一种超轻量级移动射频识别的双向认证协议

黄 琪 凌 捷
(广东工业大学计算机学院 广州 510006)

摘 要 针对移动射频识别中读写器与后端服务器之间因无线传输带来的安全问题,提出了一种超轻量级移动射频识别的双向认证协议。该协议通过级联运算动态更新标签假名和标签密钥,可有效隐藏标签真实身份,并利用循环校验函数进行标签以及读写器与后端服务器之间的身份认证,实现了系统的双向认证。安全性分析表明,该协议可抵抗跟踪攻击、假冒攻击、重放攻击、中间人攻击等多种恶意攻击。与现有的几种协议相比,该协议降低了标签端的计算开销和通信开销,具有安全性较高、成本低的优点。

关键词 射频识别,循环校验函数,双向认证,超轻量级
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.07.021

Ultra-lightweight Mutual Authentication Protocol for Mobile Radio Frequency Identification

HUANG Qi LING Jie
(School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China)

Abstract Aiming at the security problem between the reader and back-end server of mobile radio frequency identification caused by wireless transmission, an ultra-lightweight mutual authentication protocol for mobile radio frequency identification are proposed. In the protocol, the tag pseudonyms and key label are dynamically updated by cascade operation, which can effectively hide the true identity of the tag. And the cyclic check function is used for identity authentication between the tag, reader and back-end server, which can achieve the system mutual authentication. Security analysis shows that the proposed protocol can resist many kinds of malicious attacks, such as tracking attack, impersonation attack, replay attack, man-in-the-middle attack and so on. Compared with several existing protocol, the protocol reduces the computational and communication costs of the label, which are of high security and low cost.

Keywords Radio frequency identification, Cyclic check function, Mutual authentication, Ultra-lightweight

1 引言

移动射频识别技术的基本原理与传统的射频识别(Radio Frequency Identification,RFID)技术相同,都是通过射频信号在无物理接触下自动识别物体并获取相关数据信息[1]。不同的是,在移动RFID系统中,读写器是可移动的,读写器与后端服务器之间通过无线连接。因读写器的可移动性和标签的便携性等优点,移动射频识别技术已在许多领域得到应用,如仓储物流管理、资产跟踪管理、访问控制和智能感知等[2-3]。但移动RFID系统中读写器与标签和后端服务器之间的无线连接是不安全的,容易遭受恶意攻击,泄露用户隐私信息[4]。同时,由于标签计算能力和存储能力有限,无法在标签上进行复杂运算和大量的数据存储,在保证协议安全性的同时又会增加标签成本。针对移动RFID存在的上述安全隐患,本文提出一种超轻量级双向认证协议,该协议具有计算量小、成本低、安全性较高的优点。

2 相关工作

针对RFID系统中的安全认证问题,研究人员已经做了很多相关研究。文献[5]提出的认证方案不能抵抗去同步化攻击,攻击者可以通过重放消息,使读写器与标签两者之间的密钥不一致,从而破坏两者之间的后续认证;在文献[6]的方案中,攻击者可以通过重放消息,使得读写器与标签之间的密钥更新不同步,从而影响后续认证;文献[7]中的标签需要产生4个随机数,计算方面略显复杂,增加了标签成本,从而降低了认证效率;在文献[8]的方案中,攻击者可通过拒绝服务攻击来破坏读写器与标签之间的身份认证;文献[9]通过交叉位运算与移位运算进行身份认证,计算过于简单,易遭受暴力破解攻击;在文献[10]提出的认证协议中,标签身份属于静态ID,易被攻击者追踪,从而窃取隐私信息;文献[11-12]提出的

到稿日期:2016-05-31 返修日期:2016-08-29 本文受广东省科技计划项目(2014B090901053,2014B090908010,2015B090906015,2016B090918039,2016B090918058)资助。

黄 琪(1993-),女,硕士生,主要研究方向为网络与信息安全,E-mail:871722971@qq.com;凌 捷(1964-),男,博士,教授,CCF会员,主要研究方向为网络与信息安全。

认证协议缺少后端服务器对读写器的身份认证，易遭受假冒、重放攻击；文献[13]提出的协议属于轻量级认证，使用 hash 函数进行数据加密，增加了标签的计算量，标签端成本较高。

针对上述协议存在的安全隐患，本文对文献[12]中的协议进行改进，提出了一种超轻量级移动射频识别双向认证协议。本协议采用的 16bits 的循环校验函数比伪随机函数需要的门电路数少，可有效降低标签的硬件成本，同时标签端不产生随机数，只通过简单的循环校验函数和异或运算等实现读写器、标签与后端服务器之间的认证，使标签端计算量减小，运算速度提高，实现了协议的超轻量级；并且在通信过程中动态更新标签假名，隐藏了标签真实 ID，防止标签被跟踪；通过安全性分析，该协议实现了标签匿名性，可有效抵抗追踪攻击、假冒攻击、重放攻击、去同步化攻击、中间人攻击、暴力破解攻击等。

3 协议的提出

3.1 协议说明

本文提出的协议中增加了读写器标识符，标签不用产生随机数，使用 16bit 的循环校验函数处理需要传输的信息，实现标签匿名性和系统的双向认证。对协议中出现的符号进行说明：R 表示读写器，T 表示标签，S 表示后端服务器，ID_T 表示标签唯一身份标识，ID_R 表示读写器身份标识，IDS 表示标签假名，KT 表示标签密钥，KR 表示读写器密钥，x' 表示更新的 x 值，x^{old} 表示上一轮的 x 值，$\oplus$ 表示异或运算，$\|$ 表示级联运算，$CRC\text{-}16(x)$ 表示循环校验函数，$[x]_L$ 表示取计算结果 x 的前 L 位，$x \leftarrow y$ 表示 x 更新为 y。

3.2 协议流程

移动双向认证协议过程如图 1 所示。

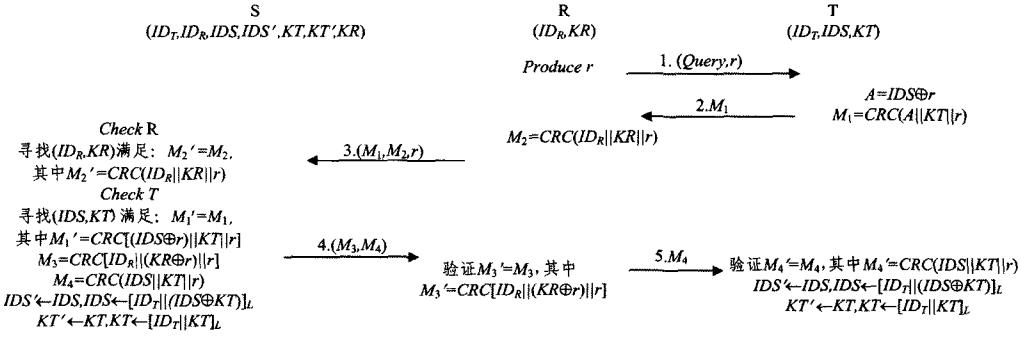

图 1 协议流程

初始化阶段：后端服务器存储标签的相关信息（ID_T，IDS，KT）以及读写器的相关信息（ID_R，KR），读写器存储自身信息（ID_R，KR），标签存储信息（ID_T，IDS，KT），读写器产生一个随机数 r，然后向标签发出 Query 请求，并把随机数 r 发送给标签。

双向认证阶段：

（1）标签收到读写器发送的消息后，首先计算 $A=IDS\oplus r$，接着计算消息 $M_1=CRC(A \| KT \| r)$，并将 M_1 发送给读写器。

（2）读写器收到消息后，首先计算 $M_2=CRC(ID_R \| KR \| r)$，再把消息 (M_1, M_2, r) 传送给后端服务器。

（3）后端服务器收到读写器发来的消息后，首先验证读写器的合法性，在数据库中寻找（ID_R，KR）并结合收到的 r 计算 $M_2'=CRC(ID_R \| KR \| r)$，判断 M_2' 与收到的 M_2 是否相等，若不相等，则认证立即终止；若相等，则说明后端服务器对读写器认证成功。然后开始验证标签的合法性，在数据库中寻找（IDS，KT）并计算 $M_1'=CRC[(IDS\oplus r) \| KT \| r]$，判断 M_1' 与收到的 M_1 是否相等，若相等，则标签合法，说明后端服务器对标签认证成功，此时开始计算 $M_3=CRC[ID_R \| (KR\oplus r) \| r]$，$M_4=CRC(IDS \| KT \| r)$，然后向读写器发送消息 (M_3, M_4)，同时更新后端服务器数据：$IDS' \leftarrow IDS$，$IDS \leftarrow [ID_T \| (IDS\oplus KT)_L$，$KT' \leftarrow KT$，$KT \leftarrow ID_T \| KT]_L$；若不相等，则在数据库中寻找（$IDS^{old}$，$KT^{old}$）计算 $M_1''=CRC[(IDS^{old}\oplus r) \| KT^{old} \| r]$，并判断 M_1'' 与收到的 M_1 是否相等，若相等，则更新数据：$IDS'=[ID_T \| (IDS^{old}\oplus KT^{old})]_L$，$KT'=[ID_T \| KT]_L$，再计算 $M_3=CRC[ID_R \| (KR\oplus r) \| r]$，$M_4=CRC(IDS' \| KT' \| r)$，最后将消息 (M_3, M_4) 发送给读写器；若不相等，则说明后端服务器认证标签失败，停止认证。

（4）读写器收到消息后，根据自身存储的（ID_R，KR）和产生的 r 计算 $M_3'=CRC[ID_R \| (KR\oplus r) \| r]$，并判断 M_3' 与收到的 M_3 是否相等，若相等，则说明标签对后端服务器认证成功，并将 M_4 发送给标签；若不相等，则认证失败，停止认证。

（5）标签收到消息后，根据自身存储的（IDS，KT）以及传来的 r 计算 $M_4'=CRC(IDS \| KT \| r)$，判断 M_4' 与收到的 M_4 是否相等，若相等，则说明标签对后端服务器认证成功，并更新数据：$IDS' \leftarrow IDS$，$IDS \leftarrow [ID_T \| (IDS\oplus KT)]_L$，$KT' \leftarrow KT$，$KT \leftarrow [ID_T \| KT]_L$，若不相等，则利用（$IDS^{old}$，$KT^{old}$）计算 $M_4''=CRC[(IDS^{old}\oplus r) \| KT^{old} \| r]$，并判断 M_4'' 与收到的 M_4 是否相等，若相等，则更新数据：$IDS'=[ID_T \| (IDS^{old}\oplus KT^{old})]_L$，$KT'=[ID_T \| KT]_L$，若不相等，则不更新数据。

4 BAN 逻辑形式化分析

本协议采用 BAN 逻辑分析方法对协议进行形式化证明。形式化证明过程中，$P \lhd X$ 表示 P 接收了消息 X，$P \mid\sim X$ 表示 P 曾发送过消息 X，$P \mid\equiv X$ 表示 P 相信消息 X，$\#(X)$ 表示 X 是新鲜的，$P \overset{K}{\leftrightarrow} Q$ 表示 P 与 Q 共享密钥 K，$P \mid\Rightarrow X$ 表示 P 对 X 有管辖权，$\{X\}_k$ 表示消息 X 通过 K 加密。下面首先给出本协议中使用的部分 BAN 逻辑推理规则。

(1)消息含义规则

$$R_1:\frac{P|\equiv Q\overset{K}{\leftrightarrow}P,P\lhd\{X\}_K}{P|\equiv Q|\sim X}$$

(2)临时值验证规则

$$R_4:\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

(3)管辖规则

$$R_5:\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$$

(4)消息新鲜性规则

$$R_{11}:\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$$

在证明之前，首先给出协议的理想化模型：

消息①　$R\rightarrow T:(Query,r)$

消息②　$T\rightarrow R:\{M_1\}$，M_1 中包含随机数 r、标签假名，并用密钥 KT 进行加密。

消息③　$R\rightarrow S:\{M_1,M_2\}$，$M_1$ 和 M_2 中都包含随机数 r，并且都是经密钥 KT 或 KR 加密后的密文。

消息④　$S\rightarrow R:\{M_3,M_4\}$，$M_3$ 和 M_4 中都包含随机数 r，并且都是经密钥 KT 或 KR 加密后的密文。

消息⑤　$R\rightarrow T:\{M_4\}$，M_4 中包含随机数 r、标签假名，并用密钥 KT 进行加密。

下面给出协议的初始化假设：

$P_1:T|\equiv S\overset{KT}{\leftrightarrow}T$，$T$ 相信 S 和 T 共享秘钥 KT。

$P_2:S|\equiv T\overset{KT}{\leftrightarrow}S$，$S$ 相信 T 和 S 共享秘钥 KT。

$P_3:R|\equiv S\overset{KR}{\leftrightarrow}R$，$R$ 相信 S 和 R 共享秘钥 KR。

$P_4:S|\equiv R\overset{KR}{\leftrightarrow}S$，$S$ 相信 R 和 S 共享秘钥 KR。

$P_5:T|\equiv\#(IDS)$，T 相信标签假名 IDS 的新鲜性。

$P_6:S|\equiv\#(IDS)$，S 相信标签假名 IDS 的新鲜性。

$P_7:S|\equiv\#(r)$，S 相信随机数 r 的新鲜性。

$P_8:R|\equiv\#(r)$，R 相信随机数 r 的新鲜性。

$P_9:S|\equiv T|\Rightarrow M_1$，$S$ 相信 T 对 M_1 的管辖权。

$P_{10}:S|\equiv R|\Rightarrow M_2$，$S$ 相信 R 对 M_2 的管辖权。

$P_{11}:R|\equiv S|\Rightarrow M_3$，$R$ 相信 S 对 M_3 的管辖权。

$P_{12}:T|\equiv S|\Rightarrow M_4$，$T$ 相信 S 对 M_4 的管辖权。

安全目标：

$G_1:S|\equiv M_1$，S 相信 M_1。

$G_2:S|\equiv M_2$，S 相信 M_2。

$G_3:R|\equiv M_3$，R 相信 M_3。

$G_4:T|\equiv M_4$，T 相信 M_4。

推理证明过程如下：

由消息③得 $P\lhd\{M_1\}_{KT}$，由初始假设 P_2 及消息含义规则 R_1，可得：

$$S|\equiv T|\sim M_1 \tag{1}$$

由假设 P_6 及消息新鲜性规则 R_{11}，可得：

$$S|\equiv\#(M_1) \tag{2}$$

由式(1)、式(2)以及临时值验证规则 R_4，可得：

$$S|\equiv T|\equiv M_1 \tag{3}$$

由式(3)、初始化假设 P_9 以及管辖规则 R_5，可知：$S|\equiv M_1$。因此目标 G_1 得到证明。

运用上述消息、假设和推理规则，同理可推出 $S|\equiv M_2$，$R|\equiv M_3$，$T|\equiv M_4$，即目标 G_2，G_3 和 G_4 得到证明，此处不再另外证明。

5　协议安全性分析

5.1　数据可靠性

本文协议中的通信信息使用随机数和循环校验进行加密，使得每次通信信息都不重复，第三方无法通过篡改或重放的方式骗过认证，确保了数据的可靠性。

5.2　标签匿名性和不可追踪性

攻击者只可能通过窃听传输的信息得到关于标签的内部消息，通信过程不涉及标签身份 ID，而标签内部包含的信息中标签假名 IDS 和密钥 KT 均通过循环校验函数进行了加密，并且每次认证都进行了数据更新，故无法得到关于标签身份的任何消息，因此标签满足匿名性；并且在认证过程中，标签每次传输的信息均是随机更新的，相互之间没有关联性，从而使攻击者无法根据传输信息推测标签的位置信息，保证了标签前向隐私的安全性。

5.3　读写器匿名性和不可追踪性

在移动射频识别系统中，读写器的可移动性可能会导致读写器的隐私在无线传输过程中被泄露。本协议中，读写器利用循环校验函数对其自身的身份信息 ID_R 和密钥 KR 进行了加密，有效隐藏了读写器的身份，保证了读写器的隐私。同时由于加密信息中包含了随机数 r，使得读写器每次传输的信息均不相同，从而使攻击者无法定位读写器，不能推测读写器的位置隐私。

5.4　抵抗假冒攻击

当攻击者企图假冒读写器，发送截获的信息欺骗标签时，由于每次认证均会生成新的随机数，并且通过 ID_R 和密钥 KR 加密生成认证信息，而攻击者无法获得读写器的身份信息，从而无法计算出一致的认证信息，因此无法通过验证；若攻击者假冒成标签，由于每次生成的认证信息包含的随机数 r、标签身份 ID_T 和密钥 KT 均不相同，导致攻击者截获的信息无法通过验证，因此能够抵抗假冒攻击。

5.5　抵抗重放攻击

每当协议一次认证结束时，标签和后端服务器都会进行数据更新，并且每次所使用的随机数 r 均不相同，即使攻击者截获了之前的交互信息 M_i，在以后的通信中重放，也不能被标签和后端服务器认证。

5.6　抵抗去同步化攻击

若攻击者通过截断消息 M_i 使标签与后端服务器之间的数据更新不同步，由于后端服务器存储着上一轮的会话信息 $(ID_T,IDS^{old},KT^{old})$，当再次发起会话时，后端服务器可在上一轮的会话信息中找到对应的标签信息进行认证，因此协议能够抵抗去同步化攻击。

5.7　抵抗中间人攻击

若攻击者通过篡改消息 M_1 或 M_4 来骗过认证，由于消息 M_1 或 M_4 由标签假名 IDS 和密钥 KT 以及随机数 r 加密得到，而攻击者必须得到标签的身份信息 (IDS,KT) 才能通过认证，由于每次通信标签身份信息都进行了更新，使得攻击者无法得出正确的标签身份信息，从而无法通过认证，因此能够抵抗中间人攻击。

5.8 抵抗暴力破解攻击

本文协议运行时，攻击者可截获消息 M_i，并通过某种手段得到循环校验码，由于使用级联运算使标签和读写器的身份信息得到了隐藏，并且标签身份信息（IDS，KT）的动态性使得攻击者无法破解标签的身份信息，因此能够抵抗暴力破解攻击。

5.9 双向认证

后端服务器通过接收的消息（M_1，M_2，r）验证标签和读写器的合法性，由于 M_1，M_2 中包含的标签身份信息和读写器身份信息唯一，因此只有合法的标签和读写器才能通过认证；而读写器收到消息 M_3 后，利用自身的身份标识计算 M_3' 与 M_3 是否匹配，匹配成功则说明认证后端服务器成功；同理，标签收到消息 M_4，可计算是否匹配，从而可验证读写器和后端服务器的合法性。

表 1 是本文协议与其他几种 RFID 认证协议之间进行的安全性比较。其中，√表示能够抵抗，×表示无法抵抗。

表 1 协议的安全性比较

安全性	文献[11]	文献[12]	文献[13]	本文协议
数据可靠性	×	×	√	√
匿名性	√	√	√	√
可追踪性	√	√	√	√
假冒攻击	×	×	√	√
重放攻击	×	×	√	√
去同步化攻击	√	√	√	√
中间人攻击	√	√	√	√
暴力破解攻击	√	√	√	√
双向认证	×	×	√	√

6 协议的性能比较

本文协议主要从标签的计算代价、存储代价、通信代价以及使用的门电路数 4 个方面与其他协议进行性能比较。

计算代价：设伪随机数代价为 T_{PRNG}，异或运算代价为 T_{XOR}，循环校验代价为 $T_{CRC}=t$，级联运算代价为 T_{AND}，Rabin 加密运算代价为 T_{Rabin}，右移运算代价为 T_{Rot}，Hash 函数代价为 T_{Hash}。异或运算、级联运算和右移运算等运算速度非常快，与其他轻量级运算相比，其运算时间可忽略不计，而 Hash 函数、伪随机数、Rabin 加密算法等运算速度均比循环校验函数慢，运算时间长于循环校验函数。文献[11]中标签端的计算代价为 $2T_{XOR}+2T_{AND}+T_{CRC}+4T_{Rabin}+3T_{Rot}+T_{PRNG}>6t$；文献[12]中标签端的计算代价为 $5T_{PRNG}+4T_{XOR}>5t$；文献[13]中标签端的计算代价为 $3T_{Hash}+T_{PRNG}+2T_{Rabin}+T_{XOR}+3T_{AND}>6t$；本协议中标签端不需要产生随机数，计算代价为 $2T_{CRC}+T_{XOR}+3T_{AND}=2t$。

存储代价：设每个数据长度为 $L=128$bits，标签真实 ID_T 的存储代价为 L_{ID_T}，标签假名 IDS 的存储代价为 L_{IDS}，标签密钥的存储代价为 L_{KT}，隐私信息 x，si，ti 的存储代价分别为 L_x，L_{si}，L_{ti}。文献[11]中标签的存储代价为 $L_{si}+L_{ti}=2L=256$bits；文献[12]中标签的存储代价为 $L_{ID_T}+L_{KT}+L_x=3L=384$bits；文献[13]中标签的存储代价为 $L_{si}+L_{ti}=2L=256$bits；本协议中标签的存储代价为 $L_{IDS}+L_{KT}+L_{ID_T}=3L=384$bits。

通信代价：设传输信息的长度为 $L=128$bits；文献[11]中标签的通信代价为 $5L=640$bits；文献[12]中标签的通信代价为 $3L=384$bits；文献[13]中标签的通信代价为 $4L=512$bits；本文协议中标签的通信代价为 $2L=256$bits。

逻辑门电路数：目前的 Hash 函数所需要的门电路数大约为 1700～2500，比伪随机函数所需的门电路数少，而 CRC-16 函数所需的门电路数大约为 10～30，文献[11,13]中使用了 Hash 函数和伪随机函数，文献[12]中使用了伪随机函数，所需的门电路数均比 CRC-16 函数所需的门电路数多，由此可说明本文协议需要更少的逻辑门电路数。

图 2 是本文协议与其他几种协议的计算代价比较图，图 3 是本文协议与其他几种协议的存储代价和通信代价比较图。由上述分析以及图 2、图 3 可看出，与其他几种协议相比，本文协议的计算代价和通信代价更小，存储代价与文献[12]相等，所需的门电路数更少，适用于低成本 RFID 系统。

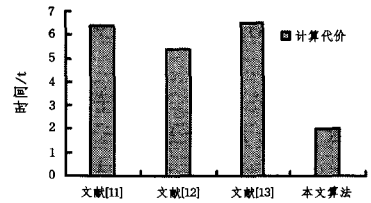

图 2 协议的计算代价比较

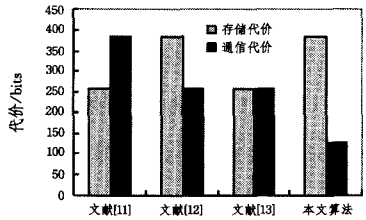

图 3 存储代价和通信代价比较

结束语 本文提出了一种超轻量级移动射频识别认证协议，充分考虑移动 RFID 系统中读写器的移动性带来的新问题，利用标签假名隐藏标签真实身份，增加读写器与后端服务器之间的双向认证，同时将大部分计算量转移到后端服务器，利用循环校验函数运算简单快速的特点，实现超轻量级运算，减小标签端的计算量，降低标签成本。在保证低成本的情况下，使协议能够有效抵抗假冒攻击、重放攻击、去同步化攻击等多种恶意攻击，使协议的安全性与效率之间尽量平衡，更具有实用价值。

参 考 文 献

[1] ZHOU S J, ZHANG W Q, Luo J Q. Overview of radio frequency identification(RFID) privacy protection technology [J]. Journal of Software, 2015, 26(4): 960-976. (in Chinese)
周世杰，张文清，罗嘉庆. 射频识别(RFID)隐私保护技术综述[J]. 软件学报，2015，26(4)：960-976.

[2] MAMUN M S I, MIYAJI A, RAHMAN M S. A secure and private RFID authentication protocol under SLPN problem[C]// Proc of the 6th Int Conf on Network and System Security. Berlin: Springer, 2012: 476-489.

[3] ALOMAIR B, CUELLAR J, POOVENDRAN R. Scalable RFID systems: A privacy-preserving protocol with constant time identification[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1536-1550.

[4] JIN Y M, WU Q Y, SHI Z Q, et al. RFID Lightweight Authenti-

cation Protocol Based on PRF[J]. Journal of Computer Research and Development,2014,51(7):1506-1514. (in Chinese)
金永明,吴棋滢,石志强,等. 基于 PRF 的 RFID 轻量级认证协议研究[J]. 计算机研究与发展,2014,51(7):1506-1514.

[5] SHEN J W,LING J. An improved ultra lightweight RFID authentication protocol[J]. Computer Applications and Software, 2015,32(2):304-306. (in Chinese)
沈金伟,凌捷. 一种改进的超轻量级 RFID 认证协议[J]. 计算机应用与软件,2015,32(2):304-306.

[6] GODOR G,IMRE S. Hash-based mutual authentication protocol for low-cost RFID systems[C]// Proc of the 18th EUNICE Conf on Information and Communications Technologies. Berlin: Springer,2012:76-87.

[7] SURESH T,M R. Mutual authentication protocol for RFID security using NFSR [C]// IEEE International Conference on Communication Software & Networks. Chengdu,2015:255-259.

[8] PENG P,ZHAO Y M,HAN W L,et al. An ultra-lightweight RFID mutual authentication protocol[J]. Computer Engineering,2011,37(16):140-142. (in Chinese)
彭朋,赵一鸣,韩伟力,等. 一种超轻量级 RFID 双向认证协议[J]. 计算机工程,2011,37(16):140-142.

[9] DU Z Y,ZHANG G A,YUAN H L. Crossover Based Ultra-lightweight RFID Authentication Protocol[J]. Computer Science, 2013,40(11):35-37. (in Chinese)
杜宗印,章国安,袁红林. 基于交叉位运算的超轻量 RFID 认证协议[J]. 计算机科学,2013,40(11):35-37.

[10] LIU P,ZHANG C H,Ou Q Y. Authentication security protocol of mobile RFID based on Hash function [J]. Journal of Computer Applications,2013,33(5):1350-1352. (in Chinese)
刘鹏,张昌宏,欧庆于. 基于 Hash 函数的移动射频识别互认证安全协议设计[J]. 计算机应用,2013,33(5):1350-1352.

[11] FU X,GUO Y. A lightweight RFID mutual authentication protocol with ownership transfer [J]. Communications in Computer and Information Science,2012,334:68-74.

[12] NIU B,ZHU X,CHI H,et al. Privacy and authentication protocol for mobile RFID systems [J]. Wireless Personal Communications,2014,77(3):1-19.

[13] TAO Y,ZHOU X,MA Y P,et al. Mutual authentication protocol of mobile RFID based on Hash function[J]. Journal of Computer Applications,2016,36(3):657-660. (in Chinese)
陶源,周喜,马玉鹏,等. 基于 Hash 函数的移动双向认证协议[J]. 计算机应用,2016,36(3):657-660.

(上接第 83 页)

[8] YANG Z,LIU Y H. Wi-Fi Radar:From RSSI to CSI [J]. Communications of the China Computer Federation,2014,10(11): 55-60. (in Chinese)
杨峥,刘云浩. Wi-Fi 雷达:从 RSSI 到 CSI [J]. 中国计算机学会通讯,2014,10(11):55-60.

[9] XIAO J,WU K S,YI Y W,et al. FIFS:Fine-grained indoor fingerprinting system[C]//21st International Conference on Computer Communications and Networks(ICCCN). 2012:1-7.

[10] CHAPRE Y,IGNJATOVIC A,SENEVIRATNE A,et al. CSI-MIMO:Indoor Wi-Fi Fingerprinting System[C]// 39th Annual IEEE Conference on Local Computer Networks. LCN, 2014: 202-209.

[11] WU K S,XIAO J,YI Y W,et al. CSI-based indoor localization [J]. IEEE Transactions on Parallel and Distributed Systems, 2012,24(7):1300-1309.

[12] KAMRAN A,LIU A X,WANG W. Keystroke Recognition Using Wi Fi Signals[C]// Proceedings of ACM Mobile Computing & Networking. ACM,2015:90-102.

[13] HE W F,WU K S,ZOU Y P,et al. WiG:Wi Fi-based Gesture Recognition System[C]// IEEE Conference on Computer Communication & Networks. 2015:1-7.

[14] PU Q,GUPTA S,GOLLAKOTA S,et al. Whole-home gesture recognition using wireless signals[C]// Proceedings of ACM Mobile Computing & Networking. ACM,2013:485-486.

[15] XI W,ZHAO J Z,ZHAO K,et al. Electronic Frog Eye:Counting Crowd Using Wi Fi[C]// IEEE Infocom-IEEE Conference on Computer Communiations. 2014:361-369.

[16] SEN S,CHOUDHURY R R,RADUNOVIC B,et al. Precise indoor localization using PHY layer information[C]//Proceedings of the 10th ACM Workshop on Hot Topics in Networks, ser. Hot Nets-X. New York,NY,USA:ACM,2011:1-6.

[17] HALPERIN D,HU W,SHETH A,et al. Predictable 802.11 Packet Delivery from Wireless Channel Measurements[J]. Proc. of ACM SIGCOMM,2010,41(4):159-170.

[18] HALPERIN D,HU W,SHETH A,et al. Tool release:gathering 802.11n traces with channel state information[J]. SIGCOMM Comput,2011,41(1):53-53.

[19] LI D,ZHANG B X. Fingerprint-based Indoor Positioning Technology [J]. ZTE Technology Journal, 2015, 21(6): 31-34. (in Chinese)
李冬,张宝贤. 基于指纹的室内定位技术[J]. 中兴通讯技术,2015,21(6):31-34.

[20] DAI H Y,ZHANG G. Based on IEEE 802.11n CSI-Tool of Wi-Fi Interference Studies and Measurement[J]. Informatization Research,2014,40(1):59-62. (in Chinese)
戴寒怡,张弓. 基于 IEEE 802.11n CSI-Tool 的 Wi-Fi 干扰研究和测量[J]. 信息化研究,2014,40(1):59-62.

[21] ZHU R,BAI G W,SHEN H,et al. CSI Indoor Positioning Method Based on Bayesian Filtering Method [J]. Computer Engineering and Design,2015,36(3):567-571. (in Chinese)
朱荣,白光伟,沈航,等. 基于贝叶斯过滤法的 CSI 室内定位方法[J]. 计算机工程与设计,2015,36(3):567-571.

[22] YANG Z,ZHOU Z M,LIU Y H. From RSSI to CSI:Indoor Location via Channel Response[J]. ACM Computing Surveys, 2013,46(2):1-32.

[23] YANG J W,CHO G H. Utilizing CSI to Improve Distance Estimation Precision in the Indoor Environment [J]. International Journal of Software Engineering and Its Applications, 2015, 9(3):49-56.

[24] CHEN Y,LIU W,XIONG Y,et al. A fuzzy similarity elimination algorithm for indoor fingerprint positioning[J]. International Journal of Distributed Sensor Networks,2015,2015:1-10.

[25] LI H,SUN L,ZHU H,et al. Achieving privacy preservation in WiFi fingerprint-based localization[J]. Proceedings-IEEE INFOCOM,2014,84(1):2337-2345.