文章编号:1001 - 9081(2008)09 - 2239 - 03

移动型 RFID 安全协议及其 GNY 逻辑分析

王新锋[1,3],刘建国[2],蒋 旭[3],刘胜利[3]
(1. 军械工程学院 计算机工程系,石家庄 050003; 2. 军械工程学院 管理工程系, 石家庄 050003;
3. 63880 部队, 河南 洛阳 471003)
(wxfabc@ yahoo. cn)

摘 要:针对现有基于 Hash 函数无线射频识别(RFID)安全协议移动性差、不能满足某些应用领域需求的不足,提出一种移动型 RFID 安全协议,并利用 GNY 逻辑进行了证明。分析表明,移动型 RFID 安全协议移动性强,具备一定的安全性,适用于民用物流运输途中、军事应用中在运资产、战时野战环境等对读写器移动性要求高的领域。

关键词:无线射频识别; 安全协议; GNY 逻辑
中图分类号: TP391.44 **文献标志码**:A

Mobile RFID security protocol and its GNY logic analysis

WANG Xin-feng[1,3], LIU Jian-guo[2], JIANG Xu[3], LIU Sheng-li[3]
(1. *Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang Hebei* 050003, *China*;
2. *Department of Management, Ordnance Engineering College, Shijiazhuang Hebei* 050003, *China*; 3. *Unit* 63880, *PLA, Luoyang Henan* 471003, *China*)

Abstract: Nowadays, Radio Frequency IDentification (RFID) security protocols based on Hash function have poor mobility and cannot satisfy the requirements of some fields. Aiming to boost up the mobility of RFID security protocols, a Mobile RFID Security Protocol was presented and GNY logic was used to prove its correctness. Analysis shows that presented protocol has satisfied mobility and security, and the protocol can be used in transmitting freight and field operation of war time, etc.

Key words: Radio Frequency IDentification (RFID); security protocol; GNY logic

由于 Hash 函数具备安全性能好、易于在低成本无线射频识别(Radio Frequency IDentification,RFID)标签上实现的特点,利用 Hash 函数构建 RFID 安全协议是解决 RFID 技术安全问题的一个重要分支[1]。但这类安全协议的不足是通常需要 RFID 读写器(Reader,缩写为 R)时刻与后台数据库连接,否则系统将陷入瘫痪状态,下面以 Hash 链(Hash-chain)协议[2]为例进行说明。另一方面,在有些应用领域需要读写器具备一定的移动性,例如民用物流运输、公交车、移动收费点以及军事应用中在运资产、战时野战环境等情况下读写器都难以保证时刻与后台数据库连接。因此建立一个使读写器可以间歇地与后台数据库(Backend,缩写为 B)相连的 RFID 安全协议,是许多应用领域的一个迫切需求[1]。

1 现有安全协议的不足

许多学者在 hash-lock 协议基础上,相继提出了各种形式的 Hash 函数安全协议[1],其中 Hash 链(Hash-Chain)协议具有较高的安全性[2]。在这里,我们将通过分析 Hash 链协议指出基于 Hash 函数的安全协议目前在可移动性和识别速度方面存在的不足。

Hash 链协议要求标签内置两个 Hash 函数电路,其流程如图 1 所示。

在系统运行之前, 标签 T 和后台数据库 B 共享一个初始秘密值 $s_{t,1}$。T 和读写器 R 之间执行第 j 次 Hash 链的过程如下:

1)R 向 T 发送 Query 认证请求;

2)T 使用当前的秘密值 $s_{t,j}$ 计算 $a_{t,j} = H(s_{t,j})$,并更新其秘密值为 $s_{t,j+1} = H(s_{t,j})$。T 将 $a_{t,j}$ 发送给 R;

3)R 将 $a_{t,j}$ 转发给后台数据库;

4)后台数据库系统针对所有的标签数据项查找并计算是否存在某个 ID_t($1 \leqslant t \leqslant n$,$n$ 为后台数据库 B 中存储的标签数据项的数量) 以及是否存在某个 j($1 \leqslant t \leqslant m$,其中 m 为系统预设置的最大链长度) 使得 $a'_{t,j} = G(H_{j-1}(s_{t,1})) = a_{t,j}$ 成立。如果有则认证通过,标签合法,B 将 ID_t 发送给 R;否则认证失败,认为标签非法。

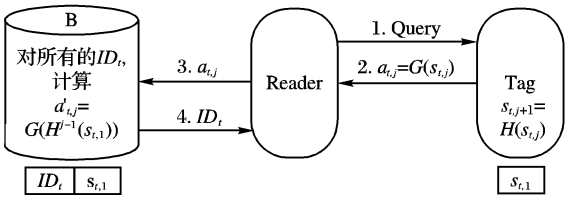

图 1 Hash 链协议

不难发现,Hash 链协议存在以下不足。

1)读写器移动性差。图 1Step 3 中,一旦 R 与 B 断开连接,R 将无法在 Step 4 中获取标签的身份信息 ID_t,致使整个 RFID 系统瘫痪。因此,读写器必须时刻与后台数据库连接,极大地限制了读写器的移动性。

2)识别速度慢。图 1 中,B 在 Step 3 收到 $a_{t,j}$ 后,需要进行穷举搜索和 Hash 运算,每搜索一个标签需要进行的 Hash 运算值可以达到 $n \times m$ 次,其中 n 是 B 中存储的标签项的个数, m 是系统预设的最大 Hash 链长度。因此,读写器的识别速度就受到极大的限制。当读写器 R 需要同时识别大量标签时,可能会因为识别速度过慢而导致漏读率增加。

与Hash链协议类似,文献[3 - 6]提出的基于Hash函数

收稿日期:2008 - 03 - 19;**修回日期**:2008 - 06 - 03。 **基金项目**:国家自然科学基金资助项目(60372042)。

作者简介:王新峰(1978 -),男,河南驻马店人,博士研究生,主要研究方向:无线传感器网、RFID 技术; 刘建国(1953 -),男,山东曹县人,副教授,主要研究方向:装备管理; 蒋旭(1976 -),男,江苏宜兴人,博士,主要研究方向:武器系统的故障诊断与仿真研究; 刘胜利(1976 -),男,河南周口人,主要研究方向:电子对抗。

的安全协议也存在同样的不足。由于篇幅限制,这里不再逐一分析。

2 实用型 RFID 安全协议

针对基于 Hash 函数安全协议的不足,本文提出一种移动型 Hash 安全协议,该协议允许读写器 R 间歇地与后台数据库 B 连接,增强了读写器的移动性能,同时该协议还具备识别速度快的特点。

2.1 协议的基本条件

在协议的描述中,涉及到三个主体:标签 T(Tag,缩写为 T)、读写器 R 和后台数据库服务器 B。

1)标签 T:T 中仅存储唯一 ID(假定标签 ID 不可更改)和相应秘密信息 s,实际数据存储在后台数据库服务器 B 中。此外,标签需要内置一个 Hash 电路,其硬件可以采用欧盟最新公布的 SHA-256 结构,这个结构需要 10 868 gates,安全程度可以达到 AES-128 水平,适用于 RFID 标签[7]。

2)读写器 R:R 具备足够的计算能力来保证 R 和 B 之间的通信安全,如采用公钥加密体系。因此我们认为 B 和 R 之间的信道是安全的,为了便于叙述,B 和 R 之间传送的数据在这里我们直接以明文表示。

3)B:对于发生交易的 T 和 R 双方,B 是可信仲裁。针对每个标签 i, B 中存储着相应的 ID_i,S_i 和 $DATA_i$。

2.2 协议的运行步骤

移动型 RFID 安全协议的运行步骤如图 2 所示。

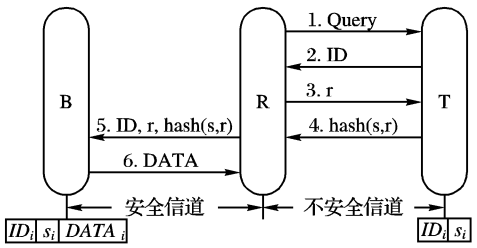

图 2 移动型 RFID 安全协议

1)读写器 R 向标签 T 发出询问命令。

2)标签 T 以自己的 ID 作为响应。

3)读写器 R 产生一个随机数 r,并发送给标签 T。

4)根据接收到的 r 和自己的秘密信息 s,标签 T 计算出 hash(r, s)并发送给 R。

5)读写器 R 把 ID, r, hash(r, s)转发给后台数据库服务器 B。

6)B 根据 ID 找到相应的秘密信息 s_B,并计算 hash(r, s_B)。如果 hash(r, s_B) = hash(r, s),则 B 认为 T 是一个合法标签,并将与 T 相关的数据 DATA 发送给 R。

例如,在军事领域的“在运资产可视化系统[10]”中,数据库服务器 B 在 6)中的数据 DATA 可能包括发货单位、收货单位、送达时间等。标签信息 DATA 经读写器传送给后方指挥中心后,指挥人员可以随时掌握货物位置、运输状况、特性等信息,实现运输途中资产的可视化。

3 协议的 GNY 逻辑分析

GNY 逻辑是一种形式化分析工具,到目前为止,它被认为是影响最大的一种 BAN 类逻辑之一[9]。形式化方法能够发现安全协议中以前不为所知的漏洞,例如 NS 协议和 Kerberos 协议的若干漏洞就是通过形式化分析方法才被发现出来,而以前通过其他方法并没有发现这些漏洞[9]。

为了验证协议的安全性,我们利用 GNY 逻辑对协议的目标、假设和消息传递进行形式化分析,证明从协议的假设出发,经过协议的运行可以达到预先设定的目标。GNY 逻辑是由 BAN 逻辑发展而来的。与 BAN 逻辑相比,它具有更强的表现能力和适应性[8]。

3.1 协议的假设、目标及其形式化

1)关于标签 T 的假设:T 拥有身份信息 ID,并认为身份信息 ID 是可以被识别的;T 拥有秘密信息 s,并认为 s 是 B 和 T 之间合格的秘密信息。

标签 T 的假设可以形式化为: $T \ni s, T|\equiv \phi(ID), T \ni ID, T|\equiv B \overset{s}{\leftrightarrow} T$。

2)关于读写器 R 的假设:R 可以产生随机数 r,并且 R 相信随机数 r 具备新鲜性;由于 B 和 R 之间为安全信道,B 和 R 之间可以通过公钥加密体系进行相互认证,因此 B 认为 R 是完全可以信任的;R 认为它发出的询问信号 Query 是可以被识别的。

读写器 R 的假设可以形式化为:$R \ni r, R|\equiv \#(r), R|\equiv B|\Rightarrow B|\equiv *, R|\equiv \phi(Query)$。

3)关于后台数据库 B 的假设:针对每个标签 T,B 存储着相应的身份信息 ID 和秘密信息 s,而且 B 认为 s 是 B 和 T 之间合格的秘密信息;与读写器 R 类似,B 认为读写器 R 是完全可以信任的。

后台数据库 B 的假设可以形式化为:$B \ni ID, B \ni s, B|\equiv B \overset{s}{\leftrightarrow} T, B|\equiv R|\Rightarrow R|\equiv *$。

4)协议的目标:作为一种自动识别技术,经过安全协议的运行读写器 R 首先要能够识别标签 T 的身份信息 ID,并进一步得到相关的数据 DATA;协议运行后能够使后台数据库 B 相信标签 T 拥有秘密信息 s,以证明标签 T 是合法的;协议运行后能够使读写器 R 相信 s 是 B 和 T 之间合格的秘密信息。

协议目标可以形式化为:$R \ni ID, R \ni DATA, B|\equiv T \ni s, R|\equiv B \overset{s}{\leftrightarrow} T$。

3.2 形式化分析

在明确了协议的假设、目标后,我们可以利用 GNY 逻辑中的推理规则[8]证明协议能够从假设出发,经协议运行后达到预先设定的目标。

图 2 中 1)可 GNY 逻辑形式化为: $T \lhd *Query \rightsquigarrow R|\equiv \phi(Query)$。

由假设知前提条件 $R|\equiv \phi(Query)$ 成立,由 GNY 推理规则 T1 和 P1[8]可得:$T \in Query$。

图 2 中 2)可 GNY 逻辑形式化为: $R \lhd *ID \rightsquigarrow T|\equiv \phi(ID)$。

由假设知前提条件 $T|\equiv \phi(ID)$ 成立,由 GNY 推理规则 T1 和 P1[8]可得:$R \ni ID$。至此,第一个目标($R \ni ID$)实现。

图 2 中 3)可 GNY 逻辑形式化为: $T \lhd *r \rightsquigarrow R|\equiv \#(r)$。

由假设知前提条件 $R|\equiv \#(r)$ 成立,由 GNY 推理规则 T1 和 P1[8]可得:$T \ni r$。

图 2 中 4)可 GNY 逻辑形式化为: $R \lhd *hash(s,r) \rightsquigarrow T|\equiv B \overset{s}{\leftrightarrow} T$。

由假设知前提条件 $T|\equiv B \overset{s}{\leftrightarrow} T$ 成立,由 GNY 推理规则 T1 和 P1[8]可得:$R \ni hash(s,r)$。

图 2 中 5)可 GNY 逻辑形式化为: $B \lhd ID, r, hash(s,r)$。

由 GNY 推理规则 P1[8]可得:$B \ni ID, B \ni r, B \ni hash(s,r)$。

下面证明第三个目标($B|\equiv T \ni s$)成立:

由假设知 $B|\equiv R|\Rightarrow R|\equiv *, R|\equiv \#(r)$ 成立。所以 $B|\equiv R|\Rightarrow R|\equiv \#(r)$。

又,由推理规则 J3[8]知:$B|\equiv R|\equiv \#(r)$,进而由推理规则

J1 知:B| ≡#(r),进而由推理规则 F1[8] 知:B| ≡#hash(r, s)。

同时又由假设知 B ∋ s,B| ≡ B$\overset{s}{\leftrightarrow}$T,由推理规则 I1[8] 知:B| ≡T ∋ s。第三个目标(B| ≡T ∋ s)成立。

图 2 中 6)可 GNY 逻辑形式化为:R ◁ *DATA ~➝ B| ≡ B$\overset{s}{\leftrightarrow}$T。

由推理规则 T1 和 P1[8] 知:R ∋ DATA,目标 2(R ∋ DATA)成立。

下面证明第四目标(R| ≡B$\overset{s}{\leftrightarrow}$T)成立:

由假设知 R| ≡B| ⇒B| ≡ *,且 B| ~ (DATA ~➝ B$\overset{s}{\leftrightarrow}$T),由推理规则 J2[8] 知:R| ≡B| ≡B$\overset{s}{\leftrightarrow}$T。

由推理规则 J1[8] 知:R| ≡B$\overset{s}{\leftrightarrow}$T。第四个目标(R| ≡B$\overset{s}{\leftrightarrow}$T)成立。

所以,通过协议的运行,该协议可以在基本假设的基础上实现预定的设计目标。

4　协议安全性及特点分析

下面分析移动型 RFID 安全协议的安全性能和特点,指出该协议移动性强、识别速度快的优点和无法防止位置跟踪的不足。对于协议的不足,文中给出了弥补建议。

4.1　协议安全性分析

根据文献[3]对 RFID 系统面临的安全隐私威胁主要包括:非法读取、位置跟踪、窃听、拒绝服务、伪装哄骗和重放攻击六种。

1)非法读取:标签内仅存储身份信息 ID 和秘密信息 s,与标签相关的数据 DATA 存储在后台数据库 B 中,由于读写器 R 和后台数据库 B 之间为安全信道,攻击者无法获取数据 DATA。对于秘密信息 s,如果攻击者冒充合法读写器非法读取标签,标签将在协议的步骤 4)中以 hash(s, r)的形式应答,攻击者无法从消息 hash(s, r)中得到秘密信息 s。

2)位置跟踪:由于协议的步骤 2)中以明文方式将身份信息 ID 发送出去,攻击者可以成功地对标签实施位置跟踪。

3)窃听:攻击者可以在协议步骤 2)中窃听到标签的身份信息 ID,无法从 B 和 R 之间的安全信道中窃听到数据 DATA,也无法从消息 hash(s, r)中得到秘密信息 s。

4)拒绝服务:由于读写器 R 和标签 T 之间以无线方式通信,攻击者可以通过发送同频干扰信号破坏 R 和 T 之间的信道,但对系统(包括 B、R 和 T)的稳定性不会造成影响。

5)伪装哄骗:如果攻击者伪装成合法标签响应读写器 R,由于攻击者无法获取标签的秘密信息 s,在协议的步骤 5)中将被后台数据库 B 识别出真实身份,协议可以有效防范伪装哄骗。

6)重放攻击:如果攻击者利用窃听得到的 r 和 hash(s, r)冒充合法标签响应读写器 R,由于随机数 r 的新鲜性,可以确保这种攻击方式在协议的步骤 5)中被后台数据库 B 发现,因此协议可有效防范重放攻击。

因此,移动型 RFID 安全协议可以防范非法读取、窃听、伪装哄骗和重放攻击。对于该协议的不足:不能防范位置跟踪,弥补的方法可以考虑在标签不需要工作时,使用"法拉第笼"将标签隔离,以防止攻击者得到标签的身份信息 ID。

4.2　协议的特点

协议具有移动性强、识别速度快的特点。

1)可离线工作,移动性强:在协议运行步骤 1) ~4)中,读写器并没有与后台数据库 B 连接。当读写器由于条件限制,无法与 B 连接时,可以先读取若干个标签的信息,获取各个标签的 ID 及 r 和 hash(r, s)。当 R 与 B 有条件连接时,再由读写器 R 逐一将协议步骤 5)中的消息发送给 B,由 B 验证各个标签身份合法性。

在"在运资产可视化系统"中,读写器经常需要在野战环境下移动地采集资产信息,甚至移动地搜索某个或某类物资[10],移动性 RFID 安全协议可以在保证系统安全的前提下满足这一需求。

2)识别速度快:后台数据库在收到协议步骤 5)中的消息 ID,r 和 hash(s, r)后,可以根据 ID 号直接确定标签身份,然后经过一次 hash 运行就可以确定标签的身份是否合法。克服了基于 Hash 函数安全协议计算量大的缺点,提高了读写器 R 识别标签的速度,使得移动型 RFID 安全协议能够适用于标签数量大的场合。

5　结语

针对现有基于 Hash 函数安全协议移动性差的特点,本文提出一种移动型 RFID 安全协议。GNY 逻辑分析表明,从该协议的假设出发经协议运行可以达到预先设定的协议目标。安全性能分析表明,该协议的优点是移动性能强、识别速度快。在安全方面的不足是无法防止位置跟踪,建议在标签不需要工作时,使用"法拉第笼"将标签隔离以弥补该协议的不足。同时,由于标签仅需要一个 Hash 函数电路,成本较低,可以在我国具备生产能力的 13.56 MHz 芯片上应用。

参考文献:

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

[2] OHKUBO M, SUZUKI K, KINOSHITA S. Hash-chain based forward secure privacy protection scheme for low-cost RFID [C]// Proceedings of t he 2004 Symposium on Cryptography and Information Security (SCIS 2004). Sendai: [s. n.], 2004: 719 - 724.

[3] 曾丽华,熊璋,张挺. Key 值更新随机 Hash 锁对 RFID 安全隐私的加强[J]. 计算机工程, 2007, 33(3): 151 - 159.

[4] AVOINE G, OECHSLIN P. A scalable and provably secure hash based RFID protocol[C]// In International Workshop on Pervasive Computing and Communication Security, Hawaii, USA, 2005. Kauai Island: IEEE Computer Society Press, 2005: 110 - 114.

[5] WEIS S A, SARMA S E, RIVEST R L. Security and privacy aspects of low-cost radio frequency identification systems [C]// First Annual Conference on Security in Pervasive Computing, Boppard, Germany, 2003. Boppard: Springer, 2003: 201 - 212.

[6] HENRICI D, MULLER P. Hash-based enhancement of location privacy for radio frequency identification devices using varying identifiers[C]// In 2nd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), Orlando, FL, USA, 2004. Orlando: IEEE Computer Society Press, 2004: 149 - 153.

[7] LEE S M, HWANG Y J, LEE D H. Efficient authentication for low-cost RFID systems[C]// International Conference Computational Science and Its Applications—ICCSA, Singapore, 2005. Singapore: Springer Lecture Notes in Computer Science Press, 2005: 619 - 627.

[8] GONG L, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocols[C]// Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, California, 1990. Oakland, California: IEEE Computer Society Press, 1990: 234 - 248.

[9] SAUL E, HUTCHISON A C M. A graphical enviroment for the facilitation of logic-based security protocol analysis [J]. South African Computer Journal, 2000(26): 196 - 200.

[10] 谢桂海, 齐子元, 王新锋, 等. "联合全资产可视化"及其关键技术[J]. 军械工程学院学报, 2005, 17(1): 43 - 46.