

引用格式:石玲玲,李敬兆.异构网络中安全数据传输机制的研究与设计[J].微电子学与计算机,2019,36(11):84-88. [SHI L L, LI J Z. Research and design of secure data transmission mechanism in heterogeneous network [J]. Microelectronics & Computer, 2019, 36(11): 84-88]

异构网络中安全数据传输机制的研究与设计

石玲玲¹, 李敬兆²

(1 安徽理工大学 现代教育技术中心, 安徽 淮南 232001; 2 安徽理工大学 电气与信息工程学院, 安徽 淮南 232001)

摘 要: 为保证无线和有线异构网络环境中数据安全传输, 采用一种基于优化的 AES-GCM 认证加密算法和基于 SHA 的数字签名算法相结合的安全数据传输机制. 该机制包括密钥的生成与管理、通信方的双向身份认证及高效安全的数据传输三部分, 采用与随机数和时间戳相关的参数生成密钥, 并使用改进的 ECDH 算法实现通信实体间的密钥共享来防止重放攻击, 保证密钥安全; 通过减少传统 AES 算法加密轮数保证消息传输高效性, 为保证消息传输安全性, 提出采用 CTR 分组加密结构, 并将通信方的物理地址、随机数和计数器值作为初始化值用于生成优化的 AES-GCM 认证加密算法的密钥流. 异构网络下的通信实验表明, 本文提出的安全数据传输机制明显缩短了加密传输时间, 保证了安全性和高效性.

关键词: 异构网络; AES-GCM; 椭圆曲线密码体制 ECC; 数字签名; 密钥管理

中图分类号: TP309.2

文献标识码: A

文章编号: 1000-7180(2019)11-0084-05

Research and design of secure data transmission mechanism in heterogeneous network

SHI Ling-ling¹, LI Jing-zhao²

(1 Modern Educational Technology Center, Anhui University of Science and Technology, Huainan 232001, China;

2 College of Electrical and Information Engineering, Anhui University of Science and Technology, Huainan 232001, China)

Abstract: In order to ensure the security of data transmission in wireless and wired heterogeneous networks, a secure data transmission mechanism based on optimized AES-GCM authentication encryption algorithm and SHA-based digital signature algorithm is adopted. This mechanism includes three parts: key generation and management, two-way identity authentication of communicators and efficient and secure data transmission. The key is generated by parameters related to random number and timestamp, and the key sharing among communication entities is realized by using improved ECDH algorithm to prevent replay attacks and ensure key security. It reduces the number of encryption rounds of traditional AES algorithm to ensure the efficiency of message transmission, in order to ensure the security of message transmission, CTR block encryption structure is proposed, and uses the physical address, random number and counter value of communicators as the initialized value to generate the key stream of the optimized AES-GCM authentication encryption algorithm. The communication experiment in heterogeneous networks shows that the secure data transmission mechanism proposed in this paper significantly shortens the encrypted transmission time and guarantees the security and efficiency.

Key words: heterogeneous network; AES-GCM; ECC; digital signature; key management

1 引言

随着网络的发展普及,网络信息安全直接影响着国家、社会和人民的安全与利益^[1]. 为保证网络通信安全,一般通过采取对消息进行数字签名和加密技术^[2]来实现. 加密理论认为密钥的安全更依赖于密钥的保密性而非加密算法. 本文通过对大量相关文献调研得出:在密钥管理方面,有基于随机密钥的管理机制^[3],基于密钥分配中心的管理机制^[4],基于对称加密的密钥管理机制^[5],但均存在密钥分配时间长,管理复杂等问题,本文提出一种基于椭圆曲线密码体制 ECC(Elliptic Curve Cryptography)的改进 ECDH 密钥管理机制^[6],设计出与随机数、时间戳和私钥相关的密钥,实现密钥自动更新,抵挡重放攻击和中间人攻击,使密钥生成与管理更安全方便. 在数据高效安全传输方面,采用具备保密性和单向认证性能^[7]的 AES-GCM 认证加密算法,改进加密轮数和密钥流生成机制,此种方案使得信息即使被截取,也能保证其他消息分组不受安全性影响,保证消息的安全性和完整性. 上述的密钥生成管理机制、消息传输机制及身份认证机制即构成了本文提出的安全数据传输机制.

2 密钥管理机制及加密算法简介

2.1 ECDH 密钥管理机制

ECDH 密钥协商算法可以在不共享任何秘密的情况下协商出一个密钥,建立在 ECDLP 数学难题之上。本文选择有限域 $GF(p)$ 上的椭圆曲线,以 (a, b, G, n, p) 定义。其中, a, b 定义三次方程 $y^2 = (x^3 + ax + b) \bmod p$, G 为加法群的基点, n 是以 G 为基点的群的阶。假设密钥交换双方为 A 和 B , 共享椭圆密钥曲线参数(椭圆曲线 E 、阶 n 、基点 G), ECDH 密钥协商过程如下:

- (1) A 生成随机整数 a , 计算 $D_A = a * G$.
 - (2) B 生成随机整数 b , 计算 $D_B = b * G$.
 - (3) A 将 D_A 传递给 B . A 的传递可以公开, 即攻击者可以获取 A .
 - (4) B 将 D_B 传递给 A . 同理, B 的传递可以公开.
 - (5) B 收到 A 传递的 D_A , 计算 $Q = b * D_A$.
 - (6) A 收到 B 传递的 D_B , 计算 $Q' = a * D_B$.
- A 、 B 双方即得 $Q = b * D_A = b * (a * G) = (b * a) * G = (a * b) * G = a * (b * G) = a * D_B = Q'$ (交换律和结合律), 即双方得到一致的密钥 Q .

2.2 AES-GCM 认证加密算法

AES-GCM 是由 NIST(美国国家标准与技术研究所)在 2007 年提出的认证加密算法^[8]. 即采用对称加密技术 AES 结合 CTR 分组加密模式并带有 GMAC 消息认证码的认证加密算法. AES-GCM 可以同时确保消息的机密性、真实性和完整性. AES-GCM 加密机制有四个输入, 分别是密钥 K , 计数器初始值 IV , 明文 P 和附加消息 A ; 有两个输出, 分别是密文 C 和标签 tag . IV 是内部用来产生流密钥的, 密文 C 是流密钥与明文异或的结果. 认证加密流程如图 1 所示, 其中, E_k 表示使用密钥 K 对输入做对称加密运算, “ $\oplus$ ”表示异或运算, M_h 表示将输入与密钥 h 在有限域 $GF(2^8)$ 上做乘法.

高级加密标准 AES 是以 Rijndael 加密算法为基础发展而来^[9],使用 SP 结构^[10],分组长度与密码的长度可以依据实际需要进行相应的变化. AES 因为长密钥的使用,且具有稳定的数学基础和抗密码分析的强度,具有相对更好的安全性^[11].

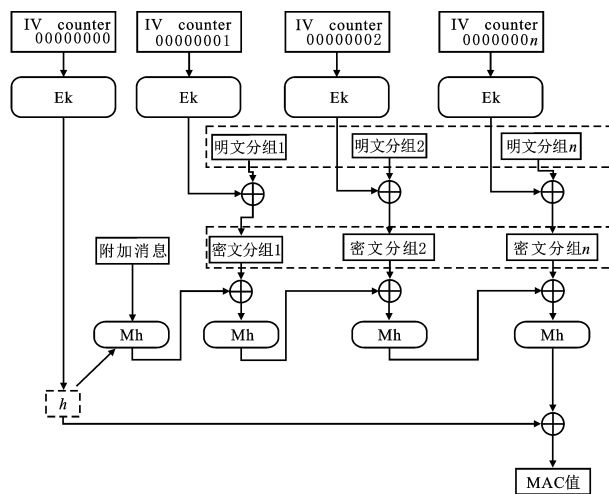


图 1 认证加密流程图

2.3 数字签名算法

安全哈希算法 SHA 是对消息摘要 MD5 的进一步研究,将任意小于 2^{64} 比特的消息转换成固定长为 160 比特的消息摘要的算法,保证了数字签名的秘密性^[12]. 无论是恢复还是寻找相同消息,SHA 算法在运算过程上不是可逆的,因此它具备高安全性.

3 安全数据传输机制设计

本文提出的安全数据传输机制设计方案由密钥生成与安全管理、通信前的双向身份认证以及完整加密数据消息传输三大部分组成. 从密钥的生成与

分发管理,通信双方的身份认证及消息数据的正确性、保密性、完整性等方面全面考虑了数据安全传输,能够抵挡重放攻击、中间人攻击。

3.1 改进的 ECDH 密钥协商算法

根据 ECC 算法原理,首先根据对方身份信息生成标识矩阵,本文提出以时间戳 T 加固定 IP 作为身份信息,即 $ID = \{T || IP\}$,对身份信息进行哈希运算 $h = \text{hash}(ID)$,其中 h_l 表示 h 的第 l 位二进制, $l = 1, 2 \cdots N$; 取小于 n 的随机数构成私钥 $SK = \sum_{l=1}^h h_l * r_l$ 算节点的公钥 $PK = \sum_{l=1}^h h_l * G_l$, $PK = SK * P$. 公钥算法和公钥矩阵由本地服务器保存和运算,不需要接入 KMC,减少风险,使用更加安全快捷. 得到公钥 PK 和私钥 SK 后,利用改进的 ECDH 算法协商密钥的具体实现过程如下:

(1) 通信方 A 生成随机数 $r_A \in [2, n-1]$, 计算 $D_A = (r_A + SK_A)G$, G 为基点, SK_A 是 A 的私钥, 发送 D_A 给通信方 B.

(2) 通信方 B 生成随机数 $r_B \in [2, n-1]$, 计算 $D_B = (r_B + SK_B)G$, SK_B 为 B 的私钥, 发送 D_B 给通信方 A.

(3) A 接收到 B 传递的 D_B , 计算 $K_{AB} = (r_A + SK_A) D_B$.

(4) B 接收到 A 传递的 D_A , 计算 $K_{BA} = (r_B + SK_B) D_A$.

经过上述四步, A、B 双方协商出共同密钥 K_{AB}/K_{BA} . 改进的 ECDH 算法相比于 ECDH 算法, 只是增加了计算量很小的加法运算, 却引入了实体的私钥信息, 抵挡中间人攻击, 增强安全性. 从以下两个方面分析该算法的会话密钥安全性.

(1) 算法具有正确性

根据该算法, 通信双方 A 和 B 能够得到相同的密钥, 计算过程如下:

A 方得到 K_{AB} 的过程为:

$$\begin{aligned} K_{AB} &= (r_A + SK_A) D_B \\ &= (r_A + SK_A) (r_B + SK_B) G \end{aligned}$$

B 方得到 K_{BA} 的过程为:

$$\begin{aligned} K_{BA} &= (r_B + SK_B) D_A \\ &= (r_B + SK_B) (r_A + SK_A) G \end{aligned}$$

显然, A、B 协商出了相同的会话密钥, 算法是正确的.

(2) 算法具有安全性

协商出的密钥随着随机数的不同而不同, 从 D_A 中计算出 $(r_A + SK_A)$ 的值是 ECDLP 难题, 同理, 从

D_B 中计算出 $(r_B + SK_B)$ 也是 ECDLP 难题, 且该密钥与双方生成的随机数和私钥都有关, 攻击方仅截取某一参数(随机数或密钥)均无法计算出会话密钥. 因此某次会话密钥的泄露不会导致其他会话密钥的泄露, 具有安全性.

3.2 密钥更新机制

本文设计的公私钥都是与时间戳相关的, 且由通信方本身生成, 只要到达密钥更新周期后, 通信节点会自动更新公私钥信息, 随机值随着时间戳的更新而重新生成, 由改进的 ECDH 算法同步各个通信节点的共享密钥.

3.3 双向认证机制设计

通信前, 需要双方验证身份合法性, 身份认证请求流程图如图 2 所示. 通信方 A 向通信方 B 发送消息: $AES(A \text{ 的物理 MAC 地址} || \text{随机数}) || \text{消息的消息摘要}$ ($||$ 表示将二进制数据连接起来), 消息摘要为发送方 MAC 地址 $||$ 随机数经过 SHA 散列函数运算后的值, 随机数是系统的 $\text{Random}()$ 函数产生的, 能够防止消息被篡改, 保证消息的不可抵赖性. 再使用 ECDH 算法协商的密钥对(物理 MAC 地址 $||$ 随机数)进行 AES 加密成密文发送. 通信方 B 接收到消息后, 用共享密钥进行解密得到 MAC 地址和随机数, 然后使用 SHA 散列函数运算得到散列值 md' , 与接收到的哈希值 md 进行比对, 若一致则认证成功, 说明通信方身份合法; 否则重新认证. 在认证过程中, 避免了密钥在通信方之间的加密传递, 能够有效防止密钥被窃取带来的不安全. 通信方 A 向通信方 B 完成身份认证后, 通信方 B 也要向通信方 A 完成相应的身份认证, 实现双向认证后, 进行数据通信.

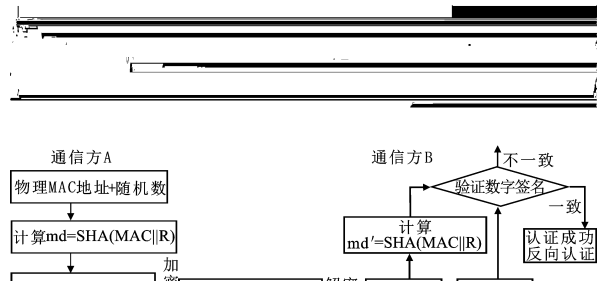


图 2 身份认证请求流程图

通信各方实现双向认证后, 即可构成异构网络签到环境. 拓扑结构如图 3 所示. 智能终端在无线 WiFi^[13] 环境下, 连接最近最强信号的 AP 热点, 通过身份认证后, 将个人信息传输至认证服务器, 认证服务器将认证通过的用户信息传输至统计服务器,

整个过程使用本文设计的安全数据传输机制对个人信息、AP 信息进行加密传输。

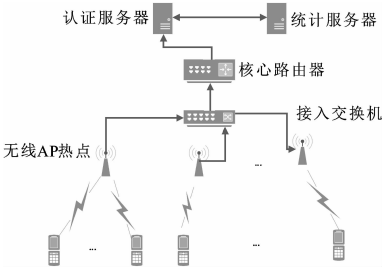


图 3 异构网络环境通信拓扑图

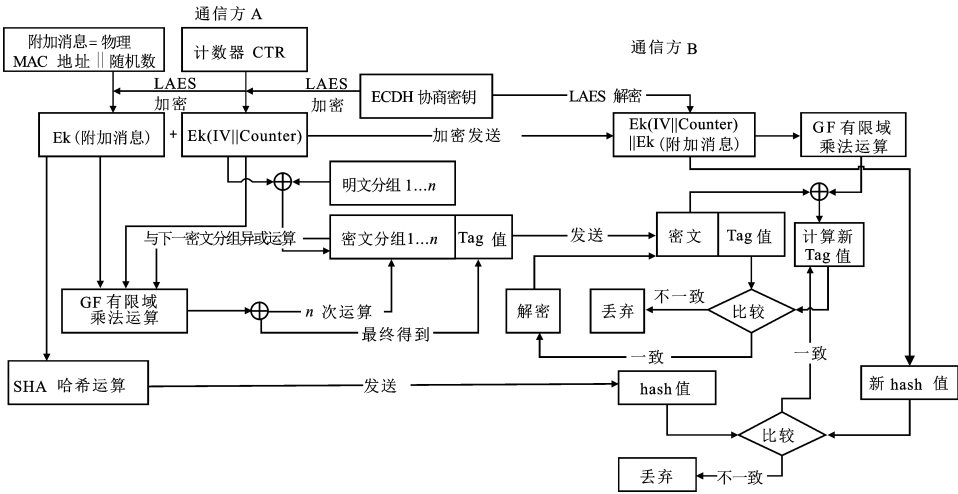


图 4 通信双方传输加密消息数据流程图

计数器的值利用协商密钥使用 LAES 加密, 然后与分组明文进行异或运算, 得到分组密文; 附加消息由物理 MAC 地址和随机数构成, 经过 LAES 加密后, 在 GF(2⁸) 有限域做乘法运算, 并与分组密文进行异或, 结果再进行有限域乘法运算, 与下一组分组密文异或运算, 最终得到消息标签 tag 值, 附加于密文之后发送给接收方, 同时将初始计数器值和附加消息进行二次加密后发送到接收方, 用于接收方进行 tag 值计算。接收方首先校验数字签名, 一致说明发送者正确, 否则丢弃; 其次对初始计数器值和附加消息进行解密, 然后与密文进行有限域乘法运算得到新的 tag 值, 与接收到的 tag 比较, 一致则说明消息是完整的, 可进行密文解密; 否则丢弃报文。同理, 接收方使用同样的加密认证方法与发送方通信。在报文的发送/接收过程中, 即使数据被窃取也不会对用户的身份和通信带来影响, 因为传送的计数器初始值和附加消息是二次加密, 密文和 tag 值也进行了加密, 上述方法保证了消息的安全性。

3.4 改进的 AES-GCM 数据完整性校验算法

通信双方完成双向认证后, 即可发送加密数据消息。本文在加密数据时, 选择分组和密钥长度均为较低的 128 比特, 采用文献[14]提出的改进的 AES 算法, 即轻量级高级加密标准 LAES(Lightweight AES)算法, 在保证加密算法安全性的前提下, 对轮数进行精简, 实验证明, 7 轮加密已足够保证安全, 极大降低算法的计算负担; 并且利用查表法优化算法的轮函数, 进一步加快算法执行速度。通信双方传输加密消息数据流程图如图 4 所示。

4 安全数据传输机制性能分析

本文提出的安全数据传输机制是从密钥安全生成与管理、双向身份认证及数据加密传输等方面提高数据传输的安全性。

4.1 安全性

- (1)双向认证确定合法身份。在正式传输加密数据之前, 所有的通信方均完成了双向身份验证。该阶段可以避免非法通信方随意接入通信环境, 一旦认证失败, 接收方立刻关闭与发起方的连接, 其后的一切操作也将无效。
- (2)抵御重放攻击。在认证阶段和加密数据传输阶段, 都采用了随机数机制, 第一次采用 LAES 加密, 第二次在消息密文中又被加密, 攻击者即使截取消息, 也很难判断具体在加密消息中的位置, 也就无法破解和重用, 能够有效抵御重放攻击。
- (3)安全的密钥协商机制。采用的是基于 ECC 算法的密钥生成与协商机制, 将公私钥设计成与随

机数和时间戳有关的值,能够实现密钥自动更新,保证密钥及时泄露也不会造成安全影响,且所有通信方的密钥通过协商机制获得,避免了密钥被二次加密再传输,方便密钥管理。

(4)数据保密性、完整性和不可抵赖性. 该认证加密算法首先对明文进行加密,接着用加密后的附加消息再次与分组密文运算得到标签 Tag 值,随密文发送,保证了消息的完整性和私密性. 每个消息都进行数字签名,保证消息的不可抵赖性。

在上述异构网络环境中,采用文本提出的基于 LAES-GCM 的安全数据传输机制监测校内某一区域连续一段时间内智能终端连接无线 AP 接入点,与认证服务器完成身份认证,并将信息传输到统计服务器,对比采用标准 ECDH 密钥管理机制和标准 AES-GCM 加密数据的加密时间,测试结果如表 1 所示。

表 1 基于 LAES-GCM 与标准 AES-GCM 的数据安全传输机制加密时间对比

算法名称	平均加密时间/ms
LAES-GCM	1.056
AES-GCM	13.724

由表 1 数据可以看出,本文提出的基于改进 ECDH 密钥协商机制和 LAES-GCM 算法的安全数据传输机制比标准算法的加密时间提高了近 13 倍,且密钥随着随机数与时间戳更新,有效防止穷举攻击、中间人攻击和重放攻击。

4.2 高效性

(1)密钥管理效率高. 本文提出的密钥是分布式生成,节点产生自身的公私钥,然后通过改进的 EC-DH 算法协商出共同密钥,密钥无需通过信任中心分发,也不需要加密传输,效率高。

(2)轻量级的 AES 算法. 文章中多次用到轻量级的 LAES 加密算法. 该算法加密轮数少,使用优化后的轮函数,在保证安全性的基础上,提高了算法的执行速度。

统计服务器分别统计教职工和学生从 2019 年 1 月 2 日至 1 月 12 日出入我校南门的占比,如图 5 所示. 上午是指每天 7:50 至 8:10 这半个小时时间段,我校上班/课时间为 8:00,下午是指每天 4:50 至 5:10 这半个小时时间段,我校下班时间为 5:10,通过统计图可以看出在周末时间段,学生明显比教工出入学校次数多,从 1 月 9 日后,我校进入考试周,学生出入人数减少. 统计服务器能够快速精准获取智能终端接入情况。

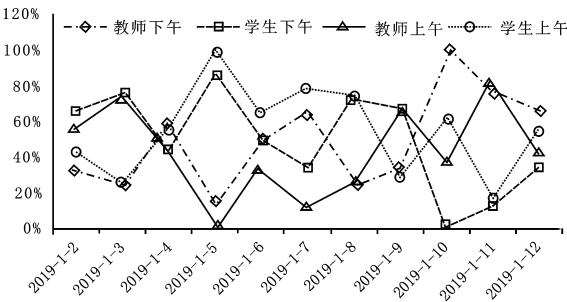


图 5 教职工/学生智能终端接入统计图

5 结束语

本文设计了一种适用于有线/无线异构网络环境的数据安全传输机制,详细介绍了本机制的工作原理,最后通过在异构网络环境中智能终端与服务器的通信实验验证本机制的安全性、精准性和高效性,可以尝试应用于外部异构网络环境,进行加密传输的压力测验。

参考文献:

[1] SERGEI SHUBIN, MARIA NESTERENKO. The Arctic: network diplomacy from the view of global security 2.0[J]. The Polar Journal,2018,8(1): 225-226.

[2] SONG L M, SONG X R. Design and implementation of a data security transmission scheme based on hybrid encryption[J]. Netinfo Security,2017(12):6-10.

[3] 邓昀,程小辉. 无线传感器网络轻量级数据加密机制设计[J]. 计算机工程与科学,2017,39(4):663-672.

[4] ZHU L N, ZHANG Z C, LI J H, et al. An improved random key predistribution scheme for wireless sensor networks using deployment knowledge[J]. International Journal of Security and Its Applications, 2016. DOI:10.14257/ijisia.2016.10.5.21.

[5] 冷飞,徐进华,栾仕喜. RSA 融合 AES 算法的网络信息安全方法[J]. 华侨大学学报(自然科学版),2017,38(1):117-120.

[6] 侯惠芳,季新生,刘光强. 异构无线网络中基于标识的匿名认证协议[J]. 通信学报,2011,32(5):153-161.

[7] 李雪松,彭长根,张弘. SMAE:一种新型认证加密算法[J]. 计算机工程与应用,2018,54(14):107-114.

[8] 雷志群. 一种基于 AES-GCM 的数据完整性校验方法[J]. 计算机与数字工程,2016,44(11):2229-2235.

[9] SREENATH THANGARAJAN, KANCHANA BH-AASKARAN V S. High speed and low power implementation of AES for wireless sensor networks[J]. Procedia Computer Science,2018(143): 736-743.

能广泛应用于目标搜索、异常检测、医疗诊断多个领域,后续能进一步扩展至目标数目未知的场景.

参考文献:

[1] CASTANON, DAVID A. Optimal search strategies in dynamic hypothesis testing [J]. IEEE transactions on systems, man, and cybernetics, 1995, 25 (7): 1130-1138.

[2] WANG C, ZHAO Q, COHEN K. Dynamic search on a tree with information-directed random walk [C]// IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). Kalamata, Greece, 2018: 1-5.

[3] KASPI Y, SHAYEVITZ O, JAVIDI T. Searching with measurement dependent noise [J]. IEEE Transactions on Information Theory, 2018, 64 (4): 2690-2705.

[4] CHERNOFF H. Sequential design of experiments [J]. The Annals of Mathematical Statistics, 1959, 30(3): 755-770.

[5] BESSLER S A. Theory and applications of the sequential design of experiments, k-actions and infinitely many experiments. part i. theory [R]. Stanford University Center for Applied Mathematics and Statistics Labs, 1960.

[6] NAGHSHVAR M, JAVIDI T. Active sequential hypothesis testing [J]. The Annals of Statistics, 2013, 41(6): 2703-2738.

[7] NAGHSHVAR M, JAVIDI T. Sequentiality and ada-

ptivity gains in active hypothesis testing [J]. IEEE J. Sel. Topics Signal Processing, 2013, 7(5): 768-782.

[8] COHEN K, ZHAO Q. Active hypothesis testing for anomaly detection [J]. IEEE Transactions on Information Theory, 2015, 61(3): 1432-1450.

[9] HUANG B, COHEN K, ZHAO Q. Active anomaly detection in heterogeneous processes [C]// 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Calgary, Alberta, Canada, 2018.

[10] VAIDHIYAN N K, SUNDARESAN R. Active search with a cost for switching actions [C]// IEEE Information Theory and Applications Workshop (ITA). San Diego, California, USA, 2015: 17-24.

[11] CHEN D, HUANG Q, FENG H, et al. Active Anomaly Detection with Switching Cost [EB/OL]. (2019-04-02). <https://arxiv.org/abs/1810.11800>, 2018.

[12] ABRAHAM W. Sequential analysis [M]. Courier Corporation, 1973.

作者简介:

谌 达 男, (1994-), 硕士. 研究方向为主动假设检验理论. E-mail: 16210720026@fudan.edu.cn.

胡 波 男, (1968-), 教授. 研究方向为数字信号处理、数字通信和系统设计.

冯 辉 男, (1980-), 副教授. 研究方向为分布式信号处理应用.

(上接第 88 页)

[10] 李湘锋, 赵有健, 全成斌. 对称密钥加密算法在 IPsec 协议中的应用 [J]. 电子测量与仪器学报, 2014, 28(1): 75-83.

[12] HE HAO, YI W D, LI M, et al. Homomorphic hashing verification for wireless sensor networks rateless codes over-the-air programming [J/OL]. Journal of Beijing Institute of Technology: 1-10 [2019-01-18]. <https://doi.org/10.15918/j.jbit1004-0579.17150>.

[13] MD IFTEKHAR HUSSAIN, ZAVED IQUBAL AHMED, NITYANANDA SARMA, et al. An efficient TDMA MAC protocol for multi-hop WiFi-based

long distance networks [J]. Wireless Personal Communications, 2016, 86(4): 150-168.

[14] 张尧, 叶玲. 基于 AES 的 WSN 加密算法 [J]. 计算机工程与设计, 2015, 36(3): 619-623.

作者简介:

石玲玲 女, (1990-), 硕士, 工程师. 研究方向为计算机网络、信息安全. E-mail: 15855401823@163.com.

李敬兆 男, (1964-), 教授, 博士生导师. 研究方向为嵌入式技术、物联网和云计算.