doi:10.3969/j.issn.1000-436x.2013.08.003

基于博弈论的身份认证协议的分析——NGUYEN L H 方案的改进

李兴华[1,2]，邓凌娟[1]，张渊[1]，马建峰[1]
（1. 西安电子科技大学 计算机学院，陕西 西安 710071； 2. 南京大学 计算机软件新技术国家重点实验室，江苏 南京 210032）

摘 要：NGUYEN L H 在博弈论思想的指导下来对身份认证协议进行了修改，协议参与方在进行协议交互之前以一定的概率 α 来发送无用数据，使得攻击者攻击协议所获得的收益比不攻击协议所获得的收益还要小，以此保证了协议的安全性。但该方案存在 2 个缺陷：考虑的攻击者过于强大，且仅仅考虑了其收益，忽略了其发起攻击所要消耗的代价；没有考虑诚实节点在什么条件下才会选择发送无用数据。针对这 2 个缺陷对 NGUYEN L H 方案进行改进，给出了更具有一般意义的 α 值。同时引入了攻击概率 β，给出了诚实节点发送无用数据的前提条件以及在不同的 β 值下 α 的取值范围。相对于原方案，改进方案的结论更具有一般性，且更全面。同时，通过 P2P 下面的一个具体案例分析证明了所提结论的正确性。

关键词：身份认证协议；博弈论；协议安全
中图分类号：TP311 **文献标识码**：A **文章编号**：1000-436X(2013)08-0018-09

Rational analysis of authentication protocols based on NGUYEN L H scheme

LI Xing-hua[1,2], DENG Ling-juan[1], ZHANG Yuan[1], MA Jian-feng[1]
(1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China;
2. State Key Lab. for Novel Software Technology, Nanjing University, Nanjing 210032, China)

Abstract: Using the ideas of game theory, NGUYEN L H transformed two families of authentication protocols where the honest party transmitted some useless data with probability α before the normal protocol run, so that even if an attacker attacks a protocol, the attacker's payoff will still be lower than that when it does not. In such a way, the security of the protocol was guaranteed. However, this scheme suffers from two shortcomings: the considered is too attacker powerful, and only its payoff was considered and the cost of the attacks was ignored; the situation in which the honest node would choose to send useless data was not considered. To improve this scheme, the value of α, with the consideration of the attack cost, of which the value is more general was given. What's more, the attack probability β was introduced. Based on this, the precondition that the honest node transmits the useless data was presented, as well as the value of α under the different β values. Compared with the original scheme, this results are more generic and comprehensive. Meanwhile, through a case analysis in the P2P network, the correctness of the conclusion is proved.

Key words: identity authentication protocol; game theory; protocol security

1 引言

博弈论的思想在密码学及信息安全领域越来越得到重视[1~6]，它与传统的密码协议模型最大的区别是传统的密码协议模型一般只考虑诚实参与者和恶意参与者，但随着应用需求的提升，密码协议的参与者可能会从利益最大化的角度来选择自己的行为。研究人员利用该思想设计和分析了不少安全方案，如：多方密钥共享方案[7,8]、安全路由方案[9,10]、身份认证协议[11,12]等。

收稿日期：2012-06-29；**修回日期**：2013-03-08
基金项目：国家科技部重大专项基金资助项目(2011ZX03005-002)；国家自然科学基金资助项目(U1135002, 61072066)；中央高校基本科研业务费基金资助项目(JY10000903001, JY10000901034)
Foundation Items: The Major National S&T Program(2011ZX03005-002); The National Natural Science Foundation of China (U1135002, 61072066); The Fundamental Research Funds for the Central Universities(JY10000903001, JY10000901034)

近来，NGUYEN L H 利用博弈论的思想来对身份认证协议进行了研究，它借鉴了 Gordon[13]和 Fuchsbauer[8]的思想：为了使得攻击者放弃对一个协议的进攻，那么必然要使攻击者获得一些收益，但该收益要比攻击者成功攻击协议本身所要获得的收益要小。在该思想的指导下，NGUYEN L H 对身份认证协议进行了修改[14]：协议参与实体在协议正常执行之前先要以一定的概率 α 来发送一些无用的数据。在此基础上，作者针对单次运行及多次运行的身份认证协议进行了博弈论分析，给出了保证这 2 类协议安全执行的 α 的下限。据 NGUYEN L H 称：它是第一个将不理性的行为引入到认证协议参与实体的[14]。NGUYEN L H 与目前研究工作最大的区别是后者绝大部分都是关注如何提高协议本身的安全性，如：如何使一个 SK 安全[15]的身份认证协议转化为通用可组合的安全协议[16]，以及从 MQV 到 HMQV 的改进[17~19]等。而 NGUYEN L H 以一个全新的角度来看待身份认证协议，他认为攻击者都是理性的，它们会选择最大化自己利益的策略来采取行动。对于一个给定的身份认证协议，论文的侧重点不在于如何对该协议本身进行改进（如使用安全性更高的加密算法、消息认证码）以提高其安全性，而是在保持该协议不变的前提下，让诚实的协议实体以一定的概率先发送一些无用数据以消耗一些资源（如：计算资源、时间及能量等），据此使攻击者获得一定的收益，从而使得攻击者攻击协议获得的期望收益小于不攻击协议所获得的期望收益，攻击者自然不会再去攻击协议。NGUYEN L H 工作的意义在于：从理性攻击者的角度来进行考虑，不对协议本身做任何改动来提高其安全性。

NGUYEN L H 方案的不足之处在于：1）它仅仅考虑了攻击能力强大的攻击者，在计算诚实节点发送无用数据概率 α 的时候，忽视了攻击者发起攻击所要消耗的代价（如计算资源和能量等）。但现实中的攻击者，在考虑是否要发起攻击时都会将攻击代价作为重要参数进行考虑，因此它所给出的结论不具有一般性；2）仅仅从攻击者的角度来考虑，给出了诚实节点发送无用数据的概率 α，但没有从诚实节点的角度来考虑它在什么条件下才会选择发送无用数据，因此其考虑它不够全面。针对以上 2 个缺陷作者展开讨论，给出了认证协议单次攻击和多次攻击下更具有一般意义的 α 值，同时引入了攻击概率 β，给出了诚实节点发送无用数据的前提条件，以及在不同的 β 值下 α 的取值范围。

2　背景知识

在一个不安全的环境中，通常会存在攻击者拦截和修改在不安全通信信道上传输的数据。这些攻击者通常会选择干预并试图破坏协议的运行，无论成功与否它总是会获得一定收益。

1) 攻击者以概率 ε 攻击成功，这意味着攻击者成功地欺骗了诚实节点，例如通信方接收并认证了损坏的数据。

2) 攻击者以概率 $1-\varepsilon$ 攻击失败，但它至少成功发起了一次拒绝服务攻击，从而阻止了诚实节点协商出相同的密钥。另外，在基于口令的认证协议中，如果口令较短，那么一次错误的猜测将会增大随后攻击成功的概率，这将鼓励攻击者发起下一次攻击。

2.1　对 NGUYEN L H 方案

NGUYEN L H 提出运用博弈论的思想对身份认证协议进行修改，使得攻击者攻击协议所获得的期望收益始终比不攻击所获得的期望收益小，从而使得理性的攻击者将不会选择对协议进行攻击，保证了协议的安全性。其主要思想在于为诚实节点引入一定概率的传输无用数据的行为。

1) 在概率 α 下，诚实节点 A 将会认证或传输一些没用的随机数据，这些数据有可能会包括一个随机的（RSA 或者 Diffe-Hellman）公钥 PK_{A}，但 A 并不知道对应的私钥。所以如果一次执行完成了，而攻击者并没有进行攻击，对于认证的另一方 B 来说，它会接收，并可能使用 PK_{A} 去加密数据并传输给 A。当这类传输发生后，过一段时间 A 将向 B 发起另一次执行，去废除之前传输的无用数据并重新开始认证有意义的数据。

2) 在概率 $1-\alpha$ 下，认证方 A 完全按照协议执行，此时如果攻击者不发起任何攻击行为，认证协议将会成功执行。

如果攻击者拦截或修改协议中传输的数据，无论 A 采取任何一种行动，攻击者的收益都为下列 3 种情况。

① 攻击者以概率 ε 攻击成功，并获得 U^{+} 的收益。

② 攻击者以概率 $1-\varepsilon$ 攻击失败，但它仍然成功地发起了一次拒绝服务攻击，阻碍了 A、B 之间合法数据的传输，此时的收益为 U^{-}。

③ 在诚实节点以α的概率传输无用数据时，对于攻击者来说，它希望看到诚实节点故意认证无用数据，这也在某种意义上达到了攻击者干扰协议正常执行的目的，攻击者在这种情况下的收益为U。

基于攻击者对协议破坏程度有：$U^+ \geqslant U \geqslant U^-$。

通过以上对认证协议的修改，NGUYEN L H得到以下的结论。

A 假设攻击者仅能对认证协议发起单次攻击，并且攻击成功的概率为ε，那么为了防止攻击者对认证协议发起攻击，需要有

$$\alpha > \frac{\varepsilon U^+ + (1-\varepsilon)U^-}{U} \tag{1}$$

B 在一个基于口令[20,21]的认证协议中，假设允许一个攻击者攻击协议的最大次数为 k 次($k \in \{1,\cdots, n=\frac{1}{\varepsilon}\}$)。攻击者将停止发起攻击，当且仅当攻击者在第 $t(t<k)$次尝试时攻击成功或者所有 k 次攻击都失败。为了防止攻击者发起对认证协议的攻击，有下列不等式成立。

$$\alpha > \frac{\varepsilon U^+ + (1-\varepsilon)U^-}{U} + (\frac{U^+ - U^-}{U})\frac{k-1}{n(2n-k-1)} \tag{2}$$

2.2 NGUYEN L H 博弈分析中的不足

在NGUYEN L H方案中攻击者只关注对认证协议可以造成怎样的阻碍和干扰，而并没有对其发起攻击的代价（如计算资源及能量等）进行考虑。但现实中，大部分攻击者在对是否发起攻击进行决策时都会将攻击代价作为重要参数进行考虑，因此它所给出的结论不具有一般性。

另一方面在 NGUYEN L H 的博弈分析中，主要是从攻击者收益的角度进行考虑，即：如何使攻击者对协议发起攻击的收益小于不攻击的收益，从而使攻击者不选择攻击。但它没从诚实节点收益的角度来考虑：是否诚实节点以一定概率发送无用数据的期望收益就一定大于正常执行协议时的期望收益？如果小于的话，诚实节点发送无用数据对它来说显然是没有意义的。也就是说它没有考虑诚实节点发送无用数据的前提条件，其考虑不够全面。

本文针对以上 2 个缺陷进行改进，将攻击者攻击的代价作为重要的参数进行考虑，给出了更具一般意义的α值。同时引入了攻击者攻击概率 β，给出了诚实节点发送无用数据的前提条件以及在不同β值的情况下诚实节点发送无用数据的概率α。

3 改进的博弈分析模型

3.1 对身份认证协议单次攻击的分析

NGUYEN L H 的分析中给出，若诚实节点以概率$\alpha > \frac{\varepsilon U^+ + (1-\varepsilon)U^-}{U}$进行无用数据的传输，那么修改后的认证协议就可以有效地防止强大的理性攻击者的攻击。作者以双人战略式博弈为基础，综合考虑诚实通信双方和攻击者的收益与损失，在给出保证身份认证协议免受攻击者攻击条件的同时，还给出了使双方都获得最大收益的纳什均衡结果。

在表 1 中，身份认证协议博弈问题中的 2 个参与方分别为诚实节点和攻击者，诚实通信双方的行动集为 $A_a=\{a_1,a_2\}$，其中，a_1 表示诚实节点非理性行为（即选择传输无用数据后进行正常协议的交互），其概率为α；a_2 表示不进行无用数据的传输而直接执行认证协议，其概率为 $1-\alpha$。攻击者的行动集为 $A_i=\{i_1,i_2\}$，其中，i_1 表示攻击者向认证协议发起攻击。

表 1　　身份认证协议博弈模型

诚实节点	攻击者	
	i_1	i_2
a_1	$U_A - E_A - [\varepsilon C_A^+ + (1-\varepsilon)C_A^-]$，$\varepsilon U^+ + (1-\varepsilon)U^- - (E_I + X)$	$-E_A$，U
a_2	$-[\varepsilon C_A^+ + (1-\varepsilon)C_A^-]$，$\varepsilon U^+ + (1-\varepsilon)U^- - E_I$	0, 0

表 1 中的参数均为正值，E_A代表诚实节点发送无用数据时在时间、能量等上的损耗值。E_I代表攻击者对正常执行的协议发起一次攻击在计算资源和能量的损耗值。将攻击者对诚实节点发送无用数据进行攻击时计算资源和能量的损耗值记为 X。攻击者成功地发起一次攻击时诚实节点的损失记为C_A^+。攻击者攻击不成功，却仍然成功发起一次拒绝服务攻击，诚实节点正常通信受到阻碍，其损失记为C_A^-。以上参数如何计算取决于实际应用环境，并不在本文的讨论范围内。

另外，根据 NGUYEN L H 的分析结果可知，诚实节点以一定概率发送无用数据使得攻击者选择不攻击协议，这在一定程度上提高了协议的安全性。因此，诚实节点发送无用数据是有一定的收益的，该收益可定义为 U_A。U_A 不可能发生在诚实节点发送无用数据而攻击者选择不攻击的情

况下。在这种情况下，诚实节点除了正常执行协议的收益外，不会有额外的收益，并且会为发送额外的无用数据损失能量。因此该收益只可能发生在诚实节点发送无用数据，而且攻击者选择攻击的情况下。在这种情况下，攻击者需要消耗能量，还有可能会让诚实通信双方意识到攻击者的存在，因此此时对诚实节点来说有一个收益 U_{A}。在表 1 所示的模型中不考虑协议正常执行过程中诚实节点的代价及收益。

定理 1　假设攻击者仅能对认证协议发起单次攻击，并且攻击成功的概率为 ε，那么为了防止攻击者对认证协议发起攻击，需要有

$$\alpha > \frac{\varepsilon(U^+ - U^-) + U^- - E_{\mathrm{I}}}{U + X} \tag{3}$$

证明　由表 1 可得，身份认证协议博弈模型中攻击者选择攻击协议（即选择策略 i_1）的期望收益为

$$\begin{aligned}&\alpha[\varepsilon U^+ + (1-\varepsilon)U^- - (E_{\mathrm{I}} + X)] + \\ &(1-\alpha)[\varepsilon U^+ + (1-\varepsilon)U^- - E_{\mathrm{I}}] \\ &= \varepsilon U^+ + (1-\varepsilon)U^- - E_{\mathrm{I}} - \alpha X\end{aligned} \tag{4}$$

攻击者选择不攻击认证协议（即选择策略 i_2）的期望收益为 αU 。

为了使攻击者不选择攻击认证协议，也就是说要使攻击者选择不攻击时的期望收益大于选择攻击时的期望收益，从而有

$$\alpha U > \varepsilon U^+ + (1-\varepsilon)U^- - E_{\mathrm{I}} - \alpha X$$

化简可得

$$\alpha > \frac{\varepsilon U^+ + (1-\varepsilon)U^- - E_{\mathrm{I}}}{U + X} = \frac{\varepsilon(U^+ - U^-) + U^- - E_{\mathrm{I}}}{U + X} \tag{5}$$

也就是说，当诚实节点选择传输无用数据的概率 α 满足式(5)时，攻击者在认证协议执行时都不会选择对协议进行攻击，从而保证了协议的安全性。

本文引入新的参数 E_{I} 和 X，这 2 个参数分别表示攻击者对正常协议发起攻击时自身的损耗以及对无用数据发起攻击时自身的损耗（如：计算资源及能耗等），对于一般的攻击者来说这 2 个损耗都是其选择是否发起攻击的重要因素。

另外，作者注意到下面不等式成立。

$$\frac{\varepsilon U^+ + (1-\varepsilon)U^- - E_{\mathrm{I}}}{U + X} < \frac{\varepsilon U^+ + (1-\varepsilon)U^-}{U}$$

在考虑了攻击者发起攻击的消耗后，诚实节点发送无用数据的概率相对于NGUYEN L H给出的概率降低了。但该概率降低并不会对其安全性造成影响，因为在这 2 种情况下，攻击者攻击协议所获得的收益都小于不攻击协议所获得的收益，理性的攻击者都会选择不攻击协议，协议自然是安全的。

另外，从 NGUYEN L H 方案可知：无论 U^+ 多大，$\varepsilon(U^+ - U^-)$ 都是相对极小的。因此，式（5）可简化为

$$\alpha > \frac{U^- - E_{\mathrm{I}}}{U + X} \tag{6}$$

在式（6）中，当攻击者足够强大时，它就不需要考虑损耗，那么 E_{I} 和 X 可以忽略不计，这样式（6）就成为

$$\alpha > \frac{U^-}{U} \tag{7}$$

该结果同NGUYEN L H 所得到的结果是一致的。

同时，从式（6）可以看出，当攻击者攻击的代价（即损耗 E_{I} 和 X）越高，α 越小。这个结论是合理的，因为攻击者攻击的代价越高，它就越不容易发起攻击（也即其发起攻击的概率就越低），这样对于诚实节点而言，发送无用数据的概率自然可以降低。

另外，根据式（5）可得

$$\varepsilon < \frac{\alpha(U + X) - (U^- - E_{\mathrm{I}})}{U^+ - U^-}$$

其中，在 α 确定的条件下，只要攻击成功概率 ε 满足该公式，那么协议就是安全的。同时，从该式可以看出，随着 α 的增大，ε 的取值范围也随之增加。也就是说：当诚实节点发送无用数据的概率 α 增加的话，攻击者攻击成功概率 ε 即使增加了，协议也仍然是安全的。由此可见，增加诚实节点发送无用数据的概率，即使攻击者攻击成功概率增加了（即：协议本身的安全性降低了），但仍然能够保护其不受攻击者攻击。

以上的分析都是从攻击者收益的角度来进行考虑，从诚实节点的角度来说，若其发送无用数据时的期望收益小于直接执行认证协议时的期望收益，那么诚实节点也不会选择发送无用数据。下面据此展开分析，这里引入了攻击者选择攻击的概率 β，也即攻击者选择 i_1 的概率为 β，选择 i_2 的概率为 $1-\beta$。

定理 2 在攻击者单次攻击身份认证协议时，只有当攻击者的攻击概率 $\beta > \frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$ 时，诚实节点才会选择发送无用数据。

证明 由表 1 可知，诚实节点选择不理性行为 a_1（即发送无用数据后进行协议执行）的期望收益为

$$\beta\{U_{\mathrm{A}} - E_{\mathrm{A}} - [\varepsilon C_{\mathrm{A}}^{+} + (1-\varepsilon)C_{\mathrm{A}}^{-}]\} + (1-\beta)(-E_{\mathrm{A}}) \quad (8)$$

诚实节点不进行无用数据的传输而直接执行认证协议（即选择 a_2）的期望收益为

$$\beta\{-[\varepsilon C_{\mathrm{A}}^{+} + (1-\varepsilon)C_{\mathrm{A}}^{-}]\} \quad (9)$$

那么要使诚实节点选择非理性行为，就有下列不等式成立。

$$\beta\{U_{\mathrm{A}} - E_{\mathrm{A}} - [\varepsilon C_{\mathrm{A}}^{+} + (1-\varepsilon)C_{\mathrm{A}}^{-}]\} + (1-\beta)(-E_{\mathrm{A}}) > \beta\{-[\varepsilon C_{\mathrm{A}}^{+} + (1-\varepsilon)C_{\mathrm{A}}^{-}]\} \quad (10)$$

化简可得

$$\beta > \frac{E_{\mathrm{A}}}{U_{\mathrm{A}}} \quad (11)$$

其中，若诚实节点不考虑自身损耗，而只希望达到防止攻击者攻击的目的，也就是说 E_{A} 可以忽略不计，约等于 0，即 $\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}} \approx 0$。而 β 本身是大于 0 的，所以自然 $\beta > \frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$，那么诚实节点肯定以 α 的概率选择不理性行为，也就如 NGUYEN L H 分析的那样，不过对于大部分通信双方而言，损耗都是不能忽视的一个重要因素。

从以上分析可以看出，当攻击者攻击概率 β 满足式(11)时，诚实节点才会发送无用数据，并且为了保证协议的安全性，其发送无用数据的概率 α 要满足式（5）；如果攻击者的攻击概率 $\beta < \frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$，那么诚实节点发送无用数据获得的期望收益还小于不发送无用数据获得的期望收益，在这种情况下诚实节点是不会选择发送无用数据的，即 α=0。

在对诚实节点和攻击者双方的收益和代价都进行理性分析后可以看出，只有当攻击者选择攻击的概率 $\beta = \frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$，且诚实节点选择以 $\alpha = \frac{\varepsilon U^{+} + (1-\varepsilon)U^{-} - E_{\mathrm{I}}}{U + X}$ 的概率发送无用数据，才能达到了均衡状态，也就是说最大化了双方的利益。

综上所述得出以下结论。

结论 1 在攻击者单次攻击身份认证协议时，理性的诚实节点为了最大化自己利益发送无用数据的概率 α 的取值为

$$\text{当}\beta > \frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}\text{时}, \alpha > \frac{\varepsilon U^{+} + (1-\varepsilon)U^{-} - E_{\mathrm{I}}}{U + X},$$

$$\text{当}\beta = \frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}\text{时}, \alpha = \frac{\varepsilon U^{+} + (1-\varepsilon)U^{-} - E_{\mathrm{I}}}{U + X},$$

$$\text{当}\beta < \frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}\text{时}, \alpha = 0$$

3.2 基于口令身份认证协议上多次攻击的分析

此处需要假设所要分析的基于口令的认证协议是免受离线搜索攻击的，并需要假设全部 n 个口令使用概率均相同。那么与 NGUYEN L H 的分析相同，攻击者可尝试攻击失败的最大次数为 k，且对于任意 $k \in \{1,\cdots,n\}$，有第 k 次攻击成功概率 $\varepsilon_k = \frac{1}{n-k+1}$。下面给出攻击者多次发起攻击的情况下，基于口令的身份认证协议中诚实节点和理性攻击者的收益和代价的详细分析。

1) 诚实节点的行动选择。

表 2 给出了在诚实节点不传输无用数据而直接执行基于口令的认证协议时，攻击者发起 k 次攻击成功（或不成功）的概率和收益。需要注意的是：k 次攻击并不一定是连续的，攻击可能交错地发生在任何一次协议执行过程中。

表 2 协议正常执行时攻击者 k 次攻击的概率与收益总结

攻击次数	结果	概率	收益
1	成功	$\varepsilon = \varepsilon_1 = \frac{1}{n}$	$U^{+} - E_{\mathrm{I}}$
2	成功	$(1-\varepsilon_1)\varepsilon_2 = \frac{1}{n}$	$U^{-} + U^{+} - 2E_{\mathrm{I}}$
3	成功	$(1-\varepsilon_1)(1-\varepsilon_2)\varepsilon_3 = \frac{1}{n}$	$2U^{-} + U^{+} - 3E_{\mathrm{I}}$
⋮	⋮	⋮	⋮
t	成功	$\varepsilon_t \prod_{i=1}^{t-1}(1-\varepsilon_i) = \frac{1}{n}$	$(t-1)U^{-} + U^{+} - tE_{\mathrm{I}}$
⋮	⋮	⋮	⋮
k	成功	$\varepsilon_k \prod_{i=1}^{k-1}(1-\varepsilon_i) = \frac{1}{n}$	$(k-1)U^{-} + U^{+} - kE_{\mathrm{I}}$
k	失败	$\prod_{i=1}^{k}(1-\varepsilon_i) = \frac{n-k}{n}$	$kU^{-} - kE_{\mathrm{I}}$

考虑如果一个攻击者允许对认证协议发起攻击的最大次数为 k，由表 2 可知期望（也就是平均）攻击次数为

$$N=\frac{1}{n}+\frac{2}{n}+\frac{3}{n}+\cdots+\frac{k}{n}+\frac{k(n-k)}{n}=\frac{k(2n-k+1)}{2n} \quad (12)$$

定理 3　在一个基于口令的认证协议中，假设允许一个攻击者攻击协议的最大次数为 k 次（$k\in\{1,\cdots,n=\frac{1}{\varepsilon}\}$）。攻击者将停止发起攻击，当且仅当攻击者在第 $t(t<k)$次尝试时攻击成功或者所有 k 次攻击都失败了。为了防止攻击者发起对认证协议的攻击，需要有下列不等式成立。

$$\alpha>\frac{\varepsilon U^{+}+(1-\varepsilon)U^{-}}{U+X}+(\frac{U^{+}-U^{-}}{U+X})\frac{k-1}{n(2n-k-1)}-\frac{E_{\mathrm{I}}}{U+X} \quad (13)$$

证明　攻击者多次攻击协议的预计累计期望收益为

$$P_{\mathrm{I}}=\frac{U^{+}}{n}+\frac{U^{-}+U^{+}}{n}+\cdots+\frac{(k-1)U^{-}+U^{+}}{n}+\frac{k(n-k)U^{-}}{n}-NE_{\mathrm{I}} \quad (14)$$

$$P_{\mathrm{I}}=\frac{kU^{+}}{n}+U^{-}[\frac{1}{n}+\frac{2}{n}+\cdots+\frac{k-1}{n}+\frac{k(n-k)}{n}]-NE_{\mathrm{I}} \quad (15)$$

$$P_{\mathrm{I}}=\frac{kU^{+}}{n}+\frac{k(2n-k-1)U^{-}}{2n}-NE_{\mathrm{I}} \quad (16)$$

对于其他几种情况，当诚实节点选择非理性行为时（即诚实节点在发送无用数据的时候），攻击者选择攻击，并不会对随后真正协议的正确执行产生任何阻碍或干扰，此时攻击者的期望收益为发起攻击对自身的期望损耗$-NX$; 若攻击者选择不攻击，诚实节点发送无用数据的行为就达到了攻击者想要干扰协议正常通信的目的，攻击者可获得的期望收益为 NU。另外当诚实节点选择直接执行认证协议，且攻击者选择不攻击时，对攻击者来说就不会产生任何收益或损失，此时的收益为 0。

因此，总的来说攻击者选择攻击的期望收益为：$-\alpha NX+P_{\mathrm{I}}$，攻击者选择不攻击的期望收益为 αNU。

要使攻击者选择攻击的期望收益小于不攻击的期望收益，从而达到攻击者不会选择攻击基于口令的认证协议的目的，则需要满足下列不等式。

$$\alpha NU>-\alpha NX+P_{\mathrm{I}} \quad (17)$$

将 N 与 P_{I} 代入不等式，化简可得到

$$\alpha>\frac{kU^{+}}{n(U+X)N}+\frac{k(2n-k-1)U^{-}}{2n(U+X)N}-\frac{E_{\mathrm{I}}}{U+X} \quad (18)$$

$$\alpha>\frac{\varepsilon U^{+}+(1-\varepsilon)U^{-}}{U+X}+(\frac{U^{+}-U^{-}}{U+X})\Delta-\frac{E_{\mathrm{I}}}{U+X} \quad (19)$$

其中，$\Delta=\frac{k-1}{n(2n-k-1)}$。

对于 α 的边界，单次攻击与多次攻击的不同之处在于$(\frac{U^{+}-U^{-}}{U+X})\Delta<\varepsilon(\frac{U^{+}-U^{-}}{U+X})$，由于随着 n 的增大，ε 将会呈指数减小，则$(\frac{U^{+}-U^{-}}{U+X})\Delta$ 可为任意小的值。

当诚实节点选择非理性行为的概率 α 满足不等式(19)时，可以有效地防止攻击者对基于口令的身份认证协议发起多次攻击，保证认证协议的安全。

由前文可知，$\varepsilon(U^{+}-U^{-})$ 是相对极小的，所以式（19）可以化简为

$$\alpha>\frac{U^{-}-E_{\mathrm{I}}}{U+X}+(\frac{U^{+}-U^{-}}{U+X})\frac{k-1}{n(2n-k-1)}$$

从式（19）可以看出，当攻击者足够强大时，它就不需要考虑损耗，那么 E_{I} 和 X 都可以忽略不计，这样式（19）就成为

$$\alpha>\frac{\varepsilon U^{+}+(1-\varepsilon)U^{-}}{U}+(\frac{U^{+}-U^{-}}{U})\Delta \quad (20)$$

该结果同 NGUYEN L H 所得到的结果是一致的。

2) 攻击者的行动选择

对攻击者行动选择的分析需要考虑的是诚实节点的收益情况。表 3 总结了诚实节点不传输无用数据而直接执行基于口令的身份认证协议，攻击者在协议执行过程中发起 k 次攻击成功（或不成功）时诚实节点的损失。

表 3　协议正常执行时攻击成功的概率与诚实节点损失

攻击次数	结果	概率	诚实节点损失
1	成功	$\varepsilon=\varepsilon_1=\frac{1}{n}$	C_{A}^{+}
2	成功	$(1-\varepsilon_1)\varepsilon_2=\frac{1}{n}$	$C_{\mathrm{A}}^{-}+C_{\mathrm{A}}^{+}$
3	成功	$(1-\varepsilon_1)(1-\varepsilon_2)\varepsilon_3=\frac{1}{n}$	$2C_{\mathrm{A}}^{-}+C_{\mathrm{A}}^{+}$
⋮	⋮	⋮	⋮
T	成功	$\varepsilon_t\prod_{i=1}^{t-1}(1-\varepsilon_i)=\frac{1}{n}$	$(t-1)C_{\mathrm{A}}^{-}+C_{\mathrm{A}}^{+}$
⋮	⋮	⋮	⋮
k	成功	$\varepsilon_k\prod_{i=1}^{k-1}(1-\varepsilon_i)=\frac{1}{n}$	$(k-1)C_{\mathrm{A}}^{-}+C_{\mathrm{A}}^{+}$
k	失败	$\prod_{i=1}^{k}(1-\varepsilon_i)=\frac{n-k}{n}$	kC_{A}^{-}

定理 4　在基于口令认证协议的多次攻击中，只

有在攻击者的攻击概率 $\beta>\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$ 时，诚实节点才会选择发送无用数据。

证明 在表3中，攻击者期望攻击次数为

$$N=\frac{1}{n}+\frac{2}{n}+\frac{3}{n}+\cdots+\frac{k}{n}+\frac{k(n-k)}{n}=\frac{k(2n-k+1)}{2n} \quad (21)$$

攻击者多次攻击，所以诚实节点的期望损失为

$$P_{\mathrm{A}}=\frac{C_{\mathrm{A}}^{+}}{n}+\frac{C_{\mathrm{A}}^{-}+C_{\mathrm{A}}^{+}}{n}+\cdots+\frac{(k-1)C_{\mathrm{A}}^{-}+C_{\mathrm{A}}^{+}}{n}+\frac{k(n-k)C_{\mathrm{A}}^{-}}{n} \quad (22)$$

$$P_{\mathrm{A}}=\frac{kC_{\mathrm{A}}^{+}}{n}+\frac{k(2n-k-1)C_{\mathrm{A}}^{-}}{2n} \quad (23)$$

诚实节点选择非理性行为所获得的期望收益为

$$\beta[N(U_{\mathrm{A}}-E_{\mathrm{A}})-P_{\mathrm{A}}]+(1-\beta)N(-E_{\mathrm{A}})$$

诚实节点不发送无用数据所获得的期望收益为 $\beta(-P_{\mathrm{A}})$。

对于诚实节点来说，只有满足下面不等式，也就是发送无用数据的期望收益大于直接执行协议的期望收益时，诚实节点才会选择发送无用数据，即

$$\beta[N(U_{\mathrm{A}}-E_{\mathrm{A}})-P_{\mathrm{A}}]+(1-\beta)N(-E_{\mathrm{A}})>\beta(-P_{\mathrm{A}}) \quad (24)$$

将 P_{A} 和 N 代入不等式，化简可得

$$\beta>\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}} \quad (25)$$

也就是说，在基于口令认证协议的多次攻击中，只有在攻击者的攻击概率 β 满足式(25)时，诚实节点发送无用数据的期望收益才会大于不发送无用数据所获得的期望收益，这样诚实节点才会选择非理性行为，即发送无用数据后执行认证协议。

该结果同作者分析单次攻击身份认证协议的结果是一致的。也就是说不管是什么样的认证协议，只有在攻击者的攻击概率 $\beta>\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$ 时，诚实节点才会选择发送无用数据。根据定理2和定理4可得推论1。

推论 1 对于所有的身份认证协议，只有在攻击概率 $\beta>\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$ 时，诚实节点才会选择发送无用数据。

综上所述，在基于口令的认证协议中，只有在攻击者的攻击概率 $\beta>\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$ 时，攻击者才会选择发送无用数据，并且为了保证协议的安全性，其发送无用数据的概率 α 要满足式(19)；如果攻击者攻击概率 $\beta<\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$，那么诚实节点发送无用数据获得的期望收益还小于不发送无用数据获得的期望收益，在这种情况下诚实节点是不会选择发送无用数据的，即 α=0。

在基于口令认证协议的多次攻击中，只有当攻击者选择攻击的概率 $\beta=\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$，且诚实节点选择以 $\alpha=\frac{\varepsilon U^{+}+(1-\varepsilon)U^{-}}{U+X}+(\frac{U^{+}-U^{-}}{U+X})\frac{k-1}{n(2n-k-1)}-\frac{E_{\mathrm{I}}}{U+X}$ 的的概率发送无用数据，才能达到了均衡状态，也就是说最大化了双方的利益。

综上所述得出结论2。

结论 2 在基于口令认证协议的多次攻击中，假设允许一个攻击者攻击协议的最大次数为 k 次($k\in\{1,\cdots,n=\frac{1}{\varepsilon}\}$)。那么理性的诚实节点为了最大化自己利益发送无用数据的概率 α 满足下面条件。

当 $\beta>\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$ 时，

$$\alpha>\frac{\varepsilon U^{+}+(1-\varepsilon)U^{-}}{U+X}+(\frac{U^{+}-U^{-}}{U+X})\cdot\frac{k-1}{n(2n-k-1)}-\frac{E_{\mathrm{I}}}{U+X}$$

当 $\beta=\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$ 时，

$$\alpha=\frac{\varepsilon U^{+}+(1-\varepsilon)U^{-}}{U+X}+(\frac{U^{+}-U^{-}}{U+X})\cdot\frac{k-1}{n(2n-k-1)}-\frac{E_{\mathrm{I}}}{U+X}$$

当 $\beta<\frac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$ 时，$\alpha=0$。

3.3 身份认证协议多次攻击的分析

由NGUYEN L H的分析可知，对于除了基于口令的身份认证协议，定理1、定理2及结论1同样适用于攻击者多次攻击身份认证协议的情况。因为对于这些身份认证协议来说，攻击者每次攻击协议成功的概率同单次攻击成功的概率是一样的。

4 实例分析

P2P（peer-to-peer）是Internet上的一种分布式控制网络技术，由于其具有开放性、匿名性、自治性等特点，通常会存在攻击者拦截和修改在不安全通信信道上传输的数据，如图1所示，这些攻击者会选择干

预并试图破坏协议的运行。因此，本文在 P2P 网络环境下，为保证身份认证协议的安全性，采用上述方案，为诚实节点引入了一定概率下传输无用数据的行为。

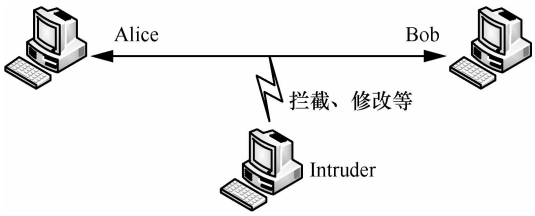


图 1　P2P 环境下攻击

在概率 α 下，诚实节点 Alice 将传输一些无用或随机数据（即选择策略 a_1）。而 Bob 会正常接收 Alice 传输的数据并对其进行处理。一段时间后，Alice 将对 Bob 发起另一次会话，通知 Bob 废弃之前传输的无用数据且开始正常协议的交互。P2P 环境中涉及到相关参数的含义及相应参数值设置如表 4~表 7 所示。

表 4　　诚实节点相关参数含义

参数	含义
U_{A}	诚实节点发送无用数据时意识到攻击者存在的收益
E_{A}	诚实节点发送无用数据时在时间、能量等上的损失
C_{A}^{+}	攻击者成功发起一次攻击时诚实节点的损失
C_{A}^{-}	攻击者攻击不成功，却仍然成功发起一次拒绝服务攻击，此时诚实节点的损失

表 5　　攻击者相关参数含义

参数	含义
E_{I}	攻击者对正常执行的协议发起一次攻击在时间、能量等上的损失
X	攻击者对诚实节点发送无用数据时进行攻击的损耗值
ε	攻击者攻击成功的概率
U^{+}	在概率 ε 下攻击者攻击成功的收益
U^{-}	在概率 $1-\varepsilon$ 下攻击者攻击失败，但它仍然成功发起了一次拒绝服务攻击，此时攻击者的收益
U	诚实节点以 α 的概率传输无用数据，即攻击者干扰协议正常执行的收益

表 6　　诚实节点相关参数值设置

参数	值
U_{A}	30
E_{A}	10
C_{A}^{+}	15
C_{A}^{-}	5

表 7　　攻击者相关参数值设置

参数	值
E_{I}	5
X	10
ε	0.5
U^{+}	15

这里仅针对单次攻击的情况，将表 6 和表 7 参数值代入表 1，得到 P2P 环境下身份认证协议博弈模型如表 8 所示。

表 8　　P2P 环境下身份认证协议博弈模型

诚实节点	攻击者	
	i_1	i_2
a_1	10, −5	−10, 10
a_2	−10,5	0,0

结合攻击者 Intruder 选择攻击（即策略 i_1）的概率 β、诚实节点传输无用或随机数据（即策略 a_1）的概率 α 和表 5，可得到诚实节点和攻击者的收益方程。

$$U_{\mathrm{Honest}} = 30\alpha\beta - 10\alpha - 10\beta$$

$$U_{\mathrm{Intruder}} = -20\alpha\beta + 10\alpha + 5\beta$$

根据第 3 节得到的结论：只有当攻击者选择攻击的概率 $\beta = \dfrac{E_{\mathrm{A}}}{U_{\mathrm{A}}}$，且诚实节点选择以 $\alpha = \dfrac{\varepsilon U^{+} + (1-\varepsilon)U^{-} - E_{\mathrm{I}}}{U + X}$ 的概率发送无用数据时，才能达到均衡状态，也就是说最大化了双方的利益，没有任何单独的一方愿意改变其策略。代入参数值得 $\alpha = \dfrac{1}{4}$，$\beta = \dfrac{1}{3}$。进而得到诚实节点和攻击者的最大收益分别为：$U_{\mathrm{Honest}} = -\dfrac{10}{3}$，$U_{\mathrm{Intruder}} = \dfrac{5}{2}$。此时，若攻击者 Intruder 单方面偏离纳什均衡结果，选择 $\beta = \dfrac{1}{4}$，那么诚实节点可选择 $\alpha = 0$，使得自身收益增加：$U'_{\mathrm{Honest}} = -\dfrac{5}{2} > U_{\mathrm{Honest}} = -\dfrac{10}{3}$，同时攻击者 Intruder 收益减少：$U'_{\mathrm{Intruder}} = \dfrac{5}{4} < U_{\mathrm{Intruder}} = \dfrac{5}{2}$，攻击者利益受损。同样，若诚实节点偏离该均衡，攻击者也存在另一个策略使自身利益增加而诚实节点利益减少。综合以上分析考虑，理性参与双方最终都不会偏离纳什均衡结果。即说明以双人战略式博弈为基础，综合考虑诚实通信双方和攻击者的收益与损失的情况下，得到的结果可使得通信双方和攻击者均获得最大收益，对于理性的参与者，没有任何单独的一方愿意偏离该结果。

若诚实节点有较强的安全性需求，即希望防止

攻击者对 P2P 认证协议交互过程中发起攻击，可设置 $\alpha > \dfrac{\varepsilon(U^+ - U^-) + U^- - E_{\mathrm{I}}}{U\ + X}$，代入参数值得 $\alpha > \dfrac{1}{4}$。这种情况下，攻击者 Intruder 在 $\beta = 0$ 时获得最大收益，即理性的攻击者会选择不对认证协议发起攻击，保证了 P2P 认证协议交互的安全性。

同理，在 P2P 环境下多次攻击基于口令身份认证协议的情况可通过类似的方式得以说明，这里不再赘述。

5　结束语

本文首先指出 NGUYEN L H 方案存在的 2 个问题：1）只考虑了功能强大的攻击者，而没有将其发起攻击的代价考虑进去；2）没有从诚实节点收益的角度来考虑，给出诚实节点发送无用数据的前提条件。针对这 2 个问题，分别对身份认证协议的单次攻击及多次攻击进行分析，给出了这 2 种情况下攻击者发送无用数据的前提条件及其发送无用数据的不同概率 α。相对于 NGUYEN L H 方案，其结论更具一般性，且更加全面。同时通过 P2P 下面的一个具体案例分析证明了所提结论的正确性。

参考文献：

[1] ALPCAN T, BASAR T. Network Security: A Decision and Game Theoretic Approach[M]. Cambridge: Cambridge University Press, 2011.

[2] GILLAT K, MONI N. Cryptography and game theory: designing protocols for exchanging information[A]. Proceedings of Theory of Cryptography Conference 2008[C]. New York, USA, 2008. 320-339.

[3] HALPERN J Y, PASS R. Game theory with costly computation: formulation and application to protocol security[A]. Proceedings of Innovations in Computer Science2010[C]. Beijing, China, 2010. 120-142.

[4] MANSHAEI M H, ZHU Q, ALPCAN T. Game Theory Meets Network Security and Privacy[R]. EPFL Report, 2010.

[5] ROY S, ELLIS C, SHIVA S, *et al*. A survey of game theory as applied to network security[A]. Proceedings of HICSS[C]. Koloa Kauai, USA, 2010. 1-10.

[6] SUN W, KONG X, HE D, *et al*. Information security problem research based on game theory[A]. Proceedings of ISECS[C]. Guangzhou, China, 2008. 554-557.

[7] GORDON S D, KATZ J. Rational secret sharing, revisited[A]. Proceedings of Security and Cryptography for Networks Lecture Notes in Computer Science[C]. Maiori, Italy, 2006. 4116:229-241.

[8] FUCHSBAUER G, KATZ J, NACCACHE D. Effcient rational secret sharing in standard communication networks[A]. Proceedings of TCC 2010[C]. RJ, USA, 2010. 419-436.

[9] OMRANI A, FALLAH M S. A game-theoretic cooperation stimulus routing protocol in MANETs[J]. IAENG International Journal of Computer Science, 2008, 35(1):174-181.

[10] PAVLIDOU F N, KOLTSIDAS G, Game theory for routing modeling in communication networks-a survey[J]. Journal of Communications and Networks, 2008, 10(3):268-286.

[11] EL N, SYRINE K, FOUAD K, *et al*. WSEAS: a bidirectional bluetooth authentication scheme based on game-theoretic framework, alfred menezes[J]. WSEAS Transactions on Communications, 2006, 15(6):1219-1227.

[12] ALMUDENA A, PALOMAR E, RIBAGORDA A, *et al*. Formal proof of cooperativeness in a multi-party P2P content authentication protocol[A]. Proceedings of TrustBus 2010[C]. Bilbao, Spain, 2010. 141-152.

[13] GORDON S D, KATZ J. Rational secret sharing, revisited[A]. Proceedings of Security and Cryptography for Networks Lecture Notes in Computer Science[C]. Maiori, Italy,2006. 4116:229-241.

[14] NGUYEN L H, Rational authentication protocols[EB/OL]. http://eprint.iacr.org/ 2011/070.pdf, 2011.

[15] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[A]. Proceedings of Eurocrypt 2001, Lecture Notes in Computer Science[C]. Innsbruck, Austria, 2001. 453-474.

[16] CANETTI R, KRAWCZYK H. Universally composable notions of key exchange and secure channel[A]. Proceedings of Eurocrypt 2002, Lecture Notes in Computer Science[C]. Amsterdam, The Netherlands, 2002. 337-351.

[17] LAW L, MENEZES A, QU M, *et al*. An efficient protocol for authenticated key agreement[J]. Designs, Codes and Cryptography, 2003, 28(2):119-134.

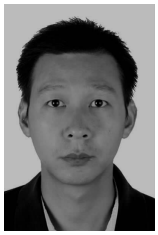
[18] MENEZES A. Another look at HMQV[J]. Journal of Mathematical Cryptology, 2007, 1(1):47-64.

[19] KRAWCZYK H. HMQV: a high-performance secure diffie-hellman protocol[J]. Lecture Notes in Computer Science, 2005, 3621:546-566.

[20] BELLOVIN S M, MERRITT M. Encrypted key exchange: password-based protocols secure against dictionary attacks[A]. Proceedings of the IEEE Symposium on Research in Security and Privacy (Oakland)[C]. Oakland, California, USA, 1992. 72-84.

[21] BOYKO V, MACKENZIE P, PATEL S. Provably secure password-authenticated key exchange using diffie-hellman[A]. Advances in Cryptology-Eurocrypt 2000, Lecture Notes in Computer Science[C]. Bruges, Belgium, 2000. 1807:156-171.

作者简介：



李兴华（1978-），男，河南南阳人，博士，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全。

邓凌娟（1989-），女，四川达州人，西安电子科技大学硕士生，主要研究方向为网络与信息安全。

张渊（1989-），女，河南周口人，西安电子科技大学硕士生，主要研究方向为网络与信息安全。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为信道编码、信息与网络安全。