

无线传感器网络用户认证协议研究进展

房卫东¹, 张武雄^{1,2}, 单联海^{1,3}, 何为¹, 陈伟⁴

(1. 中国科学院上海微系统与信息技术研究所无线传感器网络与通信重点实验室, 上海 200051;

2. 上海无线通信研究中心, 上海 201210;

3. 上海物联网有限公司, 上海 201899;

4. 中国矿业大学计算机科学与技术学院, 徐州 221116)

摘要: 无线传感器网络 (WSN, wireless sensor network) 用户认证技术是传感器网络验证用户的合法性以避免网络数据信息泄露的有效手段之一, 同时, 用户也需验证传感器网络的合法性, 避免获得错误或虚假数据信息。由于 WSN 节点能量、通信和计算能力等资源受限, 且通常部署在敌对或无人值守的区域, 因此传统用户认证协议并不完全适用于 WSN。从 WSN 认证协议的安全攻击入手, 给出其安全需求及理论基础, 归纳总结了设计流程, 针对其安全性分析, 描述了安全攻击模型, 并综述了形式化分析验证工具 AVISPA 体系结构和 HLPSL 语言构成。评述了当前的各种 WSN 用户认证协议, 建议了未来研究方向, 这些研究工作将有助于 WSN 用户认证协议的设计、分析与优化。

关键词: 无线传感器网络; 安全性; 用户认证协议; 双因素; 三因素

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00129

Survey on user authentication protocol in wireless sensor network

FANG Wei-dong¹, ZHANG Wu-xiong^{1,2}, SHAN Lian-hai^{1,3}, HE Wei¹, CHEN Wei⁴

(1. Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200051, China;

2. Shanghai Research Center for Wireless Communication, Shanghai 201210, China;

3. Shanghai Internet of Things Co., Ltd, Shanghai 201899, China;

4. School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China)

Abstract: In wireless sensor network (WSN), the user authentication technology is an effective approach, which can guarantee the user's validity, avoid WSN's information disclosure. Meanwhile, the users also need to verify the WSN's validity, avoid obtaining incorrect or false information. However, since the sensor nodes have limited energy, communications and computing capacity, and they are usually deployed in hostile or unattended environment, the traditional user authentication protocol (UAP) is not entirely suitable for WSN. The security attacks were introduced for the UAP in WSN, its secure requirements and the theoretical foundation were given, and then the UAP's design processes were summarized. For the analysis of its security, the attack model was described, and the automated validation of internet Security protocols and applications (AVISPA) and the high level protocols specification language (HLPSL) were overviewed in detail. Then, the current UAPs were reviewed in WSN, the future research directions were proposed. These researches will contribute to the design, analysis and optimization for the UAP in WSN.

Key words: WSN, security, user authentication protocol, two-factors, three-factors

收稿日期: 2016-10-17; 修回日期: 2016-11-25。通信作者: 张武雄, wuxiong.zhang@mail.sim.ac.cn

基金项目: 国家自然科学基金资助项目 (No. 61471346); 上海市自然科学基金资助项目 (No. 14ZR1439700); 国家科技重大专项基金资助项目 (No. 2014ZX03005001); 上海市科技重大基金资助项目 (No. 15DZ1100400); 中国科学院科技服务网络计划基金资助项目 (No. kfj-sw-sts-155); 国家自然科学基金委员会—山西省人民政府煤基低碳联合基金资助项目 (No.U1510115)

Foundation Items: The National Natural Science Foundation of China (No. 61471346), Shanghai Natural Science Foundation (No. 14ZR1439700), The National Science and Technology Major Project (No. 2014ZX03005001), Shanghai Municipal Science and Technology Committee Program (No. 15DZ1100400), Science and Technology Service Network Program of CAS (No. kfj-sw-sts-155), The National Natural Science Foundation and Shanxi Provincial People's Government Jointly Funded Project of China for Cool Base and Low Carbon (No.U1510115)

1 引言

随着窄带物联网 (NB-IoT, narrow band Internet of things) 标准化工作逐步完成^[1], 无线传感器网络作为前端信息感知的关键环节, 具有无可替代的重要性。目前, 无线传感器网络不但是学术界研究的热点之一, 同时, 也是产业界持续关注重点之一。对无线传感器网络而言, 产业界关心它的应用场景, 当前, 无线传感器网络已经广泛应用于多种领域, 如智慧城市^[2]、智能交通^[3]、环境监测^[4]、精准农业^[5]、远程医疗监测^[6]; 学术界则关注它的关键技术, 如路由协议与接入协议^[7]、图像识别与目标跟踪^[8]、能耗均衡与能量有效性^[9]、可信传输与信任管理机制^[10]。有一个方面是两者共同关心的, 即信息安全。对此, 学术界研究的目标之一是保障感知数据通过有效的安全机制 (如安全网络编码^[11]、安全路由协议^[12]、安全数据融合^[13]), 真实完整地传送给最终用户; 产业界的需求是即便在 WSN 遭受攻击的状态下, 依然能准确实时地完成既定的任务与功能。

无线传感器网络的安全威胁主要来源于安全攻击。这类安全攻击通常分为内部攻击 (internal attack) 与外部攻击 (external attack)^[14]。在外部攻击中, 攻击节点不是传感器网络授权的合法节点; 而节点妥协是导致内部攻击的主要因素, 与停用节点 (disabled node) 相反, 妥协节点 (compromised node) 积极寻求机会破坏或瘫痪网络。除此之外, 还有一种情况值得关注, 即用户访问 WSN 节点感知信息过程中的信息安全问题。目前, 用户获取节点感知信息有 2 种方式。一种是通过基站或网关节点, 发送查询指令, 获取相应节点回传的信息。这种方式的安全性由 WSN 安全策略保证, 但存在时延较大等问题, 适用于信息轮询或信息上传周期较长的应用场景。另一种是用户不通过基站或网关节点, 而是直接登录访问传感器节点获得实时数据, 该方式具有较高的实时性, 但用户合法性的认证就变得十分重要, 此种方式下一旦非法用户登录到传感器节点, 将造成传感器节点数据泄露, 危及整个 WSN 应用系统安全^[15], 同时, 在用户合法性认证过程

中, 用户对于 WSN 网络合法性判定同样重要。若用户访问并获取了错误或虚假的信息, 则对后续的数据处理产生难以预料的后果, 另外, 在认证过程中, 用户的隐私信息 (如用户身份、位置等) 同样是需要被保护的, 否则, 可能被攻击者追踪、甚至是破解、伪造。因此, 用户认证协议是保证 WSN 安全和用户隐私的一项重要安全机制。

目前, 尽管对 WSN 用户认证协议的研究较多, 但成果多散见于各种期刊与书籍的章节中, 系统性的研究综述较少, 另一方面, 随着各种智能终端的大量普及, 从应用的角度也需要对 WSN 用户认证协议进行评述。本文充分考虑无线传感器网络的节点资源受限、传输媒介开放以及部署环境复杂多样等技术特性, 围绕 WSN 用户认证协议的需求、设计以及安全性分析, 对近几年典型的 WSN 用户认证协议从双因素用户认证协议和三因素用户认证协议这 2 个方面进行了较为系统的综述, 并给出了未来的研究方向, 希望本文的工作能够有助于后续无线传感器网络用户认证协议的设计、分析与优化。

2 WSN 用户认证协议的设计

无线传感器网络用户认证过程的安全威胁主要来源于安全攻击。这类安全攻击通常分为内部攻击与外部攻击。本节通过对安全攻击的描述, 概述 WSN 用户认证协议安全需求, 在给出 WSN 用户认证协议设计理论基础上, 系统地阐述 WSN 用户认证协议的设计流程。

2.1 WSN 用户认证协议的安全攻击

WSN 用户认证协议存在的主要安全攻击可分为内部攻击和外部攻击^[16,17]。

1) 内部攻击

内部特权攻击 (privileged-insider attack): 当系统管理方误用或泄露用户密码及其他秘密参数时, 可能导致在同一系统或其他与之相连接的系统内触发安全攻击。

2) 外部攻击

节点妥协攻击 (node compromise attack): 攻击者妥协传感器节点, 利用节点存储的参数信息发动其他安全攻击。

密码猜测攻击 (password guessing attack):

用户为方便记忆密码,通常选择一些熟悉数字(如生日、电话号码等低熵信息)作为登录密码,因此攻击者可以从含该密码的密码池中成功猜测出用户密码。此外,攻击者可以通过密码相关参数与密码之间的关联性,猜测用户密码。

网关节点模拟攻击 (gateway node impersonation attack): 攻击者截取并篡改网关节点发送的消息,模拟网关节点与用户或传感器节点通信。

中间人攻击 (man-in-the-middle attack): 攻击者通过读取并创建通信双方的传输消息,使通信双方以攻击者作为中间人进行通信,而不知道攻击者的存在。

智能卡丢失攻击 (smart card loss attack): 当用户智能卡丢失或被窃取时,攻击者可以获得智能卡存储的参数信息,发动安全攻击,并可能在智能卡中注入错误信息。

重放攻击 (replay attack): 攻击者重放之前截取的传输消息,实现登录传感器网络,或欺骗用户相信其是合法传感器网络。

拒绝服务攻击 (denial-of-service attack): 任何能引起传感器网络拒绝提供服务的恶意或错误的攻击行为。

相同身份标识多重用户登录攻击 (many logged-in users with the same login-ID attack): 不同的用户利用相同的身份标识登录传感器网络,获取传感器节点的数据信息。

验证—窃取攻击 (stolen verifier attack): 某些与用户相关的数据存储在网关节点或传感器节点密码表或验证表中,攻击者窃取密码表或验证表,获得用户相关数据,并假装是协议合法参与实体。

2.2 WSN 用户认证协议安全需求

针对上述的安全攻击,为保障无线传感器网络用户认证协议的安全,所设计的协议需满足以下安全需求^[16]。

1) 用户和网关节点间的双向认证: 防止攻击者模拟网关节点或用户发动攻击。

2) 网关节点和传感器节点间的双向认证: 防止网关节点丢弃用户相关信息、伪造传感器节点、误导合法用户做出错误的决策等。

3) 用户和传感器节点间的双向认证: 防止传

感器节点提供错误的数据或服务。

4) 用户自由更新密码: 降低密码泄露对传感器网络和用户的威胁。

5) 用户匿名: 保护用户隐私,避免被攻击者追踪。

6) 智能卡修复性: 智能卡丢失或被攻击者窃取时,易被攻击者或非法用户误用,因此,当智能卡丢失或被窃取时,必须及时撤销智能卡。

7) 会话密钥: 用于传感器节点和用户间的安全通信,保护传输消息的机密性。

2.3 WSN 用户认证协议设计的理论基础

WSN 用户认证协议设计过程中,常用操作的理论基础如下。

1) 散列操作

$h: \{0, 1\}^* \rightarrow \{0, 1\}^l$, 任意长度比特输入 $X \in \{0, 1\}^*$, 产生固定比特输出 $h(X) \in \{0, 1\}^l$, 称为消息摘要。散列操作是文件、消息和其他数据组的“指纹”,有以下特性^[18]。

①任意长度的数据组都能应用散列操作 h 。

②给定变量 X , $h(X)$ 容易操作,易于在软件和硬件上实现。

③输出 $h(X)$ 的长度固定。

④给定 $Y=h(X)$ 和 $h(\bullet)$, 计算得出 X 是不可行的。

⑤给定变量 X , 对任何 $Y \neq X$, 得出 $h(Y) \neq h(X)$ 在计算上是不可行的。

⑥对于 (X, Y) , $Y \neq X$, 得出 $h(Y) \neq h(X)$ 在计算上是不可行的。

散列操作已经应用到很多领域中,如加/解密、信息安全、数字签名、消息认证码及其他形式的认证方法,是很多加密协议的基础。散列操作对输入变化敏感,只要输入有 1 bit 变化,就会引起输出很大变化。

2) 异或操作

异或操作是一种逻辑数字位运算,用符号 $\oplus$ 表示,如 $a \oplus b$, 如果 a 、 b 的值相同,则其结果为 0; 如果 a 、 b 的值不相同,则其结果为 1; 此外,异或操作还有一项重要特性,已知 A 、 C , 且 $A=B \oplus C$, 则 $B=A \oplus C$, 因此,常在用户认证协议中利用异或操作这一特性恢复数据信息。

3) 连接操作

连接操作是一种数字位连接操作, 用符号 $\parallel$ 表示, 用于增强数据的复杂度, 以提高数据的安全性, 如 $a \parallel b$ 表示 a 、 b 的级联。

4) 加密操作

因为传感器网络节点资源的限制, WSN 主要利用对称加密算法, 如 RC5 和 AES (advanced encryption standard) [19,20]。

① RC5: RC5 是适合软硬件操作的快速对称分组加密算法, 其加密文本长度、加密轮数和密钥长度都是可变的。因此, 可以权衡资源和安全需求, 调整加密文本长度、加密轮数和密钥长度, 使之能适用于资源受限、安全面临严峻挑战的 WSN。

② AES: AES 是一种迭代分组加密算法, 主要由线性组件、非线性组件和轮密钥组成。可以利用 128 bit、192 bit 和 256 bit 的密钥加密 128 bit 的数据, 加密轮数依赖预定密钥的大小, 通常执行 10 轮、12 轮或 14 轮。由于 WSN 资源受限, 使用 AES 加密时, 密钥长度取 128 bit, 执行 10 轮加密。

5) 模糊信息提取器

模糊信息提取器 Fuzzy Extractor(M, l, t) 是一种由 Gen 函数和 Rep 函数组成的信息提取函数[21]。

① Gen 是安全密钥生成函数, 输入生物特征标识信息 $B_i \in M$, 其中, 度量空间 M 是距离函数 $M \times M \rightarrow IR^+ = [0, \infty)$, 输出安全数据密钥 $\delta_i \in \{0, 1\}^l$ 和公共辅助参数 τ_i 。

$$B_i \rightarrow Gen \rightarrow \begin{cases} \delta_i \\ \tau_i \end{cases}$$

② Rep 是安全密钥再生函数, 输入生物特征标识信息 $B'_i \in M$ 和 τ_i , 重新生成的安全数据密钥 $\delta'_i \in \{0, 1\}^l$ 。

$$\begin{Bmatrix} B'_i \\ \tau_i \end{Bmatrix} \rightarrow Rep \rightarrow \delta'_i$$

以上安全手段可以根据具体的场景需要, 进行有效组合, 进而最终设计出满足用户特征需求的用户认证协议。

2.4 WSN 用户认证协议的设计

因为无线传感器网络中传感器节点在能源、存储、通信和计算能力等方面资源受限, 而且通

常部署在敌对环境或无人值守的户外区域, 无线信道的开放性使 WSN 用户认证协议的设计与传统网络用户认证协议的设计有较大的差别, 此外, WSN 应用导向性也使其设计要充分考虑应用场景的特性。

因此, 实用的 WSN 用户认证协议应该满足以下原则。

- ① 传感器节点的计算量要低。
- ② 有足够的安全性, 可以防御多种安全攻击。
- ③ 满足必要的安全需求。
- ④ 协议内容必须是简洁正确, 无冗余。

WSN 用户认证协议通常由注册阶段、登录阶段、认证阶段和密码更新阶段组成, 各阶段流程如下。

1) 注册阶段

网关节点通常充当注册中心, 用户向网关节点提交用户身份标识、密码和生物特征标识等相关特征信息, 网关节点基于用户提交信息进行相关计算, 生成参数信息并存储在对应用户的智能卡中, 如图 1 所示。

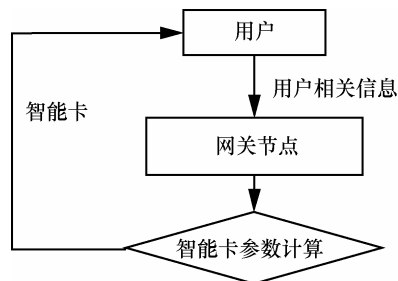


图 1 注册阶段

2) 登录阶段

用户把智能卡插入读卡器终端, 输入身份标识、密码和生物特征标识等用户相关信息。智能卡基于用户输入信息进行验证计算, 如果用户能成功通过智能卡验证, 则继续下一步操作; 如果不能, 则终止操作, 如图 2 所示。

3) 认证阶段

网关节点根据用户登录请求信息进行验证计算, 验证用户的合法性, 如果用户能成功通过验证, 则网关节点向传感器节点发送应用请求消息。传感器节点根据应用请求消息验证网关节点和用户的合法性, 如果网关节点和用户都能成功通过节点认证, 则生成会话密钥, 向用户发送回应消

息。收到传感器节点发送的回应消息后，用户首先验证节点的合法性，如果节点成功通过验证，则生成会话密钥；如果不能通过验证，则终止操作，如图3所示。

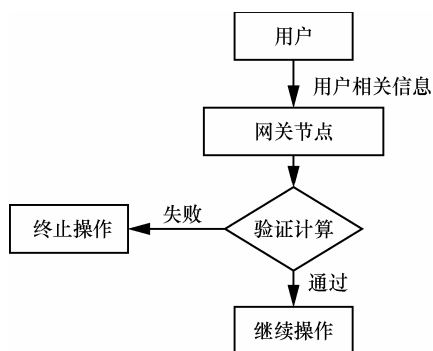


图2 登录阶段

4) 密码更新阶段

当用户和网络遇到威胁或用户密码使用时间过长时，需更新用户密码以提高网络和用户安全性。用户更新密码时，输入用户原有身份标识、密码和生物特征等信息，智能卡基于用户相关信息进行验证计算，若用户成功通过智能卡验证，则输入新密码，生成新的密码参数信息替换原有参数信息；若不能通过智能卡验证，则终止操作。如图4所示。

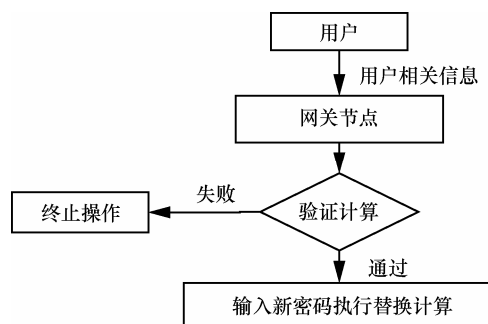


图4 密码更新阶段

3 WSN 用户认证协议的安全性分析

3.1 攻击者威胁模型

无线传感器网络通常部署在开放式的无线通信环境中，因此其安全性易受到威胁。文献[22,23]提出一个在非安全开放式通信中的攻击者威胁模型，即 Dolev-Yao 模型。

Dolev-Yao 攻击者模型定义如下。

- 1) 攻击者可以获得所有经公共信道传输的消息。
- 2) 攻击者可以冒充其他通信实体向用户发送消息。
- 3) 攻击者不能获得正确的随机数。

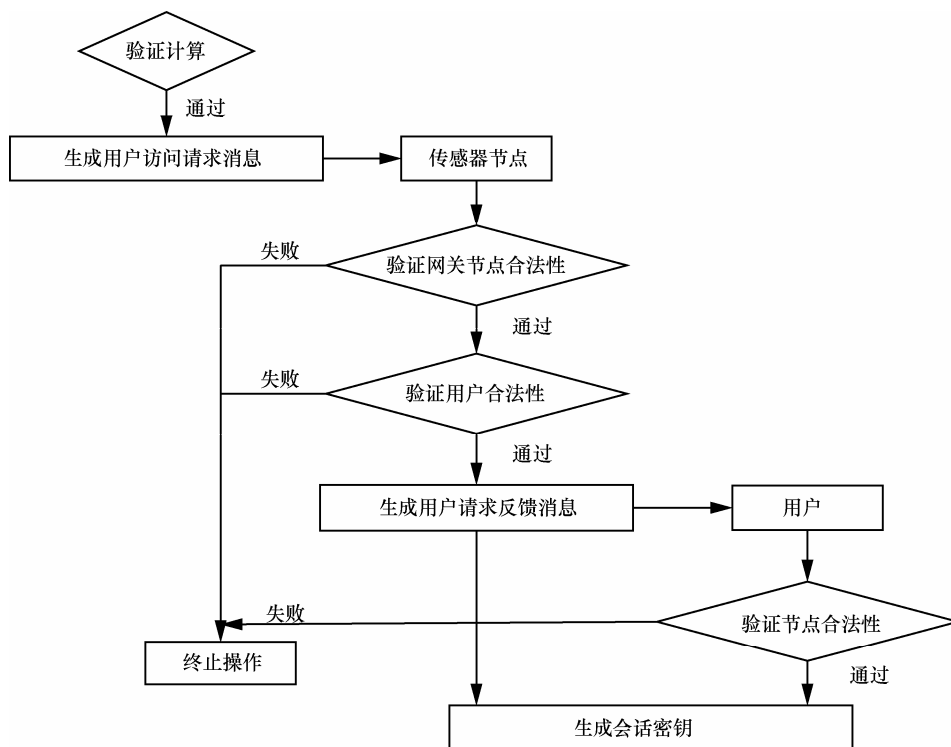


图3 认证阶段

- 4) 攻击者没有正确的密钥就不能解密消息。
- 5) 攻击者不能破坏加密算法。

针对 WSN 用户认证协议特性, 在分析用户认证协议安全性时, 文献[24]拓展了 Dolev-Yao 攻击者模型, 并做以下假设。

- 1) 传感器节点没有配置防篡改装置, 攻击者可以妥协传感器节点, 窃取传感器节点存储的参数信息。
- 2) 攻击者一旦获得用户的智能卡, 可以获得卡中存储的参数信息。
- 3) 为方便记忆, 通常用户身份标识和密码是低熵的。
- 4) 网关节点是诚实的。

3.2 安全协议形式化分析工具 AVISPA

AVISPA (automated validation of Internet security protocols and applications) 是一种用于构建网络安全协议及其自动验证的形式化工具^[25,26], 由4种不同的分析终端模块组成, 如图5所示。

1) OFMC (on-the-fly-model-checker) 模块: 通过符号技术以需求驱动方式探索状态空间, 支持与密码相关的一些数学操作。

2) CL-AtSe (constraint logic based attack searcher) 模块: 利用简化探测法和冗余排除法运行安全协议。

3) SATMC (SAT-based model-checker) 模块: 通过构建一个命题公式, 输入 SAT 状态求解器,

验证安全协议是否存在安全攻击。

4) TA⁴SP (tree automata based on automatic approximations for analysis of security protocols) 模块: 采用树形语言和重写机制评估攻击者能力, 根据不同的保密性评估安全协议是否存在缺陷。

采用 AVISPA 工具形式化验证安全协议, 需把安全协议内容转换为 HLPSSL 语言 (high level protocols specification language), HLPSSL 是一种表达能力丰富的形式化语言, 指定协议控制模式、数据结构、替代入侵模型、复杂安全属性和加密原语及其代数性质。HLPSSL 语言的基础是角色 (role), 通过角色的构建描述安全协议。HLPSSL 语言基本类型元素及其意义如下^[27]。

agent: 表示协议参与主体名称, 其中, 攻击者名称用 *i* 表示。

public_key: 表示主体公钥, 如果 *ku* 表示公钥, 则其私钥用 *inv_ku* 表示。

symmetric_key: 表示对称密钥。

channel(by): 表示 Dolev-Yao 模型信道。

text: 表示随机数和构建的消息, 如果 R_a 的类型为 *text (fresh)*, 则攻击者不能猜测 R_a 的具体数值。

nat: 表示非消息上下文中的自然数。

const: 表示常数。

Hash_func: 表示单向散列操作。

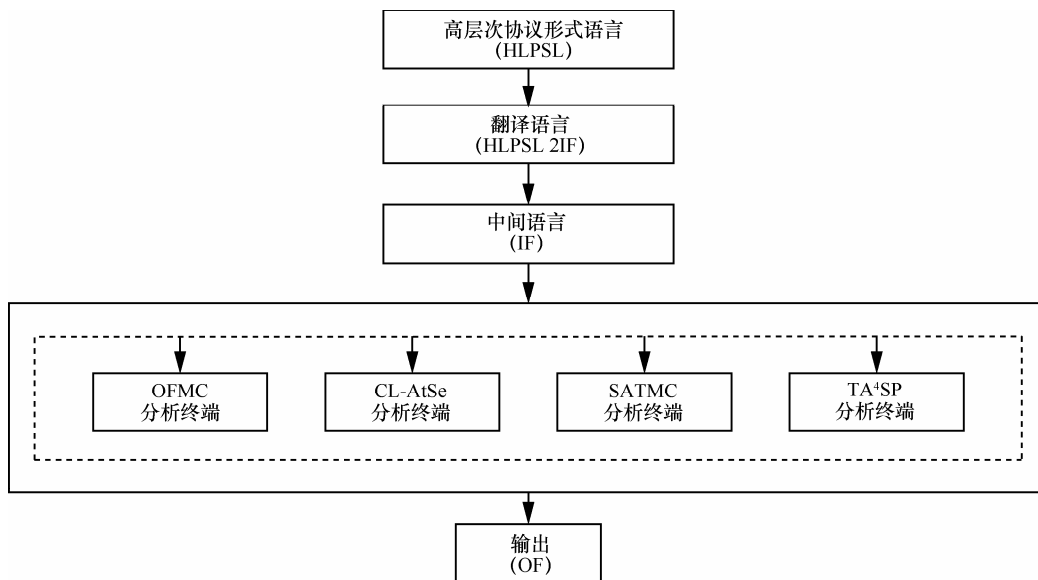


图5 AVISPA 体系结构

3.2.1 角色

在 HLPSL 中,角色被当作是对行为的具体描述,通过参数化实现,可存在一种或多种参数类型,通过 *exists* 操作声称局部标量。角色可分为基本角色和构造角色,基本角色用于描述单个协议或子协议运行时的主体行为,而构造角色由一个或多个其他角色组成,用于描述系统组件间的交互行为。

角色通常通过以下因素定义。

1) 角色声明:包括名称、形参列表和主体声明,如

```
Role trivial(A:agent, Ka:public_key) played_
by A def=
```

```
exists State: nat, Na:text (fresh)
```

```
init State = 0
```

```
end role
```

角色 *trivial* 声明局部变量 *State* 和 *Na*, *State* 初始化为 0。

2) 局部标量和自有规则声明,如

```
Role A(Id: nat, X: text) played_by Id def=...
```

```
End role
```

```
Role Many_As(X: text) def=
```

```
owns X
```

```
composition
```

```
A(1, X)  $\wedge$  A(2, X)
```

```
end role
```

表示角色 *A* 可以写出 *X*, 但不拥有 *X*, 其中 $\wedge$ 表示集合中所有元素的连接。

3) 变量初始化 (有需要), 如

```
exists Kr: agent  $\rightarrow$  public_key set
```

```
Init
```

```
 $\Lambda_{\{in(A, Agents)\}} Kr(A)=[ ]$ 
```

表示密钥环初始化为空集。

4) 状态接收声明, 如

```
accept State = 5  $\wedge$  Auth = 1
```

表示当 *State*=5、*Auth*=1 时, 认证成功。

5) 知识声明, 如

```
role Alice(A, S: agent, Ka, Ks: public_key)
```

```
play_by A def=
```

```
... % other role headers
```

```
knowledge (A)={inv (Ka), {A, Ka}inv(Ks)}
```

```
... % role body
```

```
end role
```

表示角色 *A* 拥有密钥 *Ka* 和 *S* 分配的证书。

3.2.2 变迁

HLPSL 语言中各个角色行为和状态组成了角色的复合及对话,是状态变迁的基础。状态变迁表示角色消息的发送和接收。一般情况下,一个变迁由一个预处理或一个触发者和一个触发事件行为组成,用符号= $\mid$ >表示,左边表示触发和预处理事件,右边表示触发和预处理事件产生的行为,如

```
STEP 1. State =  $\mid$ >1RRCV({Kab}_Kas)
```

```
= $\mid$ > State:=3SSND({Kab}_Kbs)
```

其中, *STEP1* 表示变迁名称,当 *State*=1 时接收触发消息,利用 *Kas* 加密 *Kab* 后变迁,得到 *State*=3,并发送消息变迁执行完成。

AVISPA 分析终端模块的输出格式如下。

1) SUMMARY: 表示协议是否安全、不安全或没有结论。

2) DETAILS: 说明协议测试条件是否安全、不安全或没有结论。

3) PROTOCOL: 表示协议名称。

4) GOAL: 表示协议目标。

5) BACK END: 表示应用的分析终端模块名称。

由于 AVISPA 中的 OFMC 分析终端模块支持对异或操作的分析,因此,可以有效地利用 OFMC 分析终端模块验证用户认证协议是否存在重放攻击、中间人攻击和被动攻击的风险。

4 WSN 用户认证协议研究现状与分析

为了实现无线传感器网络用户认证的需求,通常基于以下 3 类因素设计用户认证协议^[28]。

1) 所“拥有”(what has)因素,具备存储功能和信息处理功能,如智能卡。

2) 所“知道”(what knows)因素,具有机密性,如密码。

3) 所“独有”(what owns)因素,具有唯一性,如指纹、虹膜、掌纹等生物特征标识。

本节结合“双因素用户认证协议”与“三因素用户认证协议”,对无线传感器网络用户认证协

议的研究现状进行综述并分析。

4.1 WSN 双因素用户认证协议

WSN 双因素用户认证协议结合了用户所“拥有”因素和用户所“知道”因素,即智能卡和用户密码。其中,智能卡是一种内置集成电路的芯片,具备存储功能和信息处理功能,可以存储有关用户的个人化参数和数据,可以嵌入加密程序执行加解密操作,广泛应用于身份识别和验证。结合智能卡和密码,业界已经提出了多种 WSN 双因素用户认证协议。

Wong 等^[29]提出了一种仅利用散列操作和异或操作的简单用户认证协议,该协议允许系统配置移动装置接口,用户可以根据具体应用特性,在某一段时间内直接访问传感器节点的数据。在查询过程中,为成功登录网络,用户和距离其最近的传感器节点区域联系在一起,当预定时间截止后,用户需根据将来需求重新注册。Jamil 等^[30]指出 Wong 协议由于传感器节点要直接处理用户请求,会引起更多的网络流量,增加传感器节点能耗,因此提出了一种新的用户认证协议:传感器节点身份标识信息被嵌入到网关节点和传感器节点的防篡改芯片中,每个传感器节点身份标识是唯一的,彼此不重复。除了身份标识信息的分配,Jamil 协议不需复杂的计算能力,而身份标识信息的比特数短,因此不需要较大的内存,然而 Jamil 协议只适合小规模 WSN,如要应用到大规模 WSN 需进一步改进和提高。Tseng 等^[31]发现 Wong 协议不能防御重放攻击、验证—窃取攻击,因此提出了一种优化的用户认证协议,通过增加计算量以提高其安全性,允许用户自由更新密码提高静态密码安全。Lee^[32]指出 Wong 协议在每一次登录请求过程中,传感器节点计算消耗高于网关节点,不适合资源受限的传感器节点,因此提出了 2 种改进的用户认证协议:第一种改进协议在维持同样安全水平的条件下减少传感器节点的计算量;第二种改进协议使传感器节点取代网关节点对用户认证做最终决策,避免了攻击者通过模拟网关节点访问网络,但第二种协议的计算量和通信量均高于第一种协议。Kiani 等^[33]提出了一种改进的 Wong 用户认证协议,可以防御重放攻击和密码猜测攻击等,然而该协议只适合静态

环境,不适合拓扑频繁变换的动态环境。Ko^[34]指出 Tseng 协议不能实现用户和传感器节点及网关节点和传感器节点间的双向认证,而且攻击者通过截取登录请求消息,可以伪造合法用户的登录消息,通过在经过公共信道或不安全网络传输的消息上附加时间戳,提出了一种改进的用户认证协议。Vaidya^[35]在 Wong 协议^[29]和 Tseng 协议^[31]的基础上,提出了一种新的用户认证协议,该协议可以实现网关节点和传感器节点间双向认证,然而与 Wong 协议^[29]、Jamil 协议^[30]和 Lee 协议等^[32]认证协议相比较,其对计算能力要求较高,不适用于资源受限的 WSN。Faye^[36]等指出由于缺少传感器节点的密码验证机制,Vaidya 协议不能防御拒绝服务攻击,不能完全防御网关节点模拟攻击,因此提出了一种新的用户认证协议,尽管 Faye 协议提高了安全性,但也增加了计算量。Das^[37]提出了一种新的用户认证协议,该协议能抵御多种安全威胁,如相同身份标识多重用户登录攻击、密码猜测攻击、模拟攻击、重放攻击和验证—窃取攻击。Nyang-Lee^[38]发现 Das 协议不能防御密码猜测攻击、节点妥协攻击,没有保护来自传感器节点的用户请求回应消息的机密性,因此提出了一种改进的用户认证协议,该协议提高了用户和传感器节点间通信安全性,在不增加其他安全操作的情况下,可以有效地防御密码猜测攻击,但 Nyang-Lee 协议没有改进 Das 协议易遭受拒绝服务攻击的安全缺陷。Huang 等^[39]指出 Das 协议不能防御相同身份标识多重用户登录攻击,不能实现用户匿名的缺陷,提出了一种优化的用户认证协议,该协议在继承 Das 协议优点的基础上,实现用户匿名,允许用户自由更新密码。Chen 等^[40]发现 Das 协议不能实现用户和网关节点间的双向认证,易遭受并行会话攻击,因此提出了一种优化的用户认证协议。Khan 等^[41]发现 Das 协议不能防御内部特权攻击、网关节点旁路攻击、用户密码不能更新等安全缺陷,提出了一种改进的用户认证协议,允许用户自由更新密码,用户向网关节点提交密码的散列值而不是密码明文,网关节点与用户和传感器节点共享不同的密钥。Vaidya 等^[42]发现 Das 协议易遭受网关节点模拟攻击,当智能卡丢失或被窃取时,易遭受防御

密码猜测攻击的缺陷,提出了一种改进的用户认证协议。He 等^[43]发现 Das 协议不能有效防御内部特权攻击、内部特权攻击引起的网关节点模拟攻击的缺陷,提出了一种改进的用户认证协议,该协议允许用户自由更新密码。Kumar 等^[44]指出 He 协议不能实现用户和传感器节点间的双向认证,没有建立用户和传感器节点间的会话密钥,存在传输消息泄露的可能性,不能实现用户匿名性的缺陷。Tan^[45]指出如果用户智能卡丢失或被攻击者窃取,则 Khan 协议存在密码猜测攻击的可能性,因此提出了一种新的用户认证协议,该协议可以有效地防御密码猜测攻击,避免用户密码散列值泄露,然而 Tan 协议不能实现用户匿名,用户和网关节点及用户和传感器节点间没有实现双向认证,没有建立安全会话密钥。Fan 等^[46]提出了一种分层 WSN 双因素用户认证协议。该协议的设计考虑了 WSN 的技术特性,实现了计算量的降低与安全性的提高。Fan 协议采用散列函数、级联操作和异或操作,未使用加密操作,可以有效防御智能卡丢失攻击、验证—窃取攻击、重放攻击和拒绝服务攻击,适用于资源受限的 WSN,但无法抵御节点妥协攻击、密码猜测攻击以及内部特权攻击等。

4.2 WSN 三因素用户认证协议

结合智能卡和密码的双因素用户认证协议无法完全满足 WSN 在高安全级别场景的应用需求,如军事、国家安全、博物馆、银行。为了提高用户认证协议的安全性,在结合智能卡、密码的基础上,引入用户“独有”因素,即用户生物特征标识,构建 WSN 三因素用户认证协议,以满足高安全级别环境的应用。常用生物特征标识包括指纹、脸型、手型和掌纹等,用户“独有”因素优点有:不会丢失或忘记、不易被复制、不易伪造或分配、不易被猜测、不易破坏其他的生物特征标识^[47]。

随着模式识别技术和生物技术的快速发展,近年来,研究人员已提出多种结合智能卡、密码和生物特征标识的三因素用户认证协议。

Lee 等^[48]提出了一种基于指纹的远程三因素用户认证协议,但该认证协议不能防御用户模拟攻击。Li 等^[49]提出了一种基于生物特征密钥

的三因素用户认证协议,利用生物特征标识验证用户的合法性,但该协议不能有效防御拒绝服务攻击。Lee 等^[50]发现 Li 协议存在安全缺陷,提出了一种改进的三因素用户认证协议,然而该协议不能防御重放攻击,不能实现用户匿名。Das^[51]发现 Li 协议认证阶段不能有效实现双向认证,密码更新阶段存在安全缺陷,提出了一种新的三因素用户认证协议。Sekhar 等^[52]发现 Das 协议存在安全缺陷,不能防御用户模拟攻击、重放攻击和网关节点旁路攻击,提出了一种改进的三因素用户认证协议。An^[53]证明 Das 协议存在安全缺陷,不能防御密码猜测攻击、用户模拟攻击、服务器伪造攻击和内部特权攻击,提出了一种改进的三因素用户认证协议,并宣称其提出的认证协议的安全性高于相关认证协议。Chaturvedi 等^[54]针对 Li 协议和 An 协议存在的安全缺陷提出了一种改进的三因素用户认证协议。Yuan 等^[55]提出了一种新的 WSN 三因素用户认证协议,然而该协议没有保证交换消息的完整性,不能防御节点妥协攻击和拒绝服务攻击。Yoon 等^[56]针对 Yuan 协议存在的缺陷提出了一种用户认证协议,尽管改进了 Yuan 协议,但其依然存在安全缺陷,如传感器节点与用户间没有建立会话密钥、没有考虑传输消息的机密性、不能防御拒绝服务攻击。

4.3 未来研究方向

能量供给、计算能力、存储能力等资源受限是无线传感器网络的重要特征,能量受限已成为制约大范围、长期部署 WSN 的最主要因素之一,然而现有的用户认证协议往往需要较大的通信量、计算量和能量消耗,影响网络的生命周期。能耗和安全是 WSN 最为敏感的因素,当前传感器网络的用户认证协议,多数的出发点以安全为主,无论是基于公钥算法的认证协议,还是基于秘密共享的认证协议,以及动态认证协议等均需要对密钥的生成、分发等进行管理,故内存和计算开销较大,这对计算能力有限的节点来说是不小的挑战。同时,在交互消息的某些信息域中,出于认证安全的需要,往往会添加补充字段,这无疑也增加通信的能耗,另外,现有的用户认证协议在设计之初缺乏必要的能量有效性分析机制。

进一步研究基于能量有效性的用户认证协议、建立能量有效性分析机制、优化协议消息结构、设计轻量级的密钥生成/分发机制、减少能量消耗、降低通信时间延迟、提升用户认证协议的综合性能是未来 WSN 用户认证协议的重要研究方向。

5 结束语

在 WSN 应用中,用户认证协议是保证网络数据访问用户的合法授权性的重要安全机制。一旦攻击者利用认证协议的漏洞窃取无线传感器网络节点的数据、截获用户的隐私信息,那将会对无线传感器网络和用户构成巨大威胁。笔者后续将基于能量有效性的思想,设计一个具有能耗与安全性均衡的无线传感器网络用户认证协议。

参考文献:

- [1] GOZALVEZ J. New 3GPP standard for IoT[J]. IEEE Vehicular Technology Magazine, 2016, 11(1): 14-20.
- [2] GUO M, LIU Y, YU H, et al. An overview of smart city in China[J]. China Communications, 2016, 13(5): 203-211.
- [3] XIONG Z, SHENG H, RONG W G, et al. Intelligent transportation systems for smart cities: a progress review[J]. Science China (Information Sciences), 2012(55): 2908-2914.
- [4] MOIS G, SANISLAV T, FOLEA S C. A cyber-physical system for environmental monitoring[J]. IEEE Transactions on Instrumentation and Measurement, 2016, 65(6): 1463-1471.
- [5] ASKRABA S, PAAP A, ALAMEH K, et al. Laser-stabilized real-time plant discrimination sensor for precision agriculture[J]. IEEE Sensors Journal, 2016, 16(17): 6680-6686.
- [6] SHAH S H, IQBAL A, SHAH S S A. Remote health monitoring through an integration of wireless sensor networks, mobile phones & Cloud Computing technologies[C]//IEEE Global Humanitarian Technology Conference. 2013: 401-405.
- [7] YANG Y, ZHAO C, YAO S, et al. Delay performance of network-coding-based epidemic routing[J]. IEEE Transactions on Vehicular Technology, 2016, 65(5): 3676-3684.
- [8] CHEN W, JIANG X, TANG Z, et al. Context-based global multi-class semantic image segmentation by wireless multimedia sensor networks[J]. Artificial Intelligence Review, 2015, 43(4): 579-591.
- [9] YANG Y, ZHANG W, WEI K, et al. Power reduction for mobile devices by deploying low-power base stations[J]. IET Communications, 2014, 8(18): 3372-3380.
- [10] REN Y, ZADOROZHNY V I, OLESHCHUK V A, et al. A novel approach to trust management in unattended wireless sensor networks[J]. IEEE Transactions on Mobile Computing, 2014, 13(7): 1409-1423.
- [11] ZHANG D, LI Y, NING Z. A multi-tag secure network coding scheme against pollution attacks in WSNs[J]. Journal of Computational Information Systems, 2015, 11(12): 4413-4420.
- [12] DU X, GUIZANI M, XIAO Y, et al. Two tier secure routing protocol for heterogeneous sensor networks[J]. IEEE Transactions on Wireless Communications, 2007, 6(9): 3395-3401.
- [13] ZHU C, ZHOU M Z, XU J S, et al. A secure data fusion algorithm based on behavior trust in wireless sensor networks[C]//IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing. 2008: 1-4.
- [14] CHEN X, MAKKI K, YEN K, et al. Sensor network security: a survey[J]. IEEE Communications Surveys & Tutorials, 2009, 11(2): 52-73.
- [15] SINGH S K, SINGH M P, SINGH D K. A survey on network security and attack defense mechanism for wireless sensor networks[J]. International Journal of Computer Trends and Technology, 2011, 1(2): 9-17.
- [16] KUMARI S, KHAN M K, ATIQUZZAMAN M. User authentication schemes for wireless sensor networks: a review[J]. Ad Hoc Networks, 2015, 27: 159-194.
- [17] KAUSHAL K, KAUR T. A survey on attacks of WSN and their security mechanisms[J]. International Journal of Computer Applications, 2015, 118(18): 1-4.
- [18] HUANG Z H, WANG Y L. Survey of security Technologies on wireless sensor networks[J]. Journal of Sensors, 2015, 2015(4): 1-9.
- [19] BANERJEE P, CHATTERJEE T, DASBIT S. LoENA: low-overhead encryption based node authentication in WSN[C]//IEEE International Conference on Advances in Computing, Communications and Informatics. 2015: 2126-2132.
- [20] WANG H Y. Wireless sensor networks based on a new block encryption algorithm[J]. Applied Mechanics and Materials, 2014: 454-459.
- [21] YANG W, HU J, WANG S. A delaunay triangle-based fuzzy extractor for fingerprint authentication[C]//IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. 2012: 66-70.
- [22] RAMANUJAM R, SUNDARARAJAN V, SURESH S P. Extending dolev-yao with assertions[M]//Information Systems Security. Berlin: Springer, 2014: 50-68.
- [23] KÄHLER D, KÜSTERS R, WILKE T. A dolev-yao-based definition of abuse-free protocols[M]//Automata, Languages and Programming. Berlin Heidelberg: Springer, 2006: 95-106.
- [24] KIM J, LEE D, JEON W, et al. Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks[J]. Sensors, 2014, 14(4): 6443-6462.
- [25] HURTADO A J A, BASTARRICA M C, BERGEL A. Avispa: a tool for analyzing software process models[J]. Journal of Software:

- Evolution and Process, 2014, 26(4): 434-450.
- [26] ARMANDO A, BASIN D, BOICHUT Y, et al. The AVISPA tool for the automated validation of internet security protocols and applications[C]//Lecture Notes in Computer Science. 2005, 3576(6): 135-165.
- [27] VIGANÒ L. Automated security protocol analysis with the AVISPA tool[J]. Electronic Notes in Theoretical Computer Science, 2006, 155(1):61-86.
- [28] ROGOWSKI M, SAEED K, RYBNIK M, et al. User authentication for mobile devices[M]//Computer Information Systems and Industrial Management. Berlin Heidelberg: Springer, 2013:47-58.
- [29] WONG K H M, ZHENG Y, CAO J, et al. A dynamic user authentication scheme for wireless sensor networks[C]//IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. 2006: 1-8.
- [30] JAMIL N, SAMEON S S, MAHMOOD R. A user authentication scheme based on identity-bits commitment for wireless sensor networks[C]//IEEE Second International Conference on Network Applications Protocols and Services. 2010: 61-66.
- [31] TSENG H R, JAN R H, YANG W. An improved dynamic user authentication scheme for wireless sensor networks[C]//IEEE Global Telecommunications Conference. 2007: 986-990.
- [32] LEE T H. Simple dynamic user authentication protocols for wireless sensor networks[C]//IEEE Second International Conference on Sensor Technologies and Applications. 2008: 657-660.
- [33] KIANI F, DALKILIC G. Password renewal enhancement for dynamic authentication in wireless sensor networks[C]//IEEE Second International Conference on Computational Intelligence, Communication Systems and Networks. 2010: 143-146.
- [34] KO L C. A novel dynamic user authentication scheme for wireless sensor networks[C]//IEEE International Symposium on Wireless Communication Systems. 2008: 608-612.
- [35] VAIDYA B, SÁ SILVA J, RODRIGUES J J P C. Robust dynamic user authentication scheme for wireless sensor networks[C]//The 5th ACM Symposium on QoS and Security for Wireless and Mobile Networks. 2009: 88-91.
- [36] FAYE Y, NIANG I, GUYENNET H. A user authentication-based probabilistic risk approach for wireless sensor networks[C]//IEEE International Conference on Selected Topics in Mobile and Wireless Networking. 2012: 124-129.
- [37] DAS M L. Two-factor user authentication in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2009, 8(3):1086-1090.
- [38] NYANG D H, LEE M K. Improvement of Das's two-factor authentication protocol in wireless sensor networks[J]. IACR Cryptology ePrint Archive, 2009: 631-635.
- [39] HUANG H F, CHANG Y F, LIU C H. Enhancement of two-factor user authentication in wireless sensor networks[C]//IEEE 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 2010: 27-30.
- [40] CHEN T H, SHIH W K. A robust mutual authentication protocol for wireless sensor networks[J]. Etri Journal, 2010, 32(5): 704-712.
- [41] KHAN M K, ALGHATHBAR K. Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks[J]. Sensors, 2010, 10(3): 2450-2459.
- [42] VAIDYA B, MAKRAKIS D, MOUFTAH H T. Improved two-factor user authentication in wireless sensor networks[C]//IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications. 2010: 600-606.
- [43] HE D, GAO Y, CHAN S, et al. An enhanced two-factor user authentication scheme in wireless sensor networks[J]. Ad Hoc & Sensor Wireless Networks, 2010, 10(4): 361-371.
- [44] KUMAR P, LEE H J. Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks[C]//IEEE Wireless Advanced. 2011: 241-245.
- [45] TAN Z. Cryptanalyses of a two-factor user authentication scheme in wireless sensor networks[J]. Advances in Information Sciences and Service Sciences, 2011, 3(4): 117-126.
- [46] FAN R, HE D, PAN X. An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks[J]. Journal of Zhejiang University Science C, 2011, 12(7): 550-560.
- [47] QAZI F A. A Survey of Biometric Authentication Systems[C]//The International Conference on Security and Management. 2004: 61-67.
- [48] LEE J K, RYU S R, YOO K Y. Fingerprint-based remote user authentication scheme using smart cards[J]. Electronics Letters, 2002, 38(12): 554-555.
- [49] LI C T, HWANG M S. An efficient biometrics-based remote user authentication scheme using smart cards[J]. Journal of Network and Computer Applications, 2010, 33(1): 1-5.
- [50] LEE C C, CHANG R X, CHEN L A. Improvement of li-hwang's biometrics-based remote user authentication scheme using smart cards[J]. WSEAS Transactions on Communications, 2011, 10(7): 193-200.
- [51] DAS A K. Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards[J]. IET Information Security, 2011, 5(3):145-151.
- [52] SEKHAR V C, SARVABHATLA M. A robust biometric-based three-factor remote user authentication scheme [J]. Eprint Arxiv, 2014.
- [53] AN Y. Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards[J]. Biomed Research International, 2012(4):23-29.
- [54] CHATURVEDI A, MISHRA D, MUKHOPADHYAY S. Improved biometric-based three-factor remote user authentication scheme with key agreement using smart card[M]. Information Systems Security. Berlin Heidelberg: Springer, 2013: 63-77.
- [55] YUAN J, JIANG C, JIANG Z. A biometric-based user authentication for wireless sensor networks[J]. Wuhan University Journal of

Natural Sciences, 2010, 15(3): 272-276.

- [56] YOON E J, YOO K Y. A new biometric-based user authentication scheme without using password for wireless sensor networks[C]//The 20th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise. 2011: 279-284.

作者简介:



房卫东 (1971-), 男, 山东济南人, 博士, 中国科学院上海微系统与信息技术研究所高级工程师, 主要研究方向为无线传感器网络可信传输技术、信任管理、隐私保护。



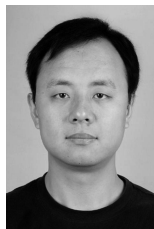
张武雄 (1985-), 男, 湖北孝感人, 博士, 中国科学院上海微系统与信息技术研究所助理研究员, 主要研究方向为车联网体系架构及组网技术、异构多网协作。



单联海 (1980-), 男, 山东潍坊人, 博士, 中国科学院上海微系统与信息技术研究所副研究员, 主要研究方向为物联网/无线传感器网络接入技术、能效均衡。



何为 (1980-), 男, 福建光泽人, 博士, 中国科学院上海微系统与信息技术研究所副研究员, 主要研究方向为物联网、信号与信息处理。



陈伟 (1978-), 男, 江苏徐州人, 博士, 中国矿业大学副教授, 主要研究方向为智能信息处理、无线通信、大数据与云计算。