基于CSP的物联网David数字图书馆协议的改进与形式化分析

吴名欢 程小辉
(桂林理工大学信息科学与工程学院 桂林 541004)

摘 要 在分析了物联网通信节点使用的David数字图书馆通信协议运行的基础上,指出了此协议存在阅读器非法扫描标签和协议主体没有会话密钥的安全隐患,提出了解决安全隐患的方案。采用通信顺序进程(CSP)的形式化分析方法对提出的方案进行了建模分析,对复杂环境下的攻击者和各协议主体建立了CSP进程。在实验中,攻击者在Dolev_Yao模型下对新的协议方案模型进行攻击,最后没有发现攻击点。实验结果表明,该协议方案能有效解决David数字图书馆协议的安全隐患,保证了协议主体的相互认证性以及会话密钥的安全性,证明了模型的可行性。

关键词 物联网,形式化分析,David数字图书馆协议,通信顺序进程
中图法分类号 TP393.04 **文献标识码** A

On CSP Improvements to David's Digital Library Protocol and Formal Analysis in Internet of Things

WU Ming-huan CHENG Xiao-hui
(Institute of Information Science&Engineering, Guilin University of Technology, Guilin 541004, China)

Abstract This paper analysed David's digital library protocol used in the Internet of Things, and pointed out the security risks of this protocol. Aiming at the security risks was put forward. this protocol, the way to solve the security risks was put-forward. Using the formal analysis method, the communicating sequential processes (CSP), role of protocol and the attackers were modeled. In the experiments, the new protocol is attacked under Dolev_Yao model by a attacker, but no attacks is finally founded. The experimental results show that the algorithm can effectively solve the security risks of this David's digital library protocol. Mutual authentication protocol role, as well as the security of the session key, and the feasibility of the model are proved.

Keywords Internet of things, Formal analysis, David's digital library protocol, Communicating sequential processes

物联网是新一代信息技术的高度集成和综合运用,推动物联网的运用和发展,有利于促进生产生活方式的改变。现在物联网还处于发展的初级阶段,关键技术有待突破,网络信息安全还存在一些隐患。在物联网的发展过程中需要增强对信息系统的安全保障,形成系统安全可用和数据安全可信的物联网应用系统[1,2]。

在物联网中安全协议是保护系统安全性的重要方法,也是对用户隐私保护的重要基础。然而设计一个完美的安全协议是一件非常艰苦和困难的工作,有些安全协议在使用了很多年后通过研究者找出了其漏洞,因此研究者研究了一些方法在设计阶段便对设计的安全协议进行分析和验证,在这些方法中,形式化的分析方法是一个非常实用而且重要的方法。

通常情况下,形式化的分析方法需要对协议系统建立完整的协议逻辑模型和数学推理,以及一些相关的验证方法,来判断协议的安全性是否达到其设计要求或者验证推理是否正确。Needham和Schroeder首先将形式化的方法应用于协议的安全性分析,后来Delov和Yao在此领域做了一些重要的研究,对攻击者的行为做了形式化的分析研究[3,4],提出了被称为Delov-Yao的攻击者模型。

用形式化方法对协议的安全性进行分析,可以归纳出两种方法,它们分别是模型检测法和定理证明法。

1. 模型检测法:这个方法认为协议运行的状态是在一个有限度的状态空间中,通过对这些状态的检测,验证其是否符合安全性说明的正确条件。如果不满足通常可以提供一个反例的迹,和定义证明方法相比,这个方法非常适合研究有穷状态协议的安全性,找出协议容易受攻击的地方。

2. 定理证明法:该方法利用相关的数学建模理论对协议的所有的状态进行分析,推理出是否满足协议的安全性说明。这个方法相对于模型检测法,其对协议的安全性进行证明更具有优势,同时它的另外一个优点就是在无限状态中能进行推理证明,而模型检验法必须是有在穷状态空间中进行。

本文利用模型检测方法中的故障发散改进检测器(Failures-Divergence Refinement,简称FDR[5])结合通信顺序进程(CSP)研究协议的安全性。通信顺序进程(CSP)是一种非常有效的通信协议建模分析方式,使用CSP对通信协议进行建模分析,即对每一个协议主体都建模为一个独立的通信进程,

到稿日期:2013-03-11 返修日期:2013-06-22 本文受国家自然基金项目(61262075),广西高等学校重大科研项目(20120120012),广西教育厅项目(201010LX192)资助。

吴名欢(1978—),男,硕士,实验师,主要研究方向为物联网安全协议、计算机网络应用,E-mail:wwmmhh8899@tom.com;程小辉(1961—),男,教授,主要研究方向为物联网系统、计算机网络安全。

彼此通过消息进行交互，然后对构成的系统进行分析[6]；目前在通信协议的形式化分析研究中 CSP 最著名，它对攻击者的能力以及协议运行环境进行了严格的规范，这样能对协议的安全性进行更深入的分析[7]。

David 数字图书馆协议是一个应用于物联网感知层的 RFID 通信协议。文献[8]对 David 数字图书馆 RFID 协议进行了介绍，文献[9]利用串空间的方法对此协议进行了分析，文献[10-12]使用 hash 函数对协议进行了分析改进。这些参考文献从不同的角度对协议进行了分析改进，但是对阅读器非法扫描标签、进行恶意跟踪的安全问题没有提出解决办法。任何人都能够使用阅读器对标签进行扫描，即使标签进行了加密处理也能通过重放加密信息对有固定加密信息的标签进行跟踪定位。

本文对 David 数字图书馆协议进行了分析，针对阅读器非法扫描标签的安全隐患提出了解决问题的办法，采用 CSP 的形式化分析方法对其进行建模分析，并通过实验对其进行验证。

1 CSP 语法

在用 CSP 分析通信协议中，对协议的不同角色建立不同的进程，例如，分别对协议发起者、响应者以及认证服务器建立不同的进程。而这些进程彼此间交互以及与环境的交互都是通过一些通信事件进行的。当执行一个通信事件时，通常需要多个进程进行合作。在 CSP 中通信表现为可见事件和动作的形式，进程也可以执行表示内部进展的不可见动作，所有的可见事件用 Σ 表示，内部动作用 τ 表示[13]，$\surd$ 表示一个进程的成功执行。假如一个进程用 p 表示，则可以用 $\alpha_P = \Sigma^{\surd}$ 表示 p 能够执行的所有可见事件集合。CSP 核心语法如定义 1。

定义 1[14] CSP 进程通过下面语法递归的方式进行定义

$P \triangleq \mathrm{STOP} \mid \mathrm{SKIP} \mid \mathrm{DIV} \mid x{:}A \to P(x) \mid P1 \Box P2 \mid P1 \sqcap P2 \mid P1 \underset{B}{\|} P2 \mid P1;P2 \mid P \backslash A \mid P[\![R]\!] \mid \mu P \cdot F(P)\mathrm{STOP}$

其中，STOP 表示进程死锁。$x{:}A \to P(x)$ 表示事件前缀选择，它提供了所有 A 中的动作，而且当环境选择任意的 $x \in A$，那么就执行 $P(x)$。SKIP 表示进程成功终止。$P1 \Box P2$ 和 $P1 \sqcap P2$ 分别表示进程 $P1$、$P2$ 进程的外部环境选择和内部选择。$P1 \underset{B}{\|} P2$ 表示进程 $P1$、$P2$ 在事件集 B 中保持同步，即 $B = \alpha P1 \cap \alpha P2$。$P1;P2$ 表示顺序组合，执行完 $P1$ 接着执行 $P2$。$P \backslash A$ 表示事件隐藏，隐藏事件集 A 中的所有事件。$P[\![R]\!]$ 表示进程重命名。$\mu P \cdot F(P)\mathrm{STOP}$ 表示递归进程。

定义 2 穿插运算符 $|||$ 允许两个进程 P1、$P2$ 彼此没有任何交互的情况下并行运算。用 $P1 ||| P2$ 表示 $P1$、$P2$ 两个进程的穿插。对一个有限索引集 I 以及进程 $P_i, i \in I$，$|||_{i \in I} P_i$ 表示所有的进程 P_i 交错执行[6]。

定义 3(信道的定义) 在一个协议的系统模型中通常需要用到以下几个通信信道。

信道 comm 用于两个代理正常信息交互；fake 信道用于攻击者伪造信息，并被诚实代理接收；intercept 信道用于攻击者截取信息，此信息由诚实代理发送；env 信道用于用户或者环境发送或者接收消息；signal 信道用于发送诚实代理的状态信息或者其它要求，形如 signal. Claim_Secret. A. s. Bs 的事件表示 A 相信除了 Bs 能知道 s 外，其他任何实体不能知道 s，而 singal. Runningn. r. A. B. vs 则表示 A 相信自己以 r 身份正在与 B 使用 vs 数据运行协议，singal. Commit. r. A. B. vs 表示 A 相信自己以 r 身份与 B 使用 vs 数据完成了协议的运行；leak 信道用于标识攻击者已经获取了某些特定的实体。

定义 4 对于进程 P 所有可能执行的事件序列集合称为迹，用 $traces(P)$ 表示，迹是 CSP 中一个重要的方法，对进行行为和性质的刻画起了很重要的作用，认证的性质可以刻画为迹的性质。下面是迹的性质：

性质 1 left 输入的前节总是 right 信道的输出，而且总是没有其他行为。如下表达式：

$\mathrm{tr} = \mathrm{tr} \upharpoonright \{\mathrm{right}, \mathrm{left}\} \wedge \mathrm{tr} \downarrow \mathrm{right} \leqslant \mathrm{tr} \downarrow \mathrm{left}$

其中，$\mathrm{tr} \downarrow \mathrm{right}$、$\mathrm{tr} \downarrow \mathrm{left}$ 分别是迹 tr 沿信道 right、left 的序列。

性质 2 在迹的特性中，事件(commit) 的每次发生都是 starting 在前，然后是 running，这两者一致发生直到最后的 commit 出现。

$\mathrm{tr} = \mathrm{tr}' \langle \mathrm{commit} \rangle \to \exists tr_1, tr_2 \cdot tr' = tr_1\ tr_2 \wedge \langle starting, running \rangle \leqslant tr_2 \upharpoonright \{\mathrm{starting}, \mathrm{running}\} \wedge tr_2 \upharpoonright \{\mathrm{commit}\} = \langle\rangle$

性质 3 事件 error 从不发生

$\mathrm{tr} \lceil \{\mathrm{error}\} = \langle\rangle$

当一个进程 P 的所有迹都满足迹的逻辑特性 $S(tr)$ 时，就把 $P\ sat\ S(tr)$ 记做：

$P\ sat\ S(tr) \Leftrightarrow \forall tr \in traces(P).\ S(tr)$ 。一般在逻辑中用 $P\ sat\ S(tr)$ 表达[13,15]。

2 David 数字图书馆协议

David 等提出了基于预共享秘密的数字图书馆 RFID 协议，此协议的运行流程如图 1 所示。在协议运行之前，用户需先在服务器中预先注册标签的 ID 值和共享的密钥 s。此协议的执行过程如下[8,16]：

1. Tag 读写器把生成的新鲜值 R_r 发送给 Tag，启动协议；

2. Tag 计算 $\delta = ID \oplus fs(0, R_r, R_T)$，其中 R_T 是 Tag 生成的新鲜值，然后返回 (R_T, δ) 给 Tag 读写器；

3. Tag 读写器把值 (R_r, R_T, δ) 直接转发给服务器；

4. 服务器遍历 (s_j, ID_j) $(0 < j \leqslant N, N$ 为已经注册的标签数)，然后计算 $ID_j ? = \delta \oplus fs_j(0, R_r, R_T)$，如果等式成立，则将 $\beta = ID_j \oplus fs_j(1, R_r, R_T)$ 发送给 Tag 读写器；

5. Tag 读写器直接转发接收到的 β 给 Tag 标签；

6. Tag 检查 $ID ? = \beta \oplus fs(1, R_r, R_T)$，等式成立则认证通过。

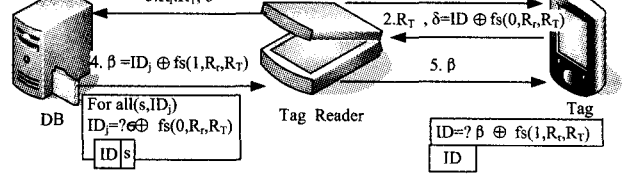

图 1 David 数字图书馆协议

从协议的运行过程来看，此协议存在以下安全隐患：

1. 服务器只对 Tag 标签进行了认证，对 Tag 阅读器没有进行任何认证等工作，攻击者便能利用此漏洞，使用非法的 Tag 阅读器进行一些攻击行为。

2. 服务器在对 Tag 标签进行认证后，没有为 Tag 标签和

Tag 阅读器之间产生会话密钥，这样 Tag 标签和 Tag 阅读器的通信信息无法加密。这样的通信显然是不安全的。

3 协议改进

第 2 节分析了 David 数字图书馆协议以及存在的安全隐患，本节将对其安全隐患提出相应的解决方案。在协议运行之前，用户在服务器中预先注册标签阅读器的 ID 值和共享的密钥 k，在协议中增加对 Tag 阅读器的认证；同时对新鲜值进行加密传送；服务器在它们进行认证的同时，产生一个会话密钥并通过加密方式传送给 Tag 阅读器和 Tag 标签，这样在后续的通信中便可以使用会话密钥进行加密传送。协议改进后的算法流程图如图 2 所示，其协议如下：

1. M1：$R \rightarrow T: R_r$；

2. M2：$T \rightarrow R: R_r, R_T, IDt \oplus fs(0, R_r, R_T)$；

3. M3：$R \rightarrow S: IDt \oplus fs(0, R_r, R_T), IDr \oplus f_k(0, R_r, R_T), R_r, R_T$；

4. M4：$S \rightarrow R: ID_j \oplus fs_j(1, R_r, R_T), fs_j(ID_j) \oplus krt, ID_i \oplus fs_i(1, R_r, R_T), fs_i(ID_i) \oplus krt$；

5. M5：$R \rightarrow T: ID_j \oplus fs_j(1, R_r, R_T), fs_j(ID_j) \oplus krt$；

6. M6：$T \rightarrow R: M \oplus krt$。

其中，R、T 和 S 分别表示 Tag 读写器、Tag 标签和服务器；M1－M6 表示消息的编号。此协议的运行过程如下。

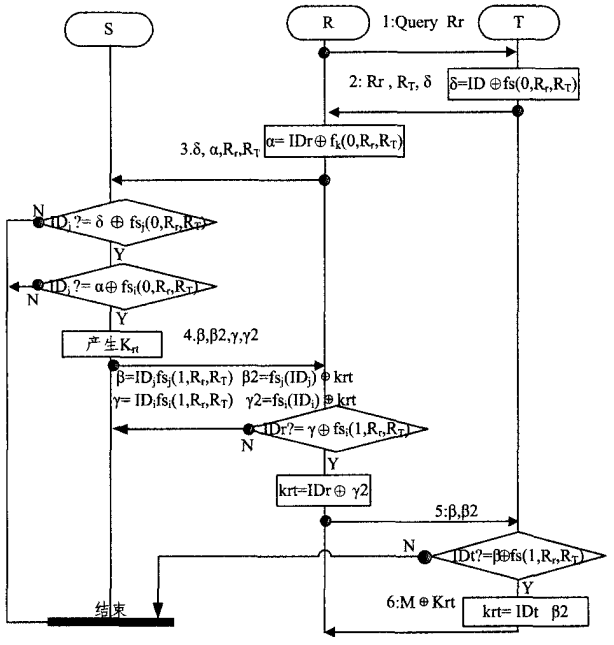

图 2 协议改进后算法流程图

1. Tag 读写器把生成的新鲜值 R_r 发送给 Tag，启动协议；

2. Tag 计算 $\delta = IDt \oplus fs(0, R_r, R_T)$，其中 R_T 是 Tag 生成的新鲜值，然后返回 (R_r, R_T, δ) 给 Tag 读写器；

3. Tag 读写器计算 $\alpha = IDr \oplus f_k(0, R_r, R_T)$，然后把 $(\delta, \alpha, R_r, R_T)$ 发给服务器；

4. 服务器遍历 $(s_j, ID_j), (s_i, ID_i)$ $(0 < j, i \leqslant N, N$ 为已经注册的标签数)，再计算 $ID_j ? = \delta \oplus fs_j(0, R_r, R_T)$ 和 $ID_i ? = \alpha \oplus fs_i(0, R_r, R_T)$，如果等式成立，则产生一个会话密钥 krt，接着分别计算 $\beta = ID_j \oplus fs_j(1, R_r, R_T)$、$\beta 2 = fs_j(ID_j) \oplus krt$、$\gamma = ID_i \oplus fs_i(1, R_r, R_T)$、$\gamma 2 = fs_i(ID_i) \oplus krt$ 的值，将它们发送给 Tag 读写器；

5. Tag 读写器检查 $IDr ? = \gamma \oplus fs_i(1, R_r, R_T)$，若等式成立，则计算 $krt = IDr \oplus \gamma 2$，并把 β 和 $\beta 2$ 的值发给 Tag 标签；

6. Tag 检查 $IDt ? = \beta \oplus fs(1, R_r, R_T)$，若等式成立则计算 $krt = IDt \oplus \beta 2$，即认证通过；

7. 把需要通信的消息 M 用会话密钥 krt 进行加密传送。

改进 David 数字图书馆协议后的协议不但对 Tag 标签进行了认证而且对 Tag 阅读器也进行了认证，同时在对它们认证的基础上产生一个会话密钥，并通过密文的方式传递给它们。

算法中采用的异或加密方法有如下等式成立，假设两个数 $k1, k2$ 进行按位异或运算：$k1 \oplus k2$ 或者用 $V(K1, K2)$ 标记，等式 $V(K1, V(K1, K2)) = K2$ 成立，所以在上述协议描述中只要代理知道异或运算的一个值便能计算出另外一个值。而在协议中应用单向性能的函数能保证认证端对被认证端的匿名性。

4 用 CSP 对协议建模

4.1 协议系统模型

在对改进后的协议系统建模的过程中，恶劣的运行环境用攻击者来表示，他们的外表接口通过 3 个通信信道来表示，分别是 comm(表示两个代理的正常通信)、intercept(表示攻击者截取信息)、fake(表示攻击者伪造信息)。它们的关系用图 3 表示。

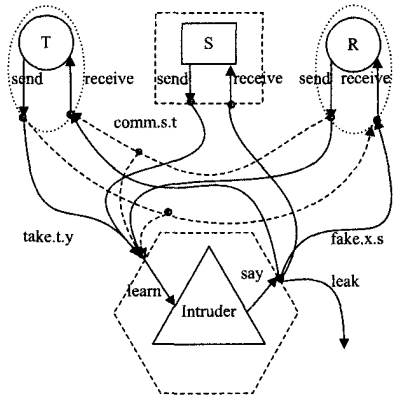

图 3 攻击者协议模型

在 R, T, S 的内部分别用 receive 和 send 信道来接受和发送信息，通过重命名机制和 comm 信道连接；在攻击者内部用 learn 和 say 来接受和发送消息，他们通过重命名机制分别与 intercept 和 fake 机制相连接。引入重命名机制后，对改进后的协议进行建模，可以表示为：

DDL2P=(Agent(R)[[fake, take/receive, send]] ||| Agent (T)[[fake, take/receive, send]] ||| (Agent(S) [[fake, take/receive, send]])

System=(DDL2P) $\underset{\{|intercept, fake, comm|\}}{\|}$ (Intruder[[comm. r. t, take. r. t, fake. r. t/learn, learn, say $|r, t \subseteq$ Agent $\cup \{$Intruder$\}$]])

协议 DDL2P 用 R、T 和 S 的穿插表示，在协议运行环境中加入攻击者角色后，整个系统用 DDL2P 与攻击者 Intruder 在 take、fake 和 comm 信道上保持同步来表示。其中各个信道的联系通过 CSP 的重命名机制来实现。

通常，在 CSP 模型中，攻击者是基于 Dolev_Yao 模型[17]的，在整个模型中假设攻击者有能力窃听、阻塞、修改和伪造信息。假如信息是由攻击者已知的密钥加密而成的密文，则

攻击者可以解密此密文并获取信息；否则攻击者记住这个信息。攻击者可以根据自身的知识随意重放或者伪造信息等等[18]。攻击者自身可以用等式表示 spy(known)：

$spy(X)=$ say? x:inter(X,Messages) →spy(X)

□learn? x→spy(close(union(X,{x})))

参数 X 表示协议实体进程所产生或者通过媒体接收的消息，并且表示所有攻击者合理创建的事物，Messages 是消息集，函数 close(X)计算所有的在加密规则下可从 X 中创建的实体[19]。攻击者可以直接监听通信，可以观察到每个通信实体的所有的消息都在攻击者的迹中出现。只要会话密钥不出现在 say 信道中，通信就是安全的[13,15]。

4.2 协议角色的 CSP 进程模型

分别给各个协议角色建立进程模型时，每一个进程运行协议表现出来的是接收或者发送的一系列的消息。首先对协议的有限状态进行建模。相关集合的定义如下：

1. 发起者集合为 Initiator(R)；
2. 响应者集合为 Responder:{S,T,Intruder}；
3. 临时值集合为 Nonce:{R_r,R_T}。

用 M1、M2、M3、M4、M5、M6 分别表示协议中的 6 条消息。

然后对协议主体 S、R 和 T 进行建模。在图 3 中定义了一些信道，但还有一些接口信道定义如下：(1) user 和 session 信道分别表示客户进行会话请求和会话的外部接口；(2) I_running. R. T 表示协议主体 R 相信正与响应者 T 会话；R_running. T. R 表示响应者 T 正与发起者 R 会话；(3)I_commit. R. T 表示发起者已经完成与响应者的会话，进行信息传递；R_commit. T. R 表示响应者与发起者完成会话，开始数据传递[7]。

从 S 作为认证服务器的角度看：

1. S 接收从 R 发送来的消息 M3；
2. S 发送消息 M4 给 R。

用 CSP 对服务器 S 接收和发送的一系列消息的进程建模如下：

SERVER(R_T,R_T,IDr,k,ID_T,s)≙

S_running. R. T→□(R∈ Initiator, T、S∈ Responder, R_r、R_T∈Nonce,krt、K、r∈Keys)

{Receive. M3. R. S. IDt ⊕ Encrypt(s,sq⟨0,R_r,R_T⟩),
IDr ⊕ Encrypt(k,sq⟨0,R_r,R_T⟩),R_r,R_T→
Check(IDt ⊕ Encrypt(s,sq⟨0,R_r,R_T⟩),R_r,R_T) →
Check(IDr ⊕ Encrypt(k,sq⟨0,R_r,R_T⟩),R_r,R_T) →
$\beta=ID_j \oplus fs_j(1,R_r,R_T)$,$\beta 2=fs_j(ID_j)\oplus krt$
$\gamma=ID_i \oplus fs_i(1,R_r,R_T)$,$\gamma 2=fs_i(ID_i)\oplus krt$
send. M4. S. R. β,$\beta 2$,γ,$\gamma 2$→
S _commit. R. T→Session. S. R. R_r. R_T. krt→Skip}

从 T 作为响应者的角度看：

1. T 接收从 R 发送来的消息 M1；
2. T 发送消息 M2 给 R；
3. T 接收从 R 发送来的消息 M5；
4. T 发送消息 M6 给 R。

用 CSP 对 T 接收和发送的一系列消息的进程建模如下：

RESPONSE(R_T,ID_T,s,S)≙

R_running. R. T→□(R∈ Initiator, T、S∈ Responder, R_r、R_T∈Nonce,krt、K、r∈Keys)

{Receive. M1. R. T. R_r→
send. M2. T. R. R_r,R_T,IDt ⊕ Encrypt(s,sq⟨0,R_r,R_T⟩)→
Receive. M5. R. T. ID_j ⊕ Encrypt(s,sq⟨1,R_r,R_T⟩),
Encrypt(s,ID_j)⊕ krt→Check(ID_j ⊕
Encrypt(s,sq⟨1,R_r,R_T⟩))→send. M6. T. R. $M\oplus krt$→
singal. claim_secret. R. T. krt→R _commit. R. T→
Session. R. T. R_r. R_T. krt→Skip}

从 R 作为初始者的角度看：

1. R 发送消息 M1 给 T；
2. R 从 T 收到消息 M2；
3. R 发送消息 M3 给 S；
4. R 从 S 收到消息 M4；
5. R 发送消息 M5 给 T；
6. R 从 T 收到消息 M6。

用 CSP 对发起者 R 接收和发送的一系列消息的进程建模如下：

INITIATOR(R_r,IDr,k,S)≙user. R? T→
I_running. R. T→comm. M1. R. T. R_r→
□(R∈ Initiator, T、S∈ Responder, R_r、R_T∈ Nonce, krt、K、r∈Keys)

{Receive. M2. T. R. R_r,R_T,IDt ⊕ Encrypt(s,sq⟨0,R_r,R_T⟩)→
send. M3. R. S. IDt ⊕ Encrypt(s,sq⟨0,R_r,R_T⟩),
IDr ⊕ Encrypt(k,sq⟨0,R_r,R_T⟩),R_r,R_T→
$\beta=ID_j \oplus fs_j(1,R_r,R_T)$,$\beta 2=fs_j(ID_j)\oplus krt$
$\gamma=ID_i \oplus fs_i(1,R_r,R_T)$,$\gamma 2=fs_i(ID_i)\oplus krt$
Receive. M4. S. R. β,$\beta 2$,γ,$\gamma 2$→
Check(γ)→send. M5. R. T. β,$\beta 2$→Check(β) →
Receive. M6. T. R. $M\oplus krt$→singal. claim_secret. R. T. krt
I_commit. R. T→Session. R. T. R_r. R_T. krt→Skip}

在这些协议角色的 CSP 进程中使用了事件 singal. claim_secret. R. T. krt，它存在如下等式：singal. claim_secret. R. T. krt in tr⇒¬(leak. krt in tr)，其中 tr 表示迹。其表示密钥 krt 不能出现在信道 leak 中，也就是在 R 和 T 之间运行时，使用的值 krt 必须在整个协议运行中是保密的；一旦在信道 leak 中出现了 krt 则表示攻击者已经获取了此密钥。以此表示保密性，同时通过 running 和 commit 在迹模型中的出现顺序或者出现与否来进行实体的认证。实体认证是对一个实体声明的身份进行确认。一个认证协议为一个代理 b 提供一个机制来达到：消息的交换证实了其他参与方 a 也加入了这个协议的运行。

5 实验性能分析

为了检验改进后的协议的安全性以及协议主体的认证性，对建立的通信主体的 CSP 进程模型进行实验。实验的环境是 vmware workstation 8 +ubuntu 12.04+FDR2.94，计算机配置为 Intel(R) Core(TM) i5 CPU M480@2.67GHZ，内存 4G。

5.1 改进后的协议安全性能

实验设计了协议主体的 CSP 进程在 FDR2.94 中运行，同时攻击者在 Dolev_Yao 模型下对协议进行攻击，即攻击者能根据自身的知识，通过任意窃听、阻塞、修改和伪造信息对

协议的正常通信发动模拟攻击，也就是说 FDR 下攻击者通过穷尽状态空间的方式进行工作，它检查协议的迹是否与协议规范迹相同，当搜索中遇到与检验模型不同的状态时，FDR 会提炼成一个不成立的一个证据，并被保存在用户提供信息的反例中。

在实验中设计了 6 个检验状态，它们是：协议主体 R、T 和 S 对会话密钥的保密性，即在协议迹中会话密钥 krt 不能出现在攻击者的 leak 信道中，否则攻击者获取密钥，攻击成功；在新鲜值和会话密钥下各协议主体的相互认证性。利用 FDR 加载 CSP 进程后检测完的状态如图 4 所示。

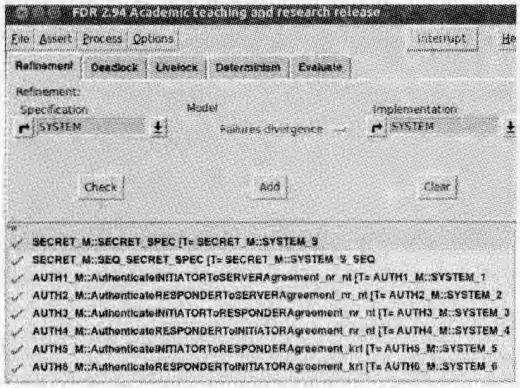

图 4　协议安全要求通过检测

图 4 中打钩的行表示检测成功，√ SECRET 表示前面定义的安全性检验通过，而其余行用来检测各个认证。√ AUTH_M::Authenticate 表示认证检测通过。

5.2　改进前的协议安全性能

在测试环境和上面的环境一样的条件下，对改进前的 David 数字图书馆协议进行实验，而 David 数字图书馆协议在同样的实验环境下没有通过 FDR 的检测。实验结果提示 Trace error after 68 states，表示 FDR 在第 68 个状态检测中发现了错误的迹，也就是攻击者在此处攻击成功。图 5 给出了反例。其中图中的 tau 符号是希腊字符 τ 的发音，它在此处表示不可见事件即内部动作。

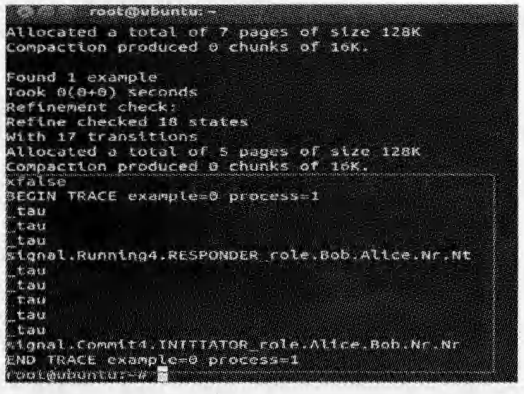

图 5　David 数字图书馆协议安全性检测失败

通过 FDR 的调试界面，可以查看出它的一个迹，测试结果如图 6 所示。

在图 6 的 performs 中看到信号量 singal. commit 的出现，CSP 理论规定在信号量 commit 之前一定要有信号量 starting 的出现，而此处迹中没有出现，可见攻击者在中间冒充了某种角色完成了此协议的运行，而实际上协议并没有在正常协议角色中完成。

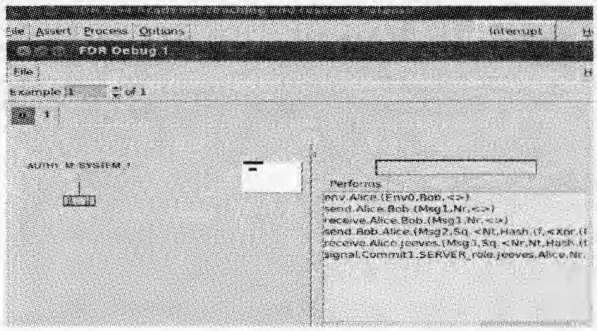

图 6　协议改进前检测失败后产生的迹

5.3　协议改进前后性能比较分析

改进后的协议与 David 数字图书馆协议、随机 Hash-lock 和 Hash-lock 链协议等相关协议安全性能比较如表 1 所列。

表 1　协议改进后与相关协议的安全性能比较

协议名称	重放	假冒	跟踪	隐私泄露	对阅读器进行认证	产生会话密钥
Hash-lock	存在	存在	存在	明文	无	无
随机 Hash-lock	存在	存在	存在	明文	无	无
Hash-lock 链协议	存在	存在	无	明文	无	无
David 数字图书馆协议	无	无	无	新鲜值为明文	无	无
协议改进后	无	无	无	加密	有	有

从表 1 中的数据看出 David 数字图书馆协议经改进后在隐私泄露、对阅读器进行认证和产生会话密钥等安全性方面有了完善。

比较协议改进前后的实验结果（见图 4－图 6）可以看出 David 数字图书馆协议的认证服务器没有成功对标签阅读器进行认证，也就是说任何拥有扫描器的人都可以追踪标签，标签会根据协议相应阅读器而且不加区分地传送信息。可以利用这个特性追踪特定的用户，进行恶意跟踪。图 4 显示改进后的 David 数字图书馆协议中认证服务器、标签阅读器和标签进行了相互认证。当非法接入的标签阅读器对标签进行非法扫描时，由于无法获得认证服务器的认证，协议将会终止运行。

改进后的 David 数字图书馆协议与 David 数字图书馆协议相比，在发送给认证服务器的消息 3 中添加了消息 $IDr \oplus f_k(0, R_r, R_T)$，以此完成对阅读器的认证。在此消息中通过异或运算和散列运算对消息进行加密，攻击者在无法同时获取消息 $IDr \oplus f_k(0, R_r, R_T)$ 中的参数时是构造不出这个消息的。同时通过提前把参数注册到认证服务器中，认证服务器在认证此阅读器的时候会重新构造这个消息，然后比较二者是否相等。如果相等则认证通过，允许阅读器和标签进行交换，否则认定阅读器非法接入，认定是非法的阅读器在非法扫描标签，终止协议允许。从而实现了防止非法阅读器非法扫描标签的安全特性。

另外，改进后的 David 数字图书馆协议与 David 数字图书馆协议相比，在消息 3 后对标签和阅读器认证通过后，在返回给阅读器的消息 4 中添加消息 $fs_j(ID_j) \oplus krt$，$fs_i(ID_i) \oplus krt$，这个消息中包含了传送给阅读器和标签的会话密钥 krt。攻击者在消息 4 中协议数据单元 $ID_j \oplus fs_j(1, R_r, R_T)$、$fs_j(ID_j) \oplus krt$ 和参数未知的情况下获取 krt 是很困难的，而且其概率可忽略，为 $(1/2)^{|hash(\cdot)|}$[20]。

（下转第 270 页）

基于主分量的奇异谱分析方法应用于其中，通过线性重复公式建立预测模型，并利用状态转移矩阵和贡献率根据残差的偏移方向修正预测值。用这一算法对国内某机场的实测数据进行预测，从常用的两种评价指标看出本文方法优于已有的SSA预测算法，能有效地提高预测精度。此外，本文提出的算法适用于具有某种趋势的时间序列的单步预测。

参考文献

[1] 张树京，齐立心. 时间序列分析简明教程[M]. 北京：北方交通大学出版社，2003

[2] Vautard R, Ghil M. Singular spect rum analysis in nonlinear dynamics, with applicat ions to paleo-climat ic series[D]. Physica D, 1989, 35: 395-424

[3] Vahabie A H, Yousefi M M R, Araabi B N, et al. Combination of singular spectrum analysis and autoregressive model for short term load forecasting[C]// Proc IEEE Pow Tech, 2007. Lausanne, 2007: 1090-1093

[4] 徐克红，程鹏飞，文汉江. 太阳黑子数时间序列的奇异谱分析与小波分析[J]. 测绘科学，2007，32(6)：35-38

[5] Hassani H, Heravi S, Zhigljavsky A. Forecasting European industrial production with singular spectrum analysis[J]. International Journal of Forecasting, 2009, 25(1): 103-118

[6] Kumar U, Jain V K. Time series models (Grey-Markov, Grey Model with rolling mechanism and singular spectrum analysis) to forecast energy consumption in India[J]. Energy, 2010, 35(4): 1709-1716

[7] 郭兴明，胡童宜，等. 心脏杂音提取和分类识别研究[J]. 计算机工程与应用，2012，48：P149-152

[8] Khelifa S, Kahlouche S, Belbachil M F. Signal and noise separation in time series of DORIS station coordinates using wavelet and singular spectrum analysis[J]. Comptes Rendus Geoscience, 2012, 344(6/7): 334-348

[9] Hassani H, Soofi A S, Zhigljavsky A A. Predicting daily exchange rate with singular spectrum analysis[J]. Nonlinear Analysis: Real World Applications, 2010, 11(3): 2023-2034

[10] Afshar K, Bigdeli N. Data analysis and short term load forecasting in Iran electricity market using singular spectral analysis (SSA)[J]. Energy, 2011: 36(5): 2620-2627

[11] Hassani H. Singular Spectrum Analysis Methodology and Comparison[M]. Journal of Data Science, 2007: 239-257

[12] Hu Bao-xin, Li Qing-mou, Smith A. Noise reduction of hyperspectral data using singular spectral analysis[J]. International Journal of Remote Sensing, 2009, 30(9): 2277-2296

(上接第 229 页)

最后改进后的协议在认证服务器对阅读器和标签认证通过以后，阅读器和标签进行会话时，都使用了会话密钥 krt 对消息 M 加密成 $M \oplus krt$，再进行传送，而 David 数字图书馆协议主要是完成对标签的认证，认证后没有分配会话密钥给阅读器和标签，这样两者的通信只能通过明文传送。

结束语 在分析了 David 数字图书馆协议并指出了它存在阅读器非法扫描标签和协议主体没有会话密钥的安全隐患的基础上，提出解决这些安全隐患的方案，并且采用了 CSP 的形式化方法对新方案的主体和协议的攻击者进行分析并建立了相应的模型。最后通过 FDR 实验环境对模型进行检验，得出了此协议的攻击者在 Dolev_Yao 模型下发动攻击时无法攻克协议密钥和协议主体相互认证的结论，解决了原有协议的安全隐患。

参考文献

[1] 赵志军，沈强，唐晖，等. 物联网架构和智能信息处理理论与关键技术[J]. 计算机科学，2011，38(8)：1-8

[2] 国务院办公厅. 国务院关于推进物联网有序健康发展的指导意见[OL]. http://www.gov.cn/zwgk/2013-02/17/content_2333141.htm 2013. 国发〔2013〕7 号

[3] 谢鸿波. 安全协议形式化分析方法的关键技术研究[D]. 成都：电子科技大学，2011

[4] 赵自强. 基于串空间模型的形式化方法的扩展与应用[D]. 成都：成都理工大学，2011

[5] Armstrong P, Goldsmith M, Lowe G, et al. Recent developments in FDR[C]// Computer Aided Verification. Springer, 2012

[6] Shaikh S A, Bush V J, Schneider S A. Specifying authentication using signal events in CSP[J]. Computers & Security, 2009, 28(5): 310-324

[7] 卿斯汉. 认证协议两种形式化分析方法的比较[J]. 软件学报，2003，14(12)：2028-2036

[8] 周永彬，冯登国. RFID 安全协议的设计与分析[J]. 计算机学报，2006(4)：4581-4589

[9] 胡游君. RFID 安全协议形式化分析研究及 DRAP 协议的建立与实现[D]. 秦皇岛：燕山大学，2007

[10] 丁振华，李锦涛，冯波. 基于 Hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展，2009，46(4)：583-592

[11] 伍新华，唐翠婷. 一种基于 Hash 的 RFID 双向认证协议[J]. 武汉理工大学学报：交通科学与工程版，2011，35(3)：571-574

[12] 周晔. 基于 Hash 链的 RFID 双向认证协议研究[D]. 成都：西南交通大学，2012

[13] Ryan S A, Schneider S, et al. 安全协议的建模与分析：CSP 方式[M]. 张玉清，莫燕，吴建耀，译. 北京：机械工业出版社，2005：30-53

[14] Palikareva H, Ouaknine J, Roscoe A W. SAT-solving in CSP trace refinement[J]. Science of Computer Programming, 2012, 77(10/11): 1178-1197

[15] 薛锐，冯登国. 安全协议的形式化分析技术与方法[J]. 计算机学报，2006(1)：1-20

[16] Molnar D, Wagner D. Privacy and security in library RFID: issues, practices, and architectures[C]// Proceedings of the 11th ACM conference on computer and communications security, 2004. Washington, DC, USA: ACM. 2004: 210-219

[17] 唐郑熠，李祥. Dolev-Yao 攻击者模型的形式化描述[J]. 计算机工程与科学，2010，32(8)：36-38+45

[18] 张忠，徐秋亮. 物联网环境下 UC 安全的组证明 RFID 协议[J]. 计算机学报，2011(7)：1188-1194

[19] Roscoe A, Smyth T, Nguyen L. Model checking cryptographic protocols subject to combinatorial attack[OL]. http://www.cs.ox.ac.uk/files/4157/guess.pdf, 2012

[20] 任伟，宋军，叶敏，等. 物联网自治安全适配层模型以及 T2ToI 中 T2T 匿名认证协议[J]. 计算机研究与发展，2011(S2)：320-325