(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101902463 A
(43)申请公布日 2010.12.01

(21)申请号 201010153734.5

(22)申请日 2010.04.22

(71)申请人 国家无线电监测中心检测中心
地址 100037 北京市西城区北礼士路 80 号
申请人 西安西电捷通无线网络通信股份有限公司

(72)发明人 宋起柱 杜志强 铁满霞 曹军 周吉阳 阚润田 王文俭

(74)专利代理机构 西安智邦专利商标代理有限公司 61211
代理人 商宇科

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 84/18(2009.01)

权利要求书 2 页 说明书 4 页

(54)发明名称

一种适用于移动用户的传感器网络访问控制方法及系统

(57)摘要

本发明所涉及的是一种适用于移动用户的传感器网络访问控制方法及系统，该方法主要包括以下步骤：1）访问控制服务器 ACS 构造访问控制列表 ACL 以及用户身份信息，并在用户访问网络之前进行协议初始化；2）用户访问网络时，由网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行认证，用户认证成功后，通过预测用户将要到达的位置，将认证成功的消息扩散到用户的下一个临时访问控制网关中的节点；3）临时访问控制网关对用户的访问进行授权管理；该控制方法避免用户由于移动无法获得认证，或在认证成功后需要重新认证的问题，能够用于传感器网络对各类用户的访问控制。

CN 101902463 A

1. 一种适用于移动用户的传感器网络访问控制方法，其特征在于：所述适用于移动用户的传感器网络访问控制方法包括以下步骤：

1) 访问控制服务器 ACS 构造访问控制列表 ACL 以及用户身份信息，并在用户访问网络之前进行协议初始化；

2) 用户访问网络时，由网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行认证，用户认证成功后，通过预测用户将要达到的位置，将认证成功的消息扩散到用户的下一个临时访问控制网关中的节点；

3) 临时访问控制网关对用户的访问进行授权管理。

2. 根据权利要求 1 所述的适用于移动用户的传感器网络访问控制方法，其特征在于：所述步骤 1) 的具体实现方式是：

1.1) 访问控制服务器 ACS 构造访问控制列表 ACL，所述访问控制列表 ACL 包括 U_ID 字段、ADT 字段、VP 字段、AI 字段，其中：

U_ID 字段：用户的身份标识；

ADT 字段：用户被授权访问的数据类型；

VP 字段：用户被授权访问网络的期限；

AI 字段：用于认证用户身份的认证依据；

在构造访问控制列表 ACL 后，访问控制服务器 ACS 对用户进行注册，注册过程如下：ACS 根据网络用户的身份标识 U_ID 确定该用户能够访问的网络数据类型 ADT 和访问期限 VP，构造该用户的身份证明以及用于认证该身份证明的认证依据 AI，并将 U_ID、ADT、VP、AI 作为新条目字段插入 ACL 列表中，记做 ACL_{U_ID}；

1.2) 用户访问传感器网络之前，先向访问控制服务器 ACS 发送身份证明请求信息；收到身份证明请求信息后，如果该用户已注册，访问控制服务器 ACS 将事先为该用户构造的身份证明发送给该用户，并将访问控制列表 ACL 列表中与该用户 U_ID 对应的、包括 ADT、VP、AI 用户访问控制信息的 ACL_{U_ID} 以认证的方式发送给所有网络节点，节点在用户的有效期 VP 之前保存这些信息；如果用户未注册，访问控制服务器 ACS 直接丢弃用户的身份证明请求信息。

3. 根据权利要求 2 所述的适用于移动用户的传感器网络访问控制方法，其特征在于：所述步骤 2) 的具体实现方式是：

2.1) 用户访问网络时，由传感器网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行访问控制，临时访问控制网关根据用户的移动不断变化；用户向临时访问控制网关发送自己的身份证明，收到用户的身份证明后，临时访问控制网关中的所有节点先判断是否保存有与该用户对应的 ACL_{U_ID} 信息，如果存有该信息，表明该用户处于有效期内，根据 ACL_{U_ID} 中的用户 AI 信息对用户的身份证明进行认证，如果认证成功，则投 PASS 票，并向临时访问控制网关内的所有节点间进行广播，如果网关中的节点收到的 PASS 票数等于或超过一个阀值 P，则表示用户认证成功，其中阀值 P 由网络所有者自定义；如果用户不在有效期内、或用户在有效期内但身份认证失败、或用户在有效期内且身份认证成功但 PASS 票数低于阀值 P，均表示认证失败，网络终止该用户的访问；

2.2) 认证成功后，临时访问控制网关中的节点根据用户的运动方向、运动速度等对时间 t 后用户将要到达的位置进行预算，并在时间 t 后根据位置预算结果将用户认证成功的

消息发送给下一个临时访问控制网关，即当前临时访问控制网关内的节点；如果用户仍处于有效期 VP 内，则当前临时访问控制网关仍然承认用户的合法性，并在经过时间 t 后，将认证成功消息发送到下一个目标区域，即临时访问控制网关内；在用户访问网络的整个过程中，临时访问控制网关中的节点不断的根据用户的运动方向、运动速度等对用户将要到达的位置进行预算，并将用户认证成功的消息扩散到用户将要到达的位置；认证成功消息利用节点间预设的安全通道在网络中进行传输。

4. 根据权利要求 3 所述的适用于移动用户的传感器网络访问控制方法，其特征在于：所述步骤 3) 的具体实现方式是：

3.1) 用户获得认证后，用户将访问请求 Q 连同用户的 U_ID 以安全的方式发送给临时访问控制网关中的节点；

3.2) 临时访问控制网关内的节点收到用户的访问请求 Q 后，首先判断该用户是否已获得认证，如果已获得认证，再判断用户是否处于有效期，如果处于有效期，根据 ADT 信息判断用户访问请求 Q 的合法性，如果合法，则将访问请求 Q 连同用户的 U_ID 以安全的方式发送给用户的目的访问节点，目的访问节点是传感器网络中的任意节点，该节点将始终认为由临时访问控制网关转发的访问请求 Q 是合法的，并将根据访问请求 Q 做出响应，授权过程结束；如果用户未获得认证、不在有效期内或访问请求 Q 不合法，节点都将直接丢弃用户的访问请求 Q，终止该用户的访问。

5. 一种适用于移动用户的传感器网络访问控制系统，其特征在于：所述适用于移动用户的传感器网络访问控制系统包括访问控制器 ACS 以及节点；所述访问控制服务器 ACS 构造访问控制列表 ACL 以及用户身份信息，并在用户访问网络之前进行协议初始化；当用户访问网络时，由网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行认证，用户认证成功后，通过预测用户将要达到的位置，将认证成功的消息扩散到用户的下一个临时访问控制网关中的节点；临时访问控制网关对用户的访问进行授权管理。

一种适用于移动用户的传感器网络访问控制方法及系统

技术领域

[0001] 本发明属信息安全技术中的无线网络安全应用领域，尤其涉及一种适用于移动用户的传感器网络访问控制方法及系统。

背景技术

[0002] 无线传感器网络由大量具有感知能力的节点构成，以 ad-hoc 方式自组成网，为用户提供数据的收集、处理、传输等服务。访问控制机制用于保护传感器网络数据，禁止非法用户的访问，控制合法用户的访问权限，是传感器网络的基本安全服务之一。

[0003] 现有的传感器网络访问控制方法均只适用于传感器网络中静止的用户，无法适用于移动的用户，而传感器网络用户在网络中通常是移动的，如战场中的士兵、坦克等。

[0004] 此外，对于传感器网络中的移动用户，由于认证延迟，实现分布式的访问控制还将面临两个问题，此处假设由传感器网络中用户的单跳通信节点构成临时访问控制网关实施对用户的访问控制。问题一，合法用户在移动时可能无法获得认证。用户在发起认证请求时临时访问控制网关中的节点持有其认证信息，但在认证结束时，由于移动，其当前的临时访问控制网关中将有部分本地节点没有其认证信息，若这部分节点的数量超过预设的上限，即使合法用户也无法获得认证。问题二，用户的移动将导致重复认证。用户在某个位置获得认证，在其有效期内，当用户移动到另外一个位置并访问网络时，因当前临时访问控制网关中有部分节点可能没有其认证信息，若这部分节点的数量超过预设的上限，将导致该用户的合法身份无法延续，想要访问网络，用户必须重新获得认证，将浪费大量网络资源。

发明内容

[0005] 为了解决背景技术中存在的上述技术问题，本发明提供了一种既适用于传感器网络对移动用户的访问控制也适用于对静止用户的访问控制的传感器网络访问控制方法及系统。

[0006] 本发明的技术解决方案是：本发明提供了一种适用于移动用户的传感器网络访问控制方法，其特殊之处在于：所述适用于移动用户的传感器网络访问控制方法包括以下步骤：

[0007] 1) 访问控制服务器 ACS 构造访问控制列表 ACL 以及用户身份信息，并在用户访问网络之前进行协议初始化；

[0008] 2) 用户访问网络时，由网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行认证，用户认证成功后，通过预测用户将要到达的位置，将认证成功的消息扩散到用户的下一个临时访问控制网关中的节点；

[0009] 3) 临时访问控制网关对用户的访问进行授权管理。

[0010] 上述步骤 1) 的具体实现方式是：

[0011] 1.1) 访问控制服务器 ACS 构造访问控制列表 ACL，所述访问控制列表 ACL 包括 U_ID 字段、ADT 字段、VP 字段、AI 字段，其中：

[0012] U_ID 字段 :用户的身份标识 ;

[0013] ADT 字段 :用户被授权访问的数据类型 ;

[0014] VP 字段 :用户被授权访问网络的期限 ;

[0015] AI 字段 :用于认证用户身份的认证依据 ;

[0016] 在构造访问控制列表 ACL 后,访问控制服务器 ACS 对用户进行注册,注册过程如下 :ACS 根据网络用户的身份标识 U_ID 确定该用户能够访问的网络数据类型 ADT 和访问期限 VP,构造该用户的身份证明以及用于认证该身份证明的认证依据 AI,并将 U_ID、ADT、VP、AI 作为新条目字段插入 ACL 列表中,记做 ACL_{U_ID} ;

[0017] 1.2) 用户访问传感器网络之前,先向访问控制服务器 ACS 发送身份证明请求信息 ;收到身份证明请求信息后,如果该用户已注册,访问控制服务器 ACS 将事先为该用户构造的身份证明发送给该用户,并将访问控制列表 ACL 列表中与该用户 U_ID 对应的、包括 ADT、VP、AI 用户访问控制信息的 ACL_{U_ID} 以认证的方式发送给所有网络节点,节点在用户的有效期 VP 之前保存这些信息 ;如果用户未注册,访问控制服务器 ACS 直接丢弃用户的身份证明请求信息。

[0018] 上述步骤 2) 的具体实现方式是 :

[0019] 2.1) 用户访问网络时,由传感器网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行访问控制,临时访问控制网关根据用户的移动不断变化 ;用户向临时访问控制网关发送自己的身份证明,收到用户的身份证明后,临时访问控制网关中的所有节点先判断是否保存有与该用户对应的 ACL_{U_ID} 信息,如果存有该信息,表明该用户处于有效期内,根据 ACL_{U_ID} 中的用户 AI 信息对用户的身份证明进行认证,如果认证成功,则投 PASS 票,并向临时访问控制网关内的所有节点间进行广播,如果网关中的节点收到的 PASS 票数等于或超过一个阀值 P,则表示用户认证成功,其中该阀值 P 由网络所有者自定义 ;如果用户不在有效期内、或用户在有效期内但身份认证失败、或用户在有效期内且身份认证成功但 PASS 票数低于阀值 P,均表示认证失败,网络终止该用户的访问 ;

[0020] 2.2) 认证成功后,临时访问控制网关中的节点根据用户的运动方向、运动速度等对 t 时间后用户将要到达的位置进行预算,并在时间 t 后根据位置预算结果将用户认证成功的消息发送给下一个临时访问控制网关,即当前临时访问控制网关内的节点 ;如果用户仍处于有效期 VP 内,则当前临时访问控制网关仍然承认用户的合法性,并在经过时间 t 后,将认证成功消息发送到下一个目标区域,即临时访问控制网关内 ;在用户访问网络的整个过程中,临时访问控制网关中的节点不断的根据用户的运动方向、运动速度等对用户将要到达的位置进行预算,并将用户认证成功的消息扩散到用户将要到达的位置 ;认证成功消息利用节点间预设的安全通道在网络中进行传输。

[0021] 上述步骤 3) 的具体实现方式是 :

[0022] 3.1) 用户获得认证后,用户将访问请求 Q 连同用户的 U_ID 以安全的方式发送给临时访问控制网关中的节点 ;

[0023] 3.2) 临时访问控制网关内的节点收到用户的访问请求 Q 后,首先判断该用户是否已获得认证,如果已获得认证,再判断用户是否处于有效期,如果处于有效期,根据 ADT 信息判断用户访问请求 Q 的合法性,如果合法,则将访问请求 Q 连同用户的 U_ID 以安全的方式发送给用户的目的访问节点,目的访问节点是传感器网络中的任意节点,该节点将始终

认为由临时访问控制网关转发的访问请求 Q 是合法的，并将根据访问请求 Q 做出响应，授权过程结束；如果用户未获得认证、不在有效期内或访问请求 Q 不合法，节点都将直接丢弃用户的访问请求 Q，终止该用户的访问。

[0024] 一种适用于移动用户的传感器网络访问控制系统，其特殊之处在于：所述适用于移动用户的传感器网络访问控制系统包括访问控制器 ACS 以及节点；所述访问控制服务器 ACS 构造访问控制列表 ACL 以及用户身份信息，并在用户访问网络之前进行协议初始化；当用户访问网络时，由网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行认证，用户认证成功后，通过预测用户将要达到的位置，将认证成功的消息扩散到用户的下一个临时访问控制网关中的节点；临时访问控制网关对用户的访问进行授权管理。

[0025] 本发明的优点是：本发明提出一种传感器网络访问控制方法，对静止和移动用户均能进行认证和授权管理。在用户认证成功后，周期性的预测用户移动过程中的目标位置，并将认证成功的消息同时扩散到该目标位置区域，避免用户由于移动无法获得认证，或在认证成功后需要重新认证的问题，能够用于传感器网络对各类用户的访问控制。

具体实施方式

[0026] 本发明提供了一种适用于移动用户的传感器网络访问控制方法，根据本发明的优选实施例，其具体方法如下：

[0027] 1) 访问控制服务器构造访问控制列表以及用户身份信息，并在用户访问网络之前进行协议初始化；

[0028] 2) 用户访问网络时，由网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行认证。在用户认证成功后，通过预测用户将要到达的位置，将认证成功的消息扩散到用户的下一个临时访问控制网关中的节点；

[0029] 3) 临时访问控制网关对用户的访问进行授权管理。

[0030] 上述步骤 1) 的具体实施方式是：

[0031] 1.1) 访问控制服务器 ACS(Access Control Server) 构造访问控制列表 ACL(Access Control List)，其中包括 U_ID 字段、ADT 字段、VP 字段、AI 字段。

[0032]

U_ID	ADT	VP	AI

[0033] U_ID 字段：用户的身份标识；

[0034] ADT 字段：用户被授权访问的数据类型；

[0035] VP 字段：用户被授权访问网络的期限；

[0036] AI 字段：用于认证用户身份的认证依据。

[0037] 在构造访问控制列表 ACL 后，访问控制服务器 ACS 对用户进行注册，注册过程如下：ACS 根据网络用户的身份标识 U_ID 确定该用户能够访问的网络数据类型 ADT 和访问期限 VP，构造该用户的身份证明以及用于认证该身份证明的认证依据 AI，并将 U_ID、ADT、VP、AI 作为新条目字段插入 ACL 列表中，记做 ACL_{U_ID}。

[0038] 1.2) 用户访问传感器网络之前，先向 ACS 发送身份证明请求信息。收到身份证明请求信息后，如果该用户已注册，ACS 将事先为该用户构造的身份证明发送给该用户，并将

ACL 列表中与该用户 U_ID 对应的、包括 ADT、VP、AI 等用户访问控制信息的 ACL_{U_ID} 以认证的方式发送给所有网络节点，节点在用户的有效期 VP 之前保存这些信息。如果用户未注册，ACS 直接丢弃用户的身份证明请求信息。

[0039] 上述步骤 2) 的具体实施方式是：

[0040] 2.1) 用户访问网络时，由传感器网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行访问控制，临时访问控制网关根据用户的移动不断变化。首先，用户向临时访问控制网关发送自己的身份证明。收到用户的身份证明后，临时访问控制网关中的所有节点先判断是否保存有与该用户对应的 ACL_{U_ID} 信息，如果存有该信息，表明该用户处于有效期内，再根据 ACL_{U_ID} 中的用户 AI 信息对用户的身份证明进行认证，如果认证成功，则投 PASS 票，并向临时访问控制网关内的所有节点间进行广播，如果网关中的节点收到的 PASS 票数等于或超过一个阀值 P（该阀值可由网络所有者自定义），则表示用户认证成功。上述如果用户不在有效期内、或用户在有效期内但身份认证失败、或用户在有效期内且身份认证成功但 PASS 票数低于阀值 P，均表示认证失败，网络终止该用户的访问。

[0041] 2.2) 认证成功后，临时访问控制网关中的节点根据用户的运动方向、运动速度等对 t 时间后用户将要到达的位置进行预算，并在时间 t 后根据位置预算结果将用户认证成功的消息发送给下一个临时访问控制网关，即当前临时访问控制网关内的节点。此时，如果用户仍处于有效期 VP 内，则当前临时访问控制网关仍然承认用户的合法性，并在经过时间 t 后，以同样的方法将认证成功消息发送到下一个目标区域，即临时访问控制网关内。在用户访问网络的整个过程中，临时访问控制网关中的节点不断的根据用户的运动方向、运动速度等对用户将要到达的位置进行预算，并将用户认证成功的消息扩散到用户将要到达的位置。认证成功消息利用节点间预设的安全通道在网络中进行传输。

[0042] 上述步骤 3) 的具体实施方式是：

[0043] 3.1) 用户获得认证后，用户将访问请求 Q 连同自己的 U_ID 以安全的方式发送给临时访问控制网关中的节点。此时，临时访问控制网关只需核实用户身份信息，不需要对其进行重新认证。

[0044] 3.2) 临时访问控制网关内的节点首先收到用户的访问请求 Q 后，首先判断该用户是否已获得认证，如果已获得认证，再判断用户是否处于有效期，如果处于有效期，再根据 ADT 信息判断用户访问请求 Q 的合法性，如果合法，则将访问请求 Q 连同用户的 U_ID 以安全的方式发送给用户的目的访问节点，目的访问节点可以是传感器网络中的任意节点，该节点将始终认为由临时访问控制网关转发的访问请求 Q 是合法的，并将根据访问请求 Q 做出响应。至此，授权过程结束。上述如果用户未获得认证、不在有效期内或访问请求 Q 不合法，节点都将直接丢弃用户的访问请求 Q，终止该用户的访问。

[0045] 本发明在提供一种适用于移动用户的传感器网络访问控制方法的同时，还提供了一种适用于移动用户的传感器网络访问控制系统，该系统包括访问控制器 ACS 以及节点；访问控制服务器 ACS 构造访问控制列表 ACL 以及用户身份信息，并在用户访问网络之前进行协议初始化；当用户访问网络时，由网络中用户的单跳通信区域内的所有节点构成临时访问控制网关对用户进行认证，用户认证成功后，通过预测用户将要达到的位置，将认证成功的消息扩散到用户的下一个临时访问控制网关中的节点；临时访问控制网关对用户的访问进行授权管理。