

无线传感器网络安全数据融合研究

曹晓梅^{1,2,3}, 李万雷^{1,2,3}, 杨 庚¹

(1. 南京邮电大学 计算机学院, 江苏 南京 210003;

2. 江苏省无线传感网高技术研究重点实验室, 江苏 南京 210003;

3. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室, 江苏 南京 210003)

摘 要:数据融合去除冗余信息, 延长网络生命周期, 有效地缓解了无线传感器网络资源瓶颈的问题。但是, 无线传感器网络经常部署在开放的甚至敌对的环境中, 使其安全问题非常突出, 数据融合在具体实施过程中, 极易受到安全攻击。因此, 安全数据融合协议的设计成为无线传感器网络安全最为基本且重要的研究领域。文中分析了无线传感器网络数据融合面临的攻击种类和安全需求及挑战, 着重比较了近年来该领域具有代表性的安全数据融合协议, 指出了该领域今后的研究热点。

关键词:无线传感器网络; 安全数据融合; 攻击种类

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2012)11-0229-06

Research on Secure Data Aggregation in Wireless Sensor Network

CAO Xiao-mei^{1,2,3}, LI Wan-lei^{1,2,3}, YANG Geng¹

(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China

3. Key Lab of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Data aggregation eliminates redundant information, increases the lifetime of the network and effectively relieves the limit-resource problem in wireless sensor network. However, wireless sensor network (WSN) is usually deployed in open area, particularly in the hostile area, its security issue is very prominent, in the implementation of data aggregation in WSN, the data is prone to security attacks. Consequently, the design of secure data aggregation protocols is one of the most important aspects and basic research field of security wireless sensor network. It analyses various attacks, security goals and challenges in wireless sensor network data aggregation, then compares the recent representative secure data aggregation schemes. The future research direction is summarized.

Key words: wireless sensor network; secure data aggregation; types of attacks

0 引言

在无线传感器网络 (Wireless Sensor Network, WSN) 中, 传感器节点具有分布密集、感知协作的特点, 它们共同完成信息收集、目标监视和感知环境的任务。数据融合技术被用来去除采集数据传输中的冗余信息、减少传输量, 进而节省节点能量, 延长网络生命周期^[1]。

WSN 的开放性和自组织性, 使其极易受到各种攻击, 而针对融合数据和聚合节点的攻击危害程度更高, 其安全问题备受关注, 目前已有许多重要研究成果。文中对该领域的主要研究成果进行了回顾与总结, 阐述了代表性协议的关键技术实现, 对各协议进行分析和比较, 指出了未来的研究方向。

1 数据融合的安全问题

1.1 攻击种类

WSN 数据融合过程面临的攻击主要包括^[2]:

a) 窃听攻击: 攻击者通过对无线信道进行监听从而非法窃取融合数据;

b) 已知明文攻击: 攻击者分析明文与密文之间对应的词典破解网络的密码体制;

c) 重放攻击: 攻击者恶意重复发送先前节点或者

收稿日期: 2012-03-05; 修回日期: 2012-06-11

基金项目: 国家自然科学基金项目 (60873231); 国家“973”重点基础研究计划项目 (2011CB302903); 江苏高校优势学科建设工程资助项目 (yx002001)

作者简介: 曹晓梅 (1974-), 女, 江苏无锡人, 博士, 副教授, 主要研究领域为计算机通信网与安全; 李万雷 (1987-), 男, 硕士, 主要研究领域为无线网络安全。

基站已经接收过的数据,拖延正常数据发送,破坏数据融合的结果;

d) 篡改攻击:恶意的聚合节点对数据融合结果进行非法的篡改;

e) Sybil 攻击:攻击者利用被俘获的节点伪造多个虚假身份,向聚合节点发送数据报文,影响数据融合结果;

f) DoS 攻击:攻击者对网络中的特定节点或者服务器恶意发送大量的数据包,使得传感器节点有限的资源被消耗殆尽,造成网络出现监测盲区或者全部瘫痪。

1.2 安全需求及挑战

WSN 数据融合及其安全问题的特殊性,使机密性、完整性、新鲜性、身份认证和可用性等安全需求面临新的挑战,需要被重新考虑。

数据机密性保证感应信息不泄露给未经授权的接收方,通常通过用密钥对传输信息加密实现。然而,许多数据融合协议无法对加密数据进行融合,聚合节点必须依次对接收到的报文进行解密、融合、再加密之后再发送报文。显然,这种在聚合节点进行解密/加密的融合过程不仅造成了延迟和能量消耗,而且无法提供端到端的数据机密性。

数据完整性保证数据在传输过程中的篡改能够被及时检测出来。然而,融合过程中数据将在聚合节点处被整合,从而基站无法实现端到端的完整性验证。此外,如果一个聚合节点被俘获,它可以在数据融合的过程中篡改数据,汇聚点无法通过验证察觉。

数据新鲜性是保证在融合过程中,必须选取最近的且没有被重传过的信息作为被融合数据,通过“没有被重传”的信息属性来防止聚合节点遭受重放攻击,在一定程度上减少了冗余信息,提高了融合效率,增强了融合信息的准确性。

身份认证是指聚合节点通过采用一定的认证机制验证发送方节点的身份,检测恶意注入和伪造报文,并可以阻止 Sybil 攻击。

可用性保证网络在遭受 DoS 攻击时仍然可用。有目的的、针对数据聚合节点的 DoS 攻击将直接导致网络部分或全部瘫痪,因此如何确保数据聚合节点的可用性尤为关键。

2 无线传感器网络安全数据融合协议

根据融合过程中聚合节点是否需要加解密,将相

关协议分成点到点和端到端的两类安全融合协议。

2.1 点到点的安全数据融合协议

在点到点的安全数据融合协议中,中间聚合节点对传输的数据先逐跳的进行解密,然后再执行融合操作,最后再将融合的结果进行加密之后传递给下一跳的数据接收节点。

经典的点到点安全数据融合协议如下:

在 SIA (Secure Information Aggregation)^[3] 协议中,首先对叶子节点探测的数据的 MAC 值建立 hash 树,然后利用 Merkle-hash 树的特点,采用融合-提交-证明三个步骤保证汇聚结果的完整性和可验证,从而保证用户接收的结果一定是真实可信的。方案指出即使攻击者捕获了汇集节点并且篡改了数据融合结果之后,依然具备很强的鲁棒性,虚假的数据将会被检测出来,保证了用户。图 1 显示了 Merkle-hash 树的构建过程。

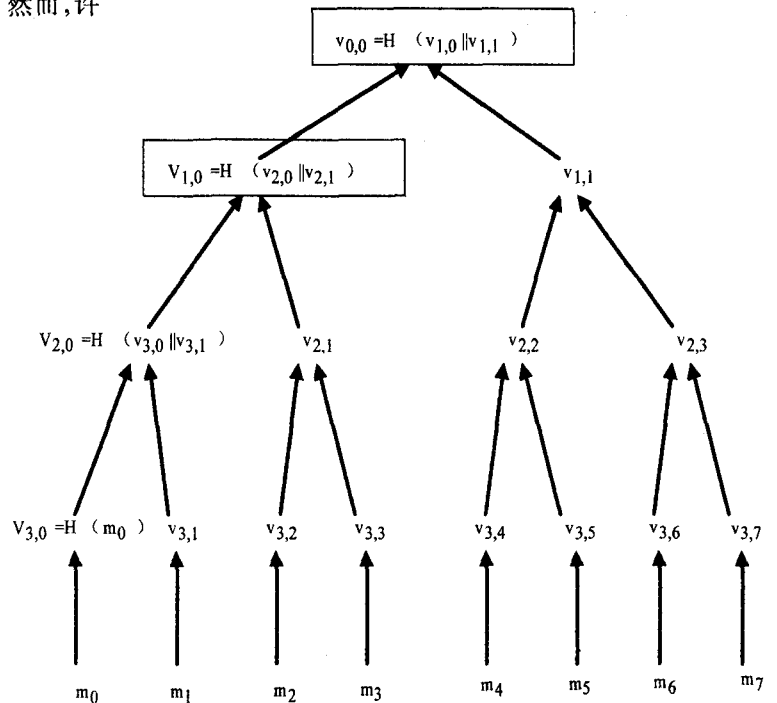


图 1 Merkle-hash 树的构建

如图 1 所示, Merkle-hash 树有两个特点:

(1) 它是由单向散列函数和完全二叉树组成,当确定好根节点之后,其他节点的值都无法改变;

(2) Merkle-hash 树不需要同事公布其他节点的值就可以认证一个叶节点的值(如需验证 m_1 , 只需公开 $v_{3,0}, v_{2,1}, v_{1,1}$ 即可)。

A. Mahimkar, T. S. Rappaport 等在文献[4]中提出了 SecureDAV (Secure Data Aggregation and Verification Protocol) 协议。它适用于分簇式的无线传感器网络,相同簇内的每一个节点都共享一个分簇密钥,簇头是融合节点,簇内各节点采用椭圆曲线算法对产生的数

据进行部分签名,再将数字签名传递给簇头节点,簇头收到各节点传来的数据计算一个均值,然后把均值再广播给簇内的其他节点,其他节点对比融合点的内容和自己探测的数据内容,节点只有在两者的不同度小于一阈值的情况下才对其部分的签名进行修改,最终簇头将各部分签名合成一个完整的签名,并将其传递给基站,最终由基站来验证签名的正确性。SecureDAV 协议保证了数据的机密性、完整性和认证性,它的主要缺点在于:数据的签名和验证将耗费较多系统运算和通信资源,且该方案只能支持求均值的数据融合函数。

Y. Yang, X. Wang 等提出了 SDAP(Secure hop-by-hop Data Aggregation Protocol)^[5] 协议, SDAP 的着眼点在于在一个融合树中,高层节点比底层节点具有更高的信任级。由于高层节点计算的融合数据来自于大量低级节点,因此如果一个接近基站的聚合节点被俘获,则该节点伪造的融合数据将对基站最终生成的结果产生较大影响。由于所有传感器节点都具有简单的硬件结构,易被俘获,因此 SDAP 协议致力于采用分而治之(divide-and-conquer)原则以减少高层节点的信任度,具体来讲:SDAP 使用随机性方法动态将拓扑树分割成大小相同的多个逻辑子树,在一个逻辑子树中高层节点控制较少的底层节点,从而如果该高层节点被俘获,潜在的安全风险减小。图 2 给出了 SDAP 划分融合树的实例。

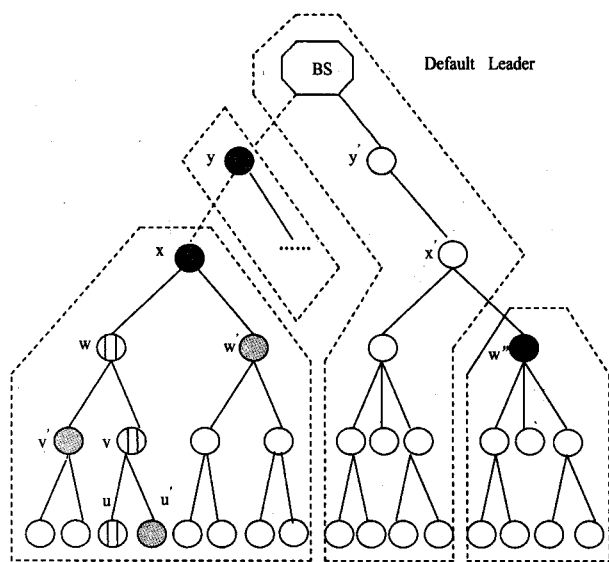


图 2 SDAP 中融合树的实例 x, y, w 是领导节点, BS 是基站

S. Ozdemir 等在文献[6]中提出了 SELDA(Secure and rELiable Data Aggregation protocol) 协议,其基本思想是传感器节点通过观察它们邻居节点的行为为环境和邻居节点建立信任级别,传感器节点利用监视机制探测邻居节点的可用性、感知和路由能力以及异常行为。这些异常行为将使贝塔分布函数被量化为信任级

别,之后节点之间交换它们的信任级别从而构建一个信任网,节点通过信任网决定一条到融合点的安全和可靠的路径。SELDA 一个重要特性是,由于采用了监视机制,因此能够及时检测出受 DoS 攻击的融合点。模拟结果表明 SELDA 在增加可容忍的通信开销的前提下提高了融合数据的可靠性。

W. L. Du 等人在文献[7]中提出一种基于相互监督机制的数据融合安全协议 WDA(Witness-Based Approach for Data Fusion Assurance)。该协议是基于分簇的结构,而实现对簇头节点进行安全监控的方法则是利用同级节点之间的相互监督。在方案设计时,一个或多个监督节点将被设置在簇头的周围。每个监督节点与基站之间共享特定的密钥,能够接收簇内所有节点的消息,并对其进行融合操作。簇内所有节点不仅将自己探测的数据发送给簇头节点,同时还发送给设置好的监督节点。簇头节点和监督节点分别对接收到的数据进行融合操作,监督节点利用融合结果和密钥计算 MAC,并将 MAC 发往簇头节点。簇头节点再将融合结果和收集到的所有 MAC 发往基站。由基站来验证最终的融合结果是否正确。

该方案的优点是:基站只需要利用簇头节点的融合数据计算针对某个监督节点的 MAC,并与监督节点发来的 MAC 相比较即可判断簇头节点操作的正确性;在簇头节点和所有监督节点不被捕获的情况下,此种方案始终有效,并且在鲁棒性方面也有很好的表现;但是该方案也存在一个明显的问题就是需要占用多个节点,数据被泄露的可能性也将大大增加,同时没有考虑数据的机密性。

H. Cam 等在文献[8]中提出了一种基于模式识别码的高效节能的安全数据融合算法 ESPDA(Energy Efficient and Secure Pattern-Based Data Aggregation),聚合操作中使用模式码,模式码用来分类和标识原始数据,每个原始的数据都对应一个模式码。在数据的传输过程中,传感器节点并不是将感应的原始数据进行上传,而是根据模式码生成算法,每个原始数据生成对应的模式码,之后将模式码传递给簇头,簇头收到模式码之后进行分类,通知具有相同模式码的其中一个节点来传递原始数据。在该算法中同时使用了同态加密机制,簇头节点可以直接对密文进行融合操作,并不需要解密工作,因此,减少了传统加解密操作带来的安全隐患,并且节省了节点能量的开销。但是 ESPDA 算法中只有一层聚合节点,因而网络规模就会受到限制,并且模式码的使用并不能得到精确的融合结果。

在文献[9]中 H. O. Sanli 等人根据模式码的方法提出 SRDA(Secure Reference-Based Data Aggregation) 协议。该协议不是直接将原始融合数据传递到基站,

而是设定一个参考数据,即融合节点融合数据的平均值,SRDA 中将感应的原始数据与参考数据进行比较得出一个“差值”,然后仅传递“差值”。这样减轻了线路负载,减少了传输的比特量,提高了聚合效率。但是 SRDA 的缺点是中间节点不执行数据融合操作,因此不能进一步减少能量。

W. B. He 等在文献[10]中采用扰动技术和切片重组技术来实现 WSN 中节点数据隐私保护(Privacy-preserving Data Aggregation, PDA),提出了两种隐秘数据融合算法:

(1) 基于簇头融合的隐秘融合算法(CPDA: Cluster-based Private Data Aggregation)。该算法中,传感器节点通过在原始数据中添加随机种子和私有随机数进行扰动来隐藏真实数据值,簇头节点利用多项式的代数性质求解出精确的聚集结果。基本步骤为:

(a) 在概率参数控制下形成簇,簇由簇头节点和成员节点构成;

(b) 簇内节点将感知数据与本节点产生的随机数以及随机种子数计算扰动数据,然后簇内节点使用两两共享密钥的逐跳加密技术交换扰动数据,各节点对所有收到的扰动数据执行加法操作后将结果发送给簇头节点,簇头节点根据聚集结果和种子建立一个满秩方程组,可通过高斯消元法求解出精确 SUM 结果;

(c) 簇头节点使用 TAG 路由将计算出的聚集结果向基站传送。

(2) 基于分布式的隐秘数据融合算法(SMART: Slice-Mix-AggRegaTe)。该算法与 CPDA 算法不同,主要针对的是多层多跳的拓扑模型。该算法中可以分成三个步骤:在步骤 1(Slicing)网络中每个节点 s_i 在 h 跳内随机选择 $J-1$ 个邻居节点构成节点集 S_i ,将感知数据 d_i 随机切分为 J 个数据切片, s_i 为本节点留下其中 1 个数据切片,将其余 $J-1$ 个数据切片加密后分别随机发送至 S_i 中节点,用 d_{ij} 表示由节点 s_i 传送到 s_j 的数据切片。在步骤 2(Mixing)每个节点 s_j 对收到的数据解密后求和得到 $r_j = \sum_{i=1}^N d_{ij}$,其中当 $j \notin S_i$ 时 $d_{ij} = 0$ 。在步骤 3(Aggregation)所有节点 s_j 使用树形路由(tree-based routing)将计算的 r_j 至基站,基站对所有 r_j 求和得到求和聚集结果 $\sum_{j=1}^N r_j$ 。

SMART 算法较好地保证了数据的机密性,但是具有较大的传输开销,为此, H. Li 提出的 EEHA 算法^[11]和 G. Yang 提出的 ESPART 算法^[12]从减少数据通信量和提高精确度方面对 SMART 进行了改进。EEHA 算法中,首先对节点采用 TAG 算法建立一棵数据融合树,与 SMART 方案不同的是,该算法中只让数据融合树中的叶子节点进行分片传输数据,由于一棵融合树

中叶子节点的数目小于中间节点的数目,因此在整个网络中大大减少了数据通信量,从而降低了能量的消耗;在保护数据隐私性方面,叶子节点采用的安全机制是 SMART 分片重组技术,而对于中间融合节点,利用数据融合本身具有丢失原始数据的特性保护了数据的隐私。由于减少了网络的数据通信量,因而降低了节点之间的数据碰撞,提高了融合的精确度。ESPART 算法中,网络初始化阶段通过 TAG 算法建立一个数据融合树,一方面依靠数据融合树型结构本身的特性,来减少数据通信量;另一方面该算法通过给节点分配随机时间片,减少了数据传输过程中的碰撞。同时对串通数据的范围也进行了有效地限制,以此来降低数据丢失对精确度的影响。最后仿真结果显示,与 SMART 相比,ESPART 算法在有效保护数据隐私的情况下,花费较少的数据通信量,并得到精确的数据融合结果。

2.2 端到端的安全数据融合协议

点到点的数据融合方案的优点是适用于如求平均值、求最大最小值等多种数据融合方式,但是其缺点是在安全性方面和均衡开销上存在很大的安全隐患,因此端到端的加密方式正逐渐引起广泛的重视。在端到端的数据融合操作中,数据融合节点直接对子节点上传的密文进行数据融合操作,有且只有基站最终能够解密得到最终的融合结果。即使攻击者捕获了数据融合节点,也无法得到有效的数据。

J. Girao 等于 2005 年针对 WSN 的数据融合提出 CDA(Concealed Data Aggregation)算法^[13]适用于无线传感器网络。该算法的实现过程是:首先每个传感器节点将数据随机分割成 d 份($d \geq 2$),然后每份数据 m_i 分别乘以密钥 R_i 生成密文,再把 d 份密文全部传递给融合节点,融合节点不需要进行解密操作,而是直接对所有密文进行模加法运算,最终将运算结果再上传给 sink 节点, sink 节点利用私钥对累计的密文进行解密得到最终的数据融合结果。

CDA 算法具有以下优点:

(1) 算法是基于随机或然性的,即每次对相同的数据采用相同的密钥进行加密,得到的密文也都不一样;

(2) 算法可以保证节点和基站之间进行端到端的加密传输;

(3) 聚合节点的计算量比较小,只需要进行简单的模加法运算。

但是该方案也同样存在一些问题:

(1) 聚合节点的开销虽然减少了,但普通叶节点由于把数据进行分割,所以增大了传输开销,进而造成全网的负载明显增加;

(2) CDA 算法使用对称密钥体制,因此算法的安

全弹性比较差。

C. Castelluccia 等于 2005 年提出了 CMT(C. Castelluccia, E. Mykletun, G. Tsudik)^[14]。算法直接采用移位密码的方法来实现同态加密,没有采用像 RSA、DES 这样复杂的加密算法。同时算法中也引入流密钥机制,采用一次一加密,可以有效地防止已知明文攻击,增加加密方案的弹性。算法中假定每个节点都与基站共享一个密钥种子,用来生成每次融合过程中使用的不同密钥,同时共享一个秘密的伪随机函数,用来生成每次数据融合过程中使用的随机数。节点直接将原始数据与密钥进行模加法运算来对数据进行加密,对加密后的密文直接进行相加来实现数据的聚合过程。数据经过加密聚合后传输到基站,基站收到的是数据的密文,然后用密文减去所有节点的密钥即可得到最后的数据融合结果。整个算法的实现简单并且高效,相比于 CDA 算法,传输开销也明显减少,并可抗击重放攻击和选择明文攻击。但这个算法要想保证最终数据融合结果的准确性,必须在实现过程中进行 ID 传输,以便于基站知道哪些节点参与了数据融合过程,从而大大增加了节点的网络传输开销。

与 CDA 和 CMT 都是以对称密码体制为基础相反,E. Mykletun 等在 2006 年在文献[15]中提出了一种基于公钥密码学的同态加密算法 ECEG(Elliptic Curve ElGamal)。该算法可以进行加法数据融合操作,但是由于采用了公钥加密体制,因此具有较高的计算开销和传输开销,所以目前的安全方案还是以对称密码体制为主。

文献[16]提出一种 n 层安全数据融合方案(n -LAD)。利用同态加密方法和交互加密机制,保证端到端数据的机密性。协议不依赖于预先构建的融合树结构,树结构是在融合过程中动态建立的,这样对于部分节点的损失具有很大的灵活性。协议保证:少于 n 个节点被俘获,攻击者不能从网络中得到任何融合的数据;超过 n 个节点被俘获,攻击者也只能得到被俘获节点的融合结果。

同态加密算法增强了数据的保密性,并缓解了数据融合节点的压力。但同态加密算法也有许多不足:

- ① 目前存在的大多数同态加密算法所进行的数据融合操作比较单一,只能够运用于加法运算,如求均值、方差等;
- ② 同态加密算法不能有效地对数据完整性进行鉴别;
- ③ 同态加密算法增加了网络的传输开销;
- ④ 同态加密算法所提供的安全性比较弱,还有待进一步提高。

Zhang 等在文献[17]中意识到现有基于同态加密

算法的网内处理协议只适用于某些特定的查询请求汇聚函数,如求和、求均值等。因此,作者提出了一种基于数字水印的端到端数据认证协议,利用统计学方法为数据融合过程提供内在支持。该方案的创新点在于不再采用传统的报文验证码(MAC)进行完整性验证,而是将认证信息改为数字水印,加载到传感器节点采集的数据上。聚合节点可以直接对加了水印的数据进行融合,而不需要进行任何检查,数据到达基站后,基站验证数据水印以判断数据是否被恶意节点篡改,确保数据完整性。

3 协议的综合分析对比和所需解决的研究问题

表 1 分别从满足的安全需求和抵御的攻击种类两个大的方面对上文中典型的安全数据融合协议进行了性能比较,“√”表示该协议拥有这项性能。

表 1 安全数据融合协议的性能比较

协议	数据机密性	数据完整性	数据新鲜性	身份认证	可用性	抵御攻击种类
SIA ^[3]	√	√	√	√		DoS, TA, EA
SecureDAV ^[4]	√	√		√		DoS, RA, EA
SDAP ^[5]	√	√	√	√		DoS, TA, EA
SELDA ^[6]		√	√	√	√	DoS
WDA ^[7]		√		√	√	DoS, RA, Sybil
ESPDA ^[8]	√	√		√		EA, TA
SRDA ^[9]	√	√		√		EA, TA
PDA ^[10]	√					EA
EEHA ^[11]	√					EA
ESPART ^[12]	√					EA
CDA ^[13]	√					EA, KP
CMT ^[14]	√					EA, RA
ECEG ^[15]	√					EA, TA
n -LAD ^[16]	√				√	EA
Zhang ^[17]	√	√		√		EA, TA

注释:EA 窃听; RA 重放攻击; TA 篡改攻击; DoS 拒绝服务攻击; Sybil 西尔比攻击; KP 已知明文攻击

从表 1 可以看出,目前的安全数据融合协议大多数实现了数据机密性的保护,部分协议完成了数据完整性和身份认证。

WSN 安全数据融合技术中很多挑战性问题有待进一步研究:

- (1) 针对数据新鲜性和可用性的研究较为欠缺;
- (2) 融合数据在静态网络中传递较为高效,但并不适应于动态网络环境,融合数据在动态网络高效传递将成为研究的重点;
- (3) 具有容侵、容错功能的数据融合安全协议值得进一步深入研究;
- (4) 节点通过监督机制来防范数据篡改通常带来高射频率能耗和传感能源消耗,因此,如何开发适合

WSN 的安全数据融合的轻量级检测机制是以后研究的重要内容;

(5) 当前协议方案都是基于同构的 WSN, 如何开发出适应于异构 WSN 的安全数据融合技术值得进一步研究。

4 结束语

物联网的兴起势必会带来无线传感器网络的又一次革新, 而安全数据融合作为一种有潜力的基本的安全服务应用, 也必将引起更大的重视。各种新的安全数据融合方案也将被提出和得到应用, 轻量级的安全数据融合方案是下一个阶段要进行的工作。

参考文献:

- [1] Sang Y, Shen H, Inoguchi Y, et al. Secure data aggregation in wireless sensor networks; a survey [C]//Proc of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies. [s. l.]: [s. n.], 2006: 315-320.
 - [2] Vu H, Mittal N, Venkatesan S. THIS: THreshold Security for Information Aggregation in Sensor Networks [C]//Proc of Fourth International Conference on Information Technology. Washington: IEEE Computer Society Press, 2007: 89-95.
 - [3] Przydatek B, Song D, Perrig A. SIA: Secure Information Aggregation in Sensor Networks [C]//Proc of 1st Conference on Embedded Networked Sensor Systems. Amsterdam: IOS Press, 2003: 255-265.
 - [4] Mahimkar A, Rappaport T S. SecureDAV: A Secure Data Aggregation and Verification Protocol for Wireless Sensor Networks [C]//Proc of the 47th IEEE Global Telecommunications Conference (Globecom). Dallas, TX: [s. n.], 2004.
 - [5] Wang Y Y, Zhu X S, Cao G. SDAP: a secure hop-by-hop data aggregation protocol for sensor networks [C]//Proc of the ACM MOBIHOC'06. [s. l.]: [s. n.], 2006.
 - [6] Ichikawa H, Ozdemir S. Secure and reliable data aggregation for wireless sensor networks [J]. LNCS, 2007, 4836: 102-109.
 - [7] Du W L, Deng J, Han Y S. A Witness-based Approach for Data Fusion Assurance Wireless Sensor Networks [C]//Proc of IEEE Global Telecommunication Conference. Washington: IEEE Computer Society Press, 2003: 1435-1439.
 - [8] Cam H, Ozdemir S, Muthuavinashiappan D. ESPDA: Energy Efficient and Secure Pattern-based Data Aggregation for Wireless Sensor Networks [C]//Proc of IEEE Sensors. Washington: IEEE Computer Society Press, 2003: 732-736.
 - [9] Sanli H O, Ozdemir S, Cam H. SRDA: secure reference-based data aggregation protocol for wireless sensor networks [C]//Proc of the IEEE VTC Fall Conference. Los Angeles, CA, 2004: 4650-4654.
 - [10] He W B, Liu X, Nguyen H. PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks [C]//Proc of 26th IEEE International Conference on Computer Communications. Washington: IEEE Computer Society Press, 2007: 2045-2053.
 - [11] Li H, Lin K, Li K. Energy-efficient and High-accuracy Secure Data Aggregation in Wireless Sensor Networks [J]. Computer Communication, 2011, 34(4): 591-597.
 - [12] 杨庚, 王安琪, 陈正宇, 等. 一种低能耗的数据融合隐私保护算法 [J]. 计算机学报, 2011, 34(5): 792-800.
 - [13] Girao J, Westhoff D, Schneider M. CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks [C]//Proc of IEEE International Conference on Communications. Washington: IEEE Computer Society Press, 2005: 3044-3049.
 - [14] Castelluccia C, Mykletun E, Tsudik G. Efficient Aggregation of Encrypted Data in Wireless Sensor Networks [C]//Proc of Second Conference on Mobile and Ubiquitous Systems. Washington: IEEE Computer Society Press, 2005: 109-117.
 - [15] Mykletun E, Girao J, Westhoff D. Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks [C]//Proc of IEEE International Conference on Communications. New York: IEEE Communications Society Press, 2006: 2288-2295.
 - [16] Rodhe I, Rohner C. n-LDA: n-Layers Data Aggregation in Sensor Networks [C]//Proc of the 28th International Conference on Distributed Computing Systems Workshops. Beijing: IEEE Computer Society Press, 2008: 400-405.
 - [17] Zhang W, Liu Y, Das S K, et al. Secure Data Aggregation in Wireless Sensor Networks: A Watermark Based Authentication Supportive Approach [J]. Elsevier Pervasive Mobile Computer, 2008(4): 658-680.
-
- (上接第 228 页)
- [5] 赵金仿, 赵艳, 缪建明. 网页信息抽取及其自动文本分类的实现 [J]. 计算机技术与发展, 2008, 18(10): 37-39.
 - [6] 宫义山, 高媛媛. 基于信息融合的推断贝叶斯网络研究 [J]. 计算机技术与发展, 2009, 19(6): 106-108.
 - [7] 马福晶, 葛润霞. 基于网络信息检索的研究 [J]. 计算机技术与发展, 2008, 18(8): 111-114.
 - [8] 张成伟, 郑诚. 基于改进 VSM 的文本信息检索研究 [J]. 计算机技术与发展, 2009, 19(1): 71-73.
 - [9] 林士敏, 王双成, 陆玉昌. Bayesian 方法的计算学习机制和问题求解 [J]. 清华大学学报 (自然科学版), 2000, 40(9): 61-64.
 - [10] 张连文, 郭海鹏. 贝叶斯网引论 [M]. 北京: 科学出版社, 2006: 18-36.
 - [11] 邵继业, 王日新, 徐敏强. 贝叶斯网络在模型诊断中的应用 [J]. 吉林大学学报 (工学版), 2010(1): 234-237.
 - [12] 刘家鹏, 詹原瑞, 刘睿. 基于贝叶斯网络的银行操作风险管理 [J]. 计算机工程, 2008, 34(18): 266-271.