说 明 书

一种结合物理认证因素的 Wi-Fi 口令动态更新方法及系统

技术领域

本发明属于无线技术、信息安全技术领域，涉及一种结合物理认证因素的 Wi-Fi 口令动态更新方法及系统；适用于单位内部的 Wi-Fi 接入认证的应用场景，同时支持访客的临时访问。

背景技术

随着互联网及移动互联网的发展，Wi-Fi 的覆盖范围已遍及住宅、工作场所、交通工具等各种场所。Wi-Fi 网络成为人们工作生活所必不可少的通信工具，询问 Wi-Fi 口令已成为人们进入新场所要做的第一件事。在 Wi-Fi 普及的同时，Wi-Fi 的安全问题也日益受到人们的关注，央视 315 晚会连续两年报道公共免费 Wi-Fi 存在安全隐患，并现场演示了通过公开 Wi-Fi 获取用户的隐私信息：用户接入晚会现场的公开 Wi-Fi 后打开一两个常用应用，浏览一下消费记录，该用户的姓名、手机号、银行卡号和身份证号等信息就在大屏幕上显示了出来。当人们通过 Wi-Fi 访问互联网时，移动终端会将通信数据以无线电波的形式发送给无线接入点，任何能够接收到无线电波的设备均可截获移动终端收发的数据。同时，公开 Wi-Fi 对其传输的数据不进行加密处理，一旦移动终端或无线接入点通过 Wi-Fi 传输了隐私数据，他人就可以获取到这些隐私信息。

为了保护经 Wi-Fi 传输的数据的机密性和完整性，同时确保只有授权用户能够访问 Wi-Fi，国际电工电子工程学会（IEEE）制定了 802.11i 标准，该标准规定了 Wi-Fi 接入认证和通讯加密等过程的安全要求及技术规范，正确应用上述标准可以确保无线通信的机密性和完整性，以及 Wi-Fi 的可控访问。802.11i 规定了多种认证协议，可以实现不同的安全目标。

其中的 WPA/2-Personal 是一种基于口令的无线认证协议，无线接入点和移动终端通过带外方式共享相同的口令。两者经过四次握手完成双向认证，同时产生后续通讯的会话密钥，通信数据使用该会话密钥加密后传输。即使移动应用在发送用户隐私数据时并未加密，无线网卡也会对其发出的数据进行加密。攻击者即使截获了通信数据，也无法获得用户的隐私数据。四次握手所需的主密钥由口令经过伪随机数生成函数产生。在 WPA/2-Personal 认证协议中，口令是身份鉴别和通信保密的基础。但在实际应用中，人们倾向于选择简单的 Wi-Fi 口令，且口令长期不变，这极易导致 Wi-Fi 口令泄露。一旦 Wi-Fi 口令泄露，该 Wi-Fi 就和公开 Wi-Fi 没有区别。非法用户不仅可以通过无线接入点的认证，抢占 Wi-Fi 流量，影响合法用户的上网体验，也能冒充无线接入点，欺骗移动终端与之建立连接，截获移动终端发送的数据

包，还能解密无线接入点和移动终端之间收发的数据包。

WPA/2-Enterprise 为 Wi-Fi 提供了更高级别的安全保障。移动终端首先和无线接入点后台的服务器进行 TLS 协商，产生的会话密钥将作为后续移动终端和无线接入点进行四次握手的主密钥，之后在 TLS 隧道中服务器鉴别移动终端的用户身份。鉴别完毕后，服务器将主密钥发送给无线接入点，无线接入点和移动终端经过四次握手完成双向认证和会话密钥的协商。在 WPA/2-Enterprise 标准中，移动终端通过 Wi-Fi 访问互联网时，加密通信数据使用的会话密钥最终由移动终端和服务器的 TLS 协商过程派生而来，通信的安全性依赖于 TLS 协议而非固定不变的口令。但是此种认证方式要求管理员为每个用户预先创建账户，对于临时访问 Wi-Fi 的用户，还需要为临时账户设置访问期。管理员需要维护不断更新的数据库，维护成本较高。

Web Portal 认证是另外一种常见的 Wi-Fi 认证方案，严格上讲，该方案是用户管理方案而非 Wi-Fi 认证方案。移动终端接入 Wi-Fi 后，无线接入点首先会拒绝其对外网的访问，用户只有在内网 Portal 网站上登录后才能访问外网。该方案支持用户自己创建用户账户，无需管理员的参与。但是此种认证方式的安全性取决于移动终端在接入 Wi-Fi 时使用的认证方式，如果 Wi-Fi 本身时公开的，那么移动终端的通信数据也是未经加密处理就传输的，同样存在隐私数据泄露的隐患。

发明内容

本发明针对单位内部的 Wi-Fi 环境，提出了一种结合物理认证因素的 Wi-Fi 口令动态更新方法及系统，能够解决 Wi-Fi 口令简单且长期不变所带来的安全隐患，同时不降低用户体验。Wi-Fi 口令按照设定的时间间隔自动更新。移动终端为了接入 Wi-Fi，必须和无线接入点共享相同的口令。一旦无线接入点更新了 Wi-Fi 口令，移动终端也必须同步更新 Wi-Fi 口令，移动终端才能按照 WPA/2-Personal 标准接入 Wi-Fi。为了更新 Wi-Fi 口令，持有移动终端的用户必须通过物理认证，进入单位内部设定的受控物理环境，移动终端才能更新 Wi-Fi 口令，从而接入 Wi-Fi。本发明提出的 Wi-Fi 口令动态更新方法包含以下流程：口令初始化、物理认证参数的更新和发布、以及无线接入点和移动终端的口令更新。

首先需要为无线接入点和移动终端设置初始口令。无线接入点的初始口令由 Wi-Fi 管理员手动设置，之后无线接入点按照设定的时间间隔自动更新口令。移动终端通过带外方式获得无线接入点当前的 Wi-Fi 口令，当前口令可以以文本消息、二维码、或者其他合适的方式传输，可以由 Wi-Fi 管理员分发给用户，也可以由获得了 Wi-Fi 口令的用户分发给其他用户。移动终端和无线接入点共享相同的 Wi-Fi 口令，移动终端能够使用标准的 WPA/2-Personal 协

议接入 Wi-Fi。

物理认证参数是指移动终端只有在受控物理环境中才能获得的参数，是更新 Wi-Fi 口令的必需参数。在设定的口令更新时点，指定的物理认证参数生成及发布设备会生成新的物理认证参数并将其发布到设定的受控物理环境中，无线接入点从物理认证参数生成及发布设备获取新的物理认证参数。

在实际的部署中，为了保证用户都能够接入 Wi-Fi、有好的服务体验，Wi-Fi 网络通常会部署多台无线接入点以保证 Wi-Fi 信号的覆盖范围，Wi-Fi 信号范围通常都会大于受控物理环境的范围。可以指定其中的一台或者多台无线接入点作为物理认证参数生成及发布设备用以生成和发布物理认证参数，称之为主无线接入点，Wi-Fi 网络内的其他无线接入点称为从无线接入点。主无线接入点借助其广播的 Wi-Fi 信标帧发布物理认证参数，参数承载于 Wi-Fi 信标帧的供应商自定义字段。为了保证只有经过物理认证、进入到受控物理环境内的移动终端才能获得物理认证参数，主无线接入点的 Wi-Fi 信号覆盖范围不得超出受控物理环境。从无线接入点的 Wi-Fi 信号覆盖范围不限于受控物理环境，但是从无线接入点不发布物理认证参数。

物理认证参数更新间隔可以固定不变，也可以根据需求动态变化：例如，当遇到重大事情时，可以缩短更新周期。从无线接入点从主无线接入点获取物理认证参数的方式可以是和主无线接入点建立长连接，当物理认证参数更新时，主无线接入点将更新情况通知与之建立长连接的从无线接入点。也可以由从无线接入点主动向主无线接入点请求物理认证参数：如果物理认证参数更新间隔固定不变，从无线接入点可以以相同的时间间隔请求物理认证参数；如果物理认证参数更新间隔动态变化，主无线接入点在响应物理认证参数的同时声明该物理认证参数对应的有效期，从无线接入点物理认证参数有效期结束时再向主无线接入点请求新的物理认证参数。或者，也可以使用其他保证所有无线接入点在较短的时延内完成物理认证参数更新的方式，例如，采取管理员人工配置的方式。

物理认证参数在主从无线接入点间传输时应当使用安全信道，例如使用专用的网线传输物理认证参数，或者在主从无线接入点间建立双向认证的 TLS 或 IPSec 信道后传输物理认证参数，或者加密后传输物理认证参数，采取管理员人工配置的方式等。

移动终端收到 Wi-Fi 信号后首先判断其拥有的 Wi-Fi 口令是否已失效：例如无线接入点可以广播其鉴别移动终端所用的 Wi-Fi 口令所属的口令更新周期，或者对应的序列号。移动终端根据 Wi-Fi 口令的序号来判断 Wi-Fi 口令是否已更新。如果 Wi-Fi 口令已更新，移动终端需要提醒用户通过物理认证，进入受控物理环境。移动终端进入主无线接入点的 Wi-Fi 信号覆盖范围后，捕捉 Wi-Fi 信标帧，解析其中的供应商自定义字段，获得物理认证参数，从而

计算出新口令，使用标准的 WPA/2-Personal 协议接入 Wi-Fi。如果用户无法通过物理认证，其持有的移动终端将无法接收到主无线接入点的 Wi-Fi 信号，无法获得主无线接入点发布的新的物理认证参数，无法计算出新口令，也就无法接入 Wi-Fi。

无线接入点按照设定的时间间隔产生或获得物理认证参数后，根据新物理认证参数和原 Wi-Fi 口令按照事先确定的公式计算新 Wi-Fi 口令。例如可以按以下公式更新口令：设原口令为 P[i - 1]，新物理认证参数为 O[i]，则新口令 P[i] = Hash(P[i - 1] XOR O[i])，其中 XOR 表示异或运算，Hash 表示单向杂凑函数，如 SM3、SHA-256 等。移动终端进入 Wi-Fi 信号覆盖范围后，首先判断 Wi-Fi 口令是否更新，如果当前 Wi-Fi 口令仍有效，则继续使用当前口令接入 Wi-Fi；如果 Wi-Fi 口令已更新，则需要获取新的物理认证参数，利用该参数和当 Wi-Fi 前口令、采用和无线接入点相同的算法计算新口令；如果最近一次更新 Wi-Fi 口令的时间距今已超过两个口令更新间隔，则移动终端无法再次接入 Wi-Fi。

如前所述，如果移动终端需要持续性地访问 Wi-Fi，移动终端在口令更新周期内必须至少进入一次受控物理环境，获取物理认证参数，从而持续性地和无线接入点同步更新口令。一旦移动终端在某个口令更新周期内未能进入受控物理环境，该设备将无法再计算出后续的所有口令，也就永久地失去了 Wi-Fi 访问权。单位内部的人员能够保证经常性的进入受控物理环境，其持有的移动终端能够一直正常接入 Wi-Fi；而临时访客，在访问期结束后，他将无法再通过物理认证进入受控物理环境更新口令，也就无法再接入 Wi-Fi，即使他能收到 Wi-Fi 信号。

若主无线接入点每次只公布当次的物理认证参数，则用户必须至少按照与口令更新频率相同的频率进入受控物理环境，才能保证持续地访问 Wi-Fi；若主无线接入点每次公布当次和下一次的物理认证参数，则用户在某次接入 Wi-Fi 后，在下一个口令更新周期就可以不进入受控物理环境，其仍然可以计算出下一个口令更新周期的口令。用户仍需要在 Wi-Fi 口令第二次更新时再进入受控物理环境，才能计算出后续的 Wi-Fi 口令。即用户可以间隔一个口令周期进入受控物理环境，也可以保证持续地访问 Wi-Fi。原因是该用户每次进入受控物理环境都可以获得当次和下次的物理认证参数，从而计算出当次和下次的口令，即使用户下次未进入受控物理环境，他仍然知道口令。通过调整发布的物理认证参数的数量，可以调整对用户进入受控物理环境的频率的限定。

本发明提出了一种新的应用于 Wi-Fi 的动态口令技术，与现有技术相比，本发明的有益效果为：

1. Wi-Fi 口令自动动态变化，降低了攻击者猜测口令的可能性和影响，同时 Wi-Fi 口令变化无需用户操作。

2. 将 Wi-Fi 认证和物理认证相结合，如果无法通过物理认证，就无法接入无线网，无需对用户作额外的访问控制，降低了无线网的管理成本。

3. 可以兼顾不同类型用户的访问需求，包括单位内部固定人员的长期访问和访客的临时访问，固定人员拥有长期的 Wi-Fi 访问权，访客在访问期结束后失去 Wi-Fi 访问权。访客的访问权的授予和终止，不需要 Wi-Fi 网络管理员的操作。

附图说明

图 1 为本发明一种结合物理认证因素的动态口令更新方法中物理认证参数生成及发布设备定期更新物理认证参数的工作流程示意图；

图 2 为本发明一种结合物理认证因素的动态口令更新方法中无线接入点定期更新 Wi-Fi 口令的工作流程示意图；

图3为本发明一种结合物理认证因素的动态口令更新方法中移动终端接入Wi-Fi的工作流程示意图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，对本发明作进一步详细说明，对发明内容中的可选方案进行了具体指定，例如以二维码的形式分发 Wi-Fi 口令、指定 Wi-Fi 网络内的一台无线接入点作为物理认证参数生成及发布设备、按照固定时间间隔更新物理认证参数、物理认证参数加密后借助 HTTP 协议传输等。技术方案包括初始口令的获得、物理认证参数的产生和发布、程序初始化、以及无线接入点和移动终端口令更新四部分。

（1）初始口令的获得

首先 Wi-Fi 管理员需要为无线接入点设置初始口令，无线接入点生成 32 字节的伪随机数作为初始口令。初始口令存储于配置文件中。Wi-Fi 口令以二维码的形式传输，Wi-Fi 管理员将当前口令生成的二维码显示在屏幕上，供合法用户扫描，合法用户也可以将当前口令生成的二维码显示在移动终端屏幕上，供其他合法用户扫描。移动终端通过扫描二维码的方式获得 Wi-Fi 口令。移动终端获得初始口令后在当前口令更新周期内即可自由访问 Wi-Fi。

（2）物理认证参数的产生和发布

物理认证参数是 32 字节的随机数，每隔固定时间间隔更新，移动终端只有在受控物理环境中才能获得。指定一台无线接入点产生并发布物理认证参数，如图 1 所示，参数通过该无线接入点的 Wi-Fi 信标帧发布，承载于 Wi-Fi 信标帧的供应商自定义字段。移动终端在捕获 Wi-Fi 信标帧后通过解析供应商自定义字段获得当前的物理认证参数，从而能够计算新口令。

指定无线接入点的 Wi-Fi 信号覆盖范围只能局限于受控物理环境，位于受控物理环境外的移动终端无法收到该无线接入点的 Wi-Fi 信号，防止外部移动终端获得物理认证参数。当然位于受控物理环境外的移动终端也可能收到属于同一 Wi-Fi 网络的 Wi-Fi 信号，但是这些 Wi-Fi 信号由属于同一 Wi-Fi 网络的其他无线接入点产生，这些无线接入点不会广播物理认证参数，移动终端只能凭借原 Wi-Fi 口令接入 Wi-Fi，而无法计算新口令。产生并发布物理认证参数的无线接入点称为主无线接入点，属于同一 Wi-Fi 网络的其他无线接入点称为从无线接入点。另外，主无线接入点应部署在用户进入单位的必经之处，以保证用户获得物理认证参数的便捷性。

除了主无线接入点和移动终端，从无线接入点也需要获得物理认证参数。主无线接入点以 Web 服务的方式向从无线接入点发布物理认证参数。主无线接入点的 IP 设置为静态 IP，同时在从无线接入点的配置文件中设置主无线接入点的 IP，从无线接入点向该 IP 请求物理认证参数。每隔固定时间间隔，从无线接入点向主无线接入点使用 HTTP 请求轮询物理认证参数。为了保证物理认证参数在主从无线接入点间传输时的机密性，物理认证参数加密后传输。在主从无线接入点的配置文件中设置相同的 SM4 加解密密钥，主无线接入点使用 SM4 加密算法加密，从无线接入点使用 SM4 解密算法解密，只有从无线接入点能够得到正确的物理认证参数。考虑到主从无线接入点的系统时间可能不同步，从无线接入点在预定口令更新时点前一小段时间就向主无线接入点请求物理认证参数。主无线接入点在响应物理认证参数的同时说明该物理认证参数对应的时间段，从无线接入点根据时间段判断收到的物理认证参数是否已更新。一旦主无线接入点更新完 Wi-Fi 口令，从无线接入点就能收到新的物理认证参数，随即更新 Wi-Fi 口令，确保主无线接入点更新完 Wi-Fi 口令后其他无线接入点也能在较短的时间内更新完口令。几乎在任何时间点，所有无线接入点均使用相同的 Wi-Fi 口令鉴别移动终端。

（3）程序初始化

无论是无线接入点上的程序还是移动终端上的程序，启动后第一步都从配置文件中读取初始口令，判断初始口令在当前口令更新周期内仍有效。首先要确定当前口令更新周期。主无线接入点根据自身的系统时间决定当前口令更新周期。从无线接入点启动后即向主无线接入点请求物理认证参数，主无线接入点在返回物理认证参数的同时返回该物理认证参数对应的时间段，以主无线接入点的当前口令更新周期决定从无线接入点的当前口令更新周期，保证所有无线接入点当前口令更新周期的一致性。考虑到移动终端和无线接入点的时间可能不同步，所有无线接入点在广播 Wi-Fi 信标帧的同时广播当前口令更新周期，时间承载于 Wi-Fi 信标帧的供应商自定义字段。移动终端如果能够收到 Wi-Fi 信号，则从 Wi-Fi 信标帧的供应

商自定义字段提取无线接入点的当前口令更新周期，以此作为自身的当前口令更新周期。通过前述方法，所有的无线接入点和移动终端最终都使用了主无线接入点的当前口令更新周期，确保无线接入点和移动终端能够共享相同的口令，顺利接入 Wi-Fi。

如果初始口令在当前口令更新周期内仍有效，则程序不需要对当前口令做任何操作，无线接入点继续使用当前口令鉴别移动终端，移动终端继续使用当前口令接入 Wi-Fi。如果初始口令已经在当前口令更新周期内已失效，但当前口令是在上一个口令更新周期内更新的，主无线接入点可以产生新的物理认证参数并发布，从而计算新口令；从无线接入点需要向主无线接入点请求当前时段的物理认证参数，从而计算新口令；移动终端需要通过物理认证、进入受控物理环境，从主无线接入点的 Wi-Fi 信标帧中解析物理认证参数，从而计算新口令。如果初始口令是在上一个口令更新周期前更新的，主无线接入点仍然可以自主地将口令更新至当前时间（依次产生多个物理认证参数，并逐次更新口令），而从无线接入点和移动终端则无法再将口令更新至当前时间，此时从无线接入点需要 Wi-Fi 管理员重新设置初始口令，而移动终端则需要从 Wi-Fi 管理员或其他合法用户处重新获取初始口令。

（4）口令更新

每到预定的口令更新时点，主无线接入点会自主地产生物理认证参数，而从无线接入点则会向主无线接入点请求物理认证参数，并按以下算法计算新口令。设原口令为 P[i - 1]，本次的物理认证参数为 O[i]，则此次的口令 P[i] = SM3(P[i - 1] XOR O[i])。无线接入点生成新口令后重启无线连接程序，无线连接程序即会使用新口令鉴别移动终端，此时移动终端只有获得物理认证参数才能计算出新口令，从而接入 Wi-Fi，如图 2 所示。

如图 3 所示，移动终端收到 Wi-Fi 信号后，首先判断是否能够继续使用当前口令接入 Wi-Fi，如果发现当前口令已过期，就会试图解析 Wi-Fi 信标帧的供应商自定义字段，获取物理认证参数。只有解析得到新的物理认证参数，才能使用前述算法计算出新口令，从而接入 Wi-Fi。

无线接入点每次重启无线连接程序后需要将新口令存入配置文件，移动终端在成功接入 Wi-Fi 后也需要将新口令存入配置文件，作为新的初始口令。即使程序因为计划或意外重启，口令也可以在现有基础上继续更新。

若主无线接入点每次只公布当次的物理认证参数，则用户必须至少按照与口令更新频率相同的频率进入受控物理环境，才能保证持续地访问 Wi-Fi；若主无线接入点每次公布当次和下一次的物理认证参数，则用户在某次接入 Wi-Fi 后，在下一个口令更新周期就可以不进入受控物理环境，其仍然可以计算出下一个口令更新周期的口令。用户仍需要在 Wi-Fi 口令第二次更新时再进入受控物理环境，才能计算出后续的 Wi-Fi 口令。即用户可以间隔一个口令周期进入受控物理环境，也可以保证持续地访问 Wi-Fi。原因是该用户每次进入受控物理环境

都可以获得当次和下次的物理认证参数，从而计算出当次和下次的口令，即使用户下次未进入受控物理环境，他仍然知道口令。通过调整发布的物理认证参数的数量，可以调整对用户进入受控物理环境的频率的限定。

虽然以上描述了本发明的具体实施方式，但是本领域的技术人员应当理解，这些仅是举例说明，本发明的保护范围是由所附权利要求书限定的。本领域的技术人员在不背离本发明的原理和实质的前提下，可以对这些实施方式做出多种变更或修改，但这些变更和修改均落入本发明的保护范围。