论 文

物联网中移动 Sensor 节点漫游的组合安全认证协议

王良民^{①②*}, 姜顺荣^①, 郭渊博^③^① 江苏大学计算机科学系, 镇江 212013^② 安徽大学计算机科学与技术学院, 合肥 230601^③ 解放军信息工程大学电子技术学院, 郑州 450004

* 通信作者. E-mail: jasonwanglm@gmail.com

收稿日期: 2011-10-09; 接受日期: 2012-04-02

国家自然科学基金 (批准号: 51108209)、江苏省自然科学基金 (批准号: BK2011464)、计算智能与信号处理教育部重点实验室开放课题 (批准号: 201107) 和江苏大学第十批学生科研立项 (批准号: 10A119) 资助项目

摘要 物联网包含感知子网和传输骨干网, 其感知子网中节点能力受限, 往往利用移动的传感器节点跨区域访问来获取信息; 而其传输骨干网络需要依托现有 Internet 的基础设施, 并利用其提供的强大服务. 在这种情况下, 移动节点的漫游带来了新的安全问题, 一方面移动节点在感知子网间跨区域漫游, 虽和 MANET 中一样需要保证移动节点漫游时高效安全地加入新的拜访域, 但因传感节点资源极端受限而对轻量级有更高数量级的要求; 另一方面资源受限的感知子网间移动节点漫游仅提供轻量级安全, 但是在接入骨干传输网时, 不可因此降低骨干网络已有的安全性, 即轻量级的安全协议和传统骨干网协议综合运用时, 需具有组合安全性. 本文针对这种基于骨干传输网的移动节点漫游问题, 提出了一个新的随机漫游认证协议 (RMRAP), 兼顾安全性和实际应用的可行性, 实现了漫游的轻量级身份认证, 保护了漫游节点的隐私, 同时实现了具有前向安全性, 会话密钥对; 并针对衔接骨干网和感知子网的基站进行了组合安全性的认证测试, 验证了 RMRAP 的安全性; 最后, 从理论分析和实验仿真两个方面, 分析了 RMRAP 协议的性能, 并和相近工作进行了对比, 对比表明, 具有组合安全性的 RMRAP 在计算、通信开销方面, 依然具有和同类协议可比较的相近性能.

关键词 无线传感网 网络安全 认证 隐私保护 轻量级

1 引言

物联网是由感知子网、传输子网和应用子网组成的典型的混合式异构网络, 一方面其感知子网由计算和通信能力极弱的、廉价的感知节点组成, 往往使用移动节点和静态节点合作, 跨区域采集信息; 另一方面其传输骨干网依托现有互联网络的固定基础设施, 共享其强大的计算、传输及信息资源服务. 感知和传输子网的结合使用, 与近期文献 [1,2] 中开始讨论的多跳无线网络 (multihop wireless networks) 结构类似. 这种物联网中移动节点漫游情形如图 1 所示: 移动节点 M_A 从初始区域 A 进入区域 B 采集信息, 并和区域 B 内的节点合作, 将信息通过多跳方式传送给区域 B 的基站 CH_B , CH_B 同时充当该区域感知子网和传输骨干网的接入网关节点. 显然, M_A 若想与区域 B 内的成员协作, 继

引用格式: 王良民, 姜顺荣, 郭渊博. 物联网中移动 Sensor 节点漫游的组合安全认证协议. 中国科学: 信息科学, 2012, 42: 815-830, doi: 10.1360/112011-1081

图 1 物联网中常见的多跳无线网络结构

Figure 1 Multi-hop wireless networks in Internet of Things

续完成其信息采集及传输任务, 首先需要通过 CH_B 的安全性检测 —— 身份认证。

这种身份认证具有几个方面的特点: 首先是轻量级的要求, 感知子网中无论移动节点还是静态节点, 都是资源极端受限的; 其次是拜访域通常是随机的, 鉴于物联网应用的未来趋势, 这种移动的漫游现象也必然是大量存在的; 最后, 移动节点加入拜访区域, 通过身份认证获取合法身份后, 可以任意获取拜访区域提供的一切网络资源, 为此该身份认证协议除保证自身单独运行时的安全性外, 不能降低拜访域及与之相关联的传输骨干网的安全性, 典型的场景是不能影响同时运行在拜访域基站上已有协议的安全性, 即要求身份认证协议是组合安全^[3,4]的。当前物联网下的认证^[5~7]和移动^[8~10]情形的研究也才刚刚开始, 都未曾涉及到随机漫游、组合安全等方面。本文将设计出满足上述场景的移动 Sensor 节点漫游认证协议, 兼顾轻量级、随机漫游和组合安全的需求。

2 相关工作

与本文工作相关的研究, 首先是普通意义上安全无线漫游 (SWR, secure wireless roaming)^[11~18], 相关工作主要是根据不同情况需要, 定义好 SWR 基本需求, 根据需求设计出兼顾效率和安全性的协议, 如文献 [12~14] 主要关注匿名性和不可追踪性; 文献 [15,17] 重在实现漫游节点在拜访子网的本地认证以避免 DOS 攻击。文献 [17] 还提出了基于动态群签名机制的本地化匿名 SWR, 以提供隐私保护功能; 文献 [18] 在文献 [17] 的基础上, 以重认证时较大的计算开销来换取强不可追踪性。整体来说, 这类协议都是基于公钥加解密机制的^[12~18], 不满足轻量级需求, 不可直接用于物联网中感知节点漫游问题。此外, 这些工作也未考虑组合安全问题。

通用组合安全 (universal composable security)^[3,4]是指某个协议不仅在独自计算的情况下是安全的, 在网络环境中运行该协议的多个实例是安全的, 而且在作为其他协议的组件时, 通过组合操作构成的大的协议仍然是安全的, 如文献 [19,20] 通过使用基于 UC 安全的形式化方式来指导协议或方案的设计。而对于移动节点漫游认证协议的组合安全性研究, 主要集中在如何实现强的安全性, 如使用组合安全的公钥签名^[21]和 DH 密钥协商算法^[22], 未曾考虑轻量级的要求。对于感知子网来说, 其计算和通信开销过于昂贵。

在认证协议中, 对轻量级需求最多的莫过于传感网了。传感网最初考虑所有节点都是静态的, 典型的认证方案, 如: Perrig 等^[5]提出的使用单向 Hash 链实现的广播认证 μ TESLA; Du 等^[6]提出的使用 Merkle Tree 构建一条基于公钥机制的认证路径, 以降低认证的通信开销; Ibriq 等^[7]提出的一种基于分层的认证管理方案。这些都是针对传感网静态节点的认证协议, 具有较好的轻量性, 但未考虑

图 2 随机漫游认证的协议

Figure 2 Random roaming authentication protocol

漫游情形.

带移动节点的传感网的安全问题在最近受到越来越多的关注, 如 Pietro 等 [8,9] 研究了移动攻击者带来的协作认证和攻击弹性问题; Han 等 [10] 考虑了移动节点在 Sink 节点间移动时的重认证问题. Han 等 [10] 的方案将初始注册的家乡簇簇头作为可信的第三方, 预先向所有的邻居簇头发布预存认证信息, 以此来降低重认证过程中的通信开销和计算开销. 但是该方案与本文的物联网场景不同, 移动节点只能访问原 Sink 周围的邻居 Sink, 不具有随机漫游的特性; 此外, 也未曾考虑本文物联网环境对组合安全性的需求.

3 移动节点随机漫游认证协议

在多跳无线网络结构下, 物联网中移动感知节点漫游通常分为两个阶段: 第一阶段是移动节点在初始区域 A 的注册阶段, 该阶段主要的目的是预部署初始密钥、认证信息等秘密材料; 第二阶段是移动节点漫游到新区域 B (拜访域), 移动节点如何在传输骨干网对认证材料传输的协助下, 完成在拜访域内的认证. 本文假设静态感知网络已经部署好, 且假设各感知区域之间存在依托于传输骨干网的安全链路.

3.1 移动节点初始注册阶段

移动节点 M_A 在其初始域 A 内进行本地注册. M_A 向 CH_A 提出注册请求时, CH_A 随机挑选一个对称会话密钥 $K_{CH_A-M_A}$ 、一个随机的认证材料 r , 计算 M_A 的身份凭证 $E_{sk_{CH_A}}(CH_A, M_A, t_b, t_e)$, 其中 sk_{CH_A} 为 CH_A 的私钥, t_b 为身份凭证的开始时间, $(t_e - t_b)$ 是身份凭证的有效时间. CH_A 将 $K_{CH_A-M_A}$, r 和 $E_{sk_{CH_A}}(CH_A, M_A, t_b, t_e)$ 离线发送给 M_A , 并由 M_A 存入内存中. 同时在 CH_A 处保存着身份凭证, 会话密钥和所对应认证材料的认证表. 我们假定这种离线传送的方式安全的.

3.2 移动节点随机漫游认证协议 (RMRAP)

区域 A 中的移动节点 M_A , 通过一段时间的移动, 进入区域 B ; 为享受来自区域 B 的网络服务, 向 CH_B 提出认证请求, 漫游认证协议执行过程如图 2 所示.

1) RMRAP-Request phase: 移动节点 M_A 没有所要加入区域 B 的先验信息, 或者说区域 B 是随机选择的. 在请求阶段, M_A 选择一个随机数 $R_1 \in \{0,1\}^a$, 并计算 $e_1 = E_{K_{CH_A-M_A}}(R_1)$, $MAC_{K_{CH_A-M_A}}(CH_A, t_1, e_1, AUTHEN)$, 向 CH_B 发送 RMRAP-Request 消息:

$$M_A \rightarrow CH_B : CH_A, t_1, e_1, AUTHEN, MAC_1, \quad (1)$$

其中 $AUTHEN = E_{sk_{CH_A}}(CH_A, M_A, t_b, t_e)$, 为 CH_A 分配给 M_A 的身份凭证, t_1 为时间戳, 下文中使用的 $t_2 \sim t_4$ 也分别为 RMRAP 协议各条消息的时间戳. $MAC_1 = MAC_{K_{CH_A-M_A}}(CH_A, t_1, e_1, AUTHEN)$ 为消息验证码, $MAC_2 \sim MAC_4$ 分别为后文各条消息的验证码.

2) RMRAP-Ask phase: CH_B 在 t^* 接受到 RMRAP-Request 消息, 在验证了 $(t^* - t_1) \leq \Delta t$ 正确性之后, 取得 $AUTHEN$, 用 CH_A 的公钥 $K_{pk_{CH_A}}$ 解密得到 CH_A^* , M_A^* , 在验证了 $CH_A^* = CH_A$, $M_A^* = M_A$ 的正确性之后, 根据 CH_A 去向移动节点 M_A 的家乡子网发送认证信息询问 RMRAP-Ask 消息:

$$CH_B \rightarrow CH_A : M_A, t_2, t_1, e_1, MAC_1, MAC_2. \quad (2)$$

3) RMRAP-Answer phase: CH_A 在接受到消息 RMRAP-Ask 后, 使用算法 $VerifyA$ 进行合法性验证, 若验证, 则可获得 R_1 , 构造给 CH_B 的应答消息 RMRAP-Answer:

$$CH_A \rightarrow CH_B : t_3, e_2, MAC_3, \quad (3)$$

其中 $e_2 = E_{K_{CH_A-CH_B}}(r, R_1)$, $MAC_3 = MAC_{K_{CH_A-CH_B}}(t_3, e_2)$.

```

VerifyA algorithm
if  $((t^* - t_2) \leq \Delta t)$ 
then computer  $MAC_2^* = MAC_{K_{CH_A-CH_B}}(M_A, t_2, t_1, e_1, MAC_1)$ ;
if  $MAC_2^* = MAC_2$ 
then  $CH_A$  find  $AUTHEN$  and  $K_{CH_A-M_A}$  by  $M_A$ ;
computer  $MAC_1^* = MAC_{K_{CH_A-M_A}}(CH_A, t_1, e_1, AUTHEN)$ ;
if  $MAC_1^* = MAC_1$ 
then computer  $R_1 = D_{K_{CH_A-M_A}}(e_1)$ ;
end if
end if
end if
    
```

4) RMRAP-Response phase: 拜访子网的基站 CH_B 在接受到消息 RMRAP-Answer 之后, 首先验证 t_3 , MAC_3 的正确性, 如果验证失败, 则结束会话; 否则提取 r , R_1 , 并随机选择一个随机数 $R_2 \in \{0, 1\}^a$, 根据式 (5) 计算出会话密钥, 同时计算异或值 $h_1 = r \oplus H(R_1)$, $h_2 = H(r) \oplus R_2$, 最后构造消息 RMRAP-Response 消息:

$$CH_B \rightarrow M_A : t_4, h_1, h_2, MAC_4. \quad (4)$$

5) 移动节点 M_A 在接受到 CH_B 节点传送的过来的 RMRAP-Response 消息后, 首先验证 t_4 是否在门限时间内, 如果不在, 则结束会话; 否则, 计算 $H(R_1)$, 并与 h_1 异或, 求得 r^* , 验证 CH_B 身份的可靠性, 如果 $r^* = r$, 则证明 CH_B 身份的可靠性, 并通过计算 $H(r) \oplus h_2$, 得到 R_2 , 最后用式 (5) 得到新的会话密钥.

$$K_{CH_B-M_A} = H(R_1 || R_2). \quad (5)$$

在完成认证产生会话密钥之后, CH_B 立即给 M_A 分发新的身份凭证以及新的认证材料 r , 同时通知 CH_A 节点删除其对 M_A 的身份标识认证材料 r .

通过上述认证的节点在区域 B 内, 其漫游过程是隐私保护的——对其他节点来说, 是不可发现的. 移动节点 M_A 取得 CH_B 的信任, 完成注册之后, CH_B 会给移动节点重新分配 ID. 当 M_A 再次漫游进入区域 C 时, 域 B 将作为这次漫游的初始区域 (家乡域), 从而外界节点无法追踪 M_A 的运动轨迹.

同时, 对于合法授权者, 移动节点的轨迹是可追溯的. 每个基站内维持着一张移动节点的 ID 源表, 表中包括移动节点的上一个基站的 ID, 以及移动节点在上一个子网内的 ID, 移动节点在新子网内的 ID, 以及加入子网的时间.

3.3 协议的安全性分析

性质 1 协议具有前向安全性.

攻击者即使获得了移动节点 M_A 和子网 CH_C 的会话密钥 $K_{CH_C-M_A}$, 也很难推导出 M_A 与 CH_C 之前的会话密钥, 例如 $K_{CH_B-M_A}$ 等. M_A 与 CH_B 的会话密钥 $K_{CH_B-M_A}$, 是由两个随机数 R_1 和 R_2 来实现的, 并且是通过式 (1) 中的密文 e_1 和式 (4) 中 Hash 异或值 h_2 传输的. 攻击者要想获得 e_1 的明文内容 R_1 , 必须要知道 M_A 与 CH_A 之间的会话密钥对 $K_{CH_A-M_A}$, 从而问题被推导成为要获取 M_A 与初始子网 CH_A 会话密钥 $K_{CH_A-M_A}$, 而 $K_{CH_A-M_A}$ 是通过离线发送的, 被假设是安全的. 同样 R_2 也是由上一个周期的值 r 通过 Hash 异或保护得来的, r 和 $K_{CH_A-M_A}$ 具有同样的安全性. 通过上面的分析, 可知协议具有前向安全性.

性质 2 协议可以实现身份认证的本地过滤.

在 RMRAP 漫游协议中, 由于 CH_B 和 M_A 之间没有任何共享信息, 按照传统的三方认证协议的做法^[13,14], M_A 的消息传递给 CH_B 后, CH_B 是无法对消息进行本地认证, 而是直接发送给可信第三方, 由第三方来认证其身份的合法性, 而式 (1) 中的 RMRAP-Request 消息包含的身份凭证 AUTHEN 是用 CH_A 的私钥加密的, CH_B 在接收到 AUTHEN 之后, 用 CH_A 的公钥 $K_{pk_{CH_A}}$ 解密得到 CH_A^* , M_A^* , 对于 $CH_A^* \neq CH_A$, $M_A^* \neq M_A$ 的漫游申请者, 式子 (2) 的 RMRAP-Ask 将没有必要发送, 很好地抵抗了一部分伪造攻击. 同时通过解密获得的 t_e , 对于使用过期身份凭证的攻击进行了过滤. AUTHEN 的使用初步实现了 CH_B 在本地对 M_A 的身份的认证, 很好地节省了资源.

性质 3 协议可以实现双方的身份认证.

在整个漫游协议的通信过程中, M_A 申请加入网络的消息是式 (1) 的 RMRAP-Request, 该条消息中包含了身份凭证的内容 AUTHEN, 通过性质 2 的分析可知, 能够实现 M_A 在 CH_B 端的初步身份认证, 完整的身份认证是 CH_A 通过算法 VerifyA 来实现的; 而拜访子网 CH_B 在移动节点 M_A 端的身份认证主要是通过随机值 r 来实现的, 存在于式 (4) 中的 RMRAP-Response 消息, 是通过 Hash 异或的值 h_1 来实现传递的, 该值产生于上一个密钥会话生成周期后, 每次都是更新的. 整个认证过程中的身份凭证和认证材料都存在于家乡子网的认证表中, 保证了身份认证的可靠性和安全性.

性质 4 协议可以防止中间人攻击.

通过对 RMRAP 协议的分析, 攻击者可以通过诱骗或者截取移动节点 M_A 发送的消息 RMRAP-Request, 来冒充移动节点, 去和拜访子网的基站通信, 使得整个协议执行下去, 最后得到反馈的 RMRAP-Response 消息, 来提取会话密钥材料, 但根据性质 1 的说明, 密钥生成材料的两个参数 R_1 和 R_2 都不是以明文形式来发送的, 要想攻破他, 必须知道先前的会话密钥, 整个问题又规约到性质 1 的问题了. 而对于中间人篡改消息的攻击, 性质 3 中提到的双方的身份认证保证了消息发送方身份的正确性, 各条消息中使用的 MAC, 保证了消息完整性, 能够防止中间人攻击.

性质 5 协议可以防止重放攻击.

移动节点 M_A 在申请加入注册拜访子网时, 发送的每条认证消息都带有当前的时间戳 (t_1, t_2, t_3, t_4), 在 Δt 时间内接受到消息被认为是有效的, 在一定程度上防止了重放攻击. 根据会话密钥的生成式 (5), 每次会话密钥的生成都选择了新的随机数, 保证了会话密钥的新鲜性, 也有效地防止了重放攻击.

4 基于认证测试的组合安全性

认证测试方法是 Guttman 等 [23,24] 提出的基于串空间理论的安全协议形式化分析方法. 认证测试方法以“挑战—应答”机制为基础, 通过构造数据唯一原发性的特殊形式变换, 来构造认证测试的实例, 以证明协议中常规结点¹⁾的存在, 来完成协议认证属性的证明. 组合安全认证测试是 Guttman^[25]在 2009 年提出, 用于证明两个协议在组合使用时不会因相互影响而破坏整体的安全目标.

4.1 协议组合性认证测试的基本框架

组合认证测试的基本思想是: 为测试 Π_2 是否具有组合安全性, 需要考虑协议 Π_1 和 Π_2 的组合使用 (组合协议记为 Π), 若组合协议 Π 依然能达到 Π_1 所确定的安全目标, 即 Π_2 的运行不会影响到 Π_1 所确定的安全目标, 则 Π_2 具有基于该认证测试的组合安全性. 本文记 TinyPK 为 Π_1 , RMRAP 为 Π_2 .

组合认证测试一般分 3 步进行, 首先用串空间有向图描述协议, 对协议执行过程进行约简, 并用谓词符号对其进行描述; 然后在协议逻辑描述的基础上, 推导出 Π_1 的安全目标, 并证明组合后协议 Π 的安全目标与 Π_1 安全目标是同构的; 同样在协议逻辑描述的基础上, 定义并描述协议运行过程中参与结点之间的角色, 通过协议 Π 执行过程中结点角色 (Π_1 或 Π_2) 的分解, 完成 Π_1 和 Π 满足强不相交加密性的证明, Π 中丛的反例求解和 Π 中丛的可实现性的证明. 而 Guttman^[25]证明了 Π_1 和 Π 的强不相交加密和反例的可实现性可以保证 Π 实现 Π_1 的安全目标, 即完成 Π_2 组合安全的认证测试. 4.2~4.4 小节分别描述这 3 个步骤.

4.2 测试协议的串空间模型与描述

本小节采用串空间模型对这两个协议进行约简, 并用逻辑语言进行描述.

TinyPK^[26] 在组合协议中的功能是实现基站间共享密钥的产生, 其串空间有向图如图 3 所示, 其中基站节点 CH_B, CH_A 为两个对等的执行实体, 所对应的结点分别为 m_0, m_1 和 n_0, n_1 . g_1, g_2 分别为标准的 DH 传输子项, 其中 $g_1 = g^x \bmod P, g_2 = g^y \bmod P, x, y$ 为随机值. $\{g_1\}(CH_A)_{sk}$ 表示用 CH_A 的私密 $(CH_A)_{sk}$ 加密 g_1 . $\text{Store}K_{CH_A-CH_B}$ 表示在 CH_B 验证在 CH_A 发送过来的消息的正确性后, 计算出共享密钥 $K_{CH_A-CH_B}$, 并存储. 协议 TinyPK(Π_1) 的基本的安全假设如下: 1) $(CH_B)_{sk}, (CH_A)_{sk} \notin K_P$ (K_P 为攻击者所掌握的密钥集合); 2) x, y 唯一产生, (3) $x \neq y$. 由图 3, 协议 Π_1 的基本的串空间集合包含:

1) 在逻辑证明领域, 相关书籍将串空间的 node 翻译为结点; 而在网络领域, node 翻译为节点. 为符合习惯, 本节逻辑证明部分采取结点、节点两种形式分别表示串空间和网络中的 node

图 3 TinyPk(Π_1)的串空间有向图Figure 3 String space map of TinyPk(Π_1) 图 4 简化的协议 Π_2 的串空间有向图Figure 4 String space map of RMRAP(Π_2)

发起者串: 协议 TinyPk(Π_1) 的发起者串用符号 S_{i1} 表示, 用 $\text{Init}[\]$ 作为发起者串的空间的标识. 则 $S_{i1} \in \text{Init}[CH_B, CH_A, \{g_1\}(CH_B)_{sk}, \{g_1, g_2\}(CH_A)_{sk}]$, 其迹如式 (6) 所述,

$$\langle \langle \sigma_1, a_1 \rangle, \langle \sigma_2, a_2 \rangle \rangle = \langle +\{\{g_1\}(CH_B)_{sk}\}, -\{\{g_1, g_2\}(CH_A)_{sk}\} \rangle. \quad (6)$$

其中, $\langle \sigma_1, a_1 \rangle$ 是迹的符号项表示形式, 符号项一般由二元组 $\langle \sigma, a \rangle$ 表示, 其中 σ 取值 + 或 -, 分别对应着发送和接收两个状态, a 是串空间的轨迹, 即消息传输的内容.

响应者串: 协议 TinyPk(Π_1) 的响应者串用符号 S_{r1} 表示, 用 $\text{Resp}[\]$ 作为响应者串的空间的标识, 则 $S_{r1} \in \text{Resp}[CH_B, CH_A, \{g_1\}(CH_B)_{sk}, \{g_1, g_2\}(CH_A)_{sk}]$, 其迹如式 (7) 所述,

$$\langle \langle \sigma_1, a_1 \rangle, \langle \sigma_2, a_2 \rangle \rangle = \langle -\{\{g_1\}(CH_B)_{sk}\}, +\{\{g_1, g_2\}(CH_A)_{sk}\} \rangle. \quad (7)$$

RMRAP 协议在组合协议中的功能是使用 TinyPk 所产生的基站间共享密钥, 来实现移动节点在新的拜访子网的认证接入, 其串空间有向图如图 4 所示, 有向图中涉及到的符号与 3.2 小节中协议描述时相同. RMRAP 协议的基本的假设如下: 1) $(M_A, CH_A)_k, (CH_A, CH_B)_k \notin K_P$, 2) R_1, R_2 唯一产生, 3) $R_1 \neq R_2$. 其中 $(M_A, CH_A)_k$ 表示 M_A 和 CH_A 会话密钥.

由图 4, 协议 Π_2 的基本的串空间集合包含:

1) 发起者串: 协议 RMRAP(Π_2) 的发起者串用符号 S_{i2} 表示, 用 $\text{Init}[\]$ 作为发起者串的空间的标识. 则 $S_{i2} \in \text{Init}[M_A, CH_B, e_1, \text{AUTHEN}, \text{MAC}_1, h_1, h_2, \text{MAC}_4]$, 其迹如式 (8) 所述,

$$\langle \langle \sigma_1, a_1 \rangle, \langle \sigma_2, a_2 \rangle \rangle = \langle +\{e_1, \text{AUTHEN}, \text{MAC}_1\}, -\{h_1, h_2, \text{MAC}_4\} \rangle. \quad (8)$$

2) 响应者串: 协议 RMRAP(Π_2) 的响应者串用符号 S_{r2} 表示, 用 $\text{Resp}[\]$ 作为响应者串的空间的标识, 则 $S_{r2} \in \text{Resp}[M_A, CH_B, CH_A, e_1, \text{AUTHEN}, \text{MAC}_1, \text{MAC}_2, e_2, \text{MAC}_3, h_1, h_2, \text{MAC}_4]$, 其迹如式 (9) 所述,

$$\begin{aligned} & \langle \langle \sigma_1, a_1 \rangle, \langle \sigma_2, a_2 \rangle, \langle \sigma_3, a_3 \rangle, \langle \sigma_4, a_4 \rangle \rangle \\ &= \langle -\{e_1, \text{AUTHEN}, \text{MAC}_1\}, +\{e_1, \text{MAC}_1, \text{MAC}_2\}, -\{e_2, \text{MAC}_3\}, +\{h_1, h_2, \text{MAC}_4\} \rangle. \end{aligned} \quad (9)$$

3) 服务者串: 协议 RMRAP(Π_2) 的服务者串用符号 S_{s2} 表示, 用 $\text{Ser}[\]$ 作为响应者串的空间的标识, 则 $S_{s2} \in \text{Ser}[CH_B, CH_A, e_1, \text{MAC}_1, \text{MAC}_2, e_2, \text{MAC}_3]$, 具体的迹如下:

$$\langle \langle \sigma_1, a_1 \rangle, \langle \sigma_2, a_2 \rangle \rangle = \langle -\{e_1, \text{MAC}_1, \text{MAC}_2\}, +\{e_2, \text{MAC}_3\} \rangle. \quad (10)$$

$$\begin{aligned}
& \forall m, x, y, g, (CH_A)_{pk}, (CH_B)_{pk}, (CH_B)_{sk}, (CH_A)_{sk}. \\
& \quad \text{if } \text{Store1}(m, (CH_A, CH_B)_K) \\
& \quad \wedge \text{Non}(pk(CH_A)) \wedge \text{Non}(pk(CH_B)) \quad (\phi 1) \\
& \quad \wedge \text{Non}(sk(CH_A)) \wedge \text{Non}(sk(CH_B)) \quad (\phi 2) \\
& \quad \text{then } \exists m_0, n_0 \\
& \quad CH_B1(m_0, x, g_1, (CH_B)_{sk}) \wedge CH_A1(n_0, g_1, (CH_B)_{pk}) \\
& \quad \text{and } \exists m_1, n_1 \\
& \quad CH_A2(n_1, g_1, y, g_2, (CH_B)_{pk}, (CH_A)_{sk}) \wedge CH_B2(m_1, x, g_1, g_2, (CH_B)_{sk}, (CH_A)_{pk}) \\
& \forall m, n, x, y, g, (CH_A)_{pk}, (CH_B)_{pk}, (CH_B)_{sk}, (CH_A)_{sk} \\
& \quad \text{if } \phi 1 \wedge \phi 2 \wedge \text{Lsn1}(n, g) \\
& \quad \text{then false}
\end{aligned}$$

图 5 协议 (Π_1) 安全目标的形式化描述Figure 5 Security goals description in $L(\Pi_1)$

4.3 Π_1 安全目标形式化描述以及 Π 安全目标的同构证明

Guttman^[25] 在串空间的基础上, 定义了一种基于一阶逻辑的目标语言 $L(\Pi)$. $L(\Pi)$ 使用经典量化语言 (classic quantified language), 集合自身定义的词法, 来描述协议 Π 执行过程. 通过对协议 Π 执行过程中关键语句的抽取, 来确定协议的安全目标. 基于该语言的文法定义, 图 5 描述了 TinyPK(Π_1) 的串空间有向图 (图 3) 协议的执行过程, 其中, 表达式 $\phi 1$ 和 $\phi 2$ 被抽取为其安全目标.

图 5 中涉及到一些新的谓词, 如 $\text{Store1}(m, (CH_A, CH_B)_K)$ 和 $\text{Non}(pk(CH_A))$, 其定义如下:

- 形如 $\text{Nov}(v)$ 的谓词, 定义为: 以 v 作为合法实体的密钥集合 (该密钥集合里的密钥假定是不被攻击者所掌握的) 的成员, 被假设是无源的, 即在协议执行之前就已经存在于各实体内. 具体到图 5 中的 $\text{Non}(pk(CH_A))$, $\text{Non}(pk(CH_B))$, $\text{Non}(sk(CH_A))$ 和 $\text{Non}(sk(CH_B))$, 其中 $sk(CH_B)$ 被定义为 CH_B 的私钥, $pk(CH_B)$ 被定为 CH_B 的公钥.

- 形如 $\text{RhoJ}(m, v_1, \dots, v_i)$ 的谓词, 是角色谓词, 定义为: 协议中某个角色实体 ρ 的第 j 个结点 m , 以及结点 m 前出现的所有变量 $v_1, \dots, v_i$. 具体到图 5 中的 $\text{Store1}(m, (CH_A, CH_B)_K)$, $CH_B1(m_0, x, g_1, (CH_B)_{sk})$, $CH_A1(n_0, g_1, (CH_B)_{pk})$, $CH_A2(n_1, g_1, y, g_2, (CH_B)_{pk}, (CH_A)_{sk})$, $CH_B2(m_1, x, g_1, g_2, (CH_B)_{sk}, (CH_A)_{pk})$.

基于串空间语言和经典量化语言的映射关系, 可以证明组合后协议基于串空间的基本安全目标和图 5 以 $\phi 1$ 和 $\phi 2$ 作为协议的安全目标是同构的.

定理 1 组合后协议 Π 的基于串空间安全目标可以表述为 $\phi 1$ 和 $\phi 2$

证明 假设 A 作为协议 Π 的某一个丛. σ 是作为丛 A 从 $L(\Pi_1)$ 的变量到协议 Π 串空间的的函数映射. 若要推导出 $A \models \phi$ (为了便于后文命题逻辑的推导, 这里用 ϕ 来代表 $\phi 1$ 和 $\phi 2$ 两个安全目标), 则需要满足对所有的函数映射 σ , 都满足 $A, \sigma \models \phi$.

命题逻辑是以标准的 Tarski 归纳条款 (Tarski inductive clauses) 为基础的经典一阶逻辑命题, 基本规则如下:

$A, \sigma \models \text{Nov}(v)$, iff $\sigma(v) \in \text{non}_A(\text{non}_A)$ 表示在丛 A 中是无源的, 即在协议运行前已经存在于角色结点里);

$A, \sigma \models \text{RhoJ}(m, v_1, \dots, v_k)$, iff $\sigma(m) \in \text{nodes}(A)$ ($\text{nodes}(A)$ 表示结点是属于丛 A 的结点), 且 $\sigma(m)$ 是角色实体 ρ 的第 j 个结点, 并且有参数 $\sigma(v_1), \dots, \sigma(v_k)$;

在图 5 中出现的谓词 $pk(CH_A)$, $pk(CH_B)$, $sk(CH_A)$, $sk(CH_B)$ 在丛 A 中是无源的, 即这 4 个谓词都满足 $\sigma(v) \in \text{non}_A$, 从而 $A, \sigma \models \text{Nov}(v)$;

同样对于图 5 中角色结点 $\text{Store1}(m, (CH_A, CH_B)_K)$, $CH_B1(m_0, x, g_1, (CH_B)_{sk})$, $CH_A1(n_0, g_1, (CH_B)_{pk})$, $CH_A2(n_1, g_1, y, g_2, (CH_B)_{pk}, (CH_A)_{sk})$, $CH_B2(m_1, x, g_1, g_2, (CH_B)_{sk}, (CH_A)_{pk})$ 分别是丛 A 角色实体的实例化的结点, 并且满足参数关系, 即满足 $A, \sigma \models \text{RhoJ}(m, v_1, \dots, v_k)$.

当对所有的函数映射 σ 都满足 $A, \sigma \models \phi$, 从而 $A \models \phi$. 定理 1 得证, 组合后协议 Π 的基于串空间模型的安全目标可以表述为 ϕ_1 和 ϕ_2 . 证毕.

4.4 RMRAP 协议组合安全性证明

根据文献 [25] 对于协议的可组合安全性的证明定理, 我们分为下面几个步骤来实现: 首先是协议 Π 和 $\text{TinyPK}(\Pi_1)$ 满足强不相交加密性的证明 (命题 1); 然后是协议 Π 中 Π_1 的反例的求解和 Π 可实现性的证明 (命题 2); 在得出上面两个命题的结论之后, 再结合文献 [25] 给出的可组合安全定理, 最终得出定理 2, 即 RMRAP 是组合安全的.

命题 1 协议 Π 和 $\text{TinyPK}(\Pi_1)$ 满足强不相交加密性.

证明 协议 Π 和 $\text{TinyPK}(\Pi_1)$ 的强不相交性, 要求在构造 $\text{RMRAP}(\Pi_2)$ 协议时, 和 $\text{TinyPK}(\Pi_1)$ 协议不存在创建冲突和抽取冲突. 创建冲突是指协议 $\text{RMRAP}(\Pi_2)$ 不能创建类似 $\text{TinyPK}(\Pi_1)$ 构造的加密信息. 抽取冲突是指协议 $\text{TinyPK}(\Pi_1)$ 加密后传输给协议 $\text{RMRAP}(\Pi_2)$ 的信息, 不能在不加密的形式下再次被传输.

根据文献 [25] 的定义, 强不相交加密性的证明分为 3 步:

第一步. 确定主要结点和次要结点: 主要结点被定义为在组合使用的协议 Π 中出现的属于 $\text{TinyPK}(\Pi_1)$ 的实例化角色结点. 出现在 Π 中, 而不出现在 $\text{TinyPK}(\Pi_1)$ 的实例化角色结点定义为次要结点. 由迹 (6) 和 (9) 的观察可知, CH_A 和 CH_B 为主要结点, M_A 为次要结点.

第二步. 确定次要结点的创建和抽取加密内容: 该步骤主要目的是找出次要结点中涉及到的所有加解密的内容. 根据迹 (8), M_A 加密相关的内容为 e_1 , MAC_1 和 AUTHEN , 且

$$e_1 \in E \subseteq (\Pi_2) = \{e_1 : \exists O_0, \alpha. e_1 \subseteq \text{msg}(\alpha(O_0)) \wedge O_0 \text{ is a role node of } \Pi_2\}, \quad (11)$$

$$\text{MAC}_1 \in E \subseteq (\Pi_2) = \{\text{MAC}_1 : \exists O_0, \alpha. \text{MAC}_1 \subseteq \text{msg}(\alpha(O_0)) \wedge O_0 \text{ is a role node of } \Pi_2\}, \quad (12)$$

$$\text{AUTHEN} \in E \subseteq (\Pi_2) = \{e_{\text{AUTHEN}} : \exists O_0, \alpha. e_{\text{AUTHEN}} \subseteq \text{msg}(\alpha(O_0)) \wedge O_0 \text{ is a role node of } \Pi_2\}, \quad (13)$$

式 (11)~(13) 中 $E \subseteq (\Pi_2)$ 表示加密内容 e_1 , MAC_1 和 AUTHEN 是在协议 Π_2 里实现的, 对应于串空间模型, 是在同构结点 O_0 处产生了这些加密内容, 并且 O_0 是属于协议 Π_2 角色结点.

第三步. 确定强不相交加密: 强不相交加密要求次要结点的加密内容和 $\text{TinyPK}(\Pi_1)$ 协议不存在抽取或创建冲突. 根据式 (11), 对照 e_1 的具体加密组成可知, e_1 相关的加密创建属于 $\text{RMRAP}(\Pi_2)$ 的加密, 与 $\text{TinyPK}(\Pi_1)$ 不相关, 不存在创建冲突. 同样 MAC_1 也是如此. 对于 AUTHEN , 首先不属于 $\text{TinyPK}(\Pi_1)$ 和 $\text{RMRAP}(\Pi_2)$, 而且 AUTHEN 解密后的内容是不在迹中流通的, 只做中间验证所用, 即使和产生 AUTHEN 的消息组合, 也不存在抽取的冲突.

由以上分析, 可以看出组合后的协议 Π 中的次要结点不存在创建冲突和抽取冲突, 从而 Π , $\text{TinyPK}(\Pi_1)$ 是满足强不相交加密的. 证毕.

命题 2 Π 协议中属于 $\Pi_1(\text{TinyPK})$ 协议的丛 A 反例的求解和 Π 协议中丛 A 可实现性的证明.

从 A 的可实现的证明是通过认证测试来实现的, 在文献 [25] 中, 提出了新的认证测试的方法. 将其作为引理 1^[25] 给出.

引理 1 c 作为从 A 中某个原子或者加密, S 是从 A 中某个加密的集合. $\exists n \subseteq \text{nodes}(A)$, 使得 $\text{Cut}(c, S, A)$ 定义为 c, S 在 A 中的 test cut. 形式化描述为

$$\text{Cut}(c, S, A) = \{n \subseteq \text{nodes}(A) : \exists m. m \leq_A n \wedge c \vdash^S \text{msg}(m)\}. \quad (14)$$

命题 2 的证明 Π 协议中属于 $\Pi_1(\text{TinyPK})$ 协议的丛 A 反例的求解是指对于任何安全目标 $G_1 \in L(\Pi_1)$, 试图从 Π 的丛 B 的反例中提取一个属于 $\text{TinyPK}(\Pi_1)$ 的丛 A_1 的反例. 通过以下两步完成: 首先, 只保留 B 中首要结点, 记为 $B \uparrow \Pi_1$ (用丛 A 来表示); 然后从丛 A 除去 (removal) 不属于协议 Π_1 中的加密 $e \notin E \ll (\Pi_1)(E \ll (\Pi_1)$ 表示属于协议 $\text{TinyPK}(\Pi_1)$ 加密), 剩下的即为丛 A_1 .

由迹 (6)~(10), 首先抽出求出 $B \uparrow \Pi_1$ 的串

$$[CH_B, CH_A, g_1 (CH_B)_{sk}, g_1, g_2 (CH_A)_{sk}, e_1, \text{MAC}_1, \text{MAC}_2, e_2, \text{MAC}_3].$$

除去 A 中不属于协议 $\text{TinyPK}(\Pi_1)$ 的加密 $e \notin E \ll (\Pi_1)$ 得, A_1 的串为

$$[CH_B, CH_A, \{g^x\}(CH_B)_{sk}, \{g_1, g_2\}(CH_A)_{sk}].$$

根据引理 1, 在 A 的串中, 有的 $\text{Cut}(g_1, S_1, A)$ 和 $\text{Cut}(g_2, S_2, A)$ 两个重要的 cut 需要解释, 其中 $\text{Cut}(g_1, \{g_1, g_2\}(CH_A)_{sk}, A)$ 在 n_1 结点处被解释, 而 $\text{Cut}(g_2, \{g_1, g_2\}(CH_A)_{sk}, A)$ 在 m_1 结点处被解释, 从而丛 A 是可实现的. 证毕.

组合性的最后判断需要用到文献 [25] 的组合安全的判定定理, 该定理如引理 2^[25] 所述.

引理 2 当 Π, Π_1 满足强不相交加密, 并且定义 $G_1 \in L(\Pi_1)$ 为安全目标. 如果 $A| = \neg G_1$ 是可实现的, 则对于作为 Π_1 的丛 $A_1, A_1| = \neg G_1$.

定理 2 RMRAP 是组合安全的.

证明 首先根据定理 1 的证明可知 $A| = \phi$ (ϕ 代表 ϕ_1 和 ϕ_2 两个安全目标, 由定理 1 的证明保证了其与 Π 的基于串空间安全目标同构), 同时命题 2 中也给出 Π 协议中丛 A 可实现性证明, 结合文献 [25] 中关于反例可认知性的定义可知, $A| = \neg G_1$.

根据引理 2, 首先要求协议 Π, Π_1 满足强不相交加密, 该命题已经在命题 1 中给出详细证明, 即协议 Π, Π_1 已经满足了引理 2 中的强不相交加密性; 同样命题 2 已经证明了 $A| = \neg G_1$ 是可实现的, 也满足了引理 2 的另一个要求. 而 A_1 作为 Π 中 Π_1 的反例已经求解出, 从而根据引理 2, 我们可以得出结论 $A_1| = \neg G_1$, 即组合后的协议 Π , 并未影响原协议 $\text{TinyPK}(\Pi_1)$ 的安全性质, 从而得证协议 RMRAP 的可组合性. 证毕.

5 协议性能分析比较

基于物联网的移动节点漫游认证协议, 有轻量级、随机漫游、组合安全等 3 个方面的需求, 本节不仅定性比较相关工作对这 3 个方面的满足情况, 并将本文工作和相关工作进行了定量分析.

5.1 相关工作的比较

表 1 列出了 RMRAP 与相关协议在轻量级、随机漫游、安全性 3 个方面的比较, 其中, 计算开销的衡量, 是以 CPU 转数作为度量值的, 而消息长度以字节数为单位, h_n 表示子网内移动节点到达基站的平均中继跳数, n_c 表示周围邻居 Sink 的平均个数, 而安全性部分 “—” 表示未曾考虑.

表 1 相关协议比较
Table 1 Comparison of related work

Protocol	Lightweigh						Random roaming	Security		
	Communi- cation		Computation overhead		Message length			Authen- ticate local filter	Prevent DOS attack	Composable security
	Whole proctocl	Mobile node	Whole protocol	Mobile node	Whole protocol	Mobile node				
Yang et al. 2007 ^[13]	8	3	$\geq 294\text{M}$	88.2 M	$> 90h_n+134$	$\geq 90h_n+66$	✓	×	×	—
Yang et al. 2008 ^[14]	4	2	205.8 M	73.5 M	$74h_n+222$	$74h_n+76$	✓	×	×	—
Yang et al. 2010 ^[17]	3	3	393.22 M	198.45 M	$74h_n+72$	$74h_n+72$	✓	—	✓	—
He et al. 2011 ^[18]	3	3	584.32 M	294 M	$188h_n+72$	$188h_n+72$	✓	—	✓	—
Han et al. 2010 ^[10]	≥ 4	3	150.388 k	53.71 k	$52h_n+88+56n_c$	$52h_n+88$	×	—	✓	—
RMRAP	4	2	128.9 k	32.226 k	$50h_n+108$	$50h_n+28$	✓	✓	✓	✓

轻量级的比较中, 包含了通信次数、计算开销和消息长度 3 个方面的比较. 在通信次数的比较上, Yang 等^[13]、Yang 等^[14]、Han 等^[10] 和我们的 RMRAP 考虑了整个认证过程, 通信次数包含了认证材料的传输; 而 Yang 等^[17] 和 He 等^[18] 仅仅考虑了移动节点参与认证过程的通信次数. 在漫游协议中, 轻量级的要求主要集中在移动节点上, 而物联网环境下移动的传感器节点, 能量、计算能力、通信能力更加受限, 因此对轻量级的要求更高. Han^[10] 和 RMRAP 均是针对这种情况设计的, Han 等^[10] 的通信次数 ≥ 4 次, 原因是每一次移动后的重认证过程, 都需要通过广播, 而一次广播的通信次数至少要按 1 次计算.

表 1 所示的消息长度的比较中, 考虑了子网内中继的跳数和周围平均邻居 Sink 对整个协议的消息长度的影响. 消息长度的度量是以基本消息格式长度假设为基础估算出来的, 其中 MAC 为 4 个字节, 时间戳为 8 个字节, 随机数为 8 个字节, 密钥为 16 个字节, 节点 ID 为 2 个字节, 指数幂运算为 50 个字节, 椭圆曲线为 20 字节. 同时, 对称加密后的消息长度为密钥的整数倍, 公钥加密后消息长度也只是按照所加密的内容长度来计算, Hash 值的长度为 Hash 函数内的消息的长度.

从表 1 的得到的消息长度可以看出, Han 等^[10] 和 RMRAP 协议所消耗的消息长度是最少的, 并且随着子网内中继跳数的增加, RMRAP 的性能更优. 此外, Han 等^[10] 的方案还和周围平均邻居 Sink 的个数 n_c 有关; n_c 较大时, 可以增强方案的漫游范围, 但是也增加了消息长度, 而其他协议均可以实现随机漫游, 与家乡子网和拜访子网的地理位置无关.

计算开销中 CPU 的转数, 主要是依据文献 [27] 提出的各算法执行的对等关系进行估算的. 在主频为 8 MHz 的 Micaz 节点上, 加密算法、CPU 转数及能耗对应关系为^[27]: 128 位的 AES 算法执行的能耗为 38 μJ , CPU 转数为 10742 转; 160 位的 ECDSA 算法执行的能耗为 52 mJ, CPU 转数为 14.7M 转.

表 1 中协议执行的基本加密算法情况如表 2 所示, 为了便于估算出具体计算开销, 还需将各加解密算法折换成文献 [27] 的加密算法. 其中 BCE (block cipher encryption) 和 MAC (message authentication

表 2 协议计算开销
Table 2 The protocol computation overhead

Protocol	Whole computation overhead	Whole energy overhead	Mobile node computation overhead	Mobile node energy overhead
Yang et al. 2007 ^[13]	≥ 10 PKE	≥ 1040 mJ	3 PKE	312 mJ
Yang et al. 2008 ^[14]	6 PKE+4 EXP	1040 mJ	2 PKE+2 EXP	416 mJ
Yang et al. 2010 ^[17]	8.75 ECSM+3 P	1391 mJ	4.5 ECSM+1.5 P	702 mJ
He et al. 2011 ^[18]	15.75 ECSM+4 P	2067 mJ	8 ECSM+2 P	1040 mJ
Han et al. 2010 ^[10]	4 BCE+10 MAC	532 μ J	1 BCE+4 MAC	190 μ J
Ours	4 BCE+8 MAC	456 μ J	1 BCE+2 MAC	114 μ J

code computer) 分别对应 1 AES 算法的耗能; PKE (public key encryption or decryption) 和 EXP (modular exponentiation) 对应 2 个 ECDSA 的耗能; ECSM (elliptic curve scalar multiplication) 对应 1 个 ECDSA 的耗能; P (elliptic curve bilinear pairing) 对应 6 个 ECDSA 的耗能. 计算开销的比较中, 未考虑各协议运行时使用的 Hash 算法的开销. 根据上述关系联合表 2, 就可以获得表 1 关于计算开销的理论估算值.

从表 1 可以直观地看出, 在计算开销上, Han 等^[10]和 RMRAP 的移动节点端低于同类协议. 这主要是由协议设计的目标所决定, Yang 等^[17]和 He 等^[18]的计算放在主频为 8 MHz 的 Micaz 节点上, 运算时间分别为 24.80625 s 和 36.75 s, 这是未考虑通信时延和任务等待的单纯计算时间, 而对于漫游服务来说耗时太长. Han 等^[10]和 RMRAP 的计算耗时分别是 6.7125 ms 和 4.028 ms, 则在计算代价上具有明显的适用性.

身份认证的本地过滤, 是针对传统三方认证协议^[13,14]提出的, RMRAP 协议通过使用 AUTHEN, 在第三方实现对移动节点身份认证前, 在拜访子网本地, 已经可以很好的过滤了一些不合法的加入者, 实现了身份的本地认证, 具体说明见 3.3 小节中对性质 2 的分析.

安全方面的比较, 在抗 DOS 攻击方面, Yang 等^[13]和 Yang 等^[14]的漫游协议都要到固定的家乡子网去进行身份认证, 不可避免的存在 DOS 攻击; Han 等^[10]和我们的 RMRAP 协议, 移动节点到达一个新子网, 取得合法的身份认证之后, 下一次漫游时, 不用回到固定的初始子网获取认证材料, 从而减少 DOS 攻击带来的危害. 组合安全性, 是 RMRAP 相对于其它轻量级协议的一个最显著的特征, 因为轻量级协议在基站使用时, 基站作为连接感知网络和骨干网的网关节点, 运行于感知网络上的轻量级协议不能影响到原有协议的安全目标. 因此在第 4 节完成这样的组合安全认证测试.

5.2 协议仿真

用 NS2-29 对协议进行仿真, 通过传输时延来量化消息长度, 测试 RMRAP 协议的可用性和高效率性. 仿真采用网状网络的拓扑结构, MAC 层协议使用的是 Zheng 等^[28]为 NS2 所写的 802.15.4 协议, 路由层采用具有最短跳数的 AODV 路由协议, 传输层使用的是 UDP 协议, 应用层传输 CBR 数据包, 消息长度如 5.1 小节中所设置的基本长度, 数据的传输速度为 250 KB/s. 采用文献^[28]所推荐的标准信标模式设置. 当相邻基站/簇头数目 $n_c = 1$ 时, 考虑随机漫游平均跳数为 $h_n = 2$, 和 $h_n = 5$ 两类情形. 此时定义了 $n_c = 1$, 只有一个指定的邻居 Sink 可以转发消息, 这样可以淡化 RMRAP 使用传输骨干网带来的益处, 而 Han 等^[10]对所有相邻簇群发消息的消耗也得最大范围的缩减, 即退化为和 Han 等^[10]一样的子网间重认证协议. 图 6 给出了仿真所获取的 500 组数据.

图 6 $h_n = 2$ 和 $h_n = 5$ 的传输时延Figure 6 Time delay while $h_n = 2$ and $h_n = 5$

图 6 中, $h_n=2$ 时, Han 等^[10] 的实际得出的平均时延值为 26.864 ms, RMRAP 的为 18.1056 ms, 对应的 $h_n = 5$ 时, Han 等^[10] 的平均时延值为 60.3689 ms, RMRAP 的为 37.04 ms. RMRAP 时延的仿真效果比理论值分析更好, 这是由于 RMRAP 协议在移动节点端少了一次消息发送, 而每一条消息发送时, 都需要加上额外的 MAC 层包头, 使得实际时延和消息长度在比例上有出入. 图中的波动效果, 主要是 h_n 的多跳性带来的, 在子网内中继节点转发的过程中, 需要消耗转发时延 (节点在转发时要重复接受和发送这个动作, 调用发送接受程序, 查找路由表等, 需要耗费更多的时延), 并且这个时间随着中继跳数 h_n 的增加, 波动性更加明显.

从以上实际仿真测得的传输时延可以看出, 整个 RMRAP 协议的随机漫游认证的过程的时延可以控制在 50 ms 之内, 符合文献 [29] 对漫游协议时延忍受范围的规定, 可以达到实际运用中无缝衔接的需要.

6 总结

随着物联网应用和研究的不断深入, 如何在拥有漫游节点的物联网中将信任关系进行传递和转移, 是其安全中需要重点关注的问题. 目前公认的物联网分为感知、传输和应用 3 个子网, 本文结合该模型设计了一个适合物联网的漫游认证协议 RMRAP. 该协议接入时简单, 离开时随意, 认证和密钥产生都是自动完成的. 安全分析表明设计的协议能够实现身份认证的基本安全需求, 同时满足可组合性、随机漫游、轻量级与隐私保护的需求. 通过性能分析可以得出, 整个方案在通信计算开销上相对较少, 适合资源严重受限的物联网应用.

参考文献

- 1 Mahmoud M E, Shen X. FESCIM: Fair, efficient, and secure cooperation incentive mechanism for multi-hop cellular networks. IEEE Trans Mob Comput, in press
- 2 Mahmoud M E, Shen X. An integrated stimulation and punishment mechanism for thwarting packet drop in multihop wireless networks. IEEE Trans Veh Technol, in press
- 3 Canetti R. Universally composable security: a new paradigm for cryptographic protocols. In: 42nd Annual Symposium on foundations of Computer Science, Las Vegas, 2001. 136–145
- 4 Canetti R. Universally composable security: a new paradigm for cryptographic protocols. Cryptol ePrint Arch, Report 2000/067, 2005

- 5 Perrig A, Szewczyk R, Tygar J D, et al. SPINS: Security protocols for sensor networks. *ACM Wirel Netw*, 2002, 8: 521–534
- 6 Du W, Wang R, Ning P. An efficient scheme for authenticating public keys in sensor Networks. In: *Proceedings of the 6th ACM international Symposium on Mobile Ad Hoc Networking and Computing*, Urbana, 2005. 58–67
- 7 Ibriq J, Mahgoub I. A hierarchical key establishment scheme for wireless sensor networks. In: *Proceedings of 21st International Conference on Advanced Networking and Applications (AINA'07)*, Niagara Falls, 2007. 210–219
- 8 Pietro R D, Soriente C, Spognardi A, et al. Collaborative authentication in unattended WSNs. In: *Proceedings of the 2nd ACM Conference on Wireless Network Security*, Zurich, 2009. 237–244
- 9 Pietro R D, Soriente C, Spognardi A, et al. Intrusion-resilience in mobile unattended WSNs. In: *Proceedings of INFOCOM*, San Diego, 2010. 1–9
- 10 Han K, Kim K. Untraceable mobile node authentication in WSN. *Sensors*, 2010, 10: 4410–4429
- 11 Hwang K F, Chang C C. A self-encryption mechanism for authentication of roaming and teleconference services. *IEEE Trans Wirel Commun*, 2003, 2: 400–407
- 12 Shi M H, Rutagemwa H, Shen X M. A service-agent-based roaming architecture for WLAN/cellular integrated networks. *IEEE Trans Veh Technol*, 2007, 56: 3168–3181
- 13 Yang G M, Wong D S, Deng X T. Anonymous and authenticated key exchange for roaming networks. *IEEE Trans Wirel Commun*, 2007, 6: 1035–1042
- 14 Yang G M, Wong S D, Deng X T. Formal security definition and efficient construction for roaming with a privacy-preserving extension. *J Univ Comput Sci*, 2008, 14: 441–462
- 15 Wan Z, Ren K, Preneel B. A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks. In: *Proceedings of the 1st ACM Conference on Wireless Network Security (ACM WiSec 2008)*, Alexandria, 2008. 62–67
- 16 Pereniguez F, Kambourakis G, Lopez R M. Privacy-enhanced fast re-authentications for EAP-based next generation network. *Comput Commun*, 2010, 33: 1682–1694
- 17 Yang G M, Huang Q, Wong S D, et al. Universal authenticated protocols for anonymous wireless communications. *IEEE Trans Wirel Commun*, 2010, 9: 168–174
- 18 He D J, Bu J J, Chan S, et al. Privacy-preserving universal authentication protocol for wireless communications. *IEEE Trans Wirel Commun*, 2011, 10: 431–436
- 19 Feng T, Li F H, Ma J F, et al. A new approach for UC security concurrent deniable authentication. *Sci China-Ser F: Inf Sci*, 2008, 51, 352–367 [冯涛, 李风华, 马建峰, 等. UC 安全的并行不可否认认证新方法. *中国科学 E 辑: 信息科学*, 2008, 38: 1220–1233]
- 20 Feng T, Ma J F, Li F H. Efficient and universally composable security oblivious transfer. *Acta Electron Sin*, 2008, 36: 17–23 [冯涛, 马建峰, 李风华. UC 安全的高效不经意传输协议. *电子学报*, 2008, 36: 17–23]
- 21 Cao C J, Yang C, Ma J F, et al. An authentication protocol for station roaming in WLAN Mesh. *J Comput Res Dev*, 2009, 46: 1102–1109 [曹春杰, 杨超, 马建峰, 等. WLAN Mesh 漫游接入认证协议. *计算机研究与发展*, 2009, 46: 1102–1109]
- 22 Guo Y B, Wang C, Wang L M. Universally composable authentication and key exchange protocol for access control in spatial information networks. *Acta Electron Sin*, 2010, 38: 2358–2364 [郭渊博, 王超, 王良民. 通用可组合安全的空间网络双向认证与密钥协商协议. *电子学报*, 2010, 38: 2358–2364]
- 23 Guttman J D, Thayer F J. Authentication tests and the structure of bundles. *Theor Comput Sci*. 2002, 283: 333–380
- 24 Doghmi S F, Guttman J D, Thayer F J. Completeness of the authentication test. In: *European Symposium on Research in Computer Security(ESORICS)*, Dresden, 2007
- 25 Guttman J D. Cryptographic protocol composition via the authentication tests. In: *Foundations of Software Science and Computation Structures(FOSSACS, 2009)*, York, 2009
- 26 Watro R, Kong D, Cuti S F, et al. TinyPK: securing sensor networks with public key technology. In: *Proceedings of the 2nd ACM workshop on Security of Ad Hoc and Sensor Networks*, New York, 2004
- 27 Meulenaer G D, Gosset F, Standaert F X, et al. On the energy cost of communication and cryptography in wireless sensor networks. In: *Proceedings of the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WIMOB 2008)*. New York: IEEE Computer Society Press, 2008. 580–585
- 28 Zheng J L, Lee M J. A Comprehensive Performance Study of IEEE 802.15.4. *Sensor Network Operations*. New York: IEEE Press, Wiley Interscience, 2006. 218–237

- 29 Li X H, Lu X, Ma J F, et al. Authentication and key management in 3G-WLAN interworking. *Mob Netw Appl*, 2010, 16: 394–407

Composable-secure authentication protocol for mobile sensors roaming in the Internet of Things

WANG LiangMin^{1,2*}, JIANG ShunRong¹ & GUO YuanBo³

1 School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China;

2 School of Computer and Technology, Anhui University, Hefei 230601, China;

3 School of Electronic Technology, Information Engineering University of PLA, Zhengzhou 450004, China

*E-mail: jasonwanglm@gmail.com

Abstract Internet of Things is composed by sensor subnets and transmission backbone network. Because of the limited capacity of nodes in sensor subnets, the mobile sensor nodes often move from one cluster to another so that they can access and obtain cross-region information. The backbone transmission network depends on the existing Internet infrastructure and provides powerful services. In this case, the roaming of mobile nodes brings about some new security problems. On one hand, we should ensure that the mobile node joins the new foreign cluster efficiently and securely during roaming, which looks like roaming demand in MANET. However it should be much more light weight because sensor nodes' resource is extremely limited. On the other hand, the security of mobile nodes is light weight which is different from that of backbone networks. The security level of backbone network should not be reduced by a mobile node roaming and joining a new cluster. So the authentication protocol should be composable security, when the light weight secure protocol connects with traditional backbone network protocol. In this paper, we focus on the sensor nodes roaming problem based on the Internet of Things, and propose a new random roaming authentication protocol (RMRAP). Our RMRAP takes into account both the security and feasibility of practical application. The protocol achieves the light weight authentication and protects the privacy of the mobile node while roaming among the clusters and generates forward security session key. We also test the composable security at cluster head which connects the backbone network and the sensor subnet serving as a gateway. We also analyze the performance of RMRAP protocol in both the theoretical analysis and experiment simulations, and compare it with some related work. The comparison shows that our RMRAP has some advantages of compose security, computation and communication overheads over these related protocols.

Keywords wireless sensor networks, network security, authentication, privacy protection, light weight

WANG LiangMin received his B.S. degree in computational mathematics in Jilin University, Changchun in 1999, and the Ph.D degree in cryptology from Xidian University, Xi'an in 2007. He has also worked with Prof. Alex KOT for a year in School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore. Currently, he is an Associate Professor in School of Computer Science and Communication Engineer, Jiangsu University, Zhenjiang, China. Now his research interests include security protocols and wireless sensor networks. Dr. Wang is a senior member of Chinese Computer Federation and a member of Chinese Cryptology Federation. He is also a member of AICIT Conference.

GUO YuanBo received his B.S. and M.S. degree in computer science from Information Engineering University, Zhengzhou in 1997 and 2000, and the Ph.D. degree in computer applications and technology from Xidian University, Xi'an in 2005. Currently, he is an Associate Professor in School of Electronic Technology, Information Engineering University, and his research interests include systems survivability

and wireless network security. Dr. Guo is a senior member of Chinese Institute of Electronics and a member of Chinese Computer Federation.

JIANG ShunRong was born in 1986. He is studying for the M.S. degree at Jiangsu University. His research interests include wireless sensor network security and cryptographic protocols.