·计算机工程与应用·

异构传感器网络的用户认证和密钥协商协议研究

闫丽丽，昌 燕，张仕斌

(成都信息工程大学信息安全工程学院 成都 610000)

【摘要】物联网应用的安全和隐私保护问题是制约其进一步发展的关键因素，该文针对物联网中外部用户需要直接访问传感器节点获得信息的应用需求，基于异构传感器网络设计一个用户认证和密钥协商协议，保证信息传输的安全。协议在实现对所有参与者身份认证的同时，完成了用户和传感器节点之间的密钥协商。最后，该文从安全性和执行效率两个方面对所设计协议进行分析、比较，结果显示所设计协议是安全、高效的。

关 键 词 认证；异构传感器网络；物联网；密钥协商；安全协议

中图分类号 TP309 **文献标志码** A doi:10.3969/j.issn.1001-0548.2017.01.009

A User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks

YAN Li-li, CHANG Yan, and ZHANG Shi-bin

(College of Information Security Engineering, Chengdu University of Information Technology Chengdu 610000)

Abstract Security and privacy are main restriction factors in the development of the Internet of Things(IOT). The external users need to directly access the sensor nodes to get data in IOT. In order to protect the security of data, we propose a user authentication and key agreement scheme based on heterogeneous wireless sensor networks. The proposed scheme can verify the identity of participants and establish a shared key between the user and senor node.The detailed analysis of the proposed scheme shows that the scheme is secure and efficient.

Key words authentication; heterogeneous wireless sensor networks; Internet of things; key agreement; security protocol

无线传感器网络最早被应用于美国军方资助项目，如DARPA(defense advanced research projects agency)[1]。这些早期的传感器网络，由于主要被应用于军事领域，都具有大规模、随机部署和传感器节点位置固定的特点，同一网络中的传感器节点通常具有相同类型，此类传感器网络被称为同构传感器网络(homogeneous sensor networks)[2]。随着物联网技术发展，对无线传感器网络有了新的需求，物联网中的无线传感器网络大多需要提前部署，传感器节点可以是固定节点，也可以是移动设备，网络中可以存在不同种类的传感器节点(如感测能力、计算能力、通信能力、存储能力和能量等不同)，这种由不同类型的传感器节点构成的网络称之为异构传感器网络(heterogeneous sensor networks)。在异构传感器网络中，除了具有低计算、存储、通讯和能量等能力的普通传感器节点，还存在汇聚节点(GWN)。汇聚节点具有大容量存储和较高的计算、通讯等能力，它作为无线传感器网络的管理中心，负责连接传感器网络和外部网络。在物联网应用中，无线传感器节点负责采集目标对象的信息，并将信息传递给远程用户，如远程医疗系统中医生需要随时了解病人的体征信息。因此，保证只有合法远程用户可以访问传感器节点获取信息，是物联网技术实际应用的基础条件。

本文基于物联网的实际应用需求，设计一个适用于异构传感器网络的用户认证和密钥协商协议，协议实现了对外部用户和内部节点的身份认证和密钥协商。

1 相关工作

近年来，针对传感器节点、用户和GWN之间的安全传输问题已经有一些解决方案被提出[3-21]。2004

收稿日期：2015－10－14；修回日期：2016－05－04
基金项目：国家自然科学基金(61402058)；数字空间安全保障四川省高校重点实验室开放基金(szjj2014-074)
作者简介：闫丽丽(1980－)，女，博士，副教授，主要从事无线传感器网络、信息安全及安全协议方面的研究.

年，文献[3]首次指出传感器网络中外部用户访问传感器内部节点时存在的安全问题，并设计相应的安全机制，实现对用户和节点的安全认证。随后，研究人员基于公钥密码体制提出解决上述问题的安全协议。文献[4]基于RSA和Diffie-Hellman算法提出了用户认证协议TinyPK。2009年，TinyPK协议被发现无法抵御中间人攻击(man-in-the-middle attack)，在协议运行时攻击者可以伪装成一个合法传感器节点完成与外部用户的通信[5]。文献[6-7]分别基于Diffie-Hellman算法设计了一个传感器网络认证和密钥协商协议。2011年，文献[8]基于椭圆密码算法提出了一个传感器网络认证协议。上述研究人员设计的安全协议都是基于公钥密码体制，存在一个共同的问题，每个传感器节点都需存储所有其他节点和用户的公钥，这对传感器节点存储资源有限的传感器网络并不适用。

2006年，文献[9]基于对称密钥体制设计了一个用户认证协议，协议只使用哈希函数实现，由此提出了一个轻量级用户认证协议的架构。但是，随后协议被发现在协议执行时，不同用户可采用相同的用户身份登录传感器网络，而且由于网关节点和传感器节点都要存储登录用户的认证信息，使得协议存在stolen-verifier attack(攻击者使用从认证服务器中盗窃的用户指纹信息冒充合法用户)[5]。文献[5]对文献[9]提出的协议进行改进，提出一个基于设备和口令的轻量级认证协议，实现对外部用户、网关节点和传感器节点之间的身份认证。随后，研究人员在Das协议的基础上做出大量工作，发现很多Das类协议存在安全缺陷，如privileged-insider attack(内部用户的特权攻击)、网关节点存在bypassing attack(旁路攻击)、协议不提供用户密钥更新和密钥协商[10-12]。2010年，文献[13]在Das协议的基础上提出一个改进协议，改进协议通过预共享密钥实现GWN和传感器节点之间的双向认证，协议还提供用户的密钥更新机制，解决Das存在的旁路攻击问题。随后，文献[14]指出Das[5]协议和Khan[13]协议都存在stolen smart card(盗取智能卡攻击)，并给出对应解决方案。此外，文献[15]基于Das协议提出一个改进方案，该方案可以实现所有节点和用户的双向认证[15]。

最近，文献[16-17]提出一个新的传感器网络双向认证和密钥协商协议，这两个方案不但实现对传感器网络外部用户、网关和传感器节点之间的身份认证，而且添加了密钥协商功能。但是，文献[18-19]指出文献[16]提出的协议需要优化设计后才能应用于实际的传感器网络。而文献[17]提出的协议被指出仍然存在stolen-verifier、离线密码猜测攻击等安全缺陷[20]。文献[21]在上述工作的基础上，提出了一个新的适用于异构传感器网络的认证和密钥协商协议。作者通过对Turkanovic协议进行分析，发现协议中存在重放攻击、智能卡窃取攻击、拒绝服务攻击(DOS)、假冒攻击、多用户登录攻击和共享密钥修改攻击。为了解决上述安全缺陷，本文提出了一个新的认证和密钥协商协议。

2 新用户认证和密钥协商协议(HUK协议)

该异构传感器网络有两类节点，低消耗、资源受限的传感器节点和GWN节点。GWN相对于普通传感器节点，具有较大的存储空间和计算能力，在安全协议中GWN担任可信第三方，即认证服务器。

HUK协议包含注册、登录、认证3个阶段，在网络初始化阶段，网络管理员预先部署GWN，为网络中的传感器节点$\{S_j \mid 1\leqslant j\leqslant m\}$预分配身份$\mathrm{SID}_j$和共享密钥$X_{\mathrm{GWN}-S_j}$，其中，$m$为网络可能添加的最大传感器节点数，GWN需存储网络中所有节点的身份SID_j和共享密钥$X_{\mathrm{GWN}-S_j}$，传感器节点出厂时需设置和存储自己的身份SID_j和共享密钥$X_{\mathrm{GWN}-S_j}$。

协议中所使用的变量和符号，如表1所示。

表1 协议中变量和符号说明

变量或符号	说明
U_i	外部用户
ID_i	用户身份
SC	智能卡
X_{GWN}	GWN的安全私钥
$X_{\mathrm{GWN}-U_i}$	GWN和用户U_i的共享密钥
$\oplus$	异或运算
$\|$	连接符号
$h(\,)$	哈希运算，如MD5

2.1 注册阶段

注册阶段分为用户注册和传感器节点注册两部分，协议中传感器节点的注册过程如下。

1) 节点S_j计算$\mathrm{MP}_j = h(X_{\mathrm{GWN}-S_j} \| \mathrm{SID}_j \| T_1)$，其中$T_1$是$S_j$的当前时间。$S_j$将$\{\mathrm{SID}_j,\ \mathrm{MP}_j,\ T_1\}$发送给GWN。

2) 当GWN收到S_j发送的数据，首先确认$(T^* - T_1) \leqslant \Delta T$，其中$T^*$是GWN的当前时间，$\Delta T$是允许消息延迟的最长时间，防止消息重放。GWN根据收到的节点身份SID_j，查找到对应共享密钥$X_{\mathrm{GWN}-S_j}$，计

算 $\mathrm{MP}_j^* = h(X_{\mathrm{GWN}-S_j} \| \mathrm{SID}_j \| T_1)$，并判断 $\mathrm{MP}_j = \mathrm{MP}_j^*$ 是否成立，确认S_j的身份，随后计算 $f_j = h(\mathrm{SID}_j \| X_{\mathrm{GWN}})$，$x_j = h(f_j \| X_{\mathrm{GWN}-S_j} \| T_2)$，其中 T_2 是S_j的当前时间。GWN发送$\{f_j, x_j, T_2\}$给S_j。

3) S_j接收$\{f_j, x_j, T_2\}$后，判断$(T^* - T_2) \leqslant \Delta T$，计算 $x_j^* = h(f_j \| X_{\mathrm{GWN}-S_j} \| T_2)$，并判断 $x_j = x_j^*$ 是否成立，如果成立，S_j存储f_j。

当用户要访问传感器节点时，也需先向GWN注册，用户注册过程如下。

4) 用户U_i选择身份ID_i，生成随机数r_i，计算 $\mathrm{MI}_i = h(r_i \| \mathrm{ID}_i)$。$U_i$将$\{h(\mathrm{ID}_i), \mathrm{MI}_i\}$通过一个安全通道[8]发送给GWN。

5) GWN接收$\{h(\mathrm{ID}_i), \mathrm{MI}_i\}$，计算 $f_i = h(\mathrm{MI}_i \| X_{\mathrm{GWN}})$，然后将参数$\mathrm{MI}_i$，$f_i$初始化到智能卡SC，通过安全信道传输给用户，并存储$h(\mathrm{ID}_i), \mathrm{MI}_i$。

6) U_i收到SC后，需将随机数r_i存储到SC。

2.2　登录阶段

用户访问传感器节点，需先使用智能卡登录。

U_i将SC插入到读卡器，并输入身份 ID_i^*。SC计算 $\mathrm{MI}_i^* = h(r_i \| \mathrm{ID}_i^*)$，判断 $\mathrm{MI}_i = \mathrm{MI}_i^*$ 是否成立，如果成立，计算 $N_i = h(K_i \| f_i \| \mathrm{SID}_j \| T_1)$，$A_i = h(h(\mathrm{ID}_i) \| T_1) \oplus K_i$，其中$T_1$是$U_i$的当前时间，$K_i$是$SC$生成的随机数，$\mathrm{SID}_j$是用户想要访问节点的身份。SC将$\{\mathrm{MI}_i, A_i, N_i, \mathrm{SID}_j, T_1\}$发送给选择的$S_j$。

2.3　认证阶段

协议认证的过程如下。

1) S_j收到$\{\mathrm{MI}_i, A_i, N_i, \mathrm{SID}_j, T_1\}$后，确认$(T^* - T_1) \leqslant \Delta T$。如果成功，计算 $B_j = h(X_{\mathrm{GWN}-S_j} \| f_j \| T_1 \| T_2)$，其中 T_2 是S_j的当前时间。S_j将$\{\mathrm{MI}_i, A_i, N_i, \mathrm{SID}_j, T_1, B_j, T_2\}$发送给GWN。

2) GWN收到消息后，确认$(T^* - T_2) \leqslant \Delta T$。如果成功，根据$\mathrm{SID}_j$查找到对应的 $X_{\mathrm{GWN}-S_j}$，计算 $f_j^* = h(\mathrm{SID}_j \| X_{\mathrm{GWN}})$，$B_j^* = h(X_{\mathrm{GWN}-S_j} \| f_j^* \| T_1 \| T_2)$，然后判断 $B_j = B_j^*$ 是否成立，如果不成立，终止操作，并向S_j发送拒绝消息；否则对S_j的身份认证成功。

GWN根据MI_i查找到对应的$h(\mathrm{ID}_i)$，计算 $K_i^* = h(h(\mathrm{ID}_i) \| T_1) \oplus A_i$，$f_i^* = h(\mathrm{MI}_i \| X_{\mathrm{GWN}})$，$N_i^* = h(K_i^* \| f_i^* \| \mathrm{SID}_j \| T_1)$，然后判断 $N_i = N_i^*$ 是否成立，如果不成立，终止操作，并向S_j发送拒绝消息，S_j收到拒绝消息后，向U_i转发拒绝消息；否则对U_i的身份认证成功。

GWN计算 $F_{ij} = K_i^* \oplus h(f_j^* \| X_{\mathrm{GWN}-S_j})$，$S_i = h(f_i^* \| T_1 \| T_2 \| T_3)$，$H_j = h(K_i^* \| X_{\mathrm{GWN}-S_j} \| T_1 \| T_2 \| T_3)$。GWN发送$\{S_i, H_j, F_{ij}, T_1, T_2, T_3\}$给$S_j$，其中$T_3$是GWN的当前时间。

3) S_j收到$\{F_{ij}, H_j, S_i, T_1, T_2, T_3\}$后，确认$(T^* - T_3) \leqslant \Delta T$。如果成功，计算 $K_i^* = F_{ij} \oplus h(f_j \| X_{\mathrm{GWN}-S_j})$，$H_j^* = h(K_i^* \| X_{\mathrm{GWN}-S_j} \| T_1 \| T_2 \| T_3)$，然后判断 $H_j = H_j^*$ 是否成立，如果不成立，发送拒绝信息给GWN；否则可以确认GWN的身份。S_j生成随机数K_j，计算 $M_{ij} = h(S_i \| K_j)$，$R_{ij} = h(K_i^* \| \mathrm{SID}_j \| T_1 \| T_2 \| T_3 \| T_4) \oplus K_j$。

S_j将$\{S_i, R_{ij}, M_{ij}, T_1, T_2, T_3, T_4\}$发送给$U_i$。计算、存储协商的共享密钥 $\mathrm{SK} = h(K_i \oplus K_j)$。

4) U_i收到$\{S_i, R_{ij}, M_{ij}, T_1, T_2, T_3, T_4\}$后，确认$(T^* - T_4) \leqslant \Delta T$。如果成功，计算 $h(f_i \| T_1 \| T_2 \| T_3)$ 并与收到的S_i进行比较，如果不相等，终止操作，并向S_j发送拒绝消息，S_j收到拒绝消息后转发给GWN；否则对GWN和S_j的身份认证成功。U_i计算 $M_{ij}^* = h(S_i \| K_j^*)$，$K_j^* = R_{ij} \oplus h(K_i \| \mathrm{SID}_j \| T_1 \| T_2 \| T_3 \| T_4)$，然后判断 $M_{ij} = M_{ij}^*$ 是否相等，如果相等，计算 $\mathrm{SK} = h(K_i \oplus K_j)$，获得协商的共享密钥SK。

用户和传感器节点完成认证后，可以使用共享密钥SK进行安全通信。

2.4　用户ID更新阶段

在协议执行过程中，用户可以通过ID更新阶段对ID进行更新。

1) U_i将SC插入到读卡器，并输入身份 ID_i^* 和 $\mathrm{ID}_{\mathrm{inew}}$。

2) SC计算 $\mathrm{MI}_i^* = h(r_i \| \mathrm{ID}_i^*)$，然后判断 $\mathrm{MI}_i = \mathrm{MI}_i^*$ 是否成立，如果不成立，终止操作；否则计算 $\mathrm{MI}_{\mathrm{inew}} = h(z_i \| \mathrm{ID}_{\mathrm{inew}})$，$\mathrm{MN}_i = h(\mathrm{ID}_i) \oplus h(\mathrm{ID}_{\mathrm{inew}})$ 和 $\mathrm{MJ}_i = h(\mathrm{MI}_{\mathrm{inew}} \| h(\mathrm{ID}_{\mathrm{inew}})^* \| T_1)$，其中$T_1$是$U_i$的当前时间，$z_i$是SC生成的随机数。将$\{\mathrm{MI}_i, \mathrm{MI}_{\mathrm{inew}}, \mathrm{MN}_i, \mathrm{MJ}_i, T_1\}$发送给选择的GWN。

3) GWN收到消息后，确认$(T^* - T_1) \leqslant \Delta T$。如果成功，根据$\mathrm{MI}_i$查找到对应的$h(\mathrm{ID}_i)^*$，计算 $h(\mathrm{ID}_{\mathrm{inew}})^* = \mathrm{MN}_i \oplus h(\mathrm{ID}_i)^*$，$\mathrm{MJ}_i^* = h(\mathrm{MI}_{\mathrm{inew}} \| h(\mathrm{ID}_{\mathrm{inew}})^* \| T_1)$，然后判断 $\mathrm{MJ}_i = \mathrm{MJ}_i^*$ 是否成立，如果成立，计算 $f_i = h(\mathrm{MI}_{\mathrm{inew}} \| \mathrm{X}_{\mathrm{GWN}})$，$\mathrm{MO}_i = h(\mathrm{ID}_{\mathrm{inew}})^* \oplus f_i$，$\mathrm{MQ}_i = h(f_i \| T_2)$。GWN发送$\{\mathrm{MI}_{\mathrm{inew}}, \mathrm{MO}_i, \mathrm{MQ}_i, T_2\}$给$U_i$，其中 T_2 是当前时间。GWN存储 $\mathrm{MI}_{\mathrm{inew}}, h(\mathrm{ID}_{\mathrm{inew}})$，替换

原来的 $\mathrm{MI}_i, h(\mathrm{ID}_i)$。

4) U_i收到消息后，确认$(T^*-T_2)\leqslant\Delta T$。如果成功，计算 $f_i^*=\mathrm{MO}_i\oplus h(\mathrm{ID}_{\mathrm{inew}})$， $\mathrm{MQ}_i^*=h(f_i^*\|T_2)$。判断 $\mathrm{MQ}_i=\mathrm{MQ}_i^*$是否成立，如不成立，终止操作，并向GWN发送拒绝消息，否则计算更新智能卡为$\mathrm{SC}=\{\mathrm{MI}_{\mathrm{inew}}, f_i^*, z_i\}$。

通过上述过程，经过一段时间，用户可以使用上述过程更新ID。

3 HUK协议的安全性

HUK协议提供对用户、传感器节点、GWN的双向认证功能，并在认证过程中实现传感器节点和用户之间的密钥协商，本节针对下面列出的常用攻击方式，采用非形式化方法进一步分析HUK协议的安全性。

1) 用户匿名(user anonymity)：在HUK协议运行过程中使用$\mathrm{MI}_i=h(r_i\|\mathrm{ID}_i)$代替用户$\mathrm{ID}_i$，其中$h(\ )$是哈希函数，因此攻击者无法获得用户的$\mathrm{ID}_i$。由于在智能卡中存储的信息$h(\mathrm{ID}_i)$、$\mathrm{MI}_i$是经过伪装后的用户$\mathrm{ID}_i$，即使智能卡被窃取，攻击者也无法获得用户$\mathrm{ID}_i$。协议实现了对用户的匿名操作。

2) 重放攻击(replay attack)：在传感器注册阶段$\mathrm{MP}_j=h(X_{\mathrm{GWN}-S_j}\|\mathrm{SID}_j\|T_1)$，$x_j=h(f_j\|X_{\mathrm{GWN}-S_j}\|T_2)$中分别包含传感器节点和GWN的当前时间$T_1$、$T_2$。在协议认证过程中，用户发送的消息$N_i=h(K_i\|f_i\|\mathrm{SID}_j\|T_1)$中包含当前时间$T_1$，传感器节点发送的消息$B_j=h(X_{\mathrm{GWN}-S_j}\|f_j\|T_1\|T_2)$，$R_{ij}=h(K_i^*\|\mathrm{SID}_j\|T_1\|T_2\|T_3\|T_4)\oplus K_j$中包含当前时间$T_2$、$T_4$，GWN发送的消息$H_j=h(K_i^*\|X_{\mathrm{GWN}-S_j}\|T_1\|T_2\|T_3)$，$S_i=h(N_i^*\|T_1\|T_2\|T_3)$中包含当前时间$T_3$。因此HUK协议中攻击者无法实现重放攻击。

3) 窃取智能卡攻击(stolen smart card)：假设攻击者窃取智能卡，并获得智能卡中存储的数据，但是由于攻击者无法得到用户ID_i，就计算不出$A_i=h(h(\mathrm{ID}_i)\|T_1)\oplus K_i$，所以其无法通过GWN的认证。因此窃取智能卡攻击，在HUK协议中无法实现。

4) 密码更改攻击(password change attack)：在HUK协议中，ID充当用户的身份和密钥，攻击者想要更改用户ID，首先必须获得旧的ID，但在协议运行过程中使用$\mathrm{MI}_i=h(r_i\|\mathrm{ID}_i)$代替用户ID，攻击者无法获得用户ID，也就无法进行密码更改攻击。

5) 假冒攻击(impersonation attack)：在HUK协议中攻击者无法冒充用户、节点和GWN。分析可见重放攻击，由于所有消息在传递过程中都添加了当前时间，因此攻击者要冒充任意角色，必须重新计算包含当前时间的对应变量，如传感器节点登录阶段的MP_j、认证阶段的N_i、B_j、H_j、S_i、R_{ij}。

6) 同一用户的重复登录攻击(many logged-in users with the same login-id attack)：由于攻击者无法获得用户ID，消息中又包含时间变量，因此攻击者无法伪装成合法用户对HUK实施此攻击。

7) 拒绝服务攻击(denial-of-attack)：由于协议中只使用了低计算量的异或和哈希函数运算，计算量较少，而且攻击者无法实施重放和假冒攻击，因此HUK协议可抵御拒绝服务攻击。

表2将HUK协议与相关协议[8, 11-17, 21]的安全性进行了对比，其中Y表示协议满足对应的安全属性，N表示协议不满足对应安全属性。由于有些协议的应用场景不同、采用的认证模式不同，所以有些安全属性在协议中没有被考虑。

表2 HUK协议与相关协议的安全性比较

安全属性	HUK协议	文献[8]协议	文献[11]协议	文献[12]协议	文献[13]协议	文献[14]协议	文献[15]协议	文献[16]协议	文献[17]协议	文献[21]协议
双向认证	Y	Y	N	N	Y	Y	Y	Y	Y	Y
密钥协商	Y	Y	N	N	N	N	N	Y	Y	Y
密钥更新	Y	N	Y	Y	Y	Y	N	Y	Y	Y
动态节点添加	Y		N	N		N	N	Y		Y
用户匿名	Y	N	Y	Y	Y	Y	Y	N	Y	Y
抵御重放攻击	Y	N	Y		Y		Y	Y	Y	N
抵御窃取智能卡攻击	Y	N	N		N		N		Y	N
抵御密码更改攻击	Y									Y
抵御假冒攻击	Y	Y	N		Y		N		Y	N
抵御GWN旁路攻击	Y	Y	N		N		N		Y	Y
抵御同一用户重复登录攻击	Y									N
抵御拒绝服务攻击	Y		N	N		Y	N	Y		N

4 HUK协议的效率分析

由于传感器网络中节点具有低存储、低计算、低电量等特点，所以在设计安全协议时，除了考虑协议的安全属性外，协议的执行效率也是一个重要考察指标。通信开销和计算开销是影响协议执行效

率的主要方面，本节将从这两个方面出发，分析设计协议的运行效率。由于针对不同应用场景设计的协议，其功能和通信方式有很大区别，因此本节在分析协议执行效率时，主要关注与HUK协议功能相似的Turkanovic协议[21]、Xue协议[17]和Das协议[16]，且针对协议的认证和密钥协商阶段。

在通信消耗方面，HUK协议、Turkanovic协议和Das协议都需要4次消息交换完成身份认证和密钥协商，而Xue协议需要6次消息交换。

在计算量方面，由于异或操作的计算量很低，因此这里主要考虑哈希运算和加、解密运算。关于计算开销的比较结果如表3所示，其中T_h是执行一次哈希运算所需的时间，T_{ED}是执行一次对称密钥算法中的加、解密运算所需的时间。

表3　HUK协议与相关协议的效率比较

协议	用户	节点	GWN	基站
HUK协议	$9T_h$	$6T_h$	$8T_h$	
文献[16]协议	$5T_h+1T_{ED}$		$2T_h+1T_{ED}$	$3T_h+3T_{ED}$
文献[17]协议	$7T_h$	$6T_h$	$13T_h$	
文献[21]协议	$7T_h$	$5T_h$	$7T_h$	

在计算开销方面，HUK协议、Turkanovic协议和Xue协议计算量相似，而Das协议中采用了对称加密算法，所以其计算开销较大。

而在存储开销上面，Turkanovic协议中节点需存储(SID_j、X_{GWN-S_j}、e_j、f_j)，GWN需存储(SID_j、X_{GWN-S_j}、MI_i、X_{GWN-U_i})。HUK协议中节点需存储(SID_j、X_{GWN-S_j}、f_j)，GWN需存储(SID_j、X_{GWN-S_j}、MI_i、$h(ID_i)$)。因此，HUK协议中节点存储的信息要少于Turkanovic协议中节点存储的信息。

5 结　束　语

外部用户直接访问传感器节点获得信息是物联网应用中的基础需求，本文为异构传感器网络设计一个新的认证和密钥协商协议，协议为所有参与者提供双向认证，并实现用户和节点之间的密钥协商。文中针对网络中的常见攻击，采用非形式化方法分析了协议的安全性。分析结果显示，协议能够满足物联网应用中外部用户直接访问传感器节点的安全需求。此外，新协议采用哈希函数和异或运算实现，是一个轻量级的安全协议，文中将所设计协议与相关协议的执行效率进行对比、分析。结果显示新协议在通信、计算和存储方面都具有较小的开销。综上所述，本文设计的协议适用于基于物联网应用环境下的传感器网络。

本文研究工作还得到成都信息工程大学科研基金(KYTZ201421)的资助，在此表示感谢。

参　考　文　献

[1] 胡永利, 孙艳丰, 尹宝才. 物联网信息感知与交互技术[J]. 计算机学报, 2012, 35(6): 1147-1163.
HU Yong-li, SUN Yan-feng, YIN Bao-cai. Information sensing and interaction technology in Internet of things[J]. Chinese Journal of Computers, 2012, 35(6): 1147-1163.

[2] 钱志鸿, 王义君. 面向物联网的无线传感器网络综述[J]. 电子与信息学报, 2013, 35(1): 215-227.
QIAN Zhi-hong, WANG Yi-jun. Internet of things-oriented wireless sensor networks review[J]. Journal of Electronics & Information Technology, 2013, 35(1): 215-227.

[3] ROMER K, MATTERN F. The design space of wireless sensor networks[J]. Wireless Commun, IEEE, 2004, 11(6): 54-61.

[4] DUARTE-MELO E J, LIU M. Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks[C]//Proceedings of the GLOBECOM 2002. New York: IEEE, 2002: 21-25.

[5] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, et al. Wireless sensor networks: a survey[J]. Comput Netw, 2002, 38(4): 393-422.

[6] OZDEMIR S, XIAO Y. Secure data aggregation in wireless sensor networks: a comprehensive overview[J]. Comput Netw, 2009, 53(12): 2022-2037.

[7] BENENSON Z, GARTNER F, KESDOGAN D. User authentication in sensor network[C]//Proceedings of Informatik Workshop on Sensor Networks. [S.l.]: [s.n.], 2004: 385-389.

[8] WATRO R, KONG D, CUTI S. TinPK: Securing sensor networks with public key technology[C]//Proceedings of ACM Workshop Security of Ad Hoc Sensor Networks. [S.l.]: ACM, 2010: 59-64.

[9] DAS M L. Two-factor user authentication in wireless sensor networks[J]. IEEE Trans Wireless Comm, 2009: 1086-1090.

[10] XU J, ZHU W T, FENG D G. An improved smart card based password authentication scheme with provable security[J]. Comput Stand Interf , 2009, 31(4): 723-728.

[11] SONG R. Advanced smart card based password authentication protocol[J]. Comput Stand Interf, 2010, 32 (5-6): 321-325.

[12] YEH H L, CHEN T H, LIU P C, et al. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography[J]. Sensors, 2011, 11(5): 4767-4779.

[13] WONG K H M, ZHENG Y, CAO J, et al. A dynamic user authentication scheme for wireless sensor network[C]//Proceedings of IEEE International Conf Sensor Network, Ubiquitous, Trustworthy Computing, IEEE Computer Society. [S.l.]: IEEE, 2006: 244-251.

[14] NYANG D H, LEE M K. Improvement of Das's two-factor authentication protocol in wireless sensor networks[C]// Proceedings of the CORD Conference. [S.l.]: [s.n.], 2009.

[15] KHAN M K, ALGHATHBAR K. Cryptanalysis and

security improvements of “two-factor user authentication in wireless sensor networks”[J]. Sensor, 2010, 10(3): 2450-2459.
[16] VAIDYA B, MAKRAKIS D, MOUFTAH H T. Improved two-factor user authentication in wireless sensor networks[C]//Proceedings of 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). [S.l.]: IEEE 2010: 600-606.
[17] XUE K, MA C, HONG P, et al. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks[J]. Journal of Network and Computer Applications, 2013, 36(1): 316-323.
[18] XU S, WANG X. A new user authentication scheme for hierarchical wireless sensor networks[J]. International Review on Computers and Software, 2013, 8(1): 197-203.
[19] TURKANOVIC M, HOLBL M. An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks[J]. Elektronika IR Elektrotechnika, 2013, 19(6): 109-116.
[20] LI C T, WENG C Y, LEE C C. An advanced temporal credentialbased security scheme with mutual authentication and key agreement for wireless sensor networks[J]. Sensors, 2013, 13(8): 9589-9603.
[21] TURKANOVIC M, BRUMEN B, HOLBL M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion[J]. Ad Hoc Network, 2014, 20: 96-112.

编 辑 蒋 晓

(上接第31页)

[7] YANG Yang, BLUM R S. MIMO radar waveform design based on mutual information and minimum mean-square error estimation[J]. IEEE Transactions on Aerospace and Electronic Systems, 2007, 43(1): 330-343.
[8] WATTS S. Modeling and simulation of coherent sea clutter[J]. IEEE Transactions on Aerospace and Electronic Systems, 2012, 48(4): 3303-3317.
[9] PERL J M, KAGAN D. Real-time HF channel parameter estimation[J]. IEEE Transactions on Communications, 1986, 34(1): 54-58.
[10] SEN S, NEHORAI A. OFDM MIMO radar with mutual-information waveform design for low-grazing angle tracking[J]. IEEE Transactions on Signal Processing, 2010, 58(6): 3152-3162.
[11] CHEN Yi-fan, NIJSURE Y, YUEN C, et al. Adaptive distributed MIMO radar waveform optimization based on mutual information[J]. IEEE Transactions on Aerospace and Electronic Systems, 2013, 49(2): 1374-1385.
[12] TANG Bo, TANG Jun, PENG Ying-ning. MIMO radar waveform design in colored noise based on information theory[J]. IEEE Transactions on Signal Processing, 2010, 58(9): 4684-4697.
[13] 叶聪. 基于MIMO体制的天波超视距雷达信号与数据处理算法研究[D]. 成都: 电子科技大学, 2013.
YE Cong. Research on signal and data processing for MIMO based sky wave over-the-horizon-radar[D]. Chengdu: University of Electronic Science and Technology of China, 2013.
[14] FRAZER G J, ABRAMOVICH Y I, JOHNSON B A. Mode-selective OTH radar: Experimental results for one-way transmission via the ionosphere[C]//Proceedings of the 2011 IEEE Radar Conference. Kansas City, Missouri, USA: IEEE, 2011: 397-402.

编 辑 税 红