对改进LMAP+协议的启发式攻击策略

王 超 秦小麟 刘亚丽
(南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要 随着无线射频识别(RFID)系统的广泛应用,RFID安全问题亟待解决。为了降低标签的计算代价,一系列只运用位与、位或、位异或、循环移位等操作的超轻量级RFID认证协议受到越来越多的关注,但是目前提出的超轻量级RFID认证协议不能保证很好的安全性。针对2012年Gurubani等人提出的改进的LMAP+协议,设计了一种基于模拟退火算法的启发式攻击策略,其能够成功推测秘密数据;并结合Jules等人提出的不可追踪性模型对改进的LMAP+协议进行追踪性攻击,通过重复攻击策略实验,完成全泄漏攻击。实验结果表明在攻击过程中仅利用窃听阅读器和标签间通信数据的被动攻击方法,推测的秘密数据就已逼近真实数据,且在完全泄漏攻击实验中约有70%的概率完全破解秘密数据,攻击过程收敛速度快,达到了较好的攻击效果。

关键词 RFID认证,模拟退火算法,启发式攻击,超轻量级,不可追踪性
中图法分类号 TP309 **文献标识码** A

Heuristic Attack Strategy Against Improved LMAP+ Protocol

WANG Chao QIN Xiao-lin LIU Ya-li
(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract With the extensive usage of radio frequency identification (RFID) systems, the challenge of security is emerging. In order to reduce the computational cost of the tag, a series of ultralightweight RFID authentication protocols that only involve simple bit-wise operations like AND, OR, XOR, rotation, have incurred many concerns. But the existing ultralightweight RFID authentication protocols are unable to guarantee the strong security property. A heuristic attack strategy based on simulated annealing algorithm was proposed to reckon the secret data against the improved LMAP+ protocol present by Gurubani in 2012. With the untraceability model proposed by Juels and Weis, a traceability attack was undertaken based on our heuristic attack strategy. And the secret values of improved LMAP+ could be disclosed successfully after repeated experiments of the attack strategy. The experiment evidences that, through the passive attack by eavesdropping the exchanged messages between the reader and the tag, the reckoned secret values are approximately equal to the genuine values of the secret data. And in a full-disclosure attack experiment, the secret data will be cracked completely with a 70 percent probability. At the same time, the attack process has a fast convergence speed with desired effectiveness.

Keywords RFID authentication, Simulated annealing algorithm, Heuristic attack, Ultralightweight, Untraceability

1 引言

无线射频识别技术(RFID)是一种能够自动化识别物体和人的技术[1]。相比条形码技术,RFID技术因其在识别过程中无需人工视觉感知、具有更远的识别距离[2]以及在恶劣环境中的出色能力等特点,应用领域更加广泛,如电子护照、物流管理等。典型的RFID系统由标签、阅读器和后端数据库3部分构成,三者间需要进行信息交互。由于无线传输的特点,阅读器与标签之间的通信信道是不安全信道,攻击者可以进行窃听、篡改等一系列非法操作,导致阅读器与标签的秘密信息更新不一致,甚至使得秘密信息完全泄漏。为了确保阅读器和标签双方的合法性及通信安全,RFID认证协议的研究成为热点。

2007年,Chien将已提出的RFID认证协议分成4类[3]。第一类是使用成熟的密码学知识实现的认证协议,如文献[4,5]。第二类称为简单的认证协议,这类协议在标签端需要实现的操作包括产生随机数和单向哈希函数等,如文献[6,7]。第三类称为轻量级的认证协议,标签需要具备产生随机

到稿日期:2013-07-12 返修日期:2013-10-28 本文受国家自然科学基金资助项目(61373015),2010年度国家教育部高等学校博士学科点专项科研基金项目(20103218110017),江苏高校优势学科建设工程资助项目(PAPD),南京航空航天大学中央高校基本科研业务费专项基金项目(NP2013307),中央高校基本科研业务费专项:江苏省普通高校研究生科研创新计划资助项目(CX10B_112Z),南京航空航天大学博士学位论文创新与创优基金资助项目(BCXJ10-07)资助。

王 超(1989—),男,硕士生,主要研究方向为物联网安全,E-mail:wangc0809@163.com;秦小麟(1953—),男,教授,博士生导师,主要研究方向为分布式环境的数据管理与安全、信息安全等;刘亚丽(1980—),女,博士生,讲师,主要研究方向为物联网安全及隐私保护技术。

数以及 CRC 校验和等功能，如文献[8-11]。最后一类称为超轻量级的认证协议，这类协议只需要进行位运算，如位与、位或、按位异或等操作，如文献[3,12-18]等。

发展至今，在 RFID 技术的大部分应用领域中，标签的体积与存储容量都很小，对于低代价的 RFID 标签，只有数百位的存储空间和 5k～10k 的逻辑门，用于实现安全功能的资源更加紧缺[13]，因此，超轻量级 RFID 认证协议受到了更多的重视。但是目前的超轻量级认证协议，如：UMAP 协议族[13,18]、SASI 协议[3]、Gossamer 协议[15]、RAPP 协议[16]等均存在安全隐患[12,19-24]。2012 年，Gurubani 等人在 LMAP+协议的基础上进行了改进，提出了新的协议[17]，该协议仅使用位加、位异或等简单的位运算方法。与 LMAP+协议相比，新协议增加了一项密钥信息，并且通信过程中未涉及唯一标识信息 *ID*，公开传输的数据表达式以及更新表达式都发生了改变。在文献[17]中，Gurubani 分析称改进的 LMAP+协议可以抵抗追踪性攻击和非同步攻击。本文设计了一种基于模拟退火算法的启发式攻击策略，对协议[17]进行了分析，并针对其提出两种攻击方案：追踪性攻击和全泄漏攻击。实验数据表明攻击方案能成功推测秘密数据，使得此协议不满足不可追踪性，并会导致秘密信息全泄漏的安全隐患。

本文的主要创新之处：(1)收敛速度的快速化：在针对改进 LMAP+协议[17]的攻击策略中，攻击者仅需要猜测一个秘密数据，其余秘密数据都可由其与窃听的公开传输数据表示，整个攻击过程收敛速度快，一次攻击策略实验耗时仅约为 1.44s。(2)评价函数的个性化：根据攻击策略并结合方案特点，自定义模拟退火算法的评价函数，使实验结果达到了预期的攻击效果，猜测的秘密数据与真实数据间的汉明距离均值在 10 以内。(3)攻击方式的被动化：本文提出的两种攻击方案仅采用被动攻击方式，攻击者仅需要对标签和阅读器间的传输数据进行简单的窃听操作，而不需要进行通信数据的篡改和截获等主动攻击方式。追踪性攻击只需要连续窃听两轮认证过程的通信数据以及第三轮的 PID，而完全泄漏攻击只需要窃听一轮认证过程和第二轮的 PID，这大大增加了攻击方案的可行性。

本文第 2 节是对相关工作的介绍；第 3 节是对改进的 LMAP+协议的描述；第 4 节详细介绍了基于模拟退火算法的攻击策略及实验结果；第 5 节在攻击策略实验数据的基础上，提出针对改进的 LMAP+协议的两种攻击方案：追踪性攻击和完全泄漏攻击；最后对文章进行总结。

2 相关工作

近年来，相比需要更大存储容量、更高计算代价的 RFID 认证协议，仅使用位运算及一些例如循环移位的简单运算方法的超轻量级认证协议受到了更多的重视。

2006 年，Peris 等人提出超轻量级认证协议族 UMAP，为 RFID 认证协议的研究开辟了新道路。但在 2007 年，Li 和 Wang 针对协议族中的 LMAP[13] 和 M2AP[18] 协议，利用截获、篡改协议认证过程中公开传输的数据等主动攻击手段，提出了非同步攻击和全泄漏攻击的攻击方案[19]。其中，非同步攻击使得 Tag 和 Reader 两端更新不同步，在之后的协议认证过程中双向认证失败。全泄漏攻击可以获得 Tag 端存储的所有秘密数据。同一年，Chien 和 Huang 在文献[12]中采用主动攻击的方法同样证明其存在非同步更新和秘密信息全泄漏的安全隐患。

2007 年，Chien 提出 SASI[3] 协议，SASI 引入了移位操作，同时为了防止两端更新不同步的问题，在标签端存储当前以及前一轮认证过程的秘密信息的记录，在很大程度上增加了安全性。但 SASI 协议的安全性能仍然未能达到理想要求，2009 年，Phan 利用 Jules 和 Weis 提出的不可追踪性模型[26]成功攻破了 SASI 协议[3]，证明其不具备不可追踪性[20]。Cao 等人通过对 SASI 协议认证过程中公开传输的数据最后一位的篡改，完成了 DOS 攻击，并分析其存在匿名追踪的安全隐患[21]。

2008 年，Peris 等人提出了新协议 Gossamer[15]，协议中使用了位异或、位加、循环左移等位运算。为了进一步提高协议的安全性，采用了嵌套式的循环移位，同时，引入了一种轻量级的运算方法 MixBits，它是一种非线性的函数，用以产生新的随机数，并且计算量很小。2010 年，Gossamer 协议被 Yeh 和 Lo 使用主动攻击攻破[22]，Yeh 等人使用一系列的挑战应答操作使得标签与阅读器两端的密钥信息不同步，造成非同步攻击。

2012 年，Tian 等人提出了 RAPP 协议[16]。相比之前的协议，RAPP 协议增加了 Per 运算，打乱了原数据的排列顺序，从而增加了安全性。不久，Ahmadian 等人提出了针对 RAPP 协议的非同步攻击方案[23]，其对于基于汉明重量和模数的两种移位操作的攻击成功率都约为 25%。2012 年，Wang 等人使用主动攻击[24]，伪装成有效的标签和阅读器收集部分认证信息，然后伪造合法的阅读器与标签通信大约 2^{30} 次，利用左移和置换排列运算的特性，得到了所有的秘密数据。

3 改进的 LMAP+协议[17]

2012 年，Gurubani 等人针对 LMAP+协议进行了改进和完善[17]。改进的 LMAP+协议与 LMAP+协议相比较，增加了一项密钥信息 K_3，改变了公开传输数据的表达式以及更新公式。

3.1 符号定义

在改进的 LMAP+协议中，只使用了位异或、位加等位操作，所有的数据都为 96bit。相关符号定义如表 1 所列。

表 1 相关符号说明

符号	说明
$ID_{tag(i)}$	标签的唯一标识
$PID^n_{tag(i)}$	标签在第 n 轮协议认证过程中的动态假名
$K^n_{1tag(i)}$，$K^n_{2tag(i)}$，$K^n_{3tag(i)}$	标签在第 n 轮协议认证过程中的密钥信息
r	阅读器产生的随机数
A,B,C	协议执行过程中阅读器和标签之间的传输消息
$\oplus$	异或运算符
$\|\|$	连接运算符
$+$	模 2 加法运算符
$(X)_n$	数据 X 的第 n 位

3.2 协议[17]描述

改进的 LMAP+协议中，Tag 和 Reader 两端都存储 *ID*、密钥信息(K_1，K_2，K_3)，以及 *PID*。具体的协议描述如图 1 所示。

Tag Identification

Reader ⟶ Tag ：Hello

Tag ⟶ Reader：$PIDn_{(i)}^{tag}$

Mutual Authentication

Reader ⟶ Tag ：A ‖ B

Tag ⟶ Reader ：C

Where：

$A=PID_{tag(i)}^{n}\oplus K_{1tag(i)}^{n}+r$

$B=PID_{tag(i)}^{n}\oplus K_{2tag(i)}^{n}+r$

$C=PID_{tag(i)}^{n}\oplus(K_{3tag(i)}^{n}+r)$

Updating

$PID_{tag(i)}^{n+1}=PID_{tag(i)}^{n}\oplus r+(K_{1tag(i)}^{n}+K_{2tag(i)}^{n+1}+K_{3tag(i)}^{n})$

$K_{1tag(i)}^{n+1}=K_{1tag(i)}^{n}\oplus r+(PID_{tag(i)}^{n+1}+K_{2tag(i)}^{n})$

$K_{2tag(i)}^{n+1}=K_{2tag(i)}^{n}\oplus r+(PID_{tag(i)}^{n+1}+K_{3tag(i)}^{n})$

$K_{3tag(i)}^{n}=K_{3tag(i)}^{n}\oplus r+(PID_{tag(i)}^{n+1}+K_{1tag(i)}^{n})$

图 1　改进的 LMAP+协议描述

协议由 3 个主要步骤构成：标签认证、相互认证及更新。

Tag 认证：Reader 发送 *hello* 给 Tag，Tag 收到消息后发送 *PID* 作为应答。只有合法的 Reader 能够通过收到的数据 *PID* 从数据库中搜索到对应的密钥信息(K_1，K_2，K_3)。

相互认证：Reader 产生一个随机数 r，使用 r、K_1、K_2、*PID* 计算得到 A、B，发送到 Tag。Tag 收到 A、B 后，分别从 A、B 中解得两个随机数，并且比较两个解得的数据是否相等；如果相等，Reader 成功认证，Tag 计算并发送消息 C。Reader 同样计算数据 C，并和从 Tag 端得到的数据进行比较，如果相等，那么 Tag 成功认证。Reader 使用收到的 *PID* 从数据库中匹配到对应的记录，并可以得到 Tag 的唯一标识 *ID*。

更新：在 Reader 和 Tag 认证成功后，两端需要同时更新假名和密钥。

对于 LMAP 协议不能抵御的非同步攻击，改进的LMAP+协议[17]与 LMAP+协议[14]采用了相同的方法，即在 Reader 和 Tag 两端设置了状态位 s。

4　基于模拟退火算法的攻击策略

本文的攻击策略基于模拟退火算法，其优势在于能以一定的概率接受评价函数劣化的情况，相比其它启发式算法，具有搜索范围更广、有效避免局部最优问题等特点，保证了经过攻击策略后，得到的猜测数据更加逼近真实秘密数据。同时，针对改进的 LMAP+协议，只需猜测一个秘密数据，即可表示剩余的不公开数据，确保了整个攻击过程收敛速度较快，有效地弱化了模拟退火算法收敛速度慢的缺点。本节主要介绍攻击策略的具体过程并针对改进的 LMAP+协议[17]给出攻击实验结果，为第 5 节对文献[17]进行追踪性攻击和全泄漏攻击的分析提供必要的基础。

4.1　主要思想

基于模拟退火算法攻击策略的主要思想是猜测部分秘密数据，并使用猜测的秘密数据与窃听的公开传输数据推导出剩余秘密数据。通过自定义评价函数，并根据模拟退火算法的思想[25]，不断调整猜测的秘密数据，使得评价值逐渐变小，进而得出猜测的秘密数据逼近真实秘密数据的攻击结果。攻击策略如图 2 所示。

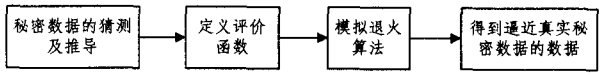

图 2　基于模拟退火算法的攻击策略图

4.2　相关操作

4.2.1　秘密数据的猜测及推导

攻击改进 LMAP+协议[17]只需要猜测秘密数据 K_1，即可推导出剩余所有的秘密数据。随机数 r 可以由截获的公开数据 A、*PID*，以及秘密数据 K_1 计算得到，猜测的 K_1 记为 $K_{1tag(i)}^{n}{}'$，推导得到的随机数记为 r'，如式(1)所示：

$$r'=A-(PID_{tag(i)}^{n}\oplus K_{1tag(i)}^{n}{}') \tag{1}$$

秘密数据 K_2 可以由截获的公开数据 B、*PID* 以及随机数 r 表示，推导得到的 K_2 记为 $K_{2tag(i)}^{n}{}'$，如式(2)所示：

$$K_{2tag(i)}^{n}{}'=B-PID_{tag(i)}^{n}-r' \tag{2}$$

秘密数据 K_3 可以由公开数据 C、*PID* 以及随机数 r 表示，推导得到的 K_3 记为 $K_{3tag(i)}^{n}{}'$，如式(3)所示：

$$K_{3tag(i)}^{n}{}'=C\oplus PID_{tag(i)}^{n}-r' \tag{3}$$

4.2.2　评价函数的定义

在模拟退火算法中，评价函数的好坏影响最终得到结果的优劣以及收敛速度。

定义 1　两个 96bit 长度的数据 X 与 Y 之间的汉明距离记为 $HD(X,Y)$。

定义 2　评价函数定义如式(4)所示。

$$CostVal=HD(PID_{tag(i)}^{n+1},PID_{tag(i)}^{n+1}{}') \tag{4}$$

其中，$PID_{tag(i)}^{n+1}{}'$是在改进 LMAP+协议[17]认证过程中，由猜测的秘密数据预测的下一轮认证过程中的 *PID*，$PID_{tag(i)}^{n+1}{}'$可以根据式(5)求得。

$$PID_{tag(i)}^{n+1}{}'=PID_{tag(i)}^{n}\oplus r'+(K_{1tag(i)}^{n}{}'+K_{2tag(i)}^{n}{}'+K_{3tag(i)}^{n}{}') \tag{5}$$

$PID_{tag(i)}^{n+1}$则是与之对应的真实 *PID*。

评价值越小，表示通过猜测的秘密数据计算得到的下一轮认证过程中的 *PID* 与对应的真实数据更加接近，在一定程度上说明猜测的秘密数据更加准确。实验结果表明此评价函数可以达到较好的实验效果。

4.3　具体描述

4.3.1　参数

下面给出实验过程中的几个重要参数。

(1)初始温度 T_0：10；

(2)降温速率 α：0.99；

(3)在每一温度上，猜测的秘密数据需改变的次数 N：200；

(4)猜测的秘密数据未接受改变时，持续降温的次数上限 *MaxFailedCycles*：20，超过此次数，则实验终止；

(5)降温次数上限 *ICMax*：600。

4.3.2　启发式攻击策略的算法描述

启发式攻击策略算法：

1. finished =false, T=T_0, IC=0, ILSinceLastAccept=0
2. randomly generate a 96-bit data as reckoned K_1, and current state is Vcurr
3. while not finished do
4. while repeatNum < N do
5. change the current reckoned K_1 (inverse 1 random bit of the reckoned K_1), the new state is Vnew

```
6.    Vnew =generateMoveFrom(Vcurr)
7.    ΔCostVal=Cost(Vnew)−Cost(Vcurr)
      //calculate the CostVal of Vnew and Vcur
8.    if ΔCostVal<=0 then
9.      Vcurr=Vnew
10.   else
11.     generate a value μ from a uniform(0,1) random variable
12.     if exp^(−ΔCostVal/T)>μ then
13.         Vcurr =Vnew
14.     else reject the change
15.     end if
16.   end if
17.   repeatNum =repeatNum +1
18. end while
19. if no move has been accepted in most recent inner loop then
20.     ILSinceLastAccept=ILSinceLastAccept+1
21. else
22.     ILSinceLastAccept =0
23. end if
24. T=T * α
25. IC=IC+1
26. if ILSinceLastAccept > MaxFailedCycles or
27.     IC>ICMax then
28:     finished =true
29.   end if
30. end while
31. the current state is the best one. vbest=Vcurr
```

在启发式攻击策略算法中，首先随机产生 96bit 长度的数据作为猜测的秘密数据 K_1；然后开始降温过程，在每一个温度上对猜测的秘密数据进行 N 次改变(改变方法是将猜测数据中的随机一位取反)，即重复执行 N 次步骤 4—18。同时在每次改变后，利用定义 2 计算改变后猜测的秘密数据的评价值，比较改变前后猜测数据评价值的大小，并按照模拟退火算法的思想判断是否接受猜测数据的改变。当降温次数超过 $ICMax$，或持续降温 $MaxFailedCycles$ 次猜测的数据都未发生改变时，算法结束，此时得到的猜测数据认为是最接近真实 K_1 的数据。

4.4 实验结果

实验运行在一台处理器为 Intel(R) Core(TM) i5-3317U，主频为 1.7GHz，内存为 4G 的计算机上。在 Win7 操作系统下，使用 VS2010 作为编程平台，C 语言为编程语言，完成攻击策略的相关实验。

实验中随机产生 5 组 96bit 的数据作为认证协议过程的真实数据，包括 K_1、K_2、K_3、随机数 r、PID，并使用这些数据按照改进 LMAP+协议[17]的表达式，计算得到对应的公开传输数据 A、B、C，以及更新后的第二轮数据 PID、K_1、K_2、K_3。当真实数据准备完备后，随机产生 1 组 96bit 长度的数据作为猜测的 K_1，结合窃听的公开传输的数据(协议认证过程中的秘密数据都认为是未知的)，开始执行基于模拟退火算法的攻击策略。最终经过优化的猜测数据逼近真实的秘密数据 K_1。

由于评价函数是根据实验得到的下一轮认证过程中的 PID 与对应真实数据的汉明距离所设计的，因此随着温度下降次数的增加评价值应越小，猜测的秘密数据也应更加逼近真实秘密数据，一次典型的实验如图 3 和图 4 所示。评价值随温度的变化趋势图显示在高温时评价值剧烈波动，随着温度的降低，波动程度逐渐变小，评价值有明显下降的趋势，并最终趋于稳定，达到预期效果。为了更好地观察到实验效果，我们在每次降温时计算了一次猜测的秘密数据与真实 K_1 的汉明距离(在真实环境中攻击者很难获知真实的秘密数据 K_1)。猜测秘密数据 K_1 与真实 K_1 的汉明距离随温度的变化趋势如图 4 所示，猜测的秘密数据 K_1 与真实 K_1 汉明距离同样随着温度的下降而变小，表明猜测的数据更加准确，最终汉明距离在 0～10 之间波动，即猜测的秘密数据与真实数据 K_1 仅有至多 10 位左右的误差(K_1 共 96 位)。

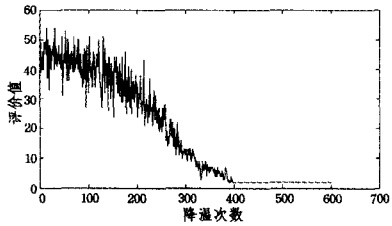

图 3 评价值随温度的变化趋势图

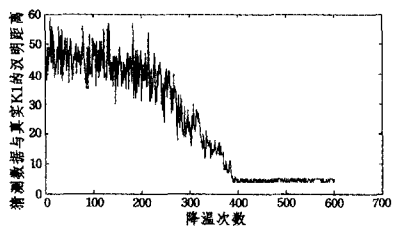

图 4 猜测秘密数据 K_1 与真实 K_1 的汉明距离随温度的变化趋势图

针对同一轮 LMAP+协议认证过程，我们随机产生了 20 组猜测的秘密数据 K_1，并且分别使用本攻击策略进行实验，观察实验前后猜测的数据与真实数据之间的汉明距离，实验结果如图 5 所示。实验前猜测的数据与真实数据 K_1 之间的汉明距离均值为 45.25，经过模拟退火算法攻击策略实验后的数据与真实数据汉明距离均值为 5.7。实验结果表明，作为猜测的秘密数据 K_1，随机产生的数据无论优劣，都可以在本攻击策略实验后逼近真实 K_1。

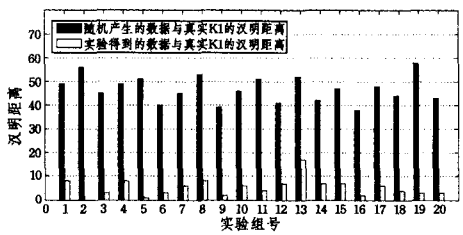

图 5 攻击策略实验前后数据与真实数据的汉明距离比较图

为了验证本攻击策略可以在任何轮次的协议认证过程中起作用，我们针对不同轮协议的认证过程，分别进行了 10 组实验，每组实验协议认证过程的真实数据都不相同，且在每组实验中分别随机产生了 50 组随机的 96bit 数据作为猜测的秘密数据 K_1，并按照攻击策略的步骤进行实验。认为实验后猜测的秘密数据 K_1 与真实 K_1 汉明距离小于等于 10 为优秀组，大于 10 小于等于 20 为合格组，大于 20 为不合格组。同时实验记录了一次攻击策略实验所需时间，统计的实验结果如表 2 所列。

表2 针对不同轮认证过程的10组实验结果表

实验号	优秀组数	合格组数	不合格组数	平均汉明距离	一次攻击策略实验平均耗时(s)
1	45	5	0	6.22	1.45
2	34	15	1	8.52	1.44
3	41	9	0	6.08	1.44
4	42	8	0	5.88	1.45
5	44	5	1	6.32	1.43
6	50	0	0	4.06	1.43
7	46	4	0	4.46	1.44
8	37	13	0	7.46	1.45
9	41	9	0	6.98	1.44
10	46	4	0	4.32	1.44

表2的统计结果表明:10组实验每一组中优秀组占据绝大多数,只有极个别出现不合格组,每组实验平均汉明距离均低于10。由此可见,在任何轮次的协议认证过程中,攻击策略均能取得较好的效果,实验获得的数据已经非常逼近真实K_1。一次攻击策略实验耗时仅约1.44s。

5 对改进LMAP+协议[17]的两种攻击方案

本节在第4节攻击策略实验结果的基础上,提出针对改进LMAP+协议[17]的两种攻击方案:追踪性攻击和完全泄漏攻击,并通过实验验证攻击效果。实验环境与第4节实验相同。

5.1 追踪性攻击

追踪性攻击方案分为以下两个步骤:(1)预测协议第三轮认证过程中的PID;(2)结合Jules和Weis提出的不可追踪性模型[26]验证协议[17]不满足不可追踪性。下面简要介绍不可追踪性模型的相关内容。

5.1.1 Jules和Weis提出的不可追踪性模型[26]

2009年,Jules和Weis提出了用于分析RFID系统安全性的不可追踪性模型[26]。模型中,标签的集合记作T,阅读器的集合记作R。攻击者A使用被动攻击和主动攻击控制所有标签和阅读器之间的认证过程。

攻击者可以发送$Execute(R,T,i)$请求,窃取R和T之间在第i轮协议认证过程中的通信数据,这属于被动攻击。同时,A也可以进行主动攻击,例如伪造合法的阅读器(标签)发送信息到指定的标签(阅读器),改变T中存储的密钥信息。本文的攻击策略只需要执行更易进行的被动攻击。攻击模型中,攻击者A通过发送$Test(i,T_0,T_1)$请求来执行一次不可追踪性的检测,A会从标签T_0、T_1对应的PID集合$\{PID_0,PID_1\}$中得到PID_b,b随机地从0和1中选择,A在不知晓b值的情况下猜测b的值$\tilde{b}$。如果猜测正确,则攻击者A成功,否则失败。在攻击模型中,A成功区分PID_0和PID_1的优势(如同抛硬币的方法猜测出b的值)记为$Adv_A^{NT}(k)$,其中k为安全系数。容易得出式(6):

$$Adv_A^{NT}(k)=|\Pr[Awins]-\Pr[random\_coin\_flip]|$$
$$=|\Pr[\tilde{b}=b]-\frac{1}{2}| \tag{6}$$

如果$Adv_A^{NT}(k)<\varepsilon(k)$,则说明RFID协议能够抵抗追踪性攻击,其中$\varepsilon(\cdot)$是可忽略函数。

为了完成一次追踪性攻击,需要预测协议第三轮认证过程中的PID,下面阐述具体的实验过程。

5.1.2 预测协议第三轮认证过程中的PID

第4节实验结果表明经过基于模拟退火算法的攻击策略得到的秘密数据K_1已经与真实K_1十分相近。实验过程中需要窃听连续两轮认证过程中公开传输的数据,包括第一轮的PID、A、B、C以及第二轮的PID。为了完成一次追踪性攻击,还需要预测出第三轮协议认证过程中的PID,本次实验需要在第4节攻击策略实验的基础上完成。

(1)窃听连续三轮认证过程中的传输数据并计算第三轮PID猜测数值

首先,进行攻击策略实验,得到第一轮秘密数据K_1的猜测数值;其次,通过猜测的第一轮K_1,以及使用其计算得到的第一轮认证过程中剩余的秘密数据,计算得到第二轮认证过程K_1的猜测数值;再次,根据窃听的第二轮公开数据A、B、C推导出其余第二轮认证过程中的秘密数据;最终,计算得到第三轮认证过程中的PID猜测数值。实验中窃听的第三轮PID是验证预测是否准确的凭证。

(2)执行多组实验得出攻击结果

针对协议不同轮次的认证过程,进行10组实验,每组实验中协议的真实数据不同,执行了500次上述预测第三轮PID的过程。通过比较预测的PID与对应的真实数据的汉明距离及其与随机数据汉明距离的大小,得出攻击实验的结果:如果前者小,则攻击成功,否则攻击失败。实验结果如表3所列。

表3 预测第三轮协议认证过程中的PID表

实验号	成功组数	失败组数	预测PID与真实数据的汉明距离均值	预测PID与随机数据的汉明距离均值
1	500	0	10.486	48.142
2	500	0	9.602	48.008
3	500	0	5.704	47.656
4	500	0	8.846	47.944
5	500	0	6.216	47.872
6	500	0	6.526	47.964
7	500	0	7.158	48.206
8	500	0	7.032	47.836
9	500	0	9.188	48.170
10	500	0	8.212	48.088

表3中的实验结果表明:预测得到的PID与真实数据的汉明距离小于其与随机数据的汉明距离的概率近乎100%,攻击者利用第4节设计的攻击策略攻击协议[17]达到预期效果。下面利用此实验结果,并结合Jules和Weis提出的不可追踪性模型[26],对改进LMAP+协议[17]进行一次追踪性攻击。

5.1.3 追踪性攻击方案的实现

根据不可追踪性模型追踪性攻击方案的3个步骤为:

(1)学习阶段

攻击者A进行被动攻击,窃听标签T_0与阅读器之间连续两轮的通信数据。

(2)挑战阶段

攻击者A选出标签T_0和标签T_1,发送$Test(i,T_0,T_1)$请求,启动一次追踪性测试。攻击者A将会得到PID_0、PID_1分别属于T_0和T_1,攻击者需要猜测给定的$PID_b\in\{PID_0,PID_1\}$中b的值,即猜测出所给定的PID_b属于T_0或是T_1。

(3)猜测阶段

攻击者利用学习阶段得到的T_0与阅读器连续两轮的通信数据,进行预测第三轮协议认证过程PID的实验。用预测

得到的 PID 分别与 PID_b 及集合$\{PID_0, PID_1\}$中另一个元素做汉明距离的比较，如果 PID_b 汉明距离更小，则 $b=0$，否则 $b=1$。

根据表 3 中的实验结果，实验预测出的 PID 与 T_0 的 PID 汉明距离小于其与 T_1 的 PID 汉明距离的概率约为 100%（T_1 的 PID 对于预测出的 PID 相当于随机数据）。如式(7)所示：

$$\Pr[HD(PID_{预测}, PID_0) < HD(PID_{预测}, PID_1)] \approx 1 \quad (7)$$

所以攻击者有近乎 100%的概率能猜测出正确的 b 值。容易得出式(8)：

$$Adv_A^{LNT}(k) = |\Pr[Awins] - \frac{1}{2}| \approx |1 - \frac{1}{2}| = \frac{1}{2} > \varepsilon(k) \quad (8)$$

通过以上分析可以得出，A 成功区分 PID_0 和 PID_1 的概率约为 100%。因此改进 LMAP+协议[17]不能够抵抗追踪性攻击，即协议[17]不满足不可追踪性。

5.2 完全泄漏攻击

根据 4.4 节的实验结果，猜测的秘密数据并没有达到 100%的概率与真实秘密数据相同，但都逼近真实数据。

为了得到更加准确的数据，针对协议同一轮的认证过程，我们通过重复执行多次攻击策略的实验，得到多个猜测的秘密数据。将猜测数据转化为二进制，记得到的数据为 N 个，针对得到数据的每一位(共 96 位)统计出现 1 的次数为 S，出现 0 的次数为 $N-S$。如果$\frac{S}{N} > \frac{1}{2}$，则对应的位置上为 1，反之为 0。实验共 20 组，每组实验针对协议的一轮认证过程，共猜测 20 个秘密数据 K_1。经过上述过程，得到如表 4 所列的实验结果。

表 4 完全泄漏攻击下的 10 组实验结果表

实验号	攻击策略实验结果与真实 K_1 的汉明距离均值	完全泄漏攻击实验得到的数据与真实 K_1 的汉明距离	实验号	攻击策略实验结果与真实 K_1 的汉明距离均值	完全泄漏攻击实验得到的数据与真实 K_1 的汉明距离
1	7.45	0	11	6.75	0
2	6.1	0	12	6.35	0
3	5.4	0	13	4.4	0
4	4.55	1	14	3.5	1
5	5.2	0	15	5.9	0
6	5.4	1	16	7	0
7	6.3	0	17	6.5	0
8	6.4	0	18	7.65	0
9	8.15	3	19	9.85	3
10	6.1	1	20	8.5	0

表 4 中的实验结果表明：实验得到的猜测数据约有 70%的概率与真实数据完全相同。判别得到的猜测数据是否与真实 K_1 相同，只需将其代入该轮认证过程，计算第二轮认证过程的 PID 是否与真实 PID 相同。如果不同，则重新执行一次攻击方案，直到得到正确的 K_1。如果相同，得到真实数据 K_1 后，根据 4.2 节的介绍，很容易得到剩余所有秘密数据，完成全泄漏攻击。

结束语 本文针对改进的 LMAP+协议设计了基于模拟退火算法的攻击策略，并对该协议进行安全性分析，通过自定义评价函数，以启发式算法的思想，使猜测数据逐渐逼近真实秘密数据。在攻击策略的基础上，结合 Jules 等人提出的不可追踪性模型完成追踪性攻击；通过重复执行攻击策略实验，完成全泄漏攻击。实验结果表明，追踪性攻击的成功率约为 100%，全泄漏攻击一次攻击的成功率约为 70%；且攻击过程收敛速度快，一次攻击策略实验耗时仅约为 1.44s，猜测的秘密数据与真实数据间的汉明距离均值稳定在 10 以内，同时具有被动攻击的可行性较高等特点，达到了预期的攻击效果。本文针对改进 LMAP+协议设计的启发式攻击策略对使用移位操作以及置换排列操作的认证协议（如 Gossamer、RAPP 等）并不能取得很好的效果。未来工作是改进攻击策略，使其能适用攻击此类协议。同时，设计出能够克服此类攻击手段的 RFID 超轻量级认证协议。

参 考 文 献

[1] Juels A. RFID security and privacy: A research survey[J]. IEEE Journal on Selected Areas in Communication, 2006, 24(2): 381-394

[2] Barrero D F, Hernández-Castro J C, Peris-Lopez P, et al. A genetic tango attack against the David-Prasad RFID ultra-lightweight authentication protocol[J]. Expert Systems, 2014, 31(4): 9-19

[3] Chien H Y. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 337-340

[4] Juels A, Molner D, Wagner D. Security and Privacy Issues in E-Passports[C]// Security and Privacy for Emerging Areas in Communications Networks, 2005. 2005: 74-88

[5] Kumar S, Paar C. Are Standards Compliant Elliptic Curve Cryptosystems Feasible on RFID? [C]// Workshop RFID Security, 2006. 2006: 12-14

[6] Rhee K, Kwak J, Kim S, et al. Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment [C]// Proc. Int'l Conf. Security in Pervasive Computing. Berlin: Springer-Verlag, 2005: 70-84

[7] Yang J, Park J, Lee H, et al. Mutual Authentication Protocol [C]// Proc. Ecrypt Workshop RFID and Lightweight Crypto, 2005. 2005

[8] Duc D N, Lee H, Kim K. Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning[M]. Auto-ID Labs Information and Communication University, 2006

[9] Juels A. Strengthening EPC Tag against Cloning [C]// Proc. ACM Workshop on Wireless Security, 2005. Cologne, 2005: 67-76

[10] 邓淼磊，黄照鹤，鲁志波. EPCGen2 标准下安全的 RFID 认证协议[J]. 计算机科学，2010，37(7)：115-117

[11] Liu Ya-li, Qin Xiao-lin, Li Bo-han, et al. A Forward-Secure Grouping-proof protocol for Multiple RFID tags [J]. International Journal of Computational Intelligence Systems, 2012, 5(5): 824-833

[12] Chien H Y, Huang C W. Security of Ultra-Lightweight RFID Authentication Protocols and Its Improvements[J]. ACM Operating System Rev., 2007, 41(2): 83-86

[13] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags[C]// Proc. Second Workshop on RFID Security, 2006. Graz: Ecrypt, 2006: 6-17

[14] Li Tie-yan. Employing lightweight primitives on low-cost rfid tags for authentication[C]// Vehicular Technology Conference, 2008(VTC 2008-Fall), IEEE 68th. IEEE, 2008:1-5

[15] Peris-Lopez P, Hernandez-Castro J C, Tapiador J M E, et al. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol[C]// Proc. International Workshop on Information Security Applications(WISA'08), 2009. Berlin: Springer Berlin Heidelberg, 2009:56-68

[16] Tian Yun, Chen Gong-liang, Li Jian-hua. A New Ultralightweight RFID Authentication Protocol with Permutation[J]. IEEE Communications Letters, 2012, 16(5):702-705

[17] Gurubani J B, Thakkar H, Patel D R. Improvements over extended LMAP+: RFID authentication protocol[C]// 6th International Conference on Trust Management-FIPTM, 2012. Surat: Springer Boston, 2012:225-231

[18] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags[C]// Proc. of UIC, 2006. Berlin: Springer-Verlag, 2006:912-923

[19] Li Tie-yan, Wang Gui-lin. Security analysis of two ultra-lightweight RFID authentication protocols[C]// Proc. of IFIP-SEC'07, 2007. Sandton: Springer US, 2007:109-120

[20] Phan R C W. Cryptanalysis of a new ultralightweight RFID authentication protocol-SASI[J]. IEEE Transactions on Dependable and Secure Computing, 2008, 6(4):316-320

[21] Cao Tianjie, Bertino E, Lei Hong. Security Analysis of the SASI Protocol[J]. IEEE Trans. Dependable and Secure Computing, 2009, 6(1):73-77

[22] Yeh K H, Lo N W. Improvement of two lightweight RFID authentication protocols[J]. Information Assurance and Security Letters, 2010, 1:6-11

[23] Ahmadian Z, Salmasizadeh M, Aref M R. Desynchronization attack on RAPP ultralightweight authentication protocol[J]. Information Processing Letters, 2013, 113(7):205-209

[24] Wang Shao-hui, Han Zhi-jie, Liu Su-juan, et al. Security analysis of RAPP: an RFID authentication protocol based on permutation [R]. Cryptology ePrint Archive, Report 2012/327. 2012

[25] Clark J A, Jacob J L. Fault Injection and a Timing Channel on an Analysis Technique[C]// International Conference on the Theory and Applications of Cryptographic Techniques, 2002. Berlin: Springer-Verlag, 2002:181-196

[26] Juels A, Weis S A. Defining Strong Privacy for RFID[J]. ACM Transactions on Information and System Security, 2009, 13(1): 342-347

(上接第 115 页)

在目标词的确定过程中，我们可以明确目标词 D 一定是名词并且目标词的出现相对于关系代表词的出现更加集中和准确。因此，在目标词的确定实验部分不再使用 *MRR* 指标，只要出现在排名第 1 位则认为准确，否则错误，因此这里只采用正确率进行衡量。从表 8 可以看出，SVMbCAR 抽取目标词的准确率达到了 90.5%，而 STAbCAR 的准确率为82.8%。

表 8 两种方法抽取目标词的结果比较

	正确个数	准确率
STAbCAR	497	0.828333
SVMbCAR	543	0.905

结束语 类比检索是一种根据已知领域知识查询未知领域知识的全新检索方式。通过分析词对间的潜在关系，类比检索可以准确地返回目标信息。即，给定查询请求 $Q=\{A:B,C:?\}$，类比检索的目标是得到?所代表的目标词 D，其中 A 与 B 的关系和 C 与 D 的关系相似。本文提出了基于 SVM 的中文类比方法。该方法首先利用 SVM 识别潜在关系句，然后抽取出潜在关系句中的相关词语作为关系代表词或目标词。本文采用从人立方中选取的 600 组人物实例对设计了两个实验，一是针对潜在关系句识别的实验，二是针对关系代表词抽取和目标词抽取的实验。实验结果表明了，本文提出的 SVMbCAR 在潜在关系句识别、关系代表词和目标词抽取两个方面的效果。

本文提出的 SVMbCAR 方法虽然取得了良好效果，但也存在一些需要改进的地方：(1)由于需要实时抓取大量网页语料进行处理，时间和空间消耗较大。接下来的研究考虑通过提高关系词的提取准确率来减少网页访问次数，以实现实时的类比检索。(2)在 SVMbCAR 算法中，特征提取的有效性对识别准确率有较大的影响，未来考虑选取更加有效的特征来构造特征向量，提高潜在关系句的识别准确率，进而提高抽取关系词和目标词的准确率。(3)进一步研究 SVM 的不同参数对实验效果的影响。

参 考 文 献

[1] Kato M P, Ohshima H, Oyama S, et al. Query by analogical example: relational search using Web search engine indices[C]// Proceedings of the 18th ACM Conference on Information and Knowledge Management. ACM, 2009:27-36

[2] Duc N T, Bollegala D, Ishizuka M. Using relational similarity between word pairs for latent relational search on the web[C]// 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT). IEEE, 2010, 1:196-199

[3] Goto T, Duc N T, Bollegala D, et al. Exploiting symmetry in relational similarity for ranking relational search results[C]//PRICAI 2010: Trends in Artificial Intelligence. Springer Berlin Heidelberg, 2010:595-600

[4] Duc N T, Bollegala D, Ishizuka M. Cross-language latent relational search: Mapping knowledge across languages[C]// Proceedings of 25th AAAI Conference on Arificial Intelligence. 2011:1237-1242

[5] Liang Chao, Lu Zhao. Chinese Latent Relational Search Based on Relational Similarity[M]// Data and Knowledge Engineering. Springer Berlin Heidelberg, 2012:115-127

[6] 中科院分词系统ICTCLAS[OL]. http://www.ictclas.org/. 2012

[7] Chang C-C, Lin C-J. LIBSVM: a library for support vector machines[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2011, 2(3):27

[8] 鲁松，白硕，黄雄. 基于向量空间模型中义项词语的无导词义消歧[J]. 软件学报，2002，13(6)：1082-1089

[9] 人立方关系搜索[OL]. http://renlifang.msra.cn/