



(12) 发明专利

(10) 授权公告号 CN 101488855 B

(45) 授权公告日 2011.06.01

(21) 申请号 200810032727.2

WO 2004/015540 A2, 2004.02.19, 全文.

(22) 申请日 2008.01.16

CN 1672384 A, 2005.09.21, 全文.

(73) 专利权人 上海摩波彼克半导体有限公司

CN 1454371 A, 2003.11.05, 全文.

地址 201203 上海市张江高科园区晨晖路
377 弄 42 号

CN 101047497 A, 2007.10.03, 全文.

审查员 陈文静

(72) 发明人 于非 张霞 杨金峰 张鑫 宁涛

(74) 专利代理机构 上海智信专利代理有限公司

31002

代理人 王洁

(51) Int. Cl.

H04L 9/32(2009.01)

H04W 12/06(2009.01)

(56) 对比文件

WO 03/096260 A2, 2003.11.20, 全文.

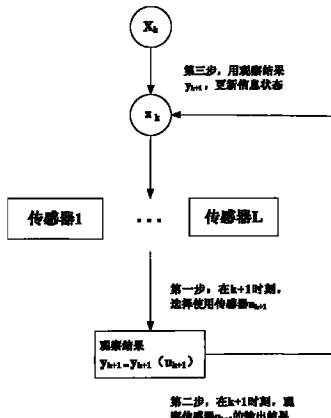
权利要求书 3 页 说明书 13 页 附图 2 页

(54) 发明名称

无线网络中移动设备实现持续鉴权联合入侵检测的方法

(57) 摘要

本发明涉及一种无线网络中移动设备实现持续鉴权联合入侵检测的方法，包括建立马尔可夫决策过程模型并确定信息状态空间和离散时间点的信息状态、建立累积成本模型并根据系统资源约束调度策略进行约束调度、根据安全需求限制条件计算出信息状态与最佳生物特征鉴权功能模块间对应关系、基于历史信息得到最佳生物特征鉴权功能模块并调度下一次鉴权、观测下一个时间点输出信息、更新信息状态并判断鉴权的结果。采用该种无线网络中移动设备实现持续鉴权联合入侵检测的方法，性能最优化，极大提高了移动设备安全性，满足对安全性要求很高的用户需求，节约了系统资源和运营成本，工作性能稳定可靠，适用范围广，为信息安全技术进一步发展奠定了坚实基础。



1. 一种无线网络中移动设备实现持续鉴权联合入侵检测的方法,包括设置于移动设备上的数个生物特征鉴权功能模块,其特征在于,所述的方法包括以下步骤:

(1) 根据持续鉴权过程建立部分可观马尔可夫决策过程系统模型,并确定该系统模型的信息状态空间以及系统在各个离散时间点的信息状态;

(2) 建立系统累积成本模型,并根据系统资源约束调度策略对系统累积成本模型进行约束调度处理;

(3) 根据系统的安全需求限制条件计算出各个信息状态与最佳的生物特征鉴权功能模块之间的对应关系;

(4) 基于历史信息得到最佳的生物特征鉴权功能模块,并在下一次的鉴权过程中使用本次确定的生物特征鉴权功能模块;

(5) 观测下一个时间点最佳的生物特征鉴权功能模块的输出信息;

(6) 通过最新的观测到的输出信息来更新系统当前的信息状态,并根据该信息状态判断鉴权的结果;

(7) 重复上述步骤(4)。

2. 根据权利要求1所述的无线网络中移动设备实现持续鉴权联合入侵检测的方法,其特征在于,所述的确定该系统模型的信息状态空间以及系统在各个离散时间点的信息状态,包括以下步骤:

(11) 根据以下公式确定该系统模型的信息状态 π_k :

$$\pi_k(i) = P(X_k = e_i | Y(k)), i = 1, 2, \dots, S,$$

$$1' s \pi = 1, 0 \leqslant \pi(i) \leqslant 1$$

其中, k 为时间点, X_k 为在时间点 k 的移动设备状态, $\{e_1, e_2, \dots, e_S\}$ 为状态空间, S 为状态总数, e_i 为状态空间中在第 i 的位置为 1、其余的位置为 0 的单一的向量, $Y(k)$ 为在时间点 k 获得的信息, $Y(k) = \{u_1, u_2, \dots, u_k, y_1, y_2, \dots, y_k\}$, u_k 为时间点 k 所选择的生物特征鉴权功能模块, $u_k \in \{1, 2, \dots, L\}$, y_k 为对生物特征鉴权功能模块 u_k 的观测结果, 1_s 为状态空间的一维向量, $1' s$ 为它的转置向量;

(12) 根据以下公式建立系统模型的马尔可夫链:

$$\pi_{k+1} = \frac{B(u_{k+1}, y_{k+1}(u_{k+1}))A'\pi_k}{1'_s B(u_{k+1}, y_{k+1}(u_{k+1}))A'\pi_k},$$

其中, B 为观测结果矩阵, $B(u_k, 0_m(u_k)) = \text{diag}[b_1(u_k, 0_m(u_k)), \dots, b_s(u_k, 0_m(u_k))]$, diag 表示对角矩阵, $b_i(u_k = 1, y_k = 0_m(1)) = P(y_k(u_k) = 0_m(u_k) | X_k = e_i, u_k = 1)$, $i = 1, 2, \dots, S$, $b_i(u_k = 1, y_k = 0_m(1))$ 为系统状态处于 e_i 在时间点 k 从所选择的第 1 个生物特征鉴权功能模块观测到结果为 m 的概率, 第 1 个生物特征鉴权功能模块观测到的结果属于有限的符号集合 $\{O_1(l), O_2(l), \dots, O_{M_l}(l)\}$, 其中 $|M_l|$ 为第 1 个生物特征鉴权功能模块可能观测到的结果的数量; A 为状态转置矩阵, $A = [a_{ij}]_{S \times S}$, 这里 $a_{ij} = P(X_k = e_j | X_{k-1} = e_i)$, $i, j \in \{1, \dots, S\}$;

且 $\pi_0 = [\pi_0(i)]_{S \times 1}$, 这里 $\pi_0(i) = P(X_0 = i)$, $i \in \{1, \dots, S\}$;

(13) 根据马尔可夫链得到各个离散时间点的信息状态,从而得到整个系统模型的信息状态空间。

3. 根据权利要求2所述的无线网络中移动设备实现持续鉴权联合入侵检测的方法,其

特征在于，所述的系统累积成本模型为：

$$J_k(\pi) = \min_{u_{k+1} \in \{1, \dots, L\}} [C_k(\pi, u_{k+1}) + \sum_{m=1}^{M_{u_{k+1}}} J_{k+1} \left(\frac{B(u_{k+1}, O_m(u_{k+1})) A' \pi}{1'_S B(u_{k+1}, O_m(u_{k+1})) A' \pi} \right) \times 1'_S B(u_{k+1}, O_m(u_{k+1})) A' \pi]$$

其中， $\pi \in P$, P 为信息状态的集合。

4. 根据权利要求 3 所述的无线网络中移动设备实现持续鉴权联合入侵检测的方法，其特征在于，所述的根据系统资源约束调度策略对系统累积成本模型进行约束调度处理，包括以下步骤：

(21) 根据以下公式确定转移概率矩阵 \bar{A} ：

$$\bar{A} = A \otimes Q,$$

其中， \otimes 为张量运算符，即克罗内积运算符， $z_k = Q' (u_k) z_{k-1}$, $z_0 = e_1$, $z_N = e_{N+1}$, z_k

为第 1 个生物特征鉴权功能模块所使用的次数， Q 为 $Q(u_k=1) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$, 且

$Q(u_k) = I_{(N_1+1) \times (N_1+1)}$, 如果 $u_k \neq 1$, I 是单位矩阵, Q' 为 Q 的转置矩阵；

(22) 根据以下公式确定系统扩展的马尔可夫链 (X_k, z_k) 的信息状态 $\bar{\pi}$ ：

$$\bar{\pi} = \pi_k \otimes z_k,$$

(23) 根据以下公式确定可观概率矩阵 \bar{B} ：

$$\bar{B}(u, O_m(u)) = B(u, O_m(u)) \otimes I_{N+1};$$

(24) 根据以下公式确定值函数 \bar{J}_k ：

$$\bar{J}_k = J_k(\pi, z), \bar{\pi} = \pi \otimes z;$$

(25) 在所述的系统累积成本模型中，用 \bar{J}_k 取代 J_k ，用 \bar{A} 替换 A , \bar{B} 替换 B 。

5. 根据权利要求 4 所述的无线网络中移动设备实现持续鉴权联合入侵检测的方法，其特征在于，所述的根据系统的安全需求限制条件计算出各个信息状态与最佳的生物特征鉴权功能模块之间的对应关系，包括以下步骤：

(31) 根据分段理论，将系统累积成本模型根据以下公式表示为有限的向量集合：

$$J_k(\pi) = \min_{i \in \Gamma_k} \gamma_{i,k}^*(u_{i,k}^*) \pi, \text{ 对所有 } \pi \in P;$$

其中， Γ_k 为一个有限的 S 维向量 $\gamma_{i,k}^*$ 的集合， $u_{i,k}^*$ 为最佳的生物特征鉴权功能模块；

(32) 根据全部生物特征鉴权功能模块的集合 ζ , 使用离线动态规划和部分可观马尔可夫决策过程算法计算出所对应的向量 $\gamma_{k,i}^\zeta$ 和相关的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$ ；

(33) 根据未受约束的生物特征鉴权功能模块的集合 $\zeta_{\bar{c}}$, 使用离线动态规划和部分可观马尔可夫决策过程算法计算出所对应的向量 $\gamma_{k,i}^{\zeta_{\bar{c}}}$ 和相关的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_{\bar{c}},*}$ ；

(34) 使用动态规划和部分可观马尔可夫决策过程算法计算出所有的信息状态 π 所对应的向量 $\gamma_{k,i}^\zeta$ 和 $\gamma_{k,i}^{\zeta_{\bar{c}}}$ ；

(35) 根据每个向量 $\gamma_{k,i}^\zeta$ 所对应的最佳的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$, 得到所有的信息

状态 π 与最佳的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$ 之间的对应关系，并根据每个向量 $\gamma_{k,i}^{\zeta_e}$ 所对应的最佳的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_e,*}$ ，得到所有的信息状态 π 与最佳的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_e,*}$ 之间的对应关系。

6. 根据权利要求 5 所述的无线网络中移动设备实现持续鉴权联合入侵检测的方法，其特征在于，所述的基于历史信息得到最优的生物特征鉴权功能模块，包括以下步骤：

(41) 根据以下公式确定安全需求限制条件的估计误差二次约束方程：

$$\sum_{m=1}^{M_u} a_{k+1}(l) \left(1 - \frac{\pi' A B^2(u, O_m(u))}{((1-1)B(u, O_m(u))A'\pi)^2} \right) \times ((1-1)B(u, O_m(u))A'\pi) < K_l, \quad l \in \zeta_c,$$

其中， ζ_c 为受约束的生物特征鉴权功能模块的集合，且 $\zeta = \{1, \dots, L\} = \{\zeta_c \cup \zeta_{\bar{c}}\}$ ；

(42) 如果系统模型的当前信息状态 $\pi(k)$ 满足以上的约束方程，则通过各个信息状态与最佳的生物特征鉴权功能模块之间的对应关系，根据系统模型的当前信息状态 $\pi(k)$ 得到对应的最优的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$ ；

(43) 如果系统模型的当前信息状态 $\pi(k)$ 不满足以上的约束方程，则通过各个信息状态与最佳的未受约束的生物特征鉴权功能模块之间的对应关系，根据系统模型的当前信息状态 $\pi(k)$ 得到对应的最优的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_e,*}$ 。

7. 根据权利要求 1 至 6 中任一项所述的无线网络中移动设备实现持续鉴权联合入侵检测的方法，其特征在于，所述的生物特征鉴权功能模块为生物传感器。

无线网络中移动设备实现持续鉴权联合入侵检测的方法

技术领域

[0001] 本发明涉及移动通信系统信息安全领域,特别涉及移动通信系统中移动设备信息安全管理技术领域,具体是指一种无线网络中移动设备实现持续鉴权联合入侵检测的方法。

背景技术

[0002] 鉴权是用来识别用户身份的,可以使用一种或多种识别方式:例如密码,令牌,以及用户的生物特征,生物特征又分为静态生物特征和动态生物特征,例如指纹,视网膜等属于静态生物特征,而脸部表情,肢体动作等属于动态生物特征。密码鉴权是比较简单的并且很容易使用,由于密码和用户本身之间没有直接的关联,所以不能确定输入密码者就是用户本身。令牌也是一样的道理。另外这两种识别方式比较容易丢失以及被破译。生物特征是唯一的用户和输入者有直接关联的识别方式。在通常的通信系统中,不管是网络对移动设备进行的鉴权,还是移动设备对用户进行的鉴权目前使用最为广泛的还是密码鉴权,也有些对安全性要求高的高端的移动设备也已经使用生物特征进行鉴权。

[0003] 由于生物特征与被鉴别的用户具有最直接的联系,所以是最能够证明用户身份的。但是每个生物特征又有自己的长处和缺点。由于应用环境的不同,所以也不能确定哪种生物特征被用来识别身份是最好的。单一模式的生物特征必须面对许多挑战,比如在遥感数据中的噪音,类型本身的变化,类型之间的相识性等等。这种问题可以使用多种生物特征融合技术。多种生物特征融合技术提供了最可靠的识别方式。在一定的环境中可以利用某个单一生物特征的优点来补偿另外一个生物特征的缺点。另外,还可以随机的选择用户提供的生物特征集中的子集来更好的保证安全性。

[0004] 随着多生物特征融合技术的使用越来越广泛,这种技术也在不断的提高。目前这种技术的运行方式主要有串行模式,并口模式,层次模式。在串行运行模式中,一个生物特征的输出只能用一次。因此在同一时刻不需要多种生物特征,而且可以在所有的生物特征被接收到之前就能够决定使用哪个生物特征。在并口运行模式中,在同一时刻需要多种生物特征。多层次运行模式适合使用很多生物特征识别来识别的系统。

[0005] 目前大部分的移动设备对用户的识别都是在用户进入到移动设备时进行一次鉴权,如果 用户进入到移动设备之后就认为此后的时间里面都是安全的。但是有时候这样的保护还是不够的,移动设备中有很重要的资料或是隐私,而又忘记关闭移动设备。比如国家安全部局工作人员使用的移动设备,移动设备中存储了等等对安全性要求很高的用户。从而需要相应的持续鉴权以及持续鉴权的算法,这样才能够满足这种对安全性要求很高的用户的需求。

[0006] 只进行持续鉴权的系统中由于各种各样的原因总是存在有不少缺点,它不能消除入侵。为了解决这个问题,入侵检测系统被用作第二层保护墙,它能够有效的帮助鉴别恶意的行为。入侵检测持续的或者周期性主动监控系统,用保存的正常外形或攻击信令比较它们,然后发起合适的响应。重新鉴权是被入侵检测系统发起的一个重要的响应类型。重新

鉴权过程后,只有一个可信的用户能够继续使用该资源设备,而危及安全的用户将被排斥在外。

[0007] 一个持续的或周期性的监控目前主动的行为,用存储的正常的配置或攻击的签名来比较他们,并发动适当的响应。基本上,入侵检测系统能够被分为基于网络的和基于主机的。基于主机的入侵检测系统,它依靠位于主机中的用户或程序产生的数据,适合无线终端设备。

[0008] 交叉错误率 (CER) 常常用于提供一个入侵检测系统的测量基线,它的描述请参阅图1所示。其中,假的正比率 (FPR) 是入侵报告恶意行为的错误的频率,而假的负比率 (FNR) 是当恶意行为发生时,入侵没有能上升到一个警告的频率。选择的 FPR 和 FNR 的值依据的是系统的安全性的要求。在图一中,我们能看出它是一个合理地模仿一个入侵作为噪声传感器,它能够检测系统安全的状态 (安全或威胁)。噪声传感器的准确性依靠于入侵的 FPR 和 FNR 的值。

[0009] 尽管对于持续鉴权和入侵检测已经做了很多研究工作,但是在之前的研究工作中都是分别研究的,并且无法结合并应用于无线终端设备中,并且两者各自的信息无法实现彼此共享,这样这两个过程就无法联合起来从而不能获得更好的有效性。

发明内容

[0010] 本发明的目的是克服了上述现有技术中的缺点,提供一种能够满足用户的高安全性要求、最大限度的节约系统资源、工作性能稳定可靠、适用范围较为广泛的无线网络中移动设备实现持续鉴权联合入侵检测的方法。

[0011] 为了实现上述的目的,本发明的无线网络中移动设备实现持续鉴权联合入侵检测的方法如下:

[0012] 该无线网络中移动设备实现持续鉴权联合入侵检测的方法,包括设置于移动设备上的数个生物特征鉴权功能模块,其主要特点是,所述的方法包括以下步骤:

[0013] (1) 根据持续鉴权过程建立部分可观马尔可夫决策过程系统模型,并确定该系统模型的信息状态空间以及系统在各个离散时间点的信息状态;

[0014] (2) 建立系统累积成本模型,并根据系统资源约束调度策略对系统累积成本模型进行约束调度处理;

[0015] (3) 根据系统的安全需求限制条件计算出各个信息状态与最佳的生物特征鉴权功能模块之间的对应关系;

[0016] (4) 基于历史信息得到最佳的生物特征鉴权功能模块,并在下一次的鉴权过程中使用本次确定的生物特征鉴权功能模块;

[0017] (5) 观测下一个时间点最佳的生物特征鉴权功能模块的输出信息;

[0018] (6) 通过最新的观测到的输出信息来更新系统当前的信息状态,并根据该信息状态判断鉴权的结果;

[0019] (7) 重复上述步骤(4)。

[0020] 该无线网络中移动设备实现持续鉴权联合入侵检测的方法中的确定该系统模型的信息状态空间以及系统在各个离散时间点的信息状态,包括以下步骤:

[0021] (11) 根据以下公式确定该系统模型的信息状态 π_k :

[0022] $\pi_k(i) = P(X_k = e_i | Y(k))$, $i = 1, 2, \dots, S$,

[0023] $1_S' \cdot \pi = 1$, $0 \leq \pi(i) \leq 1$

[0024] 其中, k 为时间点, X_k 为在时间点 k 的移动设备状态, $\{e_1, e_2, \dots, e_S\}$ 为状态空间, S 为状态总数, e_i 为状态空间中在第 i 的位置为 1、其余的位置为 0 的单一的向量, $Y(k)$ 为在时间点 k 获得的信息, $Y(k) = \{u_1, u_2, \dots, u_k, y_1, y_2, \dots, y_k\}$, u_k 为时间点 k 所选择的生物特征鉴权功能模块, $u_k \in \{1, 2, \dots, L\}$, y_k 为对生物特征鉴权功能模块 u_k 的观测结果, 1_S 为状态空间的一维向量, $1_S'$ 为它的转置向量;

[0025] (12) 根据以下公式建立系统模型的马尔可夫链:

$$[0026] \pi_{k+1} = \frac{B(u_{k+1}, y_{k+1}(u_{k+1})) A' \pi_k}{1_S' B(u_{k+1}, y_{k+1}(u_{k+1})) A' \pi_k},$$

[0027] 其中, B 为观测结果矩阵, $B(u_k, O_m(u_k)) = \text{diag}[b_1(u_k, O_m(u_k)), \dots, b_S(u_k, O_m(u_k))]$, diag 表示对角矩阵, $b_i(u_k = 1, y_k = O_m(1)) = P(y_k(u_k) = O_m(u_k) | X_k = e_i, u_k = 1)$, $i = 1, 2, \dots, S$, $b_i(u_k = 1, y_k = O_m(1))$ 为系统状态处于 e_i 在时间点 k 从所选择的第 1 个生物特征鉴权功能模块观测到结果为 m 的概率, 第 1 个生物特征鉴权功能模块观测到的结果属于有限的符号集合 $\{O_1(1), O_2(1), \dots, O_{M_1}(1)\}$, 其中 $|M_1|$ 为第 1 个生物特征鉴权功能模块可能观测到的结果的数量; A 为状态转置矩阵, $A = [a_{ij}]_{S \times S}$, 这里 $a_{ij} = P(X_k = e_j | X_{k-1} = e_i)$, $i, j \in \{1, \dots, S\}$;

[0028] 且 $\pi_0 = [\pi_0(i)]_{S \times 1}$, 这里 $\pi_0(i) = P(X_0 = i)$, $i \in \{1, \dots, S\}$;

[0029] (13) 根据马尔可夫链得到各个离散时间点的信息状态, 从而得到整个系统模型的信息状态空间。

[0030] 该无线网络中移动设备实现持续鉴权联合入侵检测的方法中的系统累积成本模型为:

[0031]

$$J_k(\pi) = \min_{u_{k+1} \in \{1, \dots, L\}} [C_k(\pi, u_{k+1}) + \sum_{m=1}^{M_{u_{k+1}}} J_{k+1} \left(\frac{B(u_{k+1}, O_m(u_{k+1})) A' \pi}{1_S' B(u_{k+1}, O_m(u_{k+1})) A' \pi} \right) \times 1_S' B(u_{k+1}, O_m(u_{k+1})) A' \pi]$$

[0032] 其中, $\pi \in P$, P 为信息状态的集合。

[0033] 该无线网络中移动设备实现持续鉴权联合入侵检测的方法中的根据系统资源约束调度策略对系统累积成本模型进行约束调度处理, 包括以下步骤:

[0034] (21) 根据以下公式确定转移概率矩阵 \bar{A} :

$$[0035] \bar{A} = A \otimes Q,$$

[0036] 其中, \otimes 为张量运算符, 即克罗内积运算符, $z_k = Q' \cdot (u_k) z_{k-1}$, $z_0 = e_1$, $z_N = e_{N+1}$,

z_k 为第 1 个生物特征鉴权功能模块所使用的次数, Q 为 $Q(u_k = 1) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$, 且

$Q(u_k) = I_{(N_1+1) \times (N_1+1)}$, 如果 $u_k \neq 1$, I 是单位矩阵, Q' 为 Q 的转置矩阵;

[0037] (22) 根据以下公式确定系统扩展的马尔可夫链 (X_k, z_k) 的信息状态 $\bar{\pi}$:

$$[0038] \bar{\pi} = \pi_k \otimes z_k,$$

[0039] (23) 根据以下公式确定可观概率矩阵 \bar{B} :

$$[\text{0040}] \quad \bar{B}(u, O_m(u)) = B(u, O_m(u)) \otimes I_{N+1};$$

[0041] (24) 根据以下公式确定值函数 \bar{J}_k :

$$[\text{0042}] \quad \bar{J}_k = J_k(\pi, z), \quad \bar{\pi} = \pi \otimes z;$$

[0043] (25) 在所述的系统累积成本模型中, 用 \bar{J}_k 取代 J_k , 用 \bar{A} 替换 A , \bar{B} 替换 B 。

[0044] 该无线网络中移动设备实现持续鉴权联合入侵检测的方法中的根据系统的安全需求限制条件计算出各个信息状态与最佳的生物特征鉴权功能模块之间的对应关系, 包括以下步骤 :

[0045] (31) 根据分段理论, 将系统累积成本模型根据以下公式表示为有限的向量集合 :

$$[\text{0046}] \quad J_k(\pi) = \min_{i \in \Gamma_k} \gamma_{i,k}^{*,'}(u_{i,k}^*)\pi, \text{ 对所有 } \pi \in P;$$

[0047] 其中, Γ_k 为一个有限的 S 维向量 $\gamma_{i,k}^{*,'}$ 的集合, $u_{i,k}^*$ 为最佳的生物特征鉴权功能模块 ;

[0048] (32) 根据全部生物特征鉴权功能模块的集合 ζ , 使用离线动态规划和部分可观马尔可夫决策过程算法计算出所对应的向量 $\gamma_{k,i}^{\zeta}$ 和相关的生物特征鉴权功能模块 $u_{k,i}^{\zeta}$;

[0049] (33) 根据未受约束的生物特征鉴权功能模块的集合 ζ_c , 使用离线动态规划和部分可观马尔可夫决策过程算法计算出所对应的向量 $\gamma_{k,i}^{\zeta_c}$ 和相关的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_c,*}$;

[0050] (34) 使用动态规划和部分可观马尔可夫决策过程算法计算出所有的信息状态 π 所对应的向量 $\gamma_{k,i}^{\zeta}$ 和 $\gamma_{k,i}^{\zeta_c}$;

[0051] (35) 根据每个向量 $\gamma_{k,i}^{\zeta}$ 所对应的最佳的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$, 得到所有的信息状态 π 与最佳的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$ 之间的对应关系, 并根据每个向量 $\gamma_{k,i}^{\zeta_c}$ 所对应的最佳的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_c,*}$, 得到所有的信息状态 π 与最佳的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_c,*}$ 之间的对应关系。

[0052] 该无线网络中移动设备实现持续鉴权联合入侵检测的方法中的基于历史信息得到最优的生物特征鉴权功能模块, 包括以下步骤 :

[0053] (41) 根据以下公式确定安全需求限制条件的估计误差二次约束方程 :

$$[\text{0054}] \quad \sum_{m=1}^{M_u} a_{k+1}(l) \left(1 - \frac{\pi' A B^2(u, O_m(u))}{((1-1)B(u, O_m(u))A'\pi)^2} \right) \times ((1-1)B(u, O_m(u))A'\pi) < K_l, \quad l \in \zeta_c,$$

[0055] 其中, ζ_c 为受约束的生物特征鉴权功能模块的集合, 且 $\zeta = \{1, \dots, L\} = \{\zeta_c \cup \zeta_c\}$;

[0056] (42) 如果系统模型的当前信息状态 $\pi(k)$ 满足以上的约束方程, 则通过各个信息状态与最佳的生物特征鉴权功能模块之间的对应关系, 根据系统模型的当前信息状态 $\pi(k)$ 得到对应的最优的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$;

[0057] (43) 如果系统模型的当前信息状态 $\pi(k)$ 不满足以上的约束方程, 则通过各个信

息状态与最佳的未受约束的生物特征鉴权功能模块之间的对应关系,根据系统模型的当前信息状态 $\pi(k)$ 得到对应的最优的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_e,*}$ 。

[0058] 该无线网络中移动设备实现持续鉴权联合入侵检测的方法中的生物特征鉴权功能模块为生物传感器。

[0059] 采用了该发明的无线网络中移动设备实现持续鉴权联合入侵检测的方法,由于其主要基于生物特征的持续鉴权,因此无线网络中的持续鉴权可以表示为生物传感器的选择问题,通过把持续鉴权问题建立为一个部分客观的马尔可夫决策过程模型,并将入侵检测和响应系统一起共同起作用,重新鉴权是一个重要的响应类型,这是被入侵发起的,在重新鉴权过程后,只有一个可信的用户能够继续使用网络资源,同时危及安全的用户将被排除出网络,将该系统建立为一个部分客观的马尔可夫决策过程模型,并且使用动态规划的隐形马尔可夫模型调度算法来获得最佳的调度策略,决定是否要选择生物传感器,以及选择何种生物传感器,以使得系统的性能最优化,从而获得最佳的持续鉴权策略,不仅可以极大的提高移动设备的安全性,满足对移动设备安全性要求很高的用户需求,而且能最佳的控制是否执行重新鉴权,以及选择哪个生物传感器进行鉴权,从而最低限度的使用系统资源;同时能最佳的控制是否激活入侵检测系统,从而最低限度的使用系统资源;而且入侵检测系统和持续鉴权能够相互共享彼此的信息,系统安全性要求的限制和资源的限制能够被保证,节约了系统运营的成本;同时本方法的工作性能稳定可靠,适用范围较为广泛,为无线网络中移动设备的信息安全技术的进一步发展奠定了坚实的基础。

附图说明

[0060] 图 1 为现有技术中入侵检测系统的交叉错误率示意图。

[0061] 图 2 为本发明的隐形马尔可夫决策过程中生物传感器的调度和信息状态更新示意图。

具体实施方式

[0062] 为了能够更清楚地理解本发明的技术内容,特举以下实施例详细说明。

[0063] 请参阅图 2 所示,该无线网络中移动设备实现持续鉴权联合入侵检测的方法,包括设置于移动设备上的数个生物特征鉴权功能模块,该生物特征鉴权功能模块可以为生物传感器,当然也可以采用其它具有生物特征采集和鉴权功能的装置,其中,所述的方法包括以下步骤:

[0064] (1) 根据持续鉴权过程建立部分可观马尔可夫决策过程系统模型,并确定该系统模型的信息状态空间以及系统在各个离散时间点的信息状态,包括以下步骤:

[0065] (a) 根据以下公式确定该系统模型的信息状态 π_k :

[0066] $\pi_k(i) = P(X_k = e_i | Y(k))$, $i = 1, 2, \dots, S$,

[0067] $1_S' \pi = 1, 0 \leqslant \pi(i) \leqslant 1$

[0068] 其中, k 为时间点, X_k 为在时间点 k 的移动设备状态, $\{e_1, e_2, \dots, e_S\}$ 为状态空间, S 为状态总数, e_i 为状态空间中在第 i 的位置为 1、其余的位置为 0 的单一的向量, $Y(k)$ 为在时间点 k 获得的信息, $Y(k) = \{u_1, u_2, \dots, u_k, y_1, y_2, \dots, y_k\}$, u_k 为时间点 k 所选择的生物特征鉴权功能模块, $u_k \in \{1, 2, \dots, L\}$, y_k 为对生物特征鉴权功能模块 u_k 的观测结果, $1_S'$

为状态空间的一维向量, $1_s'$ 为它的转置向量;

[0069] (b) 根据以下公式建立系统模型的马尔可夫链:

$$[0070] \pi_{k+1} = \frac{B(u_{k+1}, y_{k+1}(u_{k+1})) A' \pi_k}{1_S' B(u_{k+1}, y_{k+1}(u_{k+1})) A' \pi_k},$$

[0071] 其中, B 为观测结果矩阵, $B(u_k, O_m(u_k)) = \text{diag}[b_1(u_k, O_m(u_k)), \dots, b_s(u_k, O_m(u_k))]$, diag 表示对角矩阵, $b_i(u_k = 1, y_k = O_m(1)) = P(y_k(u_k) = O_m(u_k) | X_k = e_i, u_k = 1)$, $i = 1, 2, \dots, s$, 为系统状态处于 e_i 在时间点 k 从所选择的第 1 个生物特征鉴权功能模块观测到结果为 m 的概率, 第 1 个生物特征鉴权功能模块观测到的结果属于有限的符号集合 $\{O_1(1), O_2(1), \dots, O_M(1)\}$, 其中 $|M_1|$ 为第 1 个生物特征鉴权功能模块可能观测到的结果的数量; A 为状态转置矩阵, $A = [a_{ij}]_{s \times s}$, 这里 $a_{ij} = P(X_k = e_j | X_{k-1} = e_i)$, $i, j \in \{1, \dots, s\}$; 且 $\pi_0 = [\pi_0(i)]_{s \times 1}$, 这里 $\pi_0(i) = P(X_0 = i)$, $i \in \{1, \dots, s\}$;

[0072] (c) 根据马尔可夫链得到各个离散时间点的信息状态, 从而得到整个系统模型的信息状态空间;

[0073] (2) 建立系统累积成本模型, 并根据系统资源约束调度策略对系统累计成本模型进行约束调度处理; 该系统累积成本模型为:

[0074]

$$J_k(\pi) = \min_{u_{k+1} \in \{1, \dots, L\}} [C_k(\pi, u_{k+1}) + \sum_{m=1}^{M_{u_{k+1}}} J_{k+1} \left(\frac{B(u_{k+1}, O_m(u_{k+1})) A' \pi}{1_S' B(u_{k+1}, O_m(u_{k+1})) A' \pi} \right) \times 1_S' B(u_{k+1}, O_m(u_{k+1})) A' \pi]$$

[0075] 其中, $\pi \in P$, P 为信息状态的集合;

[0076] 所述的根据系统资源约束调度策略对系统累计成本模型进行约束调度处理, 包括以下步骤:

[0077] (a) 根据以下公式确定转移概率矩阵 \bar{A} :

$$[0078] \bar{A} = A \otimes Q,$$

[0079] 其中, $_$ 为张量运算符, 即克罗内积运算符, $z_k = Q'(u_k) z_{k-1}$, $z_0 = e_1$, $z_N = e_{N+1}$,

z_k 为第 1 个生物特征鉴权功能模块所使用的次数, Q 为 $Q(u_k = 1) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$, 且

$Q(u_k) = I_{(N_1+1) \times (N_1+1)}$, 如果 $u_k \neq 1$, I 是单位矩阵, Q' 为 Q 的转置矩阵;

[0080] (b) 根据以下公式确定系统扩展的马尔可夫链 (X_k, z_k) 的信息状态 $\bar{\pi}$:

$$[0081] \bar{\pi} = \pi_k \otimes z_k,$$

[0082] (c) 根据以下公式确定可观概率矩阵 \bar{B} :

$$[0083] \bar{B}(u, O_m(u)) = B(u, O_m(u)) \otimes I_{N+1};$$

[0084] (d) 根据以下公式确定值函数 \bar{J}_k :

$$[0085] \bar{J}_k = J_k(\pi, z), \bar{\pi} = \pi \otimes z;$$

[0086] (e) 在所述的系统累积成本模型中, 用 \bar{J}_k 取代 J_k , 用 \bar{A} 替换 A , \bar{B} 替换 B ;

[0087] (3) 根据系统的安全需求限制条件计算出各个信息状态与最佳的生物特征鉴权功能模块之间的对应关系; 包括以下步骤:

- [0088] (a) 根据分段理论,将系统累积成本模型根据以下公式表示为有限的向量集合 :
- [0089] $J_k(\pi) = \min_{i \in \Gamma_k} \gamma_{i,k}^{*,'}(u_{i,k}^*)\pi$, 对所有 $\pi \in P$; 对所有 $\pi \in P$;
- [0090] 其中, Γ_k 为一个有限的 S 维向量 $y_{i,k}^{*,*}$ 的集合, $u_{i,k}^*$ 为最佳的生物特征鉴权功能模块;
- [0091] (b) 根据全部生物特征鉴权功能模块的集合 ζ , 使用离线动态规划和部分可观马尔可夫决策过程算法计算出所对应的向量 $y_{k,i}^{\zeta}$ 和相关的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$;
- [0092] (c) 根据未受约束的生物特征鉴权功能模块的集合 ζ_c , 使用离线动态规划和部分可观马尔可夫决策过程算法计算出所对应的向量 $y_{k,i}^{\zeta_c}$ 和相关的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_c,*}$;
- [0093] (d) 使用动态规划和部分可观马尔可夫决策过程算法计算出所有的信息状态 π 所对应的向量 $y_{k,i}^{\zeta}$ 和 $y_{k,i}^{\zeta_c}$;
- [0094] (e) 根据每个向量 $y_{k,i}^{\zeta}$ 所对应的最佳的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$, 得到所有的信息状态 π 与最佳的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$ 之间的对应关系, 并根据每个向量 $y_{k,i}^{\zeta_c}$ 所对应的最佳的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_c,*}$, 得到所有的信息状态 π 与最佳的未受约束的生物特征鉴权功能模块 $u_{k,i}^{\zeta_c,*}$ 之间的对应关系;
- [0095] (4) 基于历史信息得到最佳的生物特征鉴权功能模块, 并在下一次的鉴权过程中使用本次确定的生物特征鉴权功能模块; 该基于历史信息得到最优的生物特征鉴权功能模块, 包括以下步骤:
- [0096] (a) 根据以下公式确定安全需求限制条件的估计误差二次约束方程:
- [0097]
$$\sum_{m=1}^{M_u} a_{k+1}(l) \left(1 - \frac{\pi' A B^2(u, O_m(u))}{((1-1)B(u, O_m(u))A'\pi)^2} \right) \times (1-1)B(u, O_m(u))A'\pi < K_l, \quad l \in \zeta_c,$$
- [0098] 其中, ζ_c 为受约束的生物特征鉴权功能模块的集合, 且 $\zeta = \{1, \dots, L\} = \{\zeta_c \cup \zeta_c\}$;
- [0099] (b) 如果系统模型的当前信息状态 $\pi(k)$ 满足以上的约束方程, 则通过各个信息状态与最佳的生物特征鉴权功能模块之间的对应关系, 根据系统模型的当前信息状态 $\pi(k)$ 得到对应的最优的生物特征鉴权功能模块 $u_{k,i}^{\zeta,*}$;
- [0100] (c) 如果系统模型的当前信息状态 $\pi(k)$ 不满足以上的约束方程, 则通过各个信息状态与最佳的未受约束的生物特征鉴权功能模块之间的对应关系, 根据系统模型的当前信息状态 $\pi(k)$ 得到对应的最优的未受约束的生物特征鉴权功能模块 $u_{k,j}^{\zeta_c,*}$;
- [0101] (5) 观测下一个时间点最佳的生物特征鉴权功能模块的输出信息;
- [0102] (6) 通过最新的观测到的输出信息来更新系统当前的信息状态, 并根据该信息状态判断鉴权的结果;
- [0103] (7) 重复上述步骤 (4)。
- [0104] 在实际应用当中, 本发明的方法涉及到移动设备的安全性管理领域, 应用基于多模型人体生物特征的持续鉴权作为移动设备对用户验证的第一道屏障, 应用入侵检测作为第二层防护。这两种方法是相互补充的。

[0105] 首先建立本发明方法的系统模型：

[0106] 该系统能够被建模为一个时间离散的，两个状态（安全和危险）的一阶马尔可夫链 $\{X_k\}$ ，其中 k 表示离散时间点。时间轴划分为时间长度相等的时间间隔，这个时间间隔就是两个操作之间的时间。系统的操作包括入侵检测和鉴权。时隙的长度取决于安全需求和系统环境。例如，如果系统用于极不安全的环境中，时间间隔将被划分的比在用于安全环境中更短，在那个时间的系统状态是 X_k ，状态空间为 $\{e_1, e_2\}$ 。这里 e_i 表示二维单位向量，在第 i 的位置为 1，其余的位置为 0。 2×2 维的转移概率矩阵 A 被定义为：

[0107] $A = [a_{ij}] 2 \times 2$, 其中 $a_{ij} = P(X_k = e_j | X_{k-1} = e_i)$, $i, j \in \{1, 2\}$

[0108] 在这个模型中，如果一个入侵检测连续不断的监视系统，它将在所有的时间点被运行。同时，在每个时间点上，重新鉴权也可以被启动。但是，入侵和鉴权要消耗大量的系统资源，如电池功率，这是无线终端设备中一个重要的问题。因此，考虑到系统安全的需求和资源的限制，在每个时间点优化入侵检测和连续鉴权的调度是很值得的。

[0109] 假设连续鉴权系统有多个生物传感器，并能够收集多个生物特征。入侵检测和基于生物 特征的持续鉴权相结合的问题可以被抽象为二个状态的部分可观马尔可夫决策过程模型。在这个模型中，有数个传感器用于连续鉴权，也有若干个传感器用于入侵检测。系统中总计有 L 个传感器。为了简化上述描述，我们假设每个时间点上可以选择一个传感器（可以是重新鉴权也可以是入侵监测系统）。注意：它将直接概括为每个时间点抽取 \bar{L} 个传感器的模型（其中 $1 \leq \bar{L} \leq L$ ）。这样的话，入侵检测系统和重新鉴权能够同时运行。 $u_k \in \{1, \dots, L\}$ ，表示在时间点 k 选择的生物传感器，并且 $y_k(u_k)$ 表示该生物传感器的观察结果。第 1 个生物传感器观测到的结果属于一个有限的符号集合 $\{0_1(1), 0_2(1), \dots, 0_M(1)\}$ ， $|M_1|$ 表示第 1 个生物传感器可能观测到的结果的数量。当系统的状态是 e_i ，在时间点 k 选择的是第 1 个生物传感器，从第 1 个生物传感器观测结果为 m 的概率如下表示：

[0110] $b_i(u_k = 1, y_k = 0_m(1)) = P(y_k(u_k) = 0_m(u_k) | X_k = e_i, u_k = 1)$, $i = 1, 2$

[0111] 定义观测结果矩阵为：

[0112] $B(u_k, 0_m(u_k)) = \text{diag}[b_1(u_k, 0_m(u_k)), \dots, b_s(u_k, 0_m(u_k))] \quad \dots \dots (1)$

[0113] 这样，在马尔可夫链的给定的状态，时间点 k 选择生物传感器 u_k 观测结果为 m 的概率是可以得到的。从生物传感器中得到的观察结果可能是“安全的”，“危险的”，以及“不存在的”当没有传感器被使用时。入侵检测系统的观察结果矩阵可以表示为：

$$[0114] B(u_k = \text{ids}) = \begin{pmatrix} 1 - FPR & FPR \\ FNR & 1 - FNR \end{pmatrix} \quad \dots \dots (2)$$

[0115] 值得注意的是，系统的状态是不能直接被观察到，因此系统的状态为隐藏的马尔可夫模型。

[0116] 与生物传感器使用相关的成本有计算评估的能量消耗，以及错误的鉴权或入侵检测获得而造成的信息被窃等。

[0117] 下面将通过部分可观马尔可夫决策过程来解决持续鉴权问题。

[0118] 由于部分可观马尔可夫决策过程和相关的算法能够在每个时间点用于优化调度入侵检测和连续鉴权过程。使用这个理论，在最大限度的降低总的成本取决于系统安全需求和系统资源限制。

[0119] (1) 信息状态

[0120] 信息状态是部分可观马尔可夫决策过程中的一个重要的概念。因而把状态的概率分布当作一个信息状态并且把整个概率空间（一组所有可能的概率分布）当作信息空间。任何一个信息状态对历史的特征都是足够的，那就意味着基于一个信息状态就可以选择一个最佳的生物传感器（例如最佳操作，入侵检测或重新鉴权）。信息状态用 π_k 表示。其中 k 表示时间点。因为历史信息包括入侵检测和连续鉴权，这两个过程能够共享彼此的信息，所以系统能既够获得更好的有效性。

[0121] 在我们的移动系统中，有两个状态，元素 π_k 被定义为：

[0122] $\pi_k(i) = P(X_k = e_i | Y_k)$, $i = 1, 2$, $\pi_k(1) + \pi_k(2) = 1$, $0 \leq \pi_k(1), \pi_k(2) \leq 1$
..... (3)

[0123] 其中， $Y_k = \{u_1, u_2, \dots, u_k, y_1, y_2, \dots, y_k\}$ ，它表示在 k 时刻可获得的信息。对于信息状态重要的是，每个状态迁移合并成为历史信息，它易于更新，请参见以下公式 (4)：

$$[0124] \pi_{k+1} = \frac{B(u_{k+1}, y_{k+1}(u_{k+1})) A' \pi_k}{(1 - B(u_{k+1}, y_{k+1}(u_{k+1})) A' \pi_k} \quad \dots \dots (4)$$

[0125] 马尔可夫链的向量初始概率表示为：

[0126] $\pi_0 = [\pi_0(1), \pi_0(2)]'$ ，其中 $\pi_0(i) = P(X_0 = i)$, $i \in \{1, 2\}$

[0127] 通过使用信息状态和系统状态之间的联系，就可以基于在某个既定的时刻信息状态，而不是确切的系统状态来选择一个生物传感器。

[0128] (2) 生物传感器调度架构

[0129] 根据上面的信息，生物传感器的调度过程可以被简单的总结为三步，请参阅图 2 所示。

[0130] a) 调度——基于信息状态 π_k 找到一个最优的生物传感器 u_{k+1} ，这个生物传感器会被用在下一次的鉴权；

[0131] b) 观测结果——观测下一个时刻最佳的生物传感器的输出 $y_{k+1}(u_{k+1})$ ；

[0132] c) 更新——通过使用最近的观测结果 Y_{k+1} 来更新信息状态 π_{k+1} 。

[0133] (3) 成本定义

[0134] 在 k 时刻，基于历史信息 $Y_k(u_k)$ ，选择生物传感器 $u_{k+1} = 1$ ，则在 k 时刻的瞬间成本为：

[0135]

$$\underbrace{a_k(l) \|X_k - \pi_k\|_D}_{\text{第1部分}} + \underbrace{c_k(X_k, l)}_{\text{第2部分}} \quad \dots \dots (5)$$

[0136] 这里， $a_k(l)$, $l = 1, 2, \dots, L$ 是正权重， D 是一个量化的模，“ $\|\cdot\|$ ”为取模运算。本方法中，选择 $D = I_2$ 。第 1 部分表示由于选择传感器调度 u_1, \dots, u_k 的状态估计的均方误差。在基于生物特征的鉴权中，状态估计错误与错误的拒绝率 (FRR) 和错误的接受率 (FAR) 紧密相关。第 2 部分表示当系统的状态为 X_k 时，使用生物传感器 u_{k+1} 时的瞬时成本。在无线终端设备中，我们认为成本就是电池的损耗，信息的泄露等等。有许多方法可以用来平衡即时 成本和长期成本。这里仅仅考虑期望的未来折扣成本。从时间点 1 到 N 的离散积累成本可以表示为：

[0137]
$$J_u = E \left\{ \sum_{k=0}^{N-1} a_k(u_{k+1}) \|X_k - \pi_k\|_D + \sum_{k=0}^{N-1} c_k(X_k, u_{k+1}) + a_N \|x_N - \pi_N\|_D \right\} \quad \dots \dots (6)$$

[0138] 对于无穷范围的折扣成本,成本值可以表示为 :

[0139]
$$E \left\{ \sum_{k=0}^{\infty} \beta^k [a(u_{k+1}) \|X_k - \pi_k\|_D + c(X_k, u_{k+1})] \right\}$$

[0140] 其中, $E \{ \}$ 表示数学期望值,约束 $0 \leq \beta < 1$ 保证数学期望值是有限的。这里需要做的就是通过选择最佳的生物传感器调度(最优策略),来最小化折扣成本。

[0141] 上面的累积成本可以表示为 :

[0142]
$$J_u = E \left\{ \sum_{k=0}^{N-1} C_k(\pi_k, u_{k+1}) C_N(\pi_N) \right\} \quad \dots \dots (7)$$

[0143] 这里 $u_{k+1} = u_{k+1}(\pi_k)$

[0144] $C_N(\pi_N) = a_N g'(\pi_N) \pi_N, C_k(\pi_k, u_{k+1}) = a_k(u_{k+1}) g'(\pi_k) \pi_k + c_k'(u_{k+1}) \pi_k, k \in \{0, \dots, N-1\} \dots \dots (8)$

[0145] 在上面的等式中, $g(\pi_k)$ 表示 2 维估算方差向量 :

[0146] $g(\pi_k) = [\|\mathbf{e}_1 - \pi_k\|_D, \|\mathbf{e}_2 - \pi_k\|_D]' \quad \dots \dots (9)$

[0147] (4) 解决生物传感器调度问题

[0148] a) 动态规划

[0149] 为了有效的计算等式 (6),这里将使用动态规划来计算最佳策略。换句话说,从时间 T 到时间 0 方向计算这个等式。等式 (7) 的函数值可以写成 :

[0150] $J_N(\pi) = C_N(\pi)$

[0151] 并且对于 $k = N-1, N-2, \dots, 0$,有 :

[0152]
$$J_k(\pi) = \min_{u_{k+1} \in \{1, \dots, L\}} [C_k(\pi, u_{k+1}) +$$

[0153]

$$\sum_{m=1}^{M_{u_{k+1}}} J_{k+1} \left(\frac{B(u_{k+1}, O_m(u_{k+1})) A' \pi}{(1 \ 1) B(u_{k+1}, O_m(u_{k+1})) A' \pi} \right) \times (1 \ 1) B(u_{k+1}, O_m(u_{k+1})) A' \pi], \quad \pi \in P \quad \dots \dots (10)$$

[0154] 根据分段理论,函数值可以重新表示为一个有限的向量集合 :

[0155]
$$J_k(\pi) = \min_{i \in \Gamma_k} \gamma'_{i,k} \pi, \text{对于所有 } \pi \in P \quad \dots \dots (11)$$

[0156] 其中 Γ_k 是一个有限的 2 维向量 $\gamma_{i,k}'$ 的集合。

[0157] b) 分段线性的计算

[0158] 在这个问题中,从等式 (8) :

[0159] $C_k(\pi_k, u_{k+1}) = a_k(u_{k+1}) g'(\pi_k) \pi_k + c_k'(u_{k+1}) \pi_k$

[0160] 可得 : $g'(\pi)\pi$ 是 l_2 的模估计误差,它不是 π 的线性函数。这使得该问题和标准的部分可观马尔可夫决策过程问题不一样。根据参考文献 :

[0161] V. Krishnamurthy, "Algorithms for Optimal Scheduling and Management of Hidden Markov Model Sensors," IEEE Trans. Signal Proc., vol. 50, no. 6, pp. 1382–1397, June 2002,

[0162] 其中已经得出,这个估计误差可以一律近似为分段线性值 :

$$[0163] \quad g'(\pi)\pi = \min_{r=1,2,\dots,R} \vec{g}_r \pi \quad \dots\dots (12)$$

[0164] 其中, R 表示用来近似估计误差的 2 维向量的个数。用这个近似值, 我们的生物传感器调度问题转化为一个标准的部分可观马尔可夫决策过程问题。所有用来解决标准部分可观马尔可夫决策过程的算法都能用于解决本发明的问题。

[0165] 二次方程的值是凸起的曲线, 在上述参考文献中有所描述。正切线的上边界近似值可以用来表示本发明的模型中近似估计误差。

[0166] c) 最佳算法

[0167] 有许多解决有限范围的部分可观马尔可夫决策过程的算法, 例如 Sondik 算法, 演进修剪算法, 成氏线性支持算法, 以及见证算法。这些算法的详细介绍在以下参考文献中描述 :A. R. Cassandra, “Tony’s POMDP Webpage,” [Online]. Available :

[0168] <http://www.cs.brown.edu/research/ai/pomdp/index.html>.

[0169] 他们有相同的基本框架, 不同的只是计算单个动态程序步骤的方式不同。以上参考文献中的演进修剪算法的代码将被修改并在本发明的例子中使用。部分可观马尔可夫决策过程的解决方案可被一组向量和最佳动作一起表示, 函数值可以写为 :

$$[0170] \quad J_k(\pi) = \min_{i \in \Gamma_k} \gamma_{i,k}^*(u_{i,k}^*)\pi, \text{ 对所有 } \pi \in P \quad \dots\dots (13) \quad \text{对 所 有 } \pi \in P. \dots\dots (13)$$

[0171] 从这个等式中可以看出, 每个向量 γ 和一个最佳的生物传感器是相联系的。因此可以通过两步来解决本发明的问题 :

[0172] 第一步 : 运行离线动态规划 : 使用最佳的生物传感器 $u_{k,i}^*$ 和部分可观马尔可夫决策过程算法来计算 $\Gamma_k = \gamma_{k,i}^*$ 。其中 $i \in 1, 2, \dots, |\Gamma_k|$ 。

[0173] 第二步 : 实时调度 : 为特殊的信息状态 $\pi(k)$ 通过上述公式 (11) 找到一个 Γ_k , 因为每个 向量都和最佳的生物传感器相联系的, 那么就能选择一个最佳的生物传感器。

[0174] d) 安全需求限制的调度算法

[0175] 不同的移动系统有不同的安全需要。对这些系统, 保证 FRR 和 FAR 的满足是必要的。在本发明的公式里, 安全需求限制和系统安全状态的估计误差直接相关。如果估计误差因某些传感器超过门限阀值而产生, 那么就会选择其它的有着更高精确性的传感器。这里本发明仅仅考虑局部时间的约束 (短期约束) 而不是全局约束 (长期约束)。估计误差被指定为我们所期望的估计误差。本发明的目标是通过期望估计误差二次方程的约束, 来使生物传感器消耗最小化。也就是定义为 :

$$[0176] \quad J_u = \min_u E \left\{ \sum_{k=0}^{N-1} c'_k(u_{k+1})\pi_k \right\} \quad \dots\dots (14)$$

[0177] 使得 :

[0178]

$$\sum_{m=1}^{M_u} a_{k+1}(l) \left(1 - \frac{\pi' A B^2(u, O_m(u))}{((1-1)B(u, O_m(u))A'\pi)^2} \right) \times (1-1)B(u, O_m(u))A'\pi < K_l, \quad l \in \zeta_c \quad \dots\dots (15)$$

[0179] 这里, ζ_c 表示受约束的一组生物传感器。 $\zeta_{\bar{c}}$ 表示未受约束的一组传感器, 并且

$\zeta = \{1, \dots, L\} = \{\zeta_c \cup \zeta_{\bar{c}}\}$ 。

[0180] 因此,解决安全需要约束问题步骤如下所示:

[0181] ●用激活的 ζ 集合运行离线动态规划:用激活的 ζ 集合运行该规划,得到向量 $y_{k,i}^{\zeta}$ 和相关的最优生物传感器 $u_{k,i}^{\zeta,*}$ 。

[0182] ●用激活的 $\zeta_{\bar{c}}$ 集合运行离线动态规划:用激活的 $\zeta_{\bar{c}}$ 集合运行该规划,得到向量 $y_{k,i}^{\zeta_{\bar{c}}}$ 和相关的最优生物传感器 $u_{k,i}^{\zeta_{\bar{c}},*}$ 。

[0183] ●运行实时调度:通过上述公式 (11) 找到特殊的信息状态 $\pi(k)$ 下的 $y_{k,i}^{\zeta}$ 和 $y_{k,i}^{\zeta_{\bar{c}}}$ 。

[0184] ●如果 $\pi(k)$ 满足公式 (15),那么与向量 $y_{k,i}^{\zeta}$ 相关的传感器 $u_{k,i}^{\zeta,*}$ 将被选择,否则,选择与矢量 $y_{k,i}^{\zeta_{\bar{c}}}$ 相关的传感器 $u_{k,i}^{\zeta_{\bar{c}},*}$ 取代。

[0185] e) 系统资源约束调度算法

[0186] 连续鉴权和入侵检测都会消耗掉大量的系统资源。因此,特定的传感器所使用的次数是有限制的。简单的说,本发明在此处假设仅仅在使用传感器 1 上有约束:在 N 维问题下,传感器 1 仅仅可以最多使用用 N1 次。

[0187] 假设 $S_1 = \{f_1, \dots, f_{N_1+1}\}$ 表示 N_1+1 维的单位向量值,这里 f_i 在 i 个位置上发生 1 次。

我们用 z_k 来表示传感器 1 所用的次数。让 z_k 等于带有状态空间 S_1 的 N_1+1 态的马尔可夫链。如果传感器用了 $i-1$ 次,那么 $z_k = f_i$ 。 z_k 动态性如下所述:

[0188] 如果传感器 1 被使用 (i.e., $u_k = 1$),则 z_k 跳到 f_{i+1} 状态。如果运行的是其它传感器,则 z_k 保持不变。这里可以用确定的马尔可夫链动态表示 z_k ,即:

[0189] $z_k = Q'(u_k) z_{k-1}, z_0 = e_1, z_N = e_{N+1} \dots \dots \quad (16)$

[0190] 为了使用前述公式 (10) 得到最优的且受资源约束的调度策略,本发明做了如下的相应调整调换。假设扩展的马尔可夫链为 (X_k, z_k) ,且转移概率矩阵为 $\bar{A} = A \otimes Q$,则 (X_k, z_k) 的信息状态为 $\bar{\pi} = \pi_k \otimes z_k$,同时可观概率矩阵为:

[0191] $\bar{B}(u, O_m(u)) = B(u, O_m(u)) \otimes I_{N+1}$

[0192] 其中, $\underline{}$ 表示张量(克罗内积)。这样,根据标准的隐形马尔可夫滤波器,扩展的信息状态 $\bar{\pi}_k$ 从 A, B 演变为 \bar{A}, \bar{B} 。值函数定义为:

[0193] $\bar{J}_k = J_k(\pi, z), \bar{\pi} = \pi \otimes z$

[0194] 现在这里用 \bar{J}_k 取代 J_k ,用 \bar{A} 替换 A, \bar{B} 替换 B,通过前述公式 (10) 求解得上述的值函数。

[0195] 这样。本发明最终在保证最低限度的利用资源的前提下实现了最优的传感器的选择,也就是最佳的进行了持续鉴权和入侵检测组合。

[0196] 采用了上述的无线网络中移动设备实现持续鉴权联合入侵检测的方法,由于其主要基于生物特征的持续鉴权,因此无线网络中的持续鉴权可以表示为生物传感器的选择问题,通过把持续鉴权问题建立为一个部分客观的马尔可夫决策过程模型,并将入侵检测和响应系统一起共同起作用,重新鉴权是一个重要的响应类型,这是被入侵发起的,在重新鉴权过程后,只有一个可信的用户能够继续使用网络资源,同时危及安全的用户将被排除出

网络,将该系统建立为一个部分客观的马尔可夫决策过程模型,并且使用动态规划的隐形马尔可夫模型调度算法来获得最佳的调度策略,决定是否要选择生物传感器,以及选择何种生物传感器,以使得系统的性能最优化,从而获得最佳的持续鉴权策略,不仅可以极大的提高移动设备的安全性,满足对移动设备安全性要求很高的用户需求,而且能最佳的控制是否执行重新鉴权,以及选择哪个生物传感器进行鉴权,从而最低限度的使用系统资源;同时能最佳的控制是否激活入侵检测系统,从而最低限度的使用系统资源;而且入侵检测系统和持续鉴权能够相互共享彼此的信息,系统安全性要求的限制和资源的限制能够被保证,节约了系统运营的成本;同时本方法的工作性能稳定可靠,适用范围较为广泛,为无线网络中移动设备的信息安全技术的进一步发展奠定了坚实的基础。

[0197] 在此说明书中,本发明已参照其特定的实施例作了描述。但是,很显然仍可以作出各种修改和变换而不背离本发明的精神和范围。因此,说明书和附图应被认为是说明性的而非限制性的。

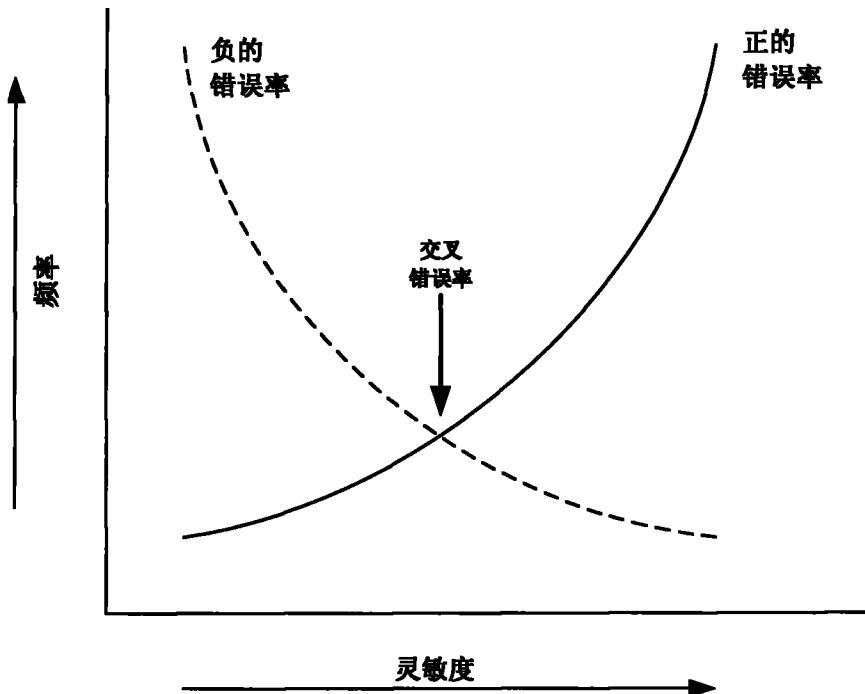


图 1

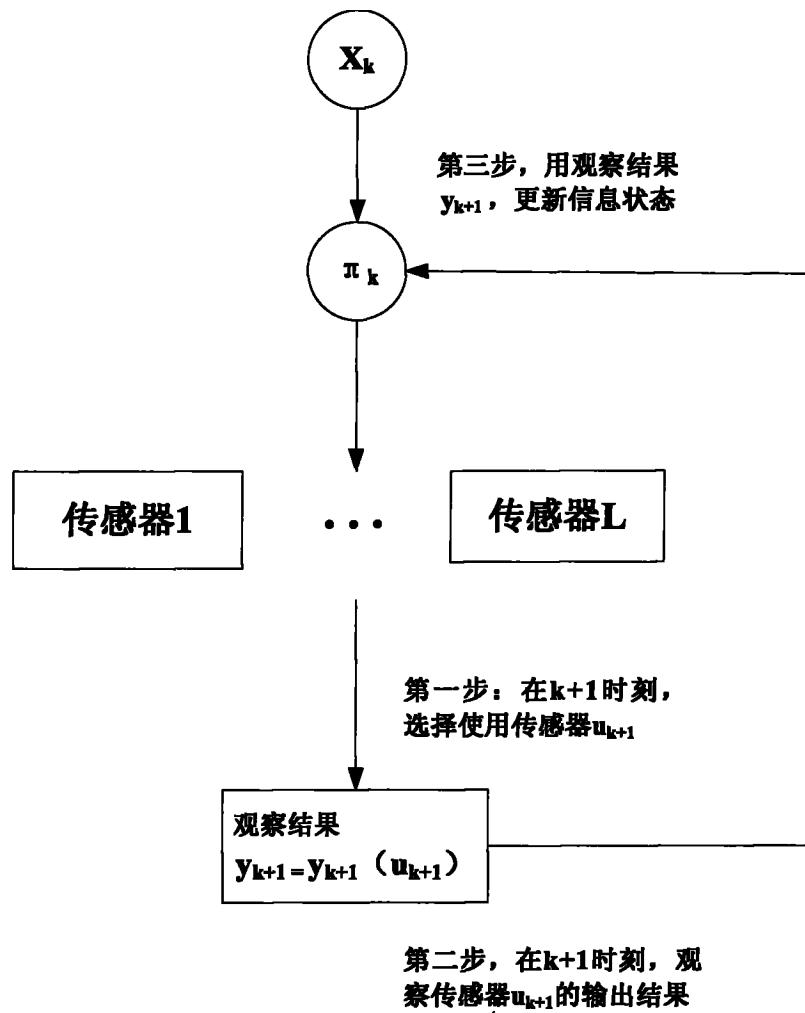


图 2