Research on RFID Security Authentication Protocol Based on Hash Function *

LIU Mingsheng[1,2*], *WANG Yan*[2], *ZHAO Xinsheng*[1]

(1. *Institute of Information Technology, Handan College, Handan Hebei* 056005, *China*;
2. *Institute of Information & Electrical Engineering, Hebei University of Engineering, Handan Hebei* 056038, *China*)

Abstract: In order to improve security and privacy between readers and tags in Radio Frequency Identification (RFID) Sensor Networks, an improved RFID security authentication protocol based on hash function is proposed by comparing with several typical current protocols. Analysis shows that this protocol resists spoofing, tracking, eavesdropping impersonation and replay attack and it is low-cost, high-efficiency and good-security. After setting up the idealized protocol model, a process of formal analysis of this protocol is presented and the security is proved theoretically by using the BAN logic.

Key words: RFID; security protocol; hash function; BAN logic

EEACC: 6150P **doi**: 10.3969/j.issn.1004-1699.2011.09.018

基于 Hash 函数的 RFID 安全认证协议的研究 *

刘明生[1,2*], 王 艳[2], 赵新生[1]

(1. 邯郸学院信息技术研究所, 河北 邯郸 056005;
2. 河北工程大学信息与电气工程学院, 河北 邯郸 056038)

摘 要: 为了改善 RFID 传感网络中阅读器与标签之间存在的安全隐私问题, 通过分析现有安全协议, 提出一种新的基于 Hash 函数的 RFID 安全认证协议。分析表明, 该协议可以有效抵御非法读取、位置跟踪、窃听、伪装哄骗和重放等不安全问题, 具有成本低、效率高、安全性高等特点。通过建立协议的理想化模型, 利用 BAN 逻辑形式化分析该协议, 在理论上证明其安全性。

关键词: 射频识别; 安全协议; Hash 函数; BAN 逻辑

中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2011)09-1317-05

射频识别(Radio Frequency Identification, RFID)技术是一种非接触式自动识别技术, 它利用射频信号自动识别目标对象并获取相关数据。作为一种快速、实时、准确地采集与处理信息的高新技术, 通过对实体对象的唯一有效标识, RFID 已经广泛应用到了生产、零售、物流、交通、国防等各个行业。但在享受 RFID 带来的诸多便捷的同时, 也必须要面对伴随而来的多种安全隐私问题。为此, 本文提出一种新的基于 Hash 函数的认证协议并利用 BAN 逻辑对该协议进行形式化分析。

1 RFID 安全协议相关研究

到目前为止, 针对 RFID 传感网络中阅读器与标签间的安全隐私问题已经提出了多种安全认证协议。典型的基于单向 Hash 函数的 RFID 安全隐私保护协议主要有 3 种: Hash-Lock 协议[1-2], 随机化 Hash-Lock 协议[3] 和 Hash 链协议[4]。

1.1 Hash-Lock 协议

Hash-Lock 协议[1-2] 是由 Sarma 等人提出的一种 RFID 安全协议, 为避免信息泄漏和被追踪, 标签的真实 ID 使用 metaID 来代替, 即 metaID = Hash(key)。初始时标签处于锁定状态, 后台数据库存储每一个标签的密钥 metaID, key, ID。认证过程如图 1 所示。

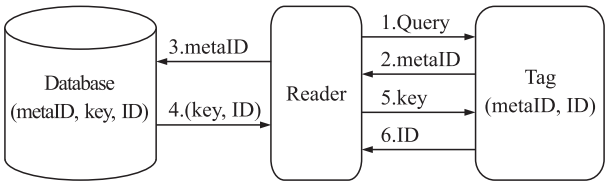


图 1 Hash-Lock 协议

该协议利用单向 Hash 函数的难解密性来加密传输中的信息, 所以在一定程度上解决了访问控制

项目来源: 河北省自然科学基金项目(F2010001923); 邯郸市科学技术研究与发展计划项目(2008HDKL001)
收稿日期: 2011-03-16 **修改日期**: 2011-06-15

的隐私保护。但是,因为每次标签回答的数据 metaID 都是固定不变的,所以该协议不能防止位置跟踪攻击;并且 ID 也以明文的形式通过不安全信道传送,攻击者很容易得到标签的信息,极易受到重传攻击和哄骗攻击,不具有不可分辨性。

1.2 随机化 Hash-Lock 协议

为了解决 Hash-Lock 协议中位置跟踪问题,weis 等人提出了随机化 Hash-Lock 协议[3]。它采用基于随机数的询问—应答机制,是对 Hash-Lock 协议的一种改进形式。标签中除 Hash 函数外,还嵌入了伪随机数发生器,以便通过添加随机数来保证传输数据的不可预测性。后台数据库中存储了所有标签的标识,设为 $ID_1, ID_2, \cdots, ID_n$。具体验证过程如图 2 所示。

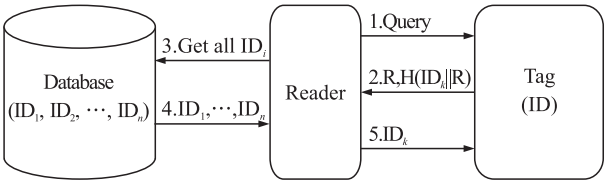


图 2 随机化 Hash-Lock 协议

该协议利用随机数的不可预测性解决了标签的位置跟踪问题。但是,在低成本和运算能力有限的标签中集成伪随机数发生器是不现实的,实现也比较困难。此外,已经通过认证的 Tag 标识 ID 仍以明文的形式通过不安全信道传送,仍然不能应对重传和哄骗攻击。每一次 Tag 认证,后台数据库都要将所有 Tag 的标识发送给阅读器,这大大增加了阅读器的运算量。就此而言,该协议仍然不实用。

1.3 Hash 链协议

Hash 链方法[4]是由 NTT 实验室提出的,是基于共享秘密的询问—应答协议。该协议的标签集成了两个不同的 Hash 函数 H 和 G。标签和后台数据库都存储了初始值 $S_{i,1}$,后台数据库存储了所有标签的标识 ID,在认证过程中不停的动态刷新标签认证所用的 ID。认证过程如图 3 所示。

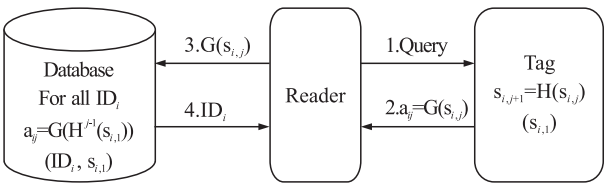


图 3 Hash 链协议

通过添加标签 ID 的动态刷新机制,该协议满足了不可分辨性和前向安全性,同时具有了较强的抗猜测抗分析能力。但是,Hash 链协议是单向认证协议,只对标签进行认证,不对阅读器进行认证,若攻击者伪装成合法阅读器,则很容易受到重传攻击和哄骗攻击。此外,该协议需要两个不同的杂凑函数 G 和 H,无形中增加了 Tag 的制造成本。后台数据库的运算量非常大,若有 N 个标签,后台数据库就需要进行 N 次搜索、$2N$ 次杂凑运算和 N 次比较。因此该协议不适用于标签和阅读器众多的情况。

2 改进的认证协议

通过对上述 3 种安全认证协议的深入学习,认识到了 RFID 传感网络中阅读器和标签间仍存在的安全隐患,从而结合几种方法的思想提出了一种改进的方案。该方案同样是基于 Hash 函数的,也仍旧采用原有的询问—应答机制。为有效抵御非法读取、位置跟踪、窃听、伪装哄骗和重放等不安全问题,标签和数据库有效性的验证仍由后台数据库执行。

2.1 初始条件及相关说明

在初始状态下,标签和阅读器都仅需要存储自己的标识,分别为 ID_t、ID_r,后台数据库要存放所有标签和阅读器的$(ID_t, H(ID_t))$、$(ID_r, H(ID_r))$数据对,其中 $H(\cdot)$是指 Hash 函数加密过的数据。

另外我们假设,标签是低成本的被动式标签,含有很少量的存储容量和较低的计算能力,Hash 函数对 RFID 应用是足够安全的,伪随机数也足够安全。还有仍采用原有的信道,即假设标签和阅读器之间的通信信道是不安全信道,而阅读器和后台数据库之间的信道是安全信道。

2.2 认证步骤

以现有的安全协议[5-9]为基础,提出了改进的基于 Hash 函数的 RFID 认证方案如图 4 所示。

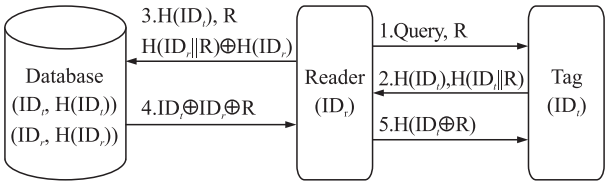


图 4 改进协议的认证过程

具体的验证过程如下:

(1)阅读器产生一个随机数 R,并将 Query,R 发送至标签作为认证请求;

(2)标签利用自身标识 ID_t 和随机数 R 计算出 $H(ID_t)$ 和 $H(ID_t \| R)$(‖ 为串联运算),并将 $H(ID_t)$、$H(ID_t \| R)$发送给阅读器作为响应;

(3)阅读器利用 Hash 函数加密自身标识 ID_r 得出 $H(ID_r)$,并与标签发送过来的 $H(ID_t \| R)$进行异或运算 $H(ID_t \| R) \oplus H(ID_r)$,最后阅读器将 R,$H(ID_t)$,$H(ID_t \| R) \oplus H(ID_r)$转发给后台数据库;

(4)后台数据库根据接收到的 $H(ID_t)$ 查找自身是否存储有相对应的 $H(ID_t)$ 值，若有则标签合法，否则认证失败。后台数据库依据 $H(ID_t)$ 得出对应的 ID_t 并将其与 R 串联计算出 $H(ID_t \| R)$，进而依据 $H(ID_t \| R) \oplus H(ID_r)$ 解出 $H(ID_r)$，查找出对应的 ID_r；

(5)后台数据库计算出 $ID_t \oplus ID_r \oplus R$，并将其转发给阅读器；

(6)阅读器根据自身标识 ID_r 和随机数 R 解出标签标识 ID_t，进而计算出 $H(ID_t \oplus R)$，并将其发送给标签；

(7)标签将自身标识 ID_t 和随机数 R 进行异或运算 $ID_t \oplus R$，进而计算出 $H^*(ID_t \oplus R)$，比较得到值 $H(ID_t \oplus R)$ 和计算得出值 $H^*(ID_t \oplus R)$ 是否相等，若相等，则阅读器合法，此时，根据阅读器发出的查询指令，后台数据库可以通过前面计算出的标签标识 ID_t 查到标签对应的信息发送给阅读器；否则认为阅读器为非法阅读器，标签不予回应。

3　改进协议的安全分析和性能比较

3.1　安全性分析

(1)前向安全性：假设攻击者截取了某次标签的输出，由于 Hash 函数的单向性和每次通信过程中随机数 R 的相异性，攻击者也不可能根据此值回溯出标签的历史数据，因此此协议具有良好的前向安全性。

(2)位置跟踪：每次通信的随机数 R 不同，决定了每次标签传输的消息也不同，这样就可以有效的防止因固定输出而引发的位置跟踪问题。

(3)窃听：所有有用信息都是经过单向散列函数—Hash 函数加密后传输的，因此，即使非法者截取信息，也无法解密 Hash 函数而得出信息的真正内容。

(4)伪装哄骗：非法者是无法获知标签和阅读器标识的，因此也根本无法伪装成合法标签和阅读器。

(5)不可分辨性：对于标签响应输出，由于使用了单向 Hash 函数和随机数，这样即使攻击者获得了多张标签的输出，也无法区分出某一张的输出；即使获得了同一张的输出，也无法区分出该张标签的某一次输出。

(6)重放攻击：非法者事先记录标签发出的信息，当阅读器再次与标签通信时，非法者通过记录下的标签信息来伪装成合法标签和阅读器通信，但随机数 R 的不同性决定了即使非法者截取了前一次的信息也无法模拟出下次的值，这样也就无法将截获信息重放给标签或阅读器。

(7)拒绝服务：标签在收到阅读器的询问信息时，不需要为它们存储随机数作为一次性密钥，且标签也没有设置读取标签的上限值。因此，本协议可以有效防止标签因同时被大量阅读器访问而造成的标签停止工作。

3.2　性能分析

为了清晰地对比改进协议与其它协议在安全性能[10]方面的特点，表 1 给出了详细比较。其中，√表示具备该项要求；×表示不具备该项要求。

表 1　安全性能比较

功能指标	Hash-Lock 协议	随机化 Hash-Lock 协议	Hash 链协议	本文协议
窃听	×	√	√	√
前向安全性	√	√	√	√
位置跟踪	×	√	√	√
拒绝服务	√	×	×	√
伪装哄骗	×	×	×	√
不可分辨性	×	√	√	√
重放攻击	×	×	×	√

假设数据库中标签的数目为 N，L 表示 128 个比特位(因为从前面对于 hash 函数的要求来看，hash 函数输出的值至少为 128 位才能保证抵御相关的攻击)，标签和阅读器标识 ID_t、ID_r 只有 128bits 也就是 1L。由分析可知，随机 Hash 锁协议，Hash 链协议等都有 N 数量级上的运算量，这使得运算量过大，对 RFID 系统的成本和运算速度带来影响。在改进的安全协议中，后台数据库最多需执行 $2N$ 个记录搜索，进行一次 Hash 运算。相比于现存协议，如 Hash 链中需计算 $2N$ 个 Hash 函数和 N 个记录搜索，本方案的计算速度快。标签中只需要 1L 的存储容量，也不需要随机数产生器，这样可以大大降低标签的成本。

此外，因大部分计算和查找都由后台数据库执行，效率也较高。本协议中标签和阅读器不需要存储对方的身份标识信息，查找相应记录和大部分计算过程全由后台数据库执行，随着标签和阅读器数目的增加，后台数据库计算时间缓慢增加，因此，该协议还可适用于标签和阅读器数目较多的情况。

4　安全性推导与分析

到目前为止，已经提出了很多 RFID 安全协议，

但大都缺乏严格的形式化分析和证明。下面将采用经典的安全协议分析方法—BAN 逻辑对改进协议进行形式化分析和证明。

4.1 BAN 逻辑

BAN 逻辑[11-12]是一种基于主体信念以及用于从已知信念推出新的信念的推理规则的逻辑。应用 BAN 逻辑时,首先要进行“理想化”,即将协议的消息转换为 BAN 逻辑中的公式,再根据具体情况进行合理假设,最后由逻辑的推理规则根据理想化协议和假设进行推理,推断出协议能否完成预期目标。

BAN 逻辑语法的基本表达式描述如下:P| ≡X:P 相信 X;P◁X:P 曾收到过 X;P| ~X:P 曾发送过 X;P| ⇒X:P 对 X 有仲裁权;(X,Y):X 和 Y 连接;#(X):X 是新的;$\{X\}_k$:密钥 K 加密 X 后的密文;$<X>_Y$:由 X 和秘密 Y 合成的消息;$P \xleftrightarrow{k} Q$:P 和 Q 共享一个密钥 K;$\xrightarrow{k} P$:k 是 P 的公开密钥;

本文使用到的 BAN 逻辑的几条基本逻辑推理规则如下:

(1)消息意义规则 $\dfrac{(P| \equiv Q \xleftrightarrow{k} P, P \lhd \{X\}_k)}{P| \equiv Q| \sim X}$

(2)随机数验证规则 $\dfrac{(P| \equiv \#(X), P| \equiv Q| \sim X)}{P| \equiv Q| \equiv X}$

(3)仲裁规则 $\dfrac{(P| \equiv Q| \Rightarrow X, P| \equiv Q| \equiv X)}{P| \equiv X}$

(4)信仰规则 $\dfrac{(P| \equiv X, P| \equiv Y)}{P| \equiv (X,Y)}$

(5)新鲜性规则 $\dfrac{P| \equiv \#(X)}{P| \equiv \#(X,Y)}$、$\dfrac{(\#(N),(N,K))}{\#(K)}$、$\dfrac{(\#(K), P \lhd \{X\}_k, P| \equiv P \xleftrightarrow{k} Q)}{(P| \equiv Q| \sim X, P| \equiv Q| \equiv P \xleftrightarrow{k} Q)}$

对于一个 Hash 函数 H(X),还有以下两条规则:

(6)$\dfrac{(P| \equiv Q| \sim H(X), P \lhd X)}{P| \equiv Q| \sim X}$

(7)$\dfrac{(P| \equiv Q| \sim H(X_1, X_2, \cdots, X_n), P \lhd X_1, P \lhd X_2, \cdots, P \lhd X_n)}{P| \equiv Q| \sim (X_1, X_2, \cdots, X_n)}$

4.2 本协议的 BAN 逻辑安全分析

4.2.1 协议的初始化假设

假设 R 代表阅读器,T 代表标签,S 代表阅读器产生的随机数,ID_t 仍代表标签标识,则协议的初始假设为:

P1:R| ≡#(S)

P2:$R| \equiv R \xleftrightarrow{S} T$

P3:$T| \equiv \#(ID_t)$

P4:$T| \equiv T \xleftrightarrow{S} R$

4.2.2 协议的理想化模型

M1:R→T:Query,S

M2:T→R:$H(ID_t)$,$H(ID_t \| S)$

M3:R→T:$H(ID_t \oplus S)$

其中 M1 是明文传输,对协议逻辑属性的分析没有作用,将以上模型转换成如下 BAN 逻辑语言时可省略,即:

M2:$R \lhd H(ID_t)$,$H(ID_t, S)$

M3:$T \lhd H(ID_t, S)$

4.2.3 协议的安全目标及分析推理

(1)$R| \equiv T| \sim \#(ID_t)$

(2)$T| \equiv R| \sim \#(ID_t)$

下面分析推理改进协议能否达到以上安全目标:

(1)证明 $R| \equiv T| \sim \#(ID_t)$

由初始假设 P1:$R| \equiv \#(S)$ 和新鲜性规则 $\dfrac{P| \equiv \#(X)}{P| \equiv \#(X,Y)}$ 可得:$\dfrac{R| \equiv \#(S)}{R| \equiv \#(S, ID_t)}$,继而推出:$R| \equiv \#(S, ID_t)$ ①

由 M2 得:$R \lhd H(ID_t, S)$,由假设 P2:$R| \equiv R \xleftrightarrow{S} T$ 和消息意义规则 $\dfrac{(P| \equiv Q \xleftrightarrow{S} P, P \lhd \{X\}_k)}{P| \equiv Q| \sim X}$ 可得:$R| \equiv T| \sim H(ID_t, S)$

由 M2 拆分消息后可知:$R \lhd ID_t$,$R \lhd S$,由规则 $\dfrac{(P| \equiv Q| \sim H(X_1, X_2, \cdots, X_n), P \lhd X_1, P \lhd X_2, \cdots, P \lhd X_n)}{P| \equiv Q| \sim (X_1, X_2, \cdots, X_n)}$ 得:$\dfrac{(R| \equiv T| \sim H(ID_t, S), R \lhd ID_t, R \lhd S)}{R| \equiv T| \sim (ID \lhd \equiv t, S)}$,继而推出:$R| \equiv T| \sim (ID_t, S)$

利用规则:$\dfrac{P| \equiv Q| \sim (X,Y)}{P| \equiv Q| \sim X}$ 可得:$R| \equiv T| \sim ID_t$ ②

由①②可得:$R| \equiv T| \sim \#(ID_t)$,即达到安全目标(1)。

(2)$T| \equiv R| \sim \#(ID_t)$

由初始假设 P4:$T| \equiv T \xleftrightarrow{S} R$ 和理想化模型 M3:$T \lhd H(ID_t, S)$ 根据消息意义规则 $\dfrac{(P| \equiv Q \xleftrightarrow{k} P, P \lhd \{X\}_k)}{P| \equiv Q| \sim X}$ 可得:$T| \equiv R| \sim H(ID_t, S)$

由 M3 拆分消息后可知:$T \lhd ID_t$,$T \lhd S$,根据规则 $\dfrac{(P| \equiv Q| \sim H(X_1, X_2, \cdots, X_n), P \lhd X_1, P \lhd X_2, \cdots, P \lhd X_n)}{P| \equiv Q| \sim (X_1, X_2, \cdots, X_n)}$

得出:$T|\equiv R|\sim(ID_t,S)$　　①

又由假设 P3 可知:$T|\equiv\#(ID_t)$　　②

由①②可得:$T|\equiv R|\sim\#(ID_t)$,即达到安全目标(2)。

4.3　BAN 分析结论

通过对本文提出的安全协议进行 BAN 逻辑形式化分析,可推导出其安全目标 $R|\equiv T|\sim\#(ID_t)$ 和 $T|\equiv R|\sim\#(ID_t)$,因此该协议能够有效地实现 RFID 传感网络中标签和阅读器的双向合法身份认证的安全目标。

5　结论

本文介绍了 RFID 传感网络中几种典型的基于 Hash 函数的 RFID 安全认证协议,针对协议中的不足提出了一种新的基于 Hash 函数的改进方案。此方案有效地解决了 RFID 传感网络中阅读器与标签间面临的多种安全隐私问题,具有成本低、效率高、安全性高等特点。最后通过建立协议的理想化模型,利用 BAN 逻辑对该协议进行形式化分析,在理论上证明了其安全性,使其在实际应用中具有较高的实用价值。

参考文献:

[1] Sarma S E, Weis S A, Engels D W. RFID Systems and Security and Privacy Implications[C]//Proc. of the 4th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2003: 454-469.

[2] Sarma S E, Weis S A, Engels D W. Radio Frequency Identification: Secure Risks and Challenges[J]. RSA Laboratories Crypto bytes, 2003, 6(1): 2-9.

[3] Weis S A, Sarma S E, Rivest R L, et al. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems[C]// Proc. of the 1st International Conference on Security in Pervasive Computing. Berlin, Germany: Springer-Verlag, 2004: 201-212.

[4] Ohkubo M, Suzuki K, Kingships S. Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID[C]//Proc. of Symposium on Cryptography and Information Security. Sendai, Japan: [s. n.], 2004: 719-724.

[5] 王健伟,王东,TIMO Korhonen,等. 一种新的 RFID 传感网络中多阅读器防碰撞协议[J]. 传感技术学报,2008,21(8):2140-6140.

[6] 陈颖,张福洪. RFID 传感网络中多阅读器碰撞算法的研究[J]. 传感技术学报,2010,23(2):1206-1210.

[7] 余恬恬,冯全源. 基于 Hash 函数的 RFID 挑战-应答认证协议[J]. 计算机工程,2009,35(24):156-157.

[8] Chen Y C, Wang Weilin, Huang M S. RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection[C]//Proc. of the 9th International Conference on Advanced Communication Technology. Phoenix Park, Korea: [s. n.], 2007.

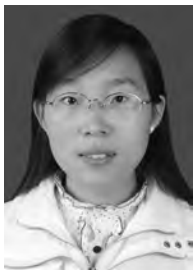
[9] 丁振华,李锦涛,冯波,等. 基于 Hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展,2009,46(4):583-592.

[10] Osaka K, Takagi T. An Efficient and Secure RFID Security Method with Ownership Transfer[C]//Proc. of Computational Intelligence and Security. Guangzhou, China: [s. n.], 2006: 1090-1095.

[11] Burrows M A, Needham R. Logic of Authentication[J]. ACM Transaction on Computer Systems, 1990, 8(1): 18-36.

[12] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报,2005,16(10):1743-1756.

刘明生(1960-),男,江苏扬中人,教授,博士生导师,主要研究方向是传感网络及其应用、网络与信息安全,liums601001@sina.com;



王　艳(1987-),女,山东济宁人,硕士研究生,主要研究方向是网络与信息安全,wangyan12061987@126.com。