



# (12) 发明专利

(10) 授权公告号 CN 110493778 B

(45) 授权公告日 2022. 03. 22

(21) 申请号 201910762379.2

(22) 申请日 2019.08.19

(65) 同一申请的已公布的文献号  
申请公布号 CN 110493778 A

(43) 申请公布日 2019.11.22

(73) 专利权人 商洛学院  
地址 726000 陕西省商洛市东店子342号

(72) 发明人 范申民

(74) 专利代理机构 北京卓特专利代理事务所  
(普通合伙) 11572

代理人 段宇

(51) Int. Cl.

H04W 12/06 (2021.01)

(56) 对比文件

CN 105450604 A, 2016.03.30

CN 105787323 A, 2016.07.20

US 2018075686 A1, 2018.03.15

谭悦平. WiFi无线网络的安全与防范措施探讨.《信息与电脑(理论版)》.2018, (第2018(09)期), 192-196.

审查员 李文聪

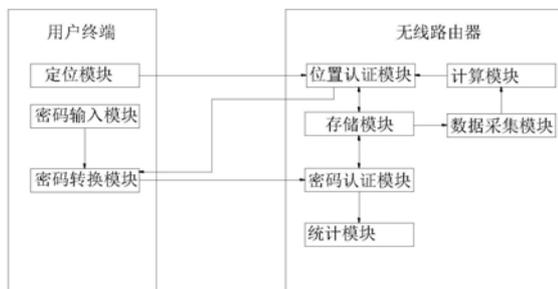
权利要求书2页 说明书4页 附图1页

(54) 发明名称

一种WiFi安全登录认证系统

(57) 摘要

本发明公开一种WiFi安全登录认证系统,用于解决现有的WiFi认证通过字母、数字和符号进行认证,安全性较低,很容易通过现有的破解软件编程进行字母、数字和符号进行排序验证进行破解;导致安全认证低的问题;包括用户终端和无线路由器;所述用户终端包括定位模块、密码输入模块和密码转换模块;无线路由器包括位置认证模块、存储模块、密码认证模块、数据采集模块、计算模块和统计模块;密码转换模块将输入的密码进行转换,得到叠加图形;密码认证模块接收到叠加图形与对比图形进行匹配,当两者完全吻合,则认证成功;通过图形叠加加密,提高密码的复杂度,避免现有的无线网破解软件,通过无线次实现进行破解。



1. 一种WiFi安全登录认证系统,包括用户终端和无线路由器;其特征在于,所述用户终端包括定位模块、密码输入模块和密码转换模块;无线路由器包括位置认证模块、存储模块、密码认证模块、数据采集模块、计算模块和统计模块;

所述定位模块用于获取用户终端的位置数据和用户终端的IP地址;定位模块将用户终端的位置数据发送至位置认证模块;所述位置认证模块用于对用户终端的位置进行认证,具体认证步骤如下:

步骤一:设定用户终端的位置记为 $A_i, i=1, \dots, n$ ;

步骤二:位置认证模块获取存储模块内存储的用户预设的指定上网区域;

步骤三:当用户终端的位置 $A_i$ 处于指定上网区域的范围内,则位置认证模块向用户终端的密码转换模块发送采集指令;当用户的位置 $A_i$ 处于指定上网区域的范围外,则不进行任何操作;

所述密码输入模块用于用户输入的密码并发送至密码转换模块;所述密码转换模块用于接收采集指令后接收密码输入模块发送的输入的密码;所述密码转换模块将输入的密码进行转换,具体转换步骤如下:

步骤一:将用户输入的密码标记为 $M_i, i=1, \dots, n$ ;输入的密码由字母、数字和符号排序组合构成;

步骤二:设定对比密码记为 $C_i, i=1, \dots, n$ ;对比密码为字母、数字或符号;每个对比密码 $C_i$ 对应一个转换图形 $D_i, i=1, \dots, n$ ;转换图形 $D_i$ 为不同大小的图形构成,图形包括正方形、圆形和三角形以及正方形、圆形、三角形内部的中心点;

步骤三:将输入的密码 $M_i$ 与对比密码 $C_i$ 进行匹配获取对应的转换图形 $D_i$ ;

步骤四:依照输入的密码排序将转换图形 $D_i$ 进行叠加,得到叠加图形;具体表现为,设定输入的密码第一个密码匹配的转换图形为 $D_1$ ,第二个密码匹配的转换图形为 $D_2$ ;第三个密码匹配的转换图形为 $D_3$ ;将转换图形 $D_1$ 置于最底层,然后将转换图形 $D_2$ 的中心点与转换图形 $D_1$ 的中心点重合,然后将转换图形 $D_3$ 的中心点与转换图形 $D_2$ 的中心点重合;

步骤五:将叠加图形发送至密码认证模块;

所述密码认证模块接收到叠加图形并对图形进行对比,具体对比过程如下:

a:密码认证模块获取存储模块内存储的用户预设的对比图形;

b:将叠加图形与对比图形进行匹配,当完全吻合,则认证成功,同时成功验证次数增加一;否,认证失败,同时,失败验证次数增加一;

c:密码认证模块将成功验证次数和失败验证次数发送至存储模块存储。

2. 根据权利要求1所述的一种WiFi安全登录认证系统,其特征在于,所述定位模块将用户终端的IP地址发送至存储模块;所述数据采集模块用于存储模块内存储的用户终端的IP地址、成功验证次数及失败验证次数;数据采集模块将获取的用户终端的IP地址、成功验证次数及失败验证次数发送至计算模块;所述计算模块用于计算用户终端的验证值,具体计算步骤如下:

S1:设定成功验证次数记为 $P_1$ ,失败验证次数记为 $P_2$ ;

S2:利用公式 $YZ = \lambda \left( \frac{P_2 * e_1}{P_1 * e_2 + 1} \right)$ 获取得到验证值YZ,其中, $e_1$ 和 $e_2$ 均为预设比例系数固

定值, $\lambda$ 为修正因子,取值为0.96231;

S3:当验证值YZ大于设定阈值,计算模块生成停止指令并发送至位置认证模块;位置认证模块接收到停止指令并停止向密码转换模块发送采集指令。

3.根据权利要求1所述的一种WiFi安全登录认证系统,其特征在于,所述统计模块用于统计无线路由器认证成功的当前在线用户并发送至预设IP地址对应的用户终端上,用于显示无线路由器的当前连接用户。

## 一种WiFi安全登录认证系统

### 技术领域

[0001] 本发明涉及WiFi认证技术领域,尤其涉及一种WiFi安全登录认证系统。

### 背景技术

[0002] WiFi技术是一种短距离无线传输技术,由于其传输速度较快,并且有效距离也比较长,因此,广泛应用于办公场地和家庭中。具有WiFi功能的终端接入WiFi路由器后,由WiFi路由器对WiFi终端进行认证,在认证通过后,允许WiFi终端访问互联网。其认证认证有三种方式,一种是共享口令方式,比如WEP、WPA、WPA2等;一种是Web Portal认证;一种是802.1X认证。

[0003] 现有的WiFi认证通过字母、数字和符号进行认证,安全性较低,很容易通过现有的破解软件编程进行字母、数字和符号进行排序验证进行破解;导致安全认证低。

### 发明内容

[0004] 本发明的目的在于提供一种WiFi安全登录认证系统;用于解决现有的WiFi认证通过字母、数字和符号进行认证,安全性较低,很容易通过现有的破解软件编程进行字母、数字和符号进行排序验证进行破解;导致安全认证低的问题。

[0005] 本发明的目的可以通过以下技术方案实现:一种WiFi安全登录认证系统,包括用户终端和无线路由器;所述用户终端包括定位模块、密码输入模块和密码转换模块;无线路由器包括位置认证模块、存储模块、密码认证模块、数据采集模块、计算模块和统计模块;

[0006] 所述定位模块用于获取用户终端的位置数据和用户终端的IP地址;定位模块将用户终端的位置数据发送至位置认证模块;所述位置认证模块用于对用户终端的位置进行认证,具体认证步骤如下:

[0007] 步骤一:设定用户终端的位置记为 $A_i, i=1, \dots, n$ ;

[0008] 步骤二:位置认证模块获取存储模块内存储的用户预设的指定上网区域;

[0009] 步骤三:当用户终端的位置 $A_i$ 处于指定上网区域的范围内,则位置认证模块向用户终端的密码转换模块发送采集指令;当用户的位置 $A_i$ ,处于指定上网区域的范围外,则不进行任何操作;

[0010] 所述密码输入模块用于用户输入的密码并发送至密码转换模块;所述密码转换模块用于接收采集指令后接收密码输入模块发送的输入的密码;所述密码转换模块将输入的密码进行转换,具体转换步骤如下:

[0011] 步骤一:将用户输入的密码标记为 $M_i, i=1, \dots, n$ ;输入的密码由字母、数字和符号排序组合构成;

[0012] 步骤二:设定对比密码记为 $C_i, i=1, \dots, n$ ;对比密码为字母、数字或符号;每个对比密码 $C_i$ 对应一个转换图形 $D_i, i=1, \dots, n$ ;转换图形 $D_i$ 为不同大小的图形构成,图形包括正方形、圆形和三角形以及正方形、圆形、三角形内部的中心点;

[0013] 步骤三:将输入的密码 $M_i$ 与对比密码 $C_i$ 进行匹配获取对应的转换图形 $D_i$ ;

[0014] 步骤四:依照输入的密码排序将转换图形 $D_i$ 进行叠加,得到叠加图形;具体表现为,设定输入的密码第一个密码匹配的转换图形为 $D_1$ ,第二个密码匹配的转换图形为 $D_2$ ;第三个密码匹配的转换图形为 $D_3$ ;将转换图形 $D_1$ 置于最底层,然后将转换图形 $D_2$ 的中心点与转换图形 $D_1$ 的中心点重合,然后将转换图形 $D_3$ 的中心点与转换图形 $D_2$ 的中心点重合;

[0015] 步骤五:将叠加图形发送至密码认证模块;

[0016] 所述密码认证模块接收到叠加图形并对图形进行对比,具体对比过程如下:

[0017] a:密码认证模块获取存储模块内存的用户预设的对比图形;

[0018] b:将叠加图形与对比图形进行匹配,当完全吻合,则认证成功,同时成功验证次数增加一;否,认证失败,同时,失败验证次数增加一;

[0019] c:密码认证模块将成功验证次数和失败验证次数及对应的失败验证次发送至存储模块存储。

[0020] 优选的,所述定位模块将用户终端的IP地址发送至存储模块;所述数据采集模块用于存储模块内存的用户终端的IP地址、成功验证次数及失败验证次数;数据采集模块将获取的用户终端的IP地址、成功验证次数及失败验证次数发送至计算模块;所述计算模块用于计算用户终端的验证值,具体计算步骤如下:

[0021] S1:设定成功验证次数记为 $P_1$ ,失败验证次数记为 $P_2$ ;

[0022] S2:利用公式  $YZ = \lambda \left( \frac{P_2 * e_1}{P_1 * e_2 + 1} \right)$  获取得到验证值 $YZ$ ,其中, $u_1$ 和 $u_2$ 均为预设比例系数固定值, $\lambda$ 为修正因子,取值为0.96231;

[0023] S3:当验证值 $YZ$ 大于设定阈值,计算模块生成停止指令并发送至位置认证模块;位置认证模块接收到停止指令并停止向密码转换模块发送采集指令。

[0024] 优选的,所述统计模块用于统计无线路由器认证成功的当前在线用户并发送至预设IP地址对应的用户终端上,用于显示无线路由器的当前连接用户;

[0025] 本发明的有益效果:本发明用户的用户终端向无线路由器发送位置数据和用户终端的IP地址,无线路由器内部的位置认证模块进行用户位置认证,当用户终端的位置位于指定上网区域的范围内,则位置认证模块向用户终端的密码转换模块发送采集指令;密码转换模块用于接收采集指令后接收密码输入模块发送的输入的密码;密码转换模块将输入的密码进行转换,得到叠加图形;密码认证模块接收到叠加图形与对比图形进行匹配,当两者完全吻合,则认证成功;通过图形叠加加密,提高密码的复杂度,避免现有的无线网破解软件,通过无线次实现进行破解。

[0025] 本发明的有益效果:本发明用户的用户终端向无线路由器发送位置数据和用户终端的IP地址,无线路由器内部的位置认证模块进行用户位置认证,当用户终端的位置位于指定上网区域的范围内,则位置认证模块向用户终端的密码转换模块发送采集指令;密码转换模块用于接收采集指令后接收密码输入模块发送的输入的密码;密码转换模块将输入的密码进行转换,得到叠加图形;密码认证模块接收到叠加图形与对比图形进行匹配,当两者完全吻合,则认证成功;通过图形叠加加密,提高密码的复杂度,避免现有的无线网破解软件,通过无线次实现进行破解。

## 附图说明

[0026] 下面结合附图对本发明作进一步的说明。

[0027] 图1是本发明一种WiFi安全登录认证系统的原理框图。

## 具体实施方式

[0028] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其它

实施例,都属于本发明保护的范围。

[0029] 请参阅图1所示,本发明为一种WiFi安全登录认证系统,包括用户终端和无线路由器;用户终端包括定位模块、密码输入模块和密码转换模块;无线路由器包括位置认证模块、存储模块、密码认证模块、数据采集模块、计算模块和统计模块;

[0030] 定位模块用于获取用户终端的位置数据和用户终端的IP地址;定位模块将用户终端的位置数据发送至位置认证模块;位置认证模块用于对用户终端的位置进行认证,具体认证步骤如下:

[0031] 步骤一:设定用户终端的位置记为 $A_i, i=1, \dots, n$ ;

[0032] 步骤二:位置认证模块获取存储模块内存储的用户预设的指定上网区域;

[0033] 步骤三:当用户终端的位置 $A_i$ 处于指定上网区域的范围内,则位置认证模块向用户终端的密码转换模块发送采集指令;当用户的位置 $A_i$ 处于指定上网区域的范围外,则不进行任何操作;

[0034] 密码输入模块用于用户输入的密码并发送至密码转换模块;密码转换模块用于接收采集指令后接收密码输入模块发送的输入的密码;密码转换模块将输入的密码进行转换,具体转换步骤如下:

[0035] 步骤一:将用户输入的密码标记为 $M_i, i=1, \dots, n$ ;输入的密码由字母、数字和符号排序组合构成;

[0036] 步骤二:设定对比密码记为 $C_i, i=1, \dots, n$ ;对比密码为字母、数字或符号;每个对比密码 $C_i$ 对应一个转换图形 $D_i, i=1, \dots, n$ ;转换图形 $D_i$ 为不同大小的图形构成,图形包括正方形、圆形和三角形以及正方形、圆形、三角形内部的中心点;

[0037] 步骤三:将输入的密码 $M_i$ 与对比密码 $C_i$ 进行匹配获取对应的转换图形 $D_i$ ;

[0038] 步骤四:依照输入的密码排序将转换图形 $D_i$ 进行叠加,得到叠加图形;具体表现为,设定输入的密码第一个密码匹配的转换图形为 $D_1$ ,第二个密码匹配的转换图形为 $D_2$ ;第三个密码匹配的转换图形为 $D_3$ ;将转换图形 $D_1$ 置于最底层,然后将转换图形 $D_2$ 的中心点与转换图形 $D_1$ 的中心点重合,然后将转换图形 $D_3$ 的中心点与转换图形 $D_2$ 的中心点重合;通过图形叠加加密,提高密码的复杂度,避免现有的无线网破解软件,通过无线次实现进行破解;

[0039] 步骤五:将叠加图形发送至密码认证模块;

[0040] 密码认证模块接收到叠加图形并对图形进行对比,具体对比过程如下:

[0041] a:密码认证模块获取存储模块内存储的用户预设的对比图形;

[0042] b:将叠加图形与对比图形进行匹配,当完全吻合,则认证成功,同时成功验证次数增加一;否,认证失败,同时,失败验证次数增加一;

[0043] c:密码认证模块将成功验证次数和失败验证次数及对应的失败验证次发送至存储模块存储;

[0044] 定位模块将用户终端的IP地址发送至存储模块;数据采集模块用于存储模块内存储的用户终端的IP地址、成功验证次数及失败验证次数;数据采集模块将获取的用户终端的IP地址、成功验证次数及失败验证次数发送至计算模块;计算模块用于计算用户终端的验证值,具体计算步骤如下:

[0045] S1:设定成功验证次数记为 $P_1$ ,失败验证次数记为 $P_2$ ;

[0046] S2:利用公式 $YZ = \lambda(\frac{P2 * e1}{P1 * e2 + 1})$ 获取得到验证值YZ,其中,u1和u2均为预设比例系数固定值, $\lambda$ 为修正因子,取值为0.96231;通过公式可得,成功验证的次数越多,验证值越小,表示用户可以验证失败的次数越多;

[0047] S3:当验证值YZ大于设定阈值,计算模块生成停止指令并发送至位置认证模块;位置认证模块接收到停止指令并停止向密码转换模块发送采集指令;通过次数的验证的限制,避免现有破解软件对无线路由器进行无线次尝试破解;

[0048] 统计模块用于统计无线路由器认证成功的当前在线用户并发送至预设IP地址对应的用户终端上,用于显示无线路由器的当前连接用户。

[0049] 本发明的工作原理:用户的用户终端向无线路由器发送位置数据和用户终端的IP地址,无线路由器内部的位置认证模块进行用户位置认证,当用户终端的位置位于指定上网区域的范围内,则位置认证模块向用户终端的密码转换模块发送采集指令;密码转换模块用于接收采集指令后接收密码输入模块发送的输入的密码;密码转换模块将输入的密码进行转换,得到叠加图形;密码认证模块接收到叠加图形与对比图形进行匹配,当两者完全吻合,则认证成功;通过图形叠加加密,提高密码的复杂度,避免现有的无线网破解软件,通过无线次实现进行破解。

[0050] 以上内容仅仅是对本发明结构所作的举例和说明,所属本技术领域的技术人员对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代,只要不偏离发明的结构或者超越本权利要求书所定义的范围,均应属于本发明的保护范围。

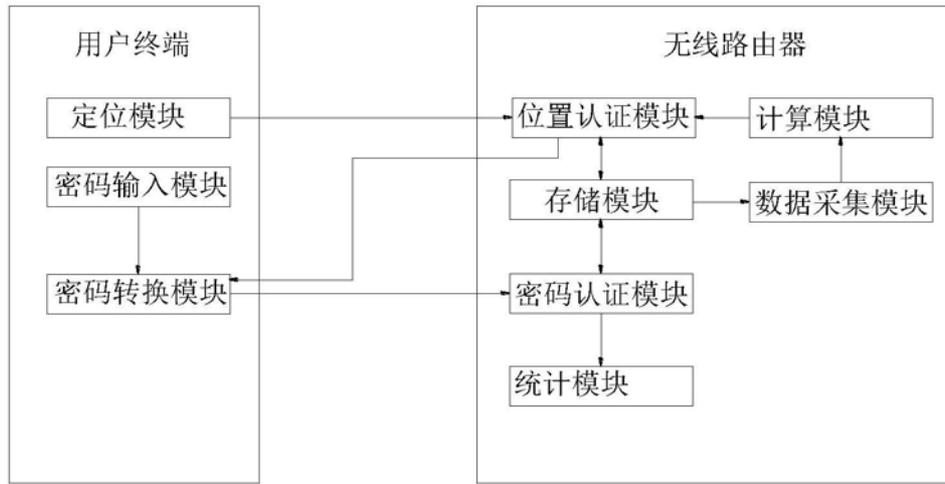


图1