

一种基于混合位交叉异或函数的超轻量级 RFID 认证协议

汪雨¹, 陆卫兵^{2,3}, 陶军¹, 刘震国², 战俊麟²

(1.东南大学网络空间安全学院, 南京, 211100)

(2.东南大学毫米波国家重点实验室, 南京, 211100)

(3.东南大学前沿科学中心, 南京, 211100)

220205125@seu.edu.cn

摘 要 RFID 技术作为物联网关键技术之一, 其标签具有成本低、体积小、适用性强等优点, 被广泛应用于物流管理、医疗、交通、农业等领域。RFID 系统的安全性直接影响了它们的稳定性。为了满足这种存储量低和计算能力弱的低成本 RFID 标签的安全性需求, 本文提出一种基于混合位交叉异或函数的超轻量级 RFID 认证协议。并且对所提出的协议进行了安全性分析和 Scyther 工具模拟验证, 以及与常见超轻量级 RFID 认证协议进行对比, 结果表明所提出协议适用于低成本的 RFID 系统。

关键词: 认证协议, RFID, 物联网, 安全

An Ultra-lightweight RFID Authentication Protocol Based on Mixed Bit Crossover XOR Function

Yu Wang¹, Wei-Bing Lu^{2,3}, Jun Tao¹, Zhen-Guo Liu², Jun-Lin Zhan²

(1. School of Cyber Science and Engineering, Southeast University, Nanjing, 211100)

(2. State Key Lab of Millimeter waves, Southeast University, Nanjing, 211100)

(3. Frontier Science Center, Southeast University, Nanjing, 211100)

220205125@seu.edu.cn

Abstract: RFID technology, as one of the key technologies of the Internet of Things, has the advantages of low cost, small size and strong applicability, and is widely used in logistics management, medical treatment, transportation, agriculture and other fields. The security of RFID systems directly affects the stability of them. In order to meet the security requirements of this low-cost RFID tag with low storage volume and weak computing power, this paper proposes an ultra-lightweight RFID authentication protocol based on mixed bit crossover XOR function. Furthermore, the proposed protocol is analyzed and simulated by Scyther tools, and compared with the common ultra-lightweight RFID authentication protocol, the results show that the proposed protocol is suitable for low-cost RFID systems.

Keywords: Authentication protocol, RFID, IoT, security

1 引言

随着物联网技术的快速发展, 射频识别(Radio Frequency Identification, RFID)技术成为物联网的重要技术之一, 取得了广泛的应用^[1]。RFID 是一种利用电磁波实现非接触式数据传输的技术, 通过将射频信号发送到标签, 从而识别物体或者数据。如今, RFID 技术广泛应用于物流管理、医疗、交通、农业等领域^[2]。

由于标签和阅读器之间通过无线信道进行通信, 这意味着标签和阅读器之间传输的无线信号易受到攻击, 攻击者可通过窃听、篡改、重放等手段对 RFID 系统进行攻击。因此, 为抵抗标签和阅读器之间可能受到的各种安全攻击, 通常使用身份认证协议。考虑到 RFID 系统在一些实际的应用场景中, 所需数量庞大, 而且要求成本低廉, 一般所采用的无源标签内部电路数量有限。针对于目前成熟的加密和解密算法, 由于需要大量的计

算成本和存储空间,无法直接应用到低成本的无源标签中。因此,针对于低成本的 RFID 标签存在的安全性问题,本文提出一种基于混合位交叉异或函数的超轻量级认证协议。分析了该协议的安全性,并与常见的认证协议进行对比。最终,Scyther 验证结果表明该协议在一定范围内不会受到主动攻击和被动攻击。

2 超轻量级 RFID 认证协议

(1) 混合位交叉异或函数

假设消息 X 和消息 Y 为 n 位,如式 (2-1) - (2-2) :

$$X = x_n x_{n-1} \dots x_2 x_1, x_i \in \{0,1\}, \quad (2-1)$$

$$i = 1, 2 \dots n$$

$$Y = y_n y_{n-1} \dots y_2 y_1, y_i \in \{0,1\}, \quad (2-2)$$

$$i = 1, 2 \dots n$$

位交叉异或函数 Cro 的计算过程如式(2-3):

$$Cro(X, Y) = x_n \oplus y_{n-1} \parallel x_{n-1} \oplus y_n \parallel \dots \parallel x_2 \oplus y_1 \parallel x_1 \oplus y_2 \quad (2-3)$$

混合位交叉异或函数的计算利用了分支结构,增加了函数的混淆扩散性。主要分为两个步骤,首先计算 $X \oplus Y$ 的汉明权重,如式 (2-4)。若结果为奇数,则按照式 (2-5) 进行计算;否则,按照式 (2-6) 进行计算。

$$H = Hw(X \oplus Y) \quad (2-4)$$

$$MixCro(X, Y) = Cro(Rot(X, X \oplus Y), X \oplus Y) \quad (2-5)$$

$$MixCro(X, Y) = Cro(Rot(Y, X \oplus Y), X) \quad (2-6)$$

混合位交叉异或函数仅利用了多种位逻辑运算的组合,实现了低复杂性、不可逆性、敏感性、高混淆扩散性的特征。

(2) 协议方案

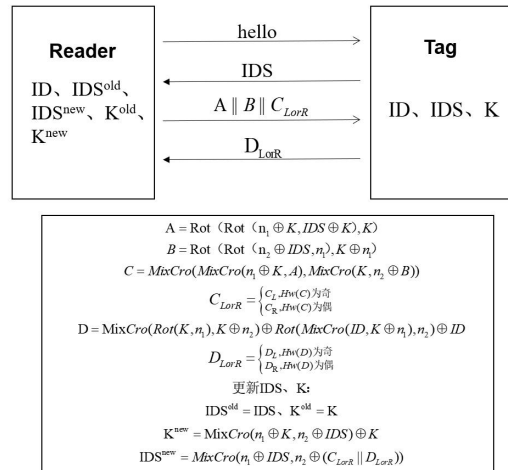


图1 所提出协议的具体操作

协议涉及三个实体:阅读器、标签和后端服务器。通常假设阅读器和后端服务器之间在安全信道下进行通信,故将其看作一个整体。每个标签中存储自己的唯一标识(ID)、索引假名(IDS)和密钥(K),阅读器中存储每个标签的唯一标识(ID)、索引假名(IDS^{new})和密钥(K^{new}),以及上一轮验证中所使用的索引假名(IDS^{new})和密钥(K^{new})。

协议的具体操作如图1所示:阅读器首先发送请求认证消息给标签,标签接收到后,响应自己的索引假名(IDS)。阅读器接收到相应的IDS后,在后端数据库中查找到对应的标签信息及密钥K,并且生成随机数 n_1 和 n_2 ,根据图中公式计算 $A \parallel B \parallel C_{LorR}$,发送给标签。标签从A、B中提取随机数 n_1 和 n_2 ,同时计算 C_{LorR} 值,判断是否与接收到的值一致。若一致,则标签成功认证阅读器,并且计算 D_{LorR} 值响应阅读器;否则认证失败,流程结束。若标签成功认证阅读器,标签更新自己的IDS值和K值。阅读器收到响应后,计算 D_{LorR} 值,判断是否与接收值一致。若一致,则阅读器认证该标签为合法标签,同时更新自己的IDS值和K值,此时,阅读器与标签之间完成了相互认证;若不一致,则阅读器认证标签

失败，流程结束。该协议仅使用了基本的位逻辑运算，因此适用于低成本的 RFID 系统。

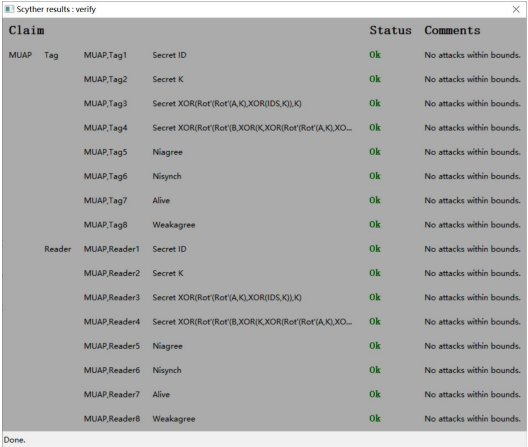
3 协议的安全性分析

(1) 非形式化安全性分析

本文提出的协议在实现了标签和阅读器之间相互认证的同时，对于标签的秘密信息（K）使用了一些位逻辑操作进行隐藏，使得攻击者根据明文信息难以破解。由于阅读器中存储了与标签在上一轮认证中所使用的 IDS 值和 K 值，当发生去同步攻击时，标签仍可以使用旧的秘密值进行身份认证。在每一次新的认证会话中，阅读器都会生成新的随机数，并且在每次会话结束后，标签的 IDS 和 K 值均会更新，即每次传输的信息均不同，因此可抵抗重放攻击，同时保证了前向安全性。

(2) Scyther 形式化分析

使用 Scyther 安全仿真工具对本文所提出的认证协议进行模拟，结果如图 2 所示，结果表明在一定范围内，该协议不会受到主动和被动攻击。



Claim	Status	Comments
MUAP.Tag MUAP.Tag1 Secret ID	Ok	No attacks within bounds.
MUAP.Tag MUAP.Tag2 Secret K	Ok	No attacks within bounds.
MUAP.Tag MUAP.Tag3 Secret XOR(Rot(A,K),XOR(IDS,K),K)	Ok	No attacks within bounds.
MUAP.Tag MUAP.Tag4 Secret XOR(Rot(B,XOR(XOR(Rot(A,K),XO...	Ok	No attacks within bounds.
MUAP.Tag MUAP.Tag5 Niagree	Ok	No attacks within bounds.
MUAP.Tag MUAP.Tag6 Nisynch	Ok	No attacks within bounds.
MUAP.Tag MUAP.Tag7 Alive	Ok	No attacks within bounds.
MUAP.Tag MUAP.Tag8 Weakagree	Ok	No attacks within bounds.
Reader MUAP.Reader1 Secret ID	Ok	No attacks within bounds.
MUAP.Reader MUAP.Reader2 Secret K	Ok	No attacks within bounds.
MUAP.Reader MUAP.Reader3 Secret XOR(Rot(A,K),XOR(IDS,K),K)	Ok	No attacks within bounds.
MUAP.Reader MUAP.Reader4 Secret XOR(Rot(B,XOR(XOR(Rot(A,K),XO...	Ok	No attacks within bounds.
MUAP.Reader MUAP.Reader5 Niagree	Ok	No attacks within bounds.
MUAP.Reader MUAP.Reader6 Nisynch	Ok	No attacks within bounds.
MUAP.Reader MUAP.Reader7 Alive	Ok	No attacks within bounds.
MUAP.Reader MUAP.Reader8 Weakagree	Ok	No attacks within bounds.

图 2 Scyther 分析结果

4 性能对比

从安全性和成本（标签的存储成本和计算成本）的角度，将本文所提出

的 RFID 认证协议与其他认证协议做对比，结果如表 1 所示。

表 1 本文协议与常见认证协议对比

	SASI ^[2]	GOASSM	LPCP ^[4]	本文
	ER ^[3]			协议
Tag 存储量	7L	7L	5L	3L
Tag 上操作	$\oplus, OR, +,$ AND, Rot	$\oplus, Rot, +,$ MixBits	$\oplus, Per,$ CRC16	$\oplus, Rot,$ MixCro
去同步攻击	NO	YES	YES	YES
重放攻击	YES	NO	NO	YES
假冒攻击	NO	NO	NO	YES

5 结论

本文提出的一种基于混合位交叉异或函数的超轻量级 RFID 认证协议，解决了低成本 RFID 系统存在的安全性问题。根据安全性分析和 Scyther 仿真结果，证明该协议可抵抗常见的攻击类型。同时，该协议所要求标签上的存储空间和计算成本较小。因此，该协议可适用于低成本的 RFID 系统。

参考文献

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

[2] Hung-Yu, SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity, IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 337-340.

[3] Peris Lopez P, Hernandez Castro J C, Tapiador J M E, et al, Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol, International Workshop on Information Security Applications, Springer, Berlin, Heidelberg, 2008: 56-68.

[4] Gao, L., et al, An ultralightweight RFID authentication protocol with CRC and permutation, Journal of Network and Computer Applications, 2014, 41: 37-46.