传感器网络安全数据融合

张 鹏 喻建平 刘宏伟
(深圳大学 ATR 国防科技重点实验室 深圳 518060)

摘 要 安全数据融合的目标是在融合数据的同时,实现传感器节点感知数据 end-to-end 机密性与可认证性。End-to-end 机密性一般由秘密同态加密技术来保障。针对 end-to-end 可认证性与数据融合的矛盾,在同态认证技术不适用于多源多消息的背景下,为了实现 end-to-end 可认证性,采用对称加密技术构造了一个安全的数据融合认证方案。采用该数据融合认证方案与秘密同态加密方案,构造了安全的数据融合协议。安全性分析表明,该安全数据融合协议能在融合数据的同时保障感知数据 end-to-end 机密性与可认证性。

关键词 传感器网络,安全数据融合,秘密同态,end-to-end 机密性,end-to-end 可认证性
中图法分类号 TP309 **文献标识码** A

Secure Data Aggregation for Sensor Networks

ZHANG Peng YU Jian-ping LIU Hong-wei
(ATR Key Laboratory of National Technology, Shenzhen University, Shenzhen 518060, China)

Abstract Secure data aggregation aims at realizing the end-to-end confidentiality and authentication of the data, which is collected and aggregated by sensor. End-to-end confidentiality is usually guaranteed by the privacy homomorphic encryption. However, the homomorphic authentic schemes are not multi-source and multi-message. For the contradictions between the end-to-end authentication and the data aggregation, a secure data aggregate authentic scheme was proposed. A secure data aggregate protocol was constructed with the proposed authentic scheme and a homomorphism encryption scheme. Security analysis result shows that the proposed data aggregate protocol can obtain the end-to-end confidentiality and authentication of the collected data.

Keywords Wireless sensor networks, Secure data aggregation, Privacy homomorphism, End-to-end confidentiality, End-to-end authentication

1 引言

传感器网络节点的能量与资源严重受限,因此要尽可能地利用节点对数据进行预处理,减少数据传送数量或减小其大小,从而实现能量与资源的有效利用。数据融合[1,2]就是这样一种精简感知数据的技术,其目标在于通过使用数据融合技术将多个感知数据转化为单个的值,进而有效减少通讯负载、节省能量开销并延长网络寿命。

数据融合技术给传感器网络安全研究带来了挑战[3]:数据融合技术倾向于在中间节点融合明文数据,但其机密性要求传感器节点所感知的数据以密文的形式在网络中传输;数据融合技术使得基站接收到的信息不再是传感器节点所感知的原始信息,但其可用性要求基站在接收到信息以后能够对原始信息进行认证。数据融合技术下的 end-to-end 机密性与可认证性是安全数据融合协议研究的两个主要目标[4]。

传统的机密性保护主要以 hop-by-hop 的加密方式[5]为主。hop-by-hop 方案的中间节点能访问下层传感器节点感知数据;但不能在融合数据的同时保障数据 end-to-end 的机密性,且在中间节点执行解密—加密操作,增加了数据融合的成本,容易导致合法通信的时间延迟。文献[6]首先采用同态加密技术[7]构造了 CDA 方案,该方案对密文数据进行融合操作,从而保障了感知数据 end-to-end 机密性。

仅仅保障融合数据的机密性是不够的,敌手在不需要任何先验知识的前提下能有效篡改融合数据并通过基站解密,使得融合结果不再有意义[8]。因此,提供安全的 end-to-end 认证机制与安全的 end-to-end 加密机制同等重要。但是由于感知数据的多源性,认证标签由不同传感器节点签署,经典的同态签名技术[9]与同态消息认证码技术[10]无法适用于传感器网络数据融合,同态加密技术给数据可用性的鉴别带来了困难。文献[11]对发送消息进行编码,从而在采用同态加密技术的同时实现了 end-to-end 的机密性,但是方案将消息编码成原始消息的 η 倍(η 为簇中的传感器节点总数),且采用基于身份的数字签名技术,使得方案计算与通信成本均大幅增加,因此并未凸现出采用融合技术的优势。

本文对安全数据融合协议进行研究,指出融合技术与安全技术在需求上的冲突,重点研究并构造了秘密同态加密技术下的 end-to-end 认证方案,提出了一种能同时保障数据融合技术 end-to-end 机密性与可认证性的安全数据融合协议。

到稿日期:2010-09-27 返修日期:2011-01-17 本文受国家自然科学基金(61001058),深圳市科技计划项目(CXB200903090020A)资助。
张 鹏(1984—),女,博士生,主要研究方向为密码学与传感器网络信息安全等,E-mail:zhangpeng_aza@126.com;喻建平(1968—),男,教授,博士生导师,主要研究方向为密码学与信息安全;刘宏伟(1975—),男,博士,副教授,主要研究方向为密码学与信息安全。

2 预备知识

2.1 网络与攻击模型

本文工作基于分布式的大规模传感器网络，网络拓扑采用多层多跳结构。每个节点都有多个邻居节点，且拥有多条前往基站的路径。假定基站是可信且不可捕获的，它掌握网络中的节点数目、网络拓扑结构以及所有节点的基本信息，且每个节点都能验证基站广播信息的真实性。

假设网络模型部署完成以后，每个节点均可以与基站建立共享密钥。攻击者的攻击方式主要包括：1)攻击者对信道进行监听，以窃听传输数据或分析通信流量；2)攻击者伪造源节点发送虚假数据；3)攻击者非法篡改传输数据。攻击者的主要目的在于：窃取有效数据、伪造非法数据、欺骗基站、消耗能量与资源并影响网络运行效率。

2.2 秘密同态

给定明文信息空间$(M_1,\cdots,M_n)$、加密函数E与解密函数D，α、β为运算法则，若$D(\alpha(E(M_1),\cdots,E(M_n)))=\beta(M_1,\cdots,M_n)$成立，则称函数族$(E,D,\alpha,\beta)$为一个秘密同态[7]。典型的秘密同态有加性同态与乘性同态，分别描述为

$$D(\alpha(E(M_1),\cdots,E(M_n)))=M_1+\cdots+M_n$$

$$D(\alpha(E(M_1),\cdots,E(M_n)))=M_1\times\cdots\times M_n$$

3 安全数据融合协议

3.1 安全数据融合认证方案

如图1数据融合树所示，源节点s_1将感知数据密文C_1及其标签tag_1发送至融合节点A_1，然后转送至上层融合节点直至基站。基站由融合后的感知数据密文C_{Agg}解密出融合明文m_{Agg}，由于进行有损数据融合，基站无法恢复出明文m_1，因此采用传统的认证机制无法对标签tag_1进行end-to-end认证。

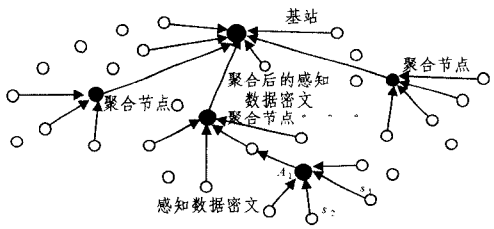

图1 传感器网络数据融合树

图1中，s_1、A_1分别与基站BS共享密钥对，s_1与A_1共享密文C_1。对tag_1进行认证的目的是：1)完整性：保障C_1在传输过程中不被篡改；2)可用性：确认C_1确实来自于源节点s_1。针对该特性，安全数据融合认证方案描述如下。

1)密钥生成算法$KeyGen(1^\lambda,n)\rightarrow(k_1,k_2,\cdots,k_n)$：输入安全参数$\lambda$与源节点总数$n$，基站执行该算法，输出对称密钥$k_i(1\leqslant i\leqslant n)$为基站与节点$s_i$的共享密钥。

2)生成标签算法$T(C_i,k_i)\rightarrow(hdr_i,tag_i)$：给定感知数据密文信息$C_i$，传感器节点$s_i$执行该算法，输出标签$tag_i=E'(H(C_i),k_i)$与首部信息$hdr_i=\{i\}$；$s_i$的上层融合节点$A_j$执行该算法输出标签$tag_i^{A_j}=E'(H(C_i),k_{A_j})$。

3)验证算法$V(hdr_i,tag_i,k_i)\rightarrow$True/False：基站收到首部信息$hdr_i$对应的标签$tag_i$与$tag_i^{A_j}$后，检验$D'(tag_i,k_i)=D'(tag_i^{A_j},k_{A_j})$是否成立，若成立则说明该感知数据密文$C_i$确实来源于$s_i$且在传输过程中未被篡改；反之亦然。

其中E'与D'分别代表对称加密方案(如AES方案)中的加密与解密函数；H为抗碰撞哈希函数。

3.2 安全数据融合协议

基于3.1节所述的安全数据融合认证方案与同态加密技术，安全数据融合协议描述如下。

1)密钥生成

源节点s_i与基站BS共享对称密钥k_i；融合节点A_j与基站BS共享对称密钥k_{A_j}。若采用公钥密码体制下的秘密同态加密技术，则BS需另外生成公私钥对(pk,sk)，并公开公钥pk。

2)加密并生成标签

源节点s_i采集到感知信息m_i后，首先加密m_i得密文$C_i=E(m_i,k_i)$或$C_i=E(m_i,pk)$，其中E为基于对称密码体制或基于公钥密码体制的同态加密函数；然后对密文C_i生成标签信息$tag_i=E'(H(C_i),k_i)$，其中E'为对称加密函数；最后将密文C_i、标签tag_i与首部信息hdr_i发送至上层融合节点。

3)融合并生成标签

融合节点A_j在接收到来自p个下层传感器节点的信息$(hdr_i,C_i,tag_i)(i=1,2,\cdots,p)$后，首先对$C_i$进行融合，得$C_{Agg}^{A_j}=\alpha(C_1,\cdots,C_p)$，其中$\alpha$为融合运算；然后对密文$C_i$分别生成标签信息$tag_i^{A_j}=E'(H(C_i),k_{A_j})$；最后将密文融合结果$C_{Agg}^{A_j}$与$(hdr_i,tag_i,tag_i^{A_j})(i=1,2,\cdots,p)$发送至上层融合节点或基站。

4)解密并验证标签

基站BS在接收到来自下层传感器节点的信息$C_{Agg}^{A_j}$与$(hdr_i,tag_i,tag_i^{A_j})(i=1,2,\cdots,p)$后：

a)验证下式是否成立。

$$D'(tag_i,k_i)=D'(tag_i^{A_j},k_{A_j}) \tag{1}$$

式中，D'为对称解密函数。若验证通过则进入步骤b，否则丢弃信息$C_{Agg}^{A_j}$；

b)解密融合结果$C_{Agg}^{A_j}$得$m_{Agg}^{A_j}=D(C_{Agg}^{A_j},k_1,\cdots,k_p)$或$m_{Agg}^{A_j}=D(C_{Agg}^{A_j},sk)$，其中$D$为基于对称密码体制或基于公钥密码体制的同态解密函数。

4 性能分析

由于安全数据融合的目的是保障数据融合技术end-to-end的机密性与可认证性，对新协议的安全性分析如下。

1)end-to-end机密性

源节点s_i采集到感知信息m_i后，首先采用与基站共享的对称密钥或基站公钥对该信息进行同态加密，然后送至融合节点A_j。信息以密文C_i的形式在信道中传输，包括融合节点在内的其它未授权实体均无法解密C_i。

融合节点A_j采用融合算法对来自下层传感器节点的密文进行融合，将融合结果$C_{Agg}^{A_j}$送至基站。基站采用秘密同态解密算法解密出融合明文$m_{Agg}^{A_j}$。

敌手在未知加密密钥或解密密钥的前提下，给定$x_0=\beta(m_{01},\cdots,m_{0n})$与$x_1=\beta(m_{11},\cdots,m_{1n})$，挑战者随机选择$b\in\{0,1\}$，加密$m_{bk}$并融合密文，由此敌手猜测$b'\in\{0,1\}$。若敌手赢得游戏的概率$Adv_{Agg}=|\Pr[b'=b]-\frac{1}{2}|$是不可忽略的，则存在敌手以$Adv_{Agg}$的概率攻破该安全数据融合协议与同态加密方案。

因此，该安全数据融合协议的end-to-end机密性基于秘

密同态加密方案的安全性，且与所采用的秘密同态加密方案是同等安全的。

2）end-to-end 可认证性

源节点 s_i 对感知信息密文 C_i 计算标签 $tag_i = E'(H(C_i), k_i)$；融合节点 A_j 收到密文 C_i 后计算标签 $tag_i^{A_j} = E'(H(C_i), k_{A_j})$。

若存在敌手篡改密文 C_i 为 C_i'，则基站计算 $C_i = D'(tag_i, k_i)$ 与 $C_i' = D'(tag_i^{A_j}, k_{A_j})$ 使得式(1)不成立，即融合信息密文 $C_{Agg}^{A_j}$ 无法通过验证，因此应丢弃。

若存在敌手冒充 s_i 发送密文 C_i'，则基站在接收到 $tag_i' = E'(H(C_i'), k_i)$ 后，由于基站采用与 s_i 共享的密钥无法解密 tag_i'，即融合信息密文 $C_{Agg}^{A_j}$ 无法通过验证，应丢弃。

因此，该安全数据融合协议的 end-to-end 可认证性是由协议所使用的对称加密算法来保障的。

本协议需要传输的标签数量为参与协议的源节点总数的 2 倍，但是由于在计算标签之前，协议首先对密文信息进行了散列，并采用对称加密算法加密散列值，且不存在信息交互，因此在计算量与通信量上，较文献[13]类采用的数字签名方案，依然存在明显的效率改善。

结束语 本文针对同态加密技术下的 end-to-end 可认证性保障问题，规避了多源多消息的同态签名技术与同态消息认证码技术，构造了新的安全数据融合认证方案，进一步构造了安全的数据融合协议。该协议能提供 end-to-end 的机密性与可认证性，有效解决了融合技术与安全技术在需求上的冲突。

在以后的工作中，将进一步深入探讨安全数据融合认证模型与方案，研究多源多消息的同态消息认证码技术与同态签名技术，彻底解决同态加密技术下的 end-to-end 可认证性保障问题。

参 考 文 献

[1] Akkaya K, Demirbas M, Aygun R S. The impact of data aggregation on the performance of wireless sensor networks[C]// Wireless Communication & Mobile Computing. 2008: 171-193

[2] 康健，左宪章，唐力伟，等. 无线传感器网络数据融合技术[J]. 计算机科学，2010，37(4)：31-35

[3] Ozdemir S, Xiao Y. Secure data aggregation in wireless senor networks: A comprehensive overview [J]. Computer Network, 2009, 53: 2022-2037

[4] Castelluccia C, Chan Aldar C-F, Mykletun E, et al. Efficient and provably secure aggregation of encrypted data in wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2009, 5(3): 1-36

[5] Yang Y, Wang X, Zhu S, et al. SDAP: A secure hop-by-hop data aggregation protocol for sensor networks[J]. ACM Transactions on Information and System Security, 2008, 11(4): 1-43

[6] Westhoff D, Girao J, Acharya M. Concealed data aggregation for reverse multicast traffic in sensor networks: encryption key distribution, and routing adaptation[J]. IEEE Transactions on Mobile Computing, 2006, 5(10): 1417-1431

[7] Domingo-Ferrer J. A provably secure additive and multiplicative privacy homomorphism[C]// Chan A H, Gligor V D, eds. ISC 2002. vol. 2433, 2002: 471-483

[8] Peter S, Piotroeski K, Langendoerfer P. On concealed data aggregation for wireless sensor networks[C]// Proc. IEEE Consumer Communications and Networking Conference. 2007: 192-196

[9] Boneh D, Freeman D, Katz J, et al. Signing a linear subspace: signature schemes for network coding[C]// Public Key Cryptography. PKC 2009, LNCS 5443. Springer Verlag, 2009: 68-87

[10] Chan Aldar C-F, Castelluccia C. On the (im)possibility of aggregate message authentication codes[C]// ISIT 2008. Toronto, Canada, 2008: 235-249

[11] Hung-min S, Yue-hsun L, Ying-chu H, et al. An efficient and verifiable concealed data aggregation scheme in wireless sensor networks[C]// The 2008 International Conference on Embedded Software and Systems. 2008: 19-26

(上接第 60 页)

4.3 鲁棒性

BPGKM 方案密钥树中每个内部节点有 3 个孩子节点，当某节点离开时，如果所在层具有两个兄弟节点，则网络拓扑图不发生变化；同理，有新节点加入，如果所在层为一个兄弟节点，则网络拓扑图也不发生变化。而在 STR 中节点加入和退出都需要改变密钥树结构，因此相对 STR 方案，BPGKM 减少了网络间的通信负载，保证了群密钥树的稳定性。

结束语 由于现有的群密钥管理方案基于 GDH 密钥协议，密钥树具有较大深度，降低了节点的群密钥操作效率，针对这一问题，本文提出了基于双线性映射的群密钥管理方案，该方案在保证安全性的前提下增加了密钥树每层的节点数，减少了同等规模网络下的密钥树的深度，提高了密钥管理效率。相对于 STR 方案，本文方案保持了群密钥操作中加入和合并的效率，同时使得离开和分离操作的效率提高一半。本文方案由于在每层上具有较多的节点，因此比现有方案具有更为稳定的密钥树结构。由此 BPKGM 更能适用大规模网络的群安全。在下一步工作中，将进一步研究 BPKGM 在 Ad-hoc 网络中的效率。

参 考 文 献

[1] Chlamtac I, Conti M, Liu J. Mobile Ad-hoc Networking: Imperatives and Challenges[J]. Ad-hoc Networks, 2003, 1(1)

[2] Basagni S. Mobile Ad-hoc Networking[M]. IEEE Press and Wiley, 2004

[3] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Transaction on Information Theory, 1976, 22(6): 644-654

[4] Steiner M, Tsudik G, Waidner M. Diffie-Hellman Key Distribution Extended to Group Communication[C]// Proceedings of ACM CCS. ACM Press, 1996: 31-37

[5] Kim Y, Perrig A, Tsudik G. Group Key Agreement Efficient in Communication[J]. IEEE Transactions on Computers, 2004, 53(7): 905-921

[6] Performance of Group Key Agreement Protocols [BP/OL]. http://www.cnds.jhu.edu/pub/papers/cnds-2001-5.pdf, 2001

[7] Sakai R, Ohgishi K, Kasahara M. Cryptosystems Based on Pairing[C]// Symp. on Cryptography and Information Security. Okinawa, Japan, Springer, 2000: 26-28

[8] Joux A. An One Round Protocol for Triphartite Diffie-Hellman [C]// Proceedings of ANTS. Heidelberg: Springer-Verlag, 2000: 385-394