mathrm{sign}(n_j)=-$ 的任意两个结点,其中 $i<j$,O 为 n_i 和 n_j 的消息相关度集合,若集合 O 能够满足以下条件之一.

(1) O 是空集;

(2) O 不为空集,但是 O 中每一个元素都不是全部明文方式存在,且协议参与者密钥不属于攻击者密钥集合.

则协议的响应者能够抵抗服务中止型 DoS.

规则 1 可以用响应者的一致性来解释,转化为证明以下命题成立.

命题 1 假设 C 是丛,则 $\leqslant_C$ 是一个偏序关系,即 $\leqslant_C$ 是自反的、传递的、反对称的关系,丛 C 任意一个非空结点集合里,都有 $\leqslant_C$-极小元.

证明 该命题可由偏序关系以及丛的定义得到.

命题 2 假设 C 是丛,E 是丛 C 的结点集,如果对任意结点 m,m',如果 m,m' 的无符号部分相同,要么 m,m' 都属于 E,要么都不属于 E,则若 n 是 E 的 $\leqslant_C$-极小元,那么 n 的符号一定为 $+$.

证明 利用反证法,要证明极小元 n 的符号为 $+$,假设 n 的符号为 $-$,依据丛的定义,一定存在一个结点 $n'\in C$,且 $n'\rightarrow n$,故有 $\mathrm{uns\_term}(n)=\mathrm{uns\_term}(n')$,所以有 $n'\in E$,表明 n 不是极小元,说明假设 n 的符号为-是不成立的,则 n 的符号一定为 $+$.

命题 3 假设 C 是丛,n 是集合 $\{m\in C: t\subset term(m)\}$ 的一个 $\leqslant_C$-极小元,则 t 产生于 n.

证明　要证明 t 产生于 n,只要证明 n 的符号为+,而且不存在 $n'\Rightarrow^{+}n, t\in \mathrm{term}(n')$. 由命题 2 可得,$n$ 的符号为+;假如存在 $n'\Rightarrow^{+}n$,根据丛的定义,则 $n'\in C$,若 $t\subset \mathrm{term}(n')$,则 n' 位于集合 $\{m\in C: t\subset \mathrm{term}(m)\}$ 中,这和题设 n 是集合 $\{m\in C: t\subset \mathrm{term}(m)\}$ 的一个 $\leqslant_C$-极小元矛盾,所以 n' 不可能在该集合中,即 $t\in \mathrm{term}(n')$ 不成立,所以不存在 $n'\Rightarrow^{+}n$ 且 $t\in \mathrm{term}(n')$ 这种情况,命题得证.

命题 4　假设 C 是丛,并且对 $K=K\backslash K_P$,其中 $K\backslash K_P$ 表示集合 K 与 K_P 的差,若 K 不源于一个正则结点,则对任何结点 $n\in C$,有 $K\not\subset \mathrm{term}(n)$,特别的,对任何攻击结点 $p\in C$,都有 $K\not\subset \mathrm{term}(p)$.

证明　利用反证法,假设集合 $S=\{n\in C: K\subset \mathrm{term}(n)\}$ 非空,根据命题 1,S 中存在 $\leqslant_C$-极小元. 根据命题 3,这些极小元产生了 K,因为 K 不源于任何一个正则结点,故这些极小元是攻击者结点. 根据命题 2,这些结点都是正结点. 接下来结合攻击者迹的可能情况,对这些正结点的所有可能性进行详细的检验.

串形式为 $<-t>$,其中 $t\in T$,但是 $K\not\subset t$;

串形式为 $<-g>$,没有正结点;

串形式为 $<-g,+g>$,没有源自于正结点的值;

串形式为 $<-g,-h,+gh>$,根据自由假设,除非一个密钥是前一个结点的子项,否则不存在密钥是该正结点的子项;

串形式为 $<-gh,+g,+h>$,没有源自于正结点的值;

串形式为 $<-K,-h,+\{h\}_k>$,根据子项关系的定义,当且仅当 $a\subset h\vee a=\{h\}_K$ 时,$a\subset\{h\}_K$ 成立,但是根据自由假设,$K\neq\{h\}_K$,因此除非密钥是前一个结点的子项,否则不存在密钥是该正节点的子项;

串形式为 $<-K^{-1},-\{h\}_K,+h>$,根据子项关系的定义,只有当 $a\subset\{h\}_K$ 时,有 $a\subset h$,所以密钥是前一个结点的子项.

综上所述,集合 S 为空集,对所有的 $n\in C$,有 $K\not\subset \mathrm{term}(n)$,特别的,对于任何攻击结点 $p\in C$,都有 $K\not\subset \mathrm{term}(n)$.

命题 4 说明假如攻击者不能掌握某个密钥,那么该密钥就不可能源自于任何一个攻击者结点. 该结论实际上对攻击者的能力给出了一个限定.

命题 5　假设

(1) $\sum$是一个安全协议的串空间,C 是$\sum$中一个丛,r 是一个响应者串,$r\in \mathrm{Resp}[I,R,t,*]$,并且 $C-\mathrm{height}(r)=n$;

(2) $K_I^{-1}\notin K_P, K_R^{-1}\notin K_P$;

(3) $N_I\neq N_R$,且 N_R 在$\sum$中是唯一起源的项;

(4) $+t\in \mathrm{term}(i_0), +t\in \mathrm{term}(i_1), -t\in \mathrm{term}(r_0), -t\in \mathrm{term}(r_1)$;且 t 不会以明文形式出现.

那么,C 包含一个发起者串 $i\in \mathrm{Init}[I,R,t,*]$,且 $C-\mathrm{height}(i)=n$.

证明　依次考察正攻击者结点的情形,证明 t 不可能在一个攻击者串上.

串形式为 $<+t_0>$,其中 $t_0\in T$,T 是原子项集合,t 不以明文形式出现,所以不可能是原子项,与假设 4 矛盾;

串形式为 $<-g>$,不含正结点,不符合;

串形式为 $<-g,+g>$,因此它的正结点不会是极小元,不符合;

串形式为 $<-g,-h,+gh>$,同样它的正结点不会是极小元,不符合;

串形式为 $<-gh,+g,+h>$,同样它的正结点不会是极小元,不符合;

串形式为 $<-K,-h,+\{h\}_k>$,同样它的正结点不会是极小元,不符合;

串形式为 $<-K^{-1},-\{h\}_K,+h>$,如果该正结点是串中的极小元,那么有 $t\not\subset h$,且 $t\subset\{h\}_K$,根据自由假设,存在一个结点 m,该结点是这个串上的第一个结点,且 $\mathrm{term}(m)=K_I^{-1}$,因为 $K_I^{-1}\notin K_P$,根据命题 4,我们可以推断出 K_I^{-1} 源自于一个正则结点,但没有发起者串或者响应者串源自于 K_I^{-1},故这种情况是不可能的.

综上所述,t 不可能出现在一个攻击者串上,必然源自于一个正则结点,由此证明了参与者的合法身份.

规则 1 表明,如果 O 是空集,说明这两条消息的处理的数据是互不相关的,响应者能够抵抗服务中止型 DoS;如果 O 不为空集,说明 n_i 中的数据和 n_j 中的数据是相关的,集合 O 中的数据必须是可认证的,响应者能够验证每一个数据的来源与准确性,保证不是来自非法的攻击者,而是源自于一个正则结点,才具有抗服务中止型 DoS 的能力.

不同于服务中止型 DoS 攻击,资源消耗型 DoS 攻击的实质是攻击者向响应者发送大量伪造的请求信息,使响应者在对这些消息进行认证以及维持连接的过程中用尽自身资源,造成 DoS. 结合代价函数的概念,提出如下规则 2.

规则 2 在安全协议的运行过程中,发起者所具有的 CPU 计算资源与存储资源所能支持的单位时间内最大消息个数为 N_i,响应者具有的 CPU 计算资源与存储资源支持的最大消息个数为 N_r,只有满足 $N_i < N_r$,即响应者同时支持的最大消息个数大于所有发起者同时发来的最大消息个数,才能保证响应者不产生拒绝服务,能够响应正常的用户请求.

证明 资源消耗型 DoS 攻击产生的直接原因就是因为发起者同时发起的连接请求数,超过了响应者同时能够处理的请求数,所以规则 2 通过计算发起者与响应者双方资源代价能够支持的对话数,来判断是否会出现 DoS 攻击,显然是合理的. 因此,要想防止资源消耗型 DoS 攻击,要求协议响应者同时能够响应的消息个数要大于发起者同时发送的消息个数.

可以用上面的两条规则形成形式化分析方法来检测安全协议的抗 DoS 攻击能力,如果一个安全协议的响应者串满足规则 1,则响应者能够抵抗服务中止型 DoS 攻击;如果响应者串满足规则 2,则能够抵抗资源消耗型 DoS 攻击.

基于上述两条规则,可行形成如下的基于扩展的串空间模型的分析安全协议抗 DoS 攻击的一般步骤:

1) 对安全协议进行扩展的串空间模型建模;

2) 确定协议参与者的消息相关度集合;

3) 利用规则一,验证消息相关度集合中元素的可认证性,从而得到安全协议抗服务中止型 DoS 性;

4) 根据参与者的系统资源配置,求出每一个参与者支持的最大消息数,利用规则 2,判断是否存在资源消耗型 DoS.

3 JFK 协议的抗 DoS 性分析

3.1 JFK 协议简介

JFK 协议是一种新的 Internet 密钥交换协议,分为 JFKr 和 JFKi 两种变种协议,其中 JFKi 主要应用在 C/S 模式,能够保护发起者的身份;JFKr 主要适用于 P2P 模式,每一个响应者都能够保护自己的身份信息. 本小节以 JFKi 为例进行分析. JFKi 协议的过程如图 2 所示,符号说明见表 2.

3.2 JFKI 抗服务中止型 DoS 分析

接下来,采用扩展后的串空间模型对 JFKi 协议进行建模,如图 3 所示.

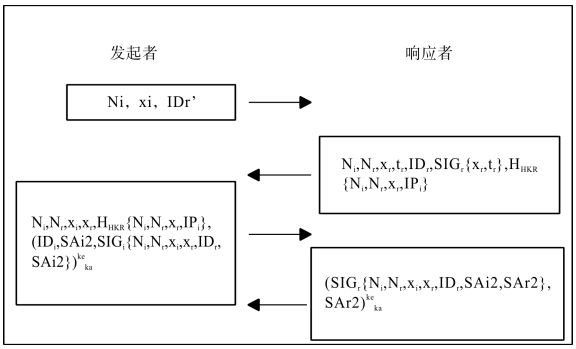

图 2 JFKi 协议示意图

Fig. 2 Schematic diagram of JFKi protocol

表 2 JFKi 协议符号说明

Tab. 2 Symbol specification of JFKi protocol

符号	含义
I	发起者
R	响应者
N_i	发起者随机数
N_r	响应者随机数
x_i	发起者公开密钥
x_r	响应者公开密钥
$SIG_r\{M\}$	使用 r 的私钥对 M 进行签名
$H_{HKR}\{M\}$	使用函数 H 和密钥 HKR 计算 M 的哈希值
IPi	I 的 IP 地址
SA	安全关联信息
$(M)^{ke}_{ka}$	利用密钥 ke 对 M 进行加密,ka 对 M 进行完整性校验

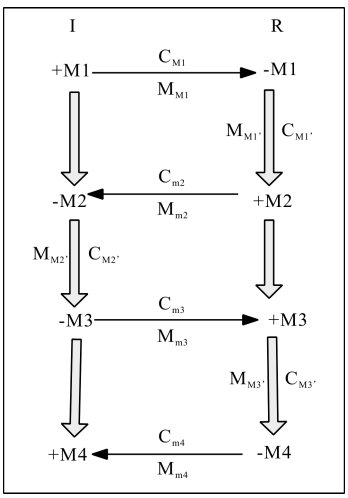

图 3 JFKi 协议扩展串空间模型

Fig. 3 Strand space model of JFKi protocol

其中:

消息 M_1: $I \rightarrow R$:

N_i, x_i, IDr'

消息 M_2: $R \rightarrow I$:

$N_i, N_r, x_r, t_r, IDr, SIG_r\{x_r, t_r\}, H_{HKR}\{N_i, N_r, x_r, IP_i\}$

消息 M_3: $I \rightarrow R$:

$N_i, N_r, x_i, x_r, H_{HKR}\{N_i, N_r, x_r, IP_i\}$,

$(ID_i, SAi_2, SIG_i\{N_i, N_r, x_i, x_r, ID_r, SAi_2\})_{ku}^{ke}$

消息 M_4: $R \rightarrow I$:

$(SIG_r\{N_i, N_r, x_i, x_r, ID_r, SAr_2, SAi_2\}, SAr_2)_{ku}^{ke}$

$JFKI$ 协议中,消息 M_1 的所有子项组成的集合 O_1:$\{N_i, x_i, IDr'\}$,消息 M_2 的所有子项组成的集合 O_2:$\{N_i, N_r, t_r, x_r, IDr, IPi\}$,消息 M_3 的所有子项组成的集合 O_3:$\{N_i, N_r, x_i, x_r, IPi, IDi, SAi_2, IDr\}$,消息 $M4$ 的所有子项组成的集合 O_4:$\{N_i, N_r, x_i, x_r, IDr, SAr_2, SAi_2\}$.

响应者收到的消息 M_1,M_3 的消息相关读集合 O_{13}:$\{N_i, x_i\}$,发起者收到的 M_2,M_4 的消息相关度集合 O_{24}:$\{N_i, N_r, x_i, x_r, IDr\}$,因为 M_3 和 M_4 中,双方的身份信息都被加密,且进行了 MAC 值计算,且双方的私钥都由自身保管,不被泄漏,收到消息后,都要进行消息完整性校验,因此保证了消息相关度集合 O_{13} 和 O_{24} 中的项都是可认证的,根据规则一,$JFKi$ 协议能够防止服务中止型 DoS 攻击.

3.3　JFKI 抗资源消耗型 DoS 分析

首先根据协议规定,计算每一条消息的长度.消息 $M1$ 长度 256 字节,消息 M_2 长度 576 字节,消息 M_3 长度 916 字节,消息 M_4 长度 276 字节.

参照表 1 中常用算法操作消耗的时钟周期数以及各个消息的长度,可以得到四条消息中相关操作消耗的时钟周期数.

发起者生成消息 M_1,产生随机数需要 $1.52 * 10^3$ 个时钟周期,对随机数进行 hash 操作需要 $1.13 * 10^3$ 个始终周期,因此发起者生成消息 M_1 付出的 CPU 计算资源代价是 $2.65 * 10^3$ 个时钟周期.

响应者生成并发送消息 M_2. 产生随机数需要消耗 $1.52 * 10^3$ 时钟周期,计算 MAC 值需要消耗 $3.05 * 10^3$ 时钟周期,因此响应者付出的 CPU 计算资源代价是 $4.57 * 10^3$ 个时钟周期.

发起者生成消息 M_3,付出的 CPU 计算资源代价是 $2740.28 * 10^3$ 个时钟周期. 响应者接收到 M_3 后,对 M_3 进行验证,付出的 CPU 计算资源代价是 $842.4 * 10^3$ 个时钟周期.

响应者生成消息 M_4. 在对消息 M_3 验证通过后,响应者生成消息 M_4,付出的 CPU 计算资源代价是 $2730 * 10^3$ 个时钟周期. 发起者就收到消息 M_4 后,对消息进行解密验证,消耗的 CPU 计算资源代价是 $150.2 * 10^3$ 个时钟周期.

在知道发起者与响应者的存储资源代价和 CPU 计算资源代价后,根据模拟实验环境,计算发起者与服务器同一时间内所能支持的最大协议运行数目,协议运行时,大量消息存在与系统中. 同样,我们分两种情况,

(1) 所有用户都是合法的. 此时服务器的 CPU 计算资源同时能够支持的最大用户数 $N_c = 866.7$,服务器的存储资源能够同时支持的最大用户数 $N_m = 3.95 * 10^6$,则服务器同时能够支持的最大用户数 $N_r = \min(N_c, N_m) = 866.7$.

(2) 来自虚假 IP 地址的攻击. 此时发起者向服务器发送大量的消息 M_1,且发起者无需存储自己伪造的虚假消息,故不考虑发起者的存储资源代价,则单位时间内,发起者 CPU 计算资源能生成的 M_1 数目 $N_i = 9.43 * 10^5$. 服务器收到消息 M_1 后,单位时间内 CPU 能产生的消息 M_2 数目 $N_{rc} = 6.84 * 10^5$,存储资源能够存储的消息 M_1、M_2 会话个数 N_{rm} 为 $9.62 * 10^6$,故服务器同时能够处理的攻击者请求个数 $N_r = 6.84 * 10^5$. 因为 $N_i > N_r$,所以攻击者对服务器的 DoS 攻击成功.

3.4　结果分析

利用扩展模型对 JFKi 协议初始交换阶段的抗 DoS 攻击能力进行分析,经过模拟实验,我们可以得出,协议均具有抗服务中止型 DoS 攻击的能力. 利用本文提出的基于扩展串空间模型的协议抗 DoS 攻击的形式化分析方法,不仅分析了 JFKi 协议抗资源消耗型 DoS 攻击的能力,而且分析了抗服务中止型 DoS 攻击的能力,比文献[14]中提出的改进的 Meadows 模型方法更加的准确与全面.

4　结　论

本文对当前安全协议中的 DoS 攻击研究现状进行总结,详细说明了这些模型方法的优点,以及存在的不足与缺陷. 由于串空间模型分析安全协议的优秀特性,选择串空间模型作为分析安全协议抗 DoS 性的基础. 首先对基本的串空间模型进行了介绍,然后,针对安全协议中存在的 DoS 的特点,从消息相关度集合和代价函数两个角度对基本串空

间模型进行扩展,其中代价主要考虑存储资源代价和 CPU 计算资源代价,并提出了分析安全协议抗 DoS 攻击的形式化分析方法步骤. 新的方法不仅分析协议抗资源消耗型 DoS 攻击的能力,而且分析了抗服务中止型 DoS 攻击的能力,更加的准确与全面.

参考文献:

[1] Saied A, Overill R E, Radizk T. Artificial neural networks in the detection of known and unknown DDoS attacks: proof-of-concept[C] // Proceedings of PAAMS 2014 InternationalWorkshops. Salamanca, Spain: PAAMS, 2014.

[2] 杨可心, 桑永胜. 基于 BP 神经网络的 DDoS 攻击检测研究[J]. 四川大学学报: 自然科学版, 2017, 54:71.

[3] 刘江, 张红旗, 杨英杰, 等. 一种面向 C/S 模式的地址跳变主动网络防御方法[J]. 电子与信息学报, 2017, 39:1007

[4] Meadows C. A formal framework and evaluation method for network denial of service[C]// Proceedings of IEEE Computer Security Foundations Workshop. California, USA: CSFW, 1999.

[5] Meadows C. A cost-based framework for analysis of denial of service innetworks[J]. J Comput Sec, 2000, 9: 143.

[6] Meadows C. Formalmethods for cryptographic protocol analysis: emerging issues and trends[J]. IEEE J Sel Area Comm, 2003, 21: 44.

[7] Groza B, Minea M. Formal modelling and automatic detection of resource exhaustion attacks[C]// Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security(ASIACCS). HongKong, China: Springer, 2011.

[8] Yu C, Gligor V. A formal specification and verification method for the prevention of denial of service [J]. IEEE Trans Software Eng, 1990, 16:581.

[9] 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: 592.

[10] Thayer F J, Herzog J C, Guttman J D. Strand space: Why is a security protocol correct[C]//Proceedings of the 1998 IEEE Symposium on Security and Privacy. California, USA: ISSP, 1998.

[11] Thayer F J, Herzog J C, Guttman J D. Strand spaces: proving security protocols correct[J]. J Comput Sec, 1999, 7: 191.

[12] Thayer F J, Herzog J C, Guttman J D. Strand spaces: honest ideals on strand spaces[C]//Proceedings of the 1998 IEEE Computer Security Foundations Workshop. Los Alamitos, USA: ISFW, 1998.

[13] 孟博, 黄伟, 王德军, 等. 协议抗拒绝服务攻击性自动化证明[J]. 通信学报, 2012, 2012: 112

[14] 常静. 关于抗 DoS 协议的形式化分析研究[D]. 北京: 中国科学院大学, 2013.

引用本文格式:

中 文: 高强, 林星辰, 林宏刚, 等. 安全协议抗 DoS 攻击的形式化分析研究[J]. 四川大学学报: 自然科学版, 2018, 55: 1211.

英 文: Gao Q, Lin X C, Lin H G, *et al*. A formal analysis for security protocol against DoS attacks[J]. J Sichuan Univ: Nat Sci Ed, 2018, 55: 1211.