

无线传感器网络中安全数据融合方法研究

季田辉, 杨 庚

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘要:随着无线传感器网络应用的不断增加,很多应用都需要保证信息或数据的隐私性和完整性,这就对数据融合提出了更高的要求和新挑战,因此设计一种兼顾数据机密性和完整性的数据融合算法就显得尤为重要。文中提出了一种基于同态加密对数据的安全性进行保护和基于同态验证码对数据的完整性进行保护的算法。同态加密可以对加密数据直接进行操作,同态验证码抗攻击性强,具有良好的完整性保护特性。同时算法依据数据融合的树结构本身的特征,减少了数据通信开销,计算复杂度低。理论分析和仿真结果显示了该方法的有效性。

关键词:无线传感器网络;数据融合;同态验证码

中图分类号:TP301

文献标识码:A

文章编号:1673-629X(2014)07-0162-04

doi:10.3969/j.issn.1673-629X.2014.07.040

Research on Security of Data Aggregation in Wireless Sensor Networks

Ji Tian-hui, YANG Geng

(College of Computer Science & Technology, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: With the increasing application of wireless sensor networks, many applications need to guarantee the privacy and integrity of the information or data, the data fusion has been put forward higher requirements and new challenges, therefore, to design an data fusion algorithm with both data confidentiality and integrity is particularly important. It presents an algorithm for data security protection based on homomorphic encryption and to promise the data integrity based on homomorphic verification code. Homomorphic verification code of strong attack resisting, has good properties of integrity protection. At the same time, the algorithm based on tree structure data fusion itself, reduces the data communication overhead with low computing complexity. Theoretical analysis and simulation results show the effectiveness of the proposed method.

Key words: wireless sensor network; data aggregation; homomorphic verification code

0 引言

随着传感器技术的发展和无线通讯技术的进步,无线传感器网络(WSN)已经在军事、商用和民用领域得到了广泛的应用。无线传感器网络由大量资源有限的节点随机地以自组织的方式组成,用来监控目标环境,例如瓦斯检测系统,环境检测,军事应用等。但是,受到网络的能量消耗巨大,通信效率低下等限制,而且大多数情况下,无线传感器网络都是部署在一些无法控制,危险性比较高的环境中。由于WSN的这些问题,数据融合技术得到了广泛的发展。

在WSN中,数据融合技术着重考虑的是数据的机密性和完整性保护。机密性是为了保证叶子节点传输的数据以及融合节点传输的融合数据不会被窃听,完整性则是防止外来攻击者对叶子节点数据以及融合节点的数据进行截取和篡改,或者以伪身份的方式让基站接收到非法的值。为了实现安全的数据融合,研究者提出了多种方案来保证融合结果的安全性。

文献[1]提出了应用同态加密和密钥共享的办法保护数据的机密性和完整性,但是对于恶意节点的检测方面没有很好的解决办法。文献[2]是基于簇状来

收稿日期:2013-08-24

修回日期:2013-11-29

网络出版时间:2014-02-24

基金项目:国家“973”重点基础研究发展计划项目(2011CB302903);国家自然科学基金资助项目(61272084,61202004);江苏省高校自然科学研究重大项目(11KJA520002);江苏省科技支撑计划(社会发展)项目(BE2011826);高等学校博士学科点专项科研基金资助课题(20113223110003,20093223120001)

作者简介:季田辉(1990-),女,硕士研究生,研究方向为无线传感器网络的数据融合;杨 庚,博士,教授,研究方向为计算机图像处理、网络安全、分布与并行计算、移动计算。

网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140224.0916.039.html

实现数据机密性的隐私保护算法,但仅在特定的融合功能中能够有效运用。文献[3]是在文献[2]的基础上加入了完整性保护的方法,同时也继承了一些文献[3]的缺点,而且在增加了完整性保护之后算法的复杂度和通信开销也变大了。文献[4]也提出一种将同态加密和消息验证码结合的方式来实现有效的数据融合,算法加密使用线性运算,容易被敌对者攻破,而且仿真结果只是局限在小的无线传感器网络中,适用面不广。

文中提出一种基于同态加密和同态验证码的算法(DMAC)实现数据的机密性和完整性保护。它是在文献[5-6]的基础上做出相应的改进,同态加密是运用在WSN中比较常见的隐私保护的方法,同态验证码是由节点产生tag值,并在QS节点验证数据的发送和接收是否一致。将两种方法结合,实现了对数据隐私保护,同时获得了很高的完整性保护。

1 相关工作

在典型的无线传感器网络中,传感器节点的能量、存储和处理能力都十分有限,为了节省能量和资源,应尽量避免网内数据传输时的碰撞次数。文献[7-8]提出的融合算法,以传感器节点都是可信任的同时监测环境是安全的为前提。然而,实际上传感器节点一般都是部署在无法控制的危险性高的环境中,节点间的通信被窃听的可能性较高。文献[9-10]主要研究关于阻止攻击者试图篡改节点或窃听传输数据的安全的数据融合算法。

在现有的大多数安全的数据融合算法中,中间融合节点都是先将收到的数据进行解密,然后依据合适的融合函数进行融合处理,最后加密融合结果进行下一步的传输。这种做法提高了节点的计算开销,增加了节点的能耗。

文献[4]对算法进行简单的描述,分为三步:广播查询阶段、数据融合阶段、认证过程。

算法的模型如图1所示。

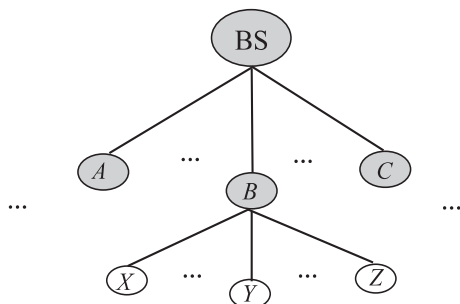


图1 无线传感器网络模型

1) 广播查询阶段。

基站广播数据查询信息,使用已存在的轻量级广

播认证机制如 p. TESLA 来进行广播认证。

2) 数据融合阶段。

图1所示为算法的网络模型,每个节点有三个不同的密钥:

- (1) 节点和基站共享的同态加密的密钥 Enc ;
- (2) 节点和其簇头节点共享的对称密钥 $k_{ni, nj}$;
- (3) 节点和基站共享的对称密钥 k_{ni} 。

若节点 x 对基站的请求进行响应,则将其数据 m 做以下的处理:

- (1) 利用同态加密算法得到 $Enc(m_x)$;
- (2) 用节点 x 和其簇头 B 共享的对称密钥 $k_{x,b}$ 进行加密得到 $k_{x,b}(m_x)$;
- (3) 使用节点与基站共享的对称密钥 k_x 对 m_x 生成信息认证码 $MAC(k_x, m_x)$;
- (4) 最后将生成的数据发送至 $B: x \rightarrow B: ID_x, Enc(m_x), k_{x,b}(m_x), MAC(k_x, m_x)$ 。

当簇头 B 接收到其所有响应的簇内节点的消息后, B 簇头做如下处理:

- (1) 将 $Enc(m_x), Enc(m_y), Enc(m_z)$ 等进行融合得到 $Enc(data_B')$;
- (2) 将 $k_{x,b}(m_x), k_{y,b}(m_y), k_{z,b}(m_z)$ 等密文进行解密,并融合得到 $data_B$;
- (3) 将所有响应节点发送到 MAC 存储;
- (4) 簇头 B 使用与基站共享的对称密钥 $k_{B, BS}$ 对接收到的 $data_B$ 加密生成 $k_{B, BS}(data_B)$;
- (5) 簇头 B 使用与基站共享的对称密钥 k_B 对自身的数据生成消息认证码 $MAC(k_B, data_B)$;
- (6) 最终发送至 BS 自己融合的数据: $ID_B, Enc(data_B'), k_{B, BS}(data_B), MAC(k_B, data_B)$ 。

当基站收到簇头的融合数据后,将其进行数据融合,然后利用对应的解密数据加密得到相应的融合数据 $data$ 和 $data'$ 。

3) 认证过程。

当 $data' = data$ 的时候,则可以说明数据在传输的过程中没有被破坏,接收。不相等则不接收,再进行节点的检测。

2 系统模型与算法实现

2.1 网络模型

在文中,无线传感器网络(WSN)由一个连通图表示,表示形式是 $G(V, E)$ 。其中的 V 是顶点,表示 WSN 中的节点; E 是边,表示节点间的通信链路。 N 记为 WSN 中节点的数量。

在 WSN 中,节点分为三种不同类型: QS (QueryServer) 节点(一般称作基站 BS)、中间融合节点和叶子节点。QS 节点发送和应答查询请求,同时也是

数据融合结果的集结处。在文中,只考虑了网络中只有一个 QS 节点的情况。中间融合节点负责给其子节点传递查询请求,并将从子节点接收的数据和自身采集的数据进行融合,再向上传递给其父节点。叶子节点负责收集数据,将收集的数据进行处理以后传递给其父节点。

2.2 数据融合模型

定义数据融合函数为 $y(t)=f(d_1(t), d_2(t), \dots, d_N(t))$, $d_i(t)$ 表示节点 i 在 t 时刻采集到的数据,数据融合示意如图 2 所示。

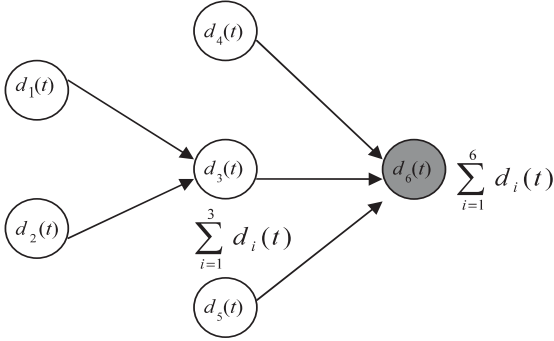


图 2 SUM 函数示意图

由于许多典型的数据融合函数,如 count、average、max、min 等都可以化简为 sum 函数,因此在文中以 sum 函数为研究对象,记 $y(t)=\sum_{i=1}^N d_i(t)$ 。

2.3 算法阐述

算法首先将信息 m 分解成 d 段, $m=(m_1, m_2, \dots, m_d)$, 系统共享密钥 $k=(k_1, k_2)$ 。

数据加密过程: $C=E_{(k_1, k_2)}(m)=E_{(k_1, k_2)}(m_1, m_2, \dots, m_d)=(m_1 \cdot k_1 \% q, m_2 \cdot k_1^2 \% q, \dots, m_d \cdot k_1^d \% q)$, 其中 $q=2^l$, l 为信息 m 的长度。

数据解密过程: $m=D_{(k_1, k_2)}(c)=D_{(k_1, k_2)}(c_1, c_2, \dots, c_d)=(c_1 \cdot k_1^{-1} \% q, c_2 \cdot k_1^{-2} \% q, \dots, c_d \cdot k_1^{-d} \% q)$

同态验证码定义如下。

同态验证码^[11]具有以下两个性质:

同态属性: 给定两个 (m, tag) 对 (m_1, t_1) 和 (m_2, t_2) , 聚合信息 $m=\alpha_1 \cdot m_1 + \alpha_2 \cdot m_2$ 的 tag 值 $t=\alpha_1 \cdot t_1 + \alpha_2 \cdot t_2$ 。其中 α_i 为信息 m_i 的权值。

安全性很高: 即使是在已知的信息攻击下, 攻击者可以知道算法将产生的 tag 值的数目, 但是对于一些线性组合的信息来说, 攻击者产生的 tag 值将会是不可行的。

同态验证码由三个多项式时间算法 (Sign, Aggregate, Verify) 组成。Sign 算法用于计算每个信息 m 的 tag 值, Aggregate 算法用于实现同态属性, Verify 用于验证发送方和接收方数据是否一致。

Sign(k, m_i, id_i): 为信息 m_i 计算 t_i 。节点 i 拥有标

识 id_i , 使用键值 k 来计算 tag 的值。Aggregate($(m_1, t_1, \alpha_1), (m_2, t_2, \alpha_2), \dots, (m_j, t_j, \alpha_j)$) 为聚合数据 $m=\sum_{i=1}^j \alpha_i m_i$ 计算 tag 值 t 。 α_i 为每一个信息 m_i 的权值。Verify(k, m, t) 利用键值 k 以及 tag 值 t , 来验证信息 m 的完整性。

2.4 算法实现

该算法在 TAG 算法的基础上建立融合树, 数据在传输之前先计算数据的 tag 值, 再对数据进行加密, 之后传输到融合节点, 对聚合信息计算 t 值, 最后传输到 QS 节点, 进行数据的验证。具体实现如下:

为了实现算法, 将信息 m 分解成 d 段, 所以可以将信息 m 看成具有 d 段数据的向量: (m_1, m_2, \dots, m_d) , $m_i \in F_q, i=1, 2, \dots, d$ 。整个系统共享一个键值对 $k=(k_1, k_2)$, 让 K_1 表示 k_1 的键值空间, K_2 表示 k_2 的键值空间。I 表示节点 id_i 的空间, 算法定义了两个伪随机函数 R_1 和 $R_2, R_1: K_1 \rightarrow F_q^d, R_2: (K_2 \times I) \rightarrow F_q$ 。

Sign(k, m_i, id_i):

1. $a=R_1(k_1)$

// 利用伪随机函数将 k_1 分解成 d 段

2. $b=R_2(k_2, \text{id}_i)$ // 伪随机函数 R_2 计算 b

3. $t_i=a \cdot m_i + b$ // $a \cdot m_i$ 为 a 和 m_i 的内积

接下来对数据进行加密: $C_i=E_{(k_1, k_2)}(m_i)=E_{(k_1, k_2)}(m_i, m_i, \dots, m_i)=(m_i \cdot k_1 \% q, m_i \cdot k_1^2 \% q, \dots, m_i \cdot k_1^d \% q)$ 。

Aggregate($(c_1, t_1, \alpha_1), (c_2, t_2, \alpha_2), \dots, (c_j, t_j, \alpha_j)$)

1. $c=\sum_{i=1}^j \alpha_i c_i$

2. $t=\sum_{i=1}^j \alpha_i t_i$

Aggregate 算法是在聚合节点完成的。

Verify(k, m, t)

1. $a=R_1(k_1)$

2. $b=\sum_{i=1}^j w_i \cdot R_2(k_2, \text{id}_i)$

3. $t'=a \cdot m + b$ // 信息 m 为聚合的加密信息 c 经过解密之后得到的

当 QS 算出 t' , 与聚合产生的 t 进行比较, 如 $t=t'$ 则说明接收的信息是完整的。否则是不完整, 不接收。

3 性能分析

主要从数据的通信开销和完整性鉴别两个方面对该算法进行性能分析, 并和文献[4]的算法进行比较。使用 TOSSIM^[12] 进行仿真, 具体的网络环境配置为: 600 个节点随机分布于 400 m×400 m 区域中, 无线信道对称, 标准室内环境, 背景噪声为 -105.0 dBm, 高斯白噪声为 4 dB, 节点的数据传输速率为 1 Mbps, 节点

的灵敏度为-108.0 dBm,节点的传输距离为50 m。

3.1 数据通信开销

DMAC 算法分为建立融合树阶段,数据融合阶段,验证阶段,数据进行一次加密并传输;文献[4]算法,原数据进行三次的加密并传输,从理论上分析来看,通信开销会比 DMAC 算法的通信开销要高。图3说明了算法的通信开销和传感器节点数目之间的关系,可以看出随着节点数目的增加,其对应的通信开销就会增加。通过分析可以知道,数据的通信量和节点数目增加成正比。

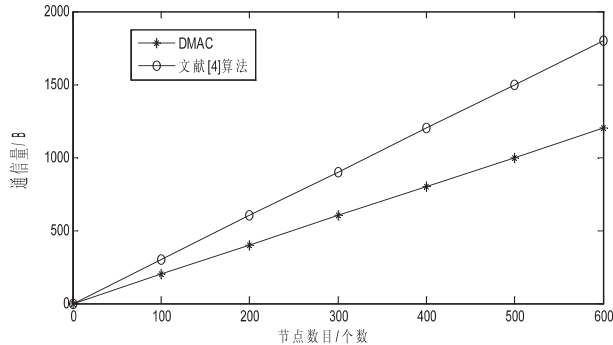


图3 通信量随节点的变化

3.2 完整性鉴别

假设 A 是敌对方,有两种类型的恶意节点 A_1 和 A_2 。同时假设两种不同的恶意节点攻击的两种可信任节点是 B_1 和 B_2 ,同时,节点都是伪随机 (PRG 和 PRF)^[13] 的节点。有以下的结论:完整性被破坏的概率小于等于 A_1 攻破 B_1 的概率, A_2 攻破 B_2 的概率, $1/q$ 三者之和。即:

$$P(\text{MAC}, A) \leq P(B_1, A_1) + P(B_2, A_2) + 1/q \quad (1)$$

证明如下:

分别定义了以下三种 Game,并且用 W_i 表示攻击者 A 在 Game_i 中攻破的事件, Game_0 表示攻击者 A 对整个同态 MAC 发起的攻击,则:

$$P[w_0] = P[A, \text{MAC}] \quad (2)$$

Game_1 和 Game_0 不同是 Sign 算法的第一步, Game_1 将 Game_0 中的 $a = R_1(k_1)$ 替换成了 $a \leftarrow F_q^d$,就是将伪随机函数产生的伪随机数值替换掉,则可表示为:

$$|P[w_0] - P[w_1]| = P(B_1, A_1) \quad (3)$$

Game_2 和 Game_1 的不同是在 Sign 算法的第二步, Game_2 将 Game_1 的 $b = R_2(k_2, \text{id}_i)$ 替换成了 $b = F_q$,就可以表示为:

$$|P[w_1] - P[w_2]| = P(B_2, A_2) \quad (4)$$

$$P[w_2] = 1/q \quad (5)$$

因为 $P[W_2^*T] = 1/q * P[T]$, $T = (\text{Sign}, \text{Combine}, \text{Verify})$, 四者相加可以得到公式(1)。公式(2)和公式(3)的概率值很小, q 是数组的大小,一般会定义

为很大,这样子防止数据的溢出,一般为256位,由此可以看出整个算法被攻破的可能性很小,完整性不易被破坏。

4 结束语

提供高效的数据融合的同时保证数据隐私是目前无线传感器网络极具挑战性的问题。许多民用方向的应用都需要隐私保护,否则居民不会同意使用无线传感器网络来采集他们的私人数据。文中提出了一种既确保了隐私性又保证了数据的完整性的方法,在仿真的基础上进行了分析,数据的通信开销也不算大,并能确保很好的完整性保护。数据融合还要进一步的研究,以达到更好的发展。

参考文献:

- [1] Papadopoulos S, Kiayias A, Papadiaz D. Exact in-network aggregation with integrity and confidentiality[J]. IEEE Transactions on Knowledge and Data Engineering, 2012, 24(10): 1760-1773.
- [2] He Weibo, Liu Xue, Nguyen H, et al. PDA: privacy-preserving data aggregation in wireless sensor networks[C]//Proc of the 26th IEEE international conference on computer communications. Washington DC, USA: IEEE Computer Society Press, 2007: 2045-2053.
- [3] He Weibo, Liu Xue, Nguyen H, et al. A cluster-based protocol to enforce integrity and preserve privacy in data aggregation[C]//Proc of the 29th IEEE international conference on distributed computing systems. Montreal, QC: IEEE Press, 2009: 14-19.
- [4] 张双杰, 魏琴芳, 秦晓良. 无线传感器网络中有效的安全数据融合机制[J]. 电视技术, 2012, 36(1): 67-70.
- [5] Girao J, Westhoff D, Schneider M. CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks[C]//Proc of 2005 IEEE international conference on communications. [s. l.]: IEEE, 2005: 3044-3049.
- [6] Li Z, Gong G. Data aggregation integrity based on homomorphic primitives in sensor networks[M]//Ad-Hoc, Mobile and Wireless Networks. Heidelberg, Berlin: Springer, 2010: 149-162.
- [7] Intanagonwiwat C, Estrin D, Govindan R, et al. Impact of network density on data aggregation in wireless sensor networks[C]//Proceedings of the 22nd international conference on distributed computing systems. [s. l.]: [s. n.], 2002: 457-458.
- [8] Tang X, Xu J. Extending network lifetime for precision constrained data aggregation in wireless sensor networks[C]//Proc of INFOCOM. Barcelona, Spain: IEEE, 2006: 1-12.
- [9] Yang Yi, Wang Xinran, Zhu Sencun, et al. SDAP: a secure hop

(下转第169页)

(6)S 替换盒界面设计。

该界面可以直接进行 S 替换盒类型的选择。

该系统对各个模块都进行了直观简洁界面的设计,满足软件专业化标准化的需求,方便用户的操作。

3.4 测试

(1)测试用例。

测试用例包含 Excel 文件、Word 文件、PDF 文件、txt 文件、mp3 文件和 rmvb 视频文件,原文件列举如下:

- 09 计软综合测评-2011-10-11(终极版). xls;
- DES 加密算法原理. pdf;
- DES 算法理论. doc;
- 一种 DES 密钥延长方法. txt;
- 董文华-军港之夜. mp3;
- 杀手代号 47_clip. rmvb。

(2)测试结果。

以“DES 算法原理及改进. txt”文件为例,加密后、解密后的内容如图 5 所示。

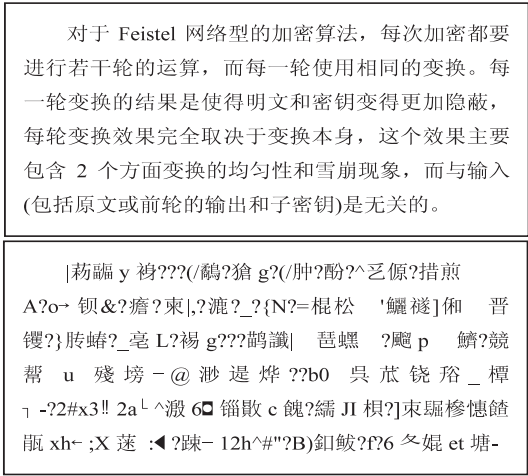


图 5 加密后与解密后文本文件

对 Excel 文件和 Word 文件进行加密后,与 txt 文件相似,再执行打开操作时都以乱码的形式表现出来;PDF 文件加密后,再打开时会显示“格式错误:不是一个 PDF 文件或该文件已损坏”;mp3 文件和 rmvb 文件加密后,再打开时也会提示“打开格式错误”。而经过解密之后,所有格式的文件都恢复为原有的内容。

该测试结果证明此算法是行之有效的。

4 结束语

文中首先提出了局部独立子密钥的二重 DES 算法,该算法结合了三重 DES 算法与具有独立子密钥算法的优点,在提高算法加密强度和有效地抵抗穷举攻击法的同时,增强了密钥安全度。然后基于此算法实现了文件加密系统,并对各种样式的文件进行了测试,测试结果证明该系统比三重 DES 算法和独立子密钥算法具有更高的加密强度和运行效率。

参考文献:

[1] Grabbe J O. The DES algorithm illustrated[J]. Laissez Faire City Times,1992,2(28):12-15.

[2] Beth T,Gollman D. Algorithm engineering for public key algorithms[J]. IEEE Journal on Selected Areas in Communications,1989,7(4):458-466.

[3] Liang Ye,Zhao Yanmin. Analysis and research of data encryption algorithm[J]. Journal of Gansu Normal Colleges,2011,16(2):14-16.

[4] Schneier B. 应用密码学[M]. 北京:机械工业出版社,2000.

[5] 伍红兵. DES 数据加密算法原理,实现[J]. 电脑编程技巧与维护,2000(3):85-88.

[6] 张 洁,朱丽娟. DES 加密算法分析与实现[J]. 软件导刊,2007(3):95-97.

[7] 徐洪波,李颖华. DES 加密算法在保护文件传输中数据安全的应用[J]. 信息安全学报,2009(6):24-26.

[8] Jain N,Kaur G. Implementing DES algorithm in cloud for data security[J]. VSRD-International Journal of Computer Science and Information Technology,2012,2(4):316-321.

[9] 姚 霁,刘建华,范九伦. 一种密钥可配置的 DES 加密算法的 FPGA 实现[J]. 电子技术应用,2009(7):145-148.

[10] 邱伟星,肖克芝,倪 昉,等. 一种 DES 密钥延长方法[J]. 计算机工程,2011,37(5):167-168.

[11] 刘晓星,胡畅霞,刘明生. 安全加密算法 DES 的分析与改进[J]. 微计算机信息,2006,22(4-3):32-33.

[12] 李少芳. DES 算法加密过程的探讨[J]. 计算机与现代化,2006(8):102-104.

[13] 董清潭. 三重 DES 加密算法原理与实现[J]. 电脑知识与技术,2011,7(12):2776-2778.

[14] 蒋 波. 一种基于三重 DES 和 RSA 的综合加密方案[J]. 微计算机信息,2007,23(6-3):52-53.

(上接第 165 页)

-by-hop data aggregation protocol for sensor networks[C]//Proc of MobiHoc. Florence, Italy:ACM,2006.


[10] Wagner D. Resilient aggregation in sensor networks[C]//Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks. New York, NY, USA:ACM,2004:78-87.

[11] Agrawal S,Boneh D. Homomorphic MACs:MAC-based integrity for network coding[C]//Proc of the 7th international conference on applied cryptography and network security. Heidelberg, Berlin:Springer-Verlag,2009:292-305.

[12] Levis P,Lee N,Welsh M,et al. TOSSIM:accurate and scalable simulation of entire TinyOS applications[C]//Proc of the 1st international conference on embedded networked sensor systems. New York, NY, USA:ACM,2003:126-137.

[13] Katz J,Lindell Y. Introduction to modern cryptography[M]. [s. l.]:CRC Press,2008.

无线传感器网络中安全数据融合方法研究

作者: [季田辉](#), [杨庚](#), [JI Tian-hui](#), [YANG Geng](#)
作者单位: [南京邮电大学 计算机学院, 江苏 南京, 210003](#)
刊名: [计算机技术与发展](#) 
英文刊名: [Computer Technology and Development](#)
年, 卷(期): 2014(7)

本文链接: http://d.wanfangdata.com.cn/Periodical_wjfz201407040.aspx