

无线传感器网络安全数据汇聚算法

归奕红, 刘 宁

(柳州职业技术学院 信息工程系, 广西 柳州 545006)

摘 要: 针对无线传感器网络数据汇聚与传输过程面临的安全威胁, 文中提出一种基于安全数据汇聚与信息重构的多路由数据传输算法——MDT. 该算法允许网络中存在妥协节点, 也允许丢失部分数据. 通过理论分析与仿真实验, 证实该算法在不增加网络整体能耗的前提下, 能有效地抵御侦听、数据篡改和拒绝服务攻击, 全面提高系统的安全性和可靠性.

关键词: 无线传感器网络; 数据汇聚; 安全通信; Hash 鉴定函数

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2011)04-0115-03

Secure Data Aggregation Arithmetic in Wireless Sensor Network

GUI Yi-hong, LIU Ning

(Department of Information & Engineering, Liuzhou Vocational & Technical College, Liuzhou 545006, China)

Abstract: In order to solve the problem of data aggregation and data transmission in wireless sensor network, a Multipath Data Transport (MDT) algorithm based on secure data aggregation and data reconstruction was proposed in the paper. The algorithm allows the network nodes exist in a few compromises, but also allows the loss of part of the data. The theory analysis and simulation result showed that the sensor network with the MDT algorithm could protect against availably eavesdropping, data tampering and Denial of Service attacks. The security and reliability of the network were improved.

Key words: WSN; data aggregation; Security communication; Hash function identification

1 引言

无线传感器网络(Wireless Sensor Network, WSN)是由一定数量的传感器节点通过某种无线通信协议联结而成的测控系统,其作用是协作地感知、采集和处理网络覆盖区域中感知对象的信息,并发送给观察者. WSN 的应用领域包括:军事侦察、环境观测、农业生产、医疗护理、智能家居、建筑物状态监控等. 传感器在实现各种网络协议和应用系统时,存在以下一些约束:电源能量有限、通信能力有限、计算和存储能力有限等. 此外,由于 WSN 通常部署在应用者无法接近的区域,存在受到破坏的可能性,以及无线电网络的广播特性. 因此,WSN 存在较大的能量和安全方面的隐患^[1].

数据汇聚可以去掉冗余数据,减少了需要传输的数据量,减轻了网络的传输拥塞,降低数据的传输延时,因此,数据汇聚是提高网络能源效率的重要手段. 然而,目前已有的数据汇聚方案都没有充分考虑汇聚过程的安全性问题. 一个节点的妥协可能会危害到通过该节点进行数据汇聚的整条路由. 文献[2-3]的方案能够确保汇聚数据的完整性,但不能提供机密性,也不能抵御拒绝服务(Denial of Service, DoS)攻击. 文献[4]的方案虽然能保证数据的完整性,并在有妥协节点的情况下保证安全性,但是无法解决存在两个连续妥协节点的情况.

2 数据汇聚存在的安全威胁

目前,在 WSN 中进行数据汇聚通常存在以下

收稿日期: 2010-04-19; 修回日期: 2010-06-05

基金项目: 广西教育厅科研基金项目(200708LX260)

三种安全威胁.

(1) 侦听

当攻击者攻陷一个汇聚节点时,将可以侦听到经过该节点的信息. 由于一个汇聚节点收集来自网络中多个节点的信息流量,因此,不仅泄露该妥协节点的信息,还泄露许多其它节点的信息.

(2) 数据篡改

因为一个汇聚节点包含来自许多其它节点的信息,所以攻击者更感兴趣破获这样的节点. 一个攻击者可以通过篡改数据或输入假消息,使基站最后收到错误的信息,从而造成严重的后果.

(3) 拒绝服务(DoS)

一个妥协节点可以停止汇聚数据或转发数据. 其结果造成基站无法收到来自网络中许多节点的信息. 如果其它节点没有注意到这种异常情况,继续交换路由信息,将会令异常情况变得更加严重,最终导致拒绝服务情况的发生.

3 多路由数据传输算法

文中提出多路由数据传输(Multipath Data Transport, MDT)算法,其主要思想是将收集到的数据分成若干小块,并通过多条路由向基站进行转发,此算法抵御了上述三种主要的安全威胁,为数据汇聚提供了安全的保障.

3.1 基本原理及特征

文中讨论的是较大规模的 WSN,基于如下假设:基站的能量是充足的、不受限制的;而普通传感器节点的能量有限,计算和存储能力也有限,并假设它们的初始能量基本相同;每个传感器节点都可以接入基站;初始网络中不存在恶意节点.

MDT 算法基于信息拆分是一个普遍应用于采用冗余和防御恶意攻击的技术. MDT 的基本原理,是每个源节点将感测到的数据向汇聚节点传输,汇聚节点将收集到的数据进行汇聚处理后,再将其按一定长度进行拆分,形成许多小块数据,然后将这些小块数据分别通过不同的且不相交的路由向基站转发(如图 1 所示). 在转发期间,各小块数据都可以被中继节点进行汇聚处理. 一旦基站收集到足够的小块数据,它就能进行数据重组,从而恢复出原始信息. MDT 算法采用文献[5]的方法获得多条路由,各路路由具有加密能力.

中继节点仅仅记录一部分小块数据,因此它是不可能重构信息的.

MDT 算法的主要特性,是重构信息所需要的小块数据的数量小于被传输的小块数据的数量,即

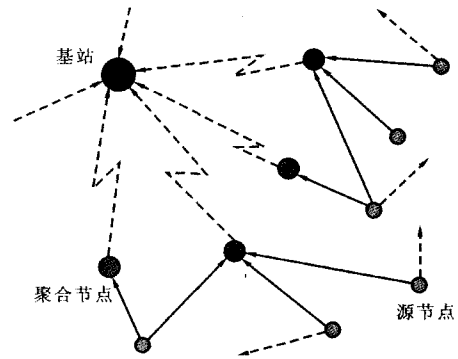


图 1 MDT 网络结构

允许网络中存在部分数据丢失的情况.

3.2 MDT 算法

基于假设网络配置初始不存在恶意节点,因此传感器节点可以安全地预先加载相同的 $c \times r$ 矩阵 $A = [a_{i,j}]$. 当感测到数据时,一个传感器节点 i 将聚集这些数据到一个长度为 L 的内部缓存区,形成一个数据块: $D_i = [d_{i,1} \ d_{i,2} \ \dots \ d_{i,L}]$,一旦这个缓冲区装满,节点就将它们分离成 r 个统一长度的小块数据,并沿着不同的路由发送出去. 这些小块数据是 F 的各拆分部分: $F = D_i \times A$.

假设基站至少需要 c ($1 \leq c \leq r$) 条小块数据才能进行数据重组,以恢复出完整的原始信息. 则当基站收到 c 条小块数据后,将按如下算法进行数据重构. 假定基站收到信息为 $F_i = [f_{i,j1} \ f_{i,j2} \ \dots \ f_{i,jc}]$, 则信息 $d_{i,1} \ d_{i,2} \ \dots \ d_{i,c}$ 可以通过以下多项式解出:

$$\begin{cases} d_{i,1}a_{1,j1} + d_{i,2}a_{2,j1} + \dots + d_{i,c}a_{c,j1} = f_{i,j1} \\ d_{i,1}a_{1,j2} + d_{i,2}a_{2,j2} + \dots + d_{i,c}a_{c,j2} = f_{i,j2} \\ \dots \\ d_{i,1}a_{1,jc} + d_{i,2}a_{2,jc} + \dots + d_{i,c}a_{c,jc} = f_{i,jc} \end{cases} \quad (1)$$

该方程组可利用一个简单高斯消去法求解.

MDT 算法允许数据汇聚,因此可以假设信息 $f_{x,q}$ 和 $f_{y,q}$ 被节点 x 和 y 在 j 条路由上发送,一个汇聚节点对该信息进行汇聚运算,可以得到:

$$f_{x,j} + f_{y,j} = (d_{x,k} + d_{y,k})a_{k,j} \quad (2)$$

至少接收 c 个这样的数据,基站才能用类似公式(1)的方法重构每一个 $d_{x,k} + d_{y,k}$:

$$\begin{cases} (d_{x,1} + d_{y,1})a_{1,j1} + \dots + (d_{x,c} + d_{y,c})a_{c,j1} = f_{x,j1} + f_{y,j1} \\ (d_{x,1} + d_{y,1})a_{1,j2} + \dots + (d_{x,c} + d_{y,c})a_{c,j2} = f_{x,j2} + f_{y,j2} \\ \dots \\ (d_{x,1} + d_{y,1})a_{1,jc} + \dots + (d_{x,c} + d_{y,c})a_{c,jc} = f_{x,jc} + f_{y,jc} \end{cases} \quad (3)$$

从上述分析可以看出,MDT算法是高效的.因为它仅仅需要 c 个大小相同的小块数据就能重构信息.然而,考虑到抵御DoS攻击,建议使用更多的小块数据.

3.3 Hash 鉴定函数

攻击者可能会侦听信息并伪造数据,那么基站如何判断收到的数据是真实的呢?

采用Hash鉴定函数,用一段包括序列信息和依靠一个在节点 i 和基站中保密共享的成分来代替数据 D_i 的最后部分.假设 $D_i = [d_{i,1} \cdots d_{i,n} h(k_i, n)]$,其中 $h(\cdot)$ 是一个保密的Hash函数, k_i 是一个在节点 i 和基站之间共享的密钥, n 是一个序号.对 $\sum D_i$ 重构信息后,基站需要验证这最后的部分是否与 $\sum h(k_i, n)$ 相等,如果不相等,可以假定某个汇聚节点被欺骗,基站将使用另外的小块数据来重构 $\sum D_i$.

4 MDT 算法的安全性分析

假设网络中存在一定数量的妥协节点,在此情况下作算法的安全性分析.如果攻击者没有完全掌握网络的拓扑结构,将很难猜测到哪些是汇聚节点,从而采取针对它们的攻击.假设网络中不存在常规性的数据丢失,每条路由仅仅发送一条小块数据.

4.1 抵御侦听

攻陷某些传感器节点以获得一些小块数据是攻击者获得信息的主要来源.然而,由于每一条小块数据只包含一条完整信息的 $1/r$,要想将小于 $c(1 \leq c \leq r)$ 条小块数据进行信息重构是不可能的.

为了重构信息,共享的集合应该包含来自相同的节点提供的数据.然而,小块数据通过不同的路由传播,在这些路由中,汇聚节点收到来自各种不同节点的数据,这使得侦听攻击难以执行.例如,假设 $c=2$,如果攻击者在两条路由上攻陷了两个节点 X 和 Y ,如果 X 收集的小块数据来自节点 a 和 b , Y 收集的小块数据来自节点 c 和 d ,那么重构信息是不可能的,尽管攻击者已经攻陷了两条不同的路由,除非 Y 收集的小块数据也来自节点 a 和 b .基站是所有路由的终点,它收集的数据来自所有节点,因此它可以重构来自所有节点的所有信息.

4.2 抵御数据篡改

即使攻击者成功地攻陷了至少 c 个汇聚节点,然而,基站不一定采用这 c 个节点提供的小块数据来重构信息(基站可能采用来自没有被攻陷的路由

的数据).此外,由于MDT算法提供了Hash鉴定函数,对于攻击者来说,进行数据篡改必须修改重构后的Hash鉴定值,这是非常困难的.因此,进行数据篡改攻击几乎是不可能成功的.

4.3 抵御拒绝服务

进行DoS攻击可以有两种方式:停止发送数据或发送垃圾数据.对于停止发送数据,可以将该节点当作能量已经耗尽;对于发送垃圾数据,则根据3.3节的Hash鉴定方法,这些无效的数据将被基站拒绝接收.

如果要实施DoS攻击阻止基站收集 c 条小块数据,攻击者至少需要攻陷 $r-c+1$ 条不同的路由(即攻陷 $r-c+1$ 个节点).由于攻击者不知道具体的路由拓扑,他只能随机地攻击节点,进行DoS攻击几乎不可能成功.因此,攻击者不得不攻陷比 $r-c+1$ 更多的节点,其难度之大不言而喻.

5 MDT 算法的能耗分析

一般来说,提高安全性意味着增加能量的消耗.MDT算法对数据进行拆分传送,基站需要重构信息,并利用Hash鉴定函数进一步提高数据的安全性,在一定程度上增加了能量的消耗.但是,基于基站的能量是不受限制的,以及无线通信模块是WSN的主要耗能部件(传输1比特信息所需要的电能大约可以执行3000条计算指令^[6]).因此,MDT算法的计算开销不会影响网络的整体寿命.

为了验证该理论,通过NS2进行仿真实验,对比MDT算法与普通树结构的能量消耗.建立仿真模型如下:

在 $300\text{m} \times 300\text{m}$ 的区域内随机分布150个同类型的节点,每个节点的数据传送范围为200米.运行仿真程序,进行了40次实验,得到如图2所示数据.图中显示出MDT算法与普通树结构的网络总剩余能量基本相同.

6 结束语

数据汇聚是WSN的核心问题,汇聚数据的安全性更是WSN研究的关键问题.文中对WSN汇聚的算法进行研究,系统分析了WSN数据汇聚过程面临的安全威胁,提出MDT算法,全面解决了诸如侦听、数据篡改和DoS等攻击.该算法不同于目前已有的汇聚方案,允许存在妥协节点,也允许存在部分数据丢失,并在不增加通信开销的情况下保障了网络的安全性.

(下转第121页)

但还是不如 LRU 的性能. 对于测试程序 mcf, Cache 容量增加到 2M 以后其 IPC 增加幅度将保持不变, 其性能与 LRU 相当.

■ 1M □ 2M ▨ 4M ▩ 8M ▩ 16M ▩ 32M ▩ 64M

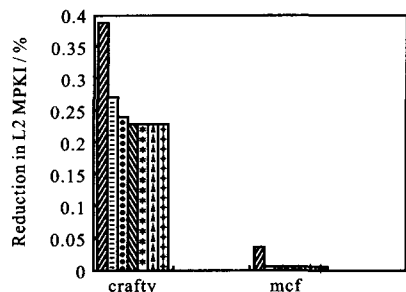


图 4 Cache 对 MPKI 的影响

5 结束语

文中将冒泡替换算法应用到多核共享 L2 Cache 中, 通过分析仿真实验数据, 在小 Cache 容量下算法可以降低 MPKI, 精确度和命中率都比 LRU 有所提高; 但当 Cache 容量达到一定数值后, LRU 算法与文中算法效果相当.

参考文献:

- [1] 戴梅萼. 高性能计算机系统中 Cache 的组织方式及性能分析[J]. 微电子学与计算机, 2000(5): 15-18.

- [2] Wong W, Baer J L. Modified LRU policies for improving second-level cache behavior[J]. HPCA-6, 2000: 49-60.
- [3] Method for implementing a pseudo least recent used (LRU) mechanism in a four-way cache memory within a data processing system[EB/OL](2001)[2010-04-26]. <http://www.patentstorm.us/patents/6240489/description.html>.
- [4] 所光, 杨学军. 双核处理器性能最优的共享 Cache 划分[J]. 微电子学与计算机, 2008, 25(9): 28-30.
- [5] 廖鑫. 一种基于 LRU 算法改进的缓存方案研究与实现[J]. 电子工程师, 2007, 34(7): 46-48.
- [6] Renau J. SESC[EB/OL]. [2010-04-26]. <http://sesc.sourceforge.net>, 2004.

作者简介:

林晓敏 女, (1958-), 实验师. 研究方向为图像处理、嵌入式系统.

桂婷 女, (1974-), 实验师. 研究方向为数字图像处理与模式识别.

乔福明 男, (1984-), 硕士研究生. 研究方向为软硬件节能设计.

胡同森 男, (1954-), 教授. 研究方向为数字图像处理、模式识别.

(上接第 117 页)

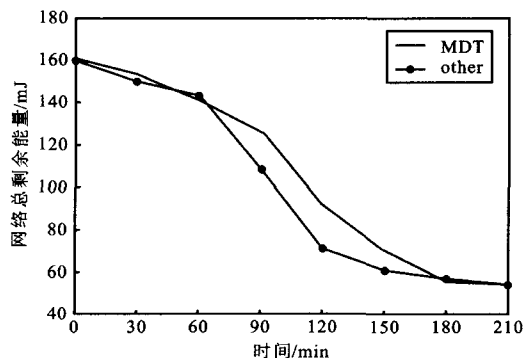


图 2 网络能效比较

参考文献:

- [1] 刘拥民, 蒋新华, 年晓红, 等. 无线传感器网络通信协议[J]. 微电子学与计算机, 2007, 24(10): 71-73.
- [2] Przydatek B, Song D, Perrig A. SIA: secure information aggregation in sensor networks[J]. SenSys, 2003, (3): 255-265.
- [3] Yang Y, Wang X, Zhu S. SDAP: a secure hop-by-hop

data aggregation protocol for sensor networks[J]. MobiHoc, 2006(6): 356-367.

- [4] Hu L, Evans D. Secure aggregation for wireless networks[J]. Workshop on Security and Assurance in Ad hoc Networks, 2003(3): 384-387.
- [5] Ganesan D, Govindan R, Shenker S, et al. Highly-resilient, energy-efficient multipath routing in wireless sensor networks[J]. MobiHoc, 2001(4): 251-254.
- [6] Estrin D, Tutorial. Wireless Sensor networks Part IV: Sensor Network Protocols. MobiCom, 2002[C]// The Eight Annual International Conference on Mobile Computing and Networking Atlanta, Georgia, USA: ACM, 2002: 140-147.

作者简介:

归奕红 女, (1969-), 副教授, 硕士. 研究方向为网络技术、信息安全.

刘宁 男, (1971-), 硕士研究生, 讲师. 研究方向为网络技术、信息安全.