

SDT 安全方案在无线传感器网络的运用研究

刘 宁

(柳州职业技术学院 信息工程系, 广西 柳州 545006)

摘 要: 克服无线传感器范围限制的方法是依靠中继节点进行数据聚合, 关键问题是如何保证点到点的安全传输. 提出分段数据传输(Subsection Data Transport, SDT)安全方案, 依靠多条路由确保数据能安全地聚合. 通过仿真实验, 证明该方案具有良好的安全性, 即使存在妥协节点, 也能有效地抵御偷听、数据篡改和拒绝服务(Denial of Service, DoS)攻击.

关键词: 无线传感器网络; 数据聚合; 分段数据传输; 安全通信

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)10-0050-03

Research on SDT Security Scheme for Wireless Sensor Network

LIU Ning

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

Abstract: A common approach to overcome the limited of sensor networks is to aggregate data relying on intermediate nodes. The pivotal issue is to guarantee end-to-end security transmission. In the paper, Subsection Data Transport security scheme is presented. Data are safely aggregated relying on multipath routing. The scheme has better security in the simulation. A sensor network can protection against available eavesdropping, data tampering and Denial of Service attacks even in the presence of compromised nodes.

Key words: WSN; data aggregation; SDT; security communication

1 引言

由于 WSN 通常运行在敌对环境或人无法接近的远程环境中, 安全性要求很高, 电源不可补充, 因此其安全性和能耗问题显得至关重要^[1].

节约能耗普遍采用的方法是进行数据聚合, 即从多个源节点收集数据, 意义相近的包就会被聚合, 从而减少传输的数据量, 达到能量的有效保存. 然而, 目前已有的数据聚合方案都没有充分考虑聚合过程的安全性问题. 如果攻击者攻陷一个节点, 可能会危害到通过该节点进行数据聚合的整条路由. 文献[2-3]提出使用“提交-检验”技术来确保聚合数据的完整性, 但不能提供机密性, 也不能抵御 DoS 攻击. 文献[4]可以保证数据的完整性, 也能在有妥

协节点的情况下保证安全性, 但是不能解决存在两个连续妥协节点的情况.

2 SDT 安全方案

本文提出分段数据传输(Subsection Data Transport, SDT)方案, 能为数据聚合提供安全保障.

SDT 方案的基本原理: 一个传感器节点将它收集到的数据分离成若干部分(称为零散数据), 并从不同的路由发送它们, 每一条零散数据都通过各自的路径到达 Sink(即汇聚节点). 在转发期间, 每一条零散数据都可以被聚合节点进行处理. 一旦 Sink 收集到足够的零散数据, 它就能重构成完整的信息. 对于中继节点仅仅记录一部分零散数据是不能重构信息的.

SDT 方案的主要特性: 被传输的零散数据的数

收稿日期: 2009-09-04; 修回日期: 2009-11-02

基金项目: 广西教育厅科研基金项目(200708LX260); 广西高等教育工程“十一五”建设项目《网络安全技术》(桂教高教[2007]179号)

量和重构信息所需要的零散数据的数量是不相等的,这意味着系统允许部分数据丢失。

2.1 初始假设

SDT 算法基于以下几点基本假设。

Sink 的能量不受限,即认为 Sink 的能量是充足的;每个节点的初始能量基本相同且严格受限;每个节点都可以接入 Sink。

在较大规模 WSN 中,每一个源节点将感测到的数据向聚合节点传输,聚合节点将收集到的数据进行聚合处理后,再将其按一定长度分段,形成许多零散数据,然后将这些零散数据分别通过不同的且不相交的路由向 Sink 转发(如图 1 所示);Sink 能对转发来的零散数据进行数据重组,从而恢复出原始信息;方案采用文献[5]的方法获得多条路由;路由具有加密能力。

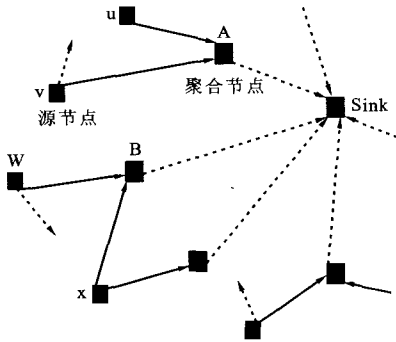


图 1 SDT 网络结构

2.2 SDT 方案

假设一个聚合节点将数据分段后通过 r 条路由到达 Sink,其中 $c-1$ ($1 \leq c \leq r$) 条路由可能受到攻击,Sink 需要至少 c 条零散数据才能进行数据重组恢复原始信息。取一个接近原始信息的参数为 s_i ,节点 i 选择一个随机的 $c-1$ 次多项式 $K_i(x)$,使之满足条件 $K_i(0) = s_i$,选择一个随机数 $a_{i,t}$, $\forall t \in [1, c-1]$,可以构成一个多项式 $K_i(x) = r_i + a_{i,1}x + a_{i,2}x^2 + \dots + a_{i,c-1}x^{c-1}$ 。把 r 块数据的每一块组合成值 $K_i(q)$ ($1 \leq q \leq r$),然后节点 i 沿着 r 条路由分别发送 $K_i(1) \sim K_i(q)$ 信息。

为了恢复出 s_i ,首先必须使用多项式内插法恢复 K_i ,然后计算 $s_i = K_i(0)$,这个操作需要至少 c 条不同的零散数据,因此, $c-1$ 个妥协节点不能推测出关于 K_i 和 s_i 的任何信息。Sink 节点只需要 c 条零散数据就可以重构信息 s_i ,即允许存在 $r-c$ 个无回应节点数。因此,该方案不仅提供了保密性,还能在存在少数妥协节点的情况下,较好地抵御 DoS 攻击。此外, Sink 的记录里不需要构造一些对起作用的一

系列节点的假设,也就是说,只需要网络中的一部分节点就可以进行数据聚合处理。

中继聚合节点可以聚合零散数据,假设一个聚合节点沿着一条路由 m 必须合并来自节点 i 和 j 的数据: $s_i = K_i(0)$ 和 $s_j = K_j(0)$,因为在路由 m 上,只能接收到的数据是 $K_i(m)$ 和 $K_j(m)$,它转发 $K_i(m) + K_j(m) = (K_i + K_j)(m)$,这个操作在其他节点的不同路由上同样被执行。通过收集到的 c 条零散数据, Sink 可以恢复出 $K_i + K_j$,然后得到 $(K_i + K_j)(0) = s_i + s_j$ 。一个攻击者如果没有收集到 c 条零散数据是不可能推测到任何关于传感器节点的信息的,因此,SDT 方案提供了强壮的保密性。

一个恶意的攻击者可以偷听并复制听到的信息,也可以在不被发现的情况下发送许多垃圾信息代替有用的数据。当然, Sink 可以通过执行两次重构不同系列的零散数据并注意到结果的明显不同,从而发现攻击现象,但是,这还不能判定结果是正确的。因此,方案提出使用一种 Hash 鉴定函数来验证数据的真实性,用一段包括序列信息和依靠一个在节点 i 和 Sink 中保密共享的成分来代替数据 S_i 的最后部分。假设: $S_i = [s_{i,1} \dots s_{i,c} h(k_i, n)]$,其中 $h()$ 是一个保密的 Hash 函数, k_i 是一个在节点 i 和 Sink 之间共享的密钥, n 是一个序号。

对 $\sum S_i$ 重构信息后, Sink 节点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,可以假定某个聚合节点被欺骗, Sink 不得不使用另外的部分信息来重构 $\sum S_i$ 。

3 安全性分析

我们对存在一定数量妥协节点情况下的安全性分析。如果攻击者没有完全了解网络的拓扑结构,将很难猜测到有用的聚合节点,从而采取针对它们的攻击。我们假设不存在常规性的丢失,每一条路由仅仅发送一条零散数据,SDT 方案在路由不相交的情况下作研究。

3.1 偷听攻击

在此我们将分析当偷听攻击发生时,SDT 方案提供的网络恢复能力。

3.1.1 零散数据泄漏

由于每一条零散数据包含了 $1/c$ 部分信息,因此,每一条零散数据泄漏一些信息是攻击者获得信息的来源。然而,要想将小于 c 条零散数据进行信息重构,目前还没有办法。

3.1.2 通过 c 条妥协路由重构信息的可能性

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,零散数据通过不同的路由传播,在这些路由中,聚合节点收到来自各种不同节点的数据,这使得偷听攻击难以执行.

如图 1 中假设的情况, $c = 2$,一个攻击者在两条路由上成功地攻陷了两个节点 A 和 B,如果被节点 A 收集的零散数据来自节点 u 和 v ,被节点 B 收集的零散数据来自节点 w 和 x ,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.如果节点 B 收集的零散数据也来自节点 u 和 v ,那么重构信息将是可能的.而 Sink 是每一条路由的终点,它收集的数据来自所有节点,因此它不存在上述问题.

3.2 虚假信息注入攻击

一个攻陷了至少 c 个聚合节点的攻击者能否向网络注入虚假信息呢?即使攻击者操纵了 c 个妥协节点,但不能保证 Sink 将使用由这 c 个节点提供的零散数据来重构信息(Sink 可能使用来自没有被攻陷的路由的数据).另外,由于 SDT 提供了 Hash 鉴定函数,攻击者无法对一些数据进行重构,通过数据篡改欺骗 Sink 几乎不存在可能:攻击者不知道预期的鉴定值;对于攻击者来说,注入一段假信息来修改原有数据是非常困难的,除非修改重构后的鉴定值.

3.3 DoS 攻击

进行 DoS 攻击可分为两种类型:无数据 - DoS 攻击(即停止发送数据),垃圾数据 - DoS 攻击(即发送垃圾数据).无数据 - DoS 攻击可以看作一个传感器节点完全失效(比如其能量已消耗尽),而要处理垃圾数据 - DoS 攻击则较困难.在没有数据鉴定的情况下,攻击者仅仅需要攻陷一条路由并不断地发送垃圾数据即可.在这种情况下,Sink 为了重构信息可能有多倍的输出量,但不知道哪些信息是有用的.当存在数据鉴定的情况下,垃圾数据 - DoS 攻击与无数据 - DoS 攻击是没有区别的:无效的重构被拒绝,如同错误的零散数据不可能到达一样.

通过实施 DoS 攻击达到阻止 Sink 收集 c 个有效的零散数据的目的,攻击者需要攻陷至少 $r - c + 1$ 条不同的路由(即攻陷 $r - c + 1$ 个节点),如果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.而对于一个攻击者要攻陷更多的节点,其难度远远大于理论值.

3.4 仿真实验

采用 NS2 对 SDT 方案进行安全性分析,建立

仿真模型如下:

在 $400\text{m} \times 400\text{m}$ 的区域内随机分布 200 个同类型的节点,每个节点的数据传送范围为 150m . 随机选择一些被攻击的节点,分别在不同的被攻击节点数目下,运行仿真程序,执行了 40 次,用 SDT 方案与普通的树结构方案进行对比,计算两种情况下正常通信被截获的概率,结果显示如图 2 所示.

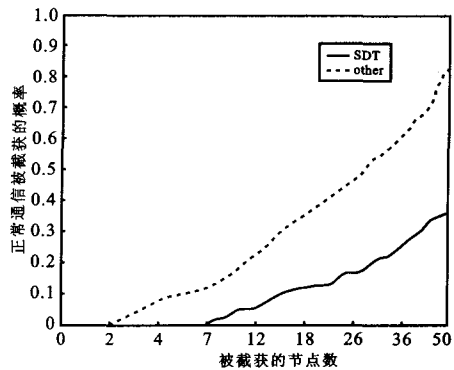


图2 网络安全性能比较

从图中可以看出,普通的树结构方案正常通信被截获的概率明显高于 SDT 方案,说明该方案由于采用零散数据重构信息具有更高的安全性.

4 能效分析

由于集成电路工艺的进步,处理器和传感器模块的功耗变得很低,绝大部分能量消耗在无线通信模块上^[6].传感器节点传输 1bit 信息 100m 距离需要的能量大约相当于执行 3 000 条计算指令消耗的能量.

根据网络的初始假设, Sink 的能量是不受限的,而且 Sink 只对 c 条零散数据作处理,计算复杂度为 $O(1)$.因此, Sink 对零散数据作验证并重构信息的计算所消耗的能量不会影响整个网络的寿命.

聚合节点对数据进行聚合计算,其计算复杂度为 $O(1)$,实现了数据存储空间和数据传输量的精简,有效地降低了网络的能量消耗.这与普通树结构的能耗近似.

图 3 给出了采用 SDT 方案和普通树结构方案时网络总的剩余能量随着数据传输轮次(即有效数据传输量)的变化规律,可以看出:采用 SDT 方案与普通树结构方案网络总剩余能量基本相同.

5 结束语

本文的创新之处在于:(1)在传感器网络中使用多路由进行数据聚合的研究中,讨论了存在妥协节

(下转第 56 页)

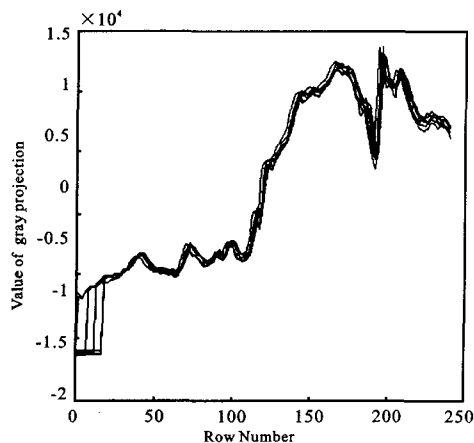


图5 稳像后的列投影

曲线做一次互相关运算来求其图像序列帧间的运动矢量,因此计算量小,速度快,能够满足连续图像的实时性要求.仿真试验证明,该算法具有较好的稳像效果,是实现平移运动或旋转运动较小的图像序列电子稳像的较理想算法,但对剧烈旋转运动条件下的稳像应用存在一定的局限性.

参考文献:

- [1] Engelsberg A, Schmidt G. A comparative review of digital

image stabilising algorithms for mobile video communications[J]. IEEE Transactions on Consumer Electronics, 1999, 45(3):591-597.

- [2] Ko S J, Lee S H, Jeon S W, et al. Fast digital image stabilizer based on gray-coded bit-plane matching[J]. IEEE Transaction on Consumer Electronics, 1999, 45(3): 598-603.
- [3] 赵天云,郭雷,余博.基于灰度投影的快速电子稳像算法[J].微电子学与计算机,2008,25(11):233-236.
- [4] 张永祥,赵晓旭,张伟功,等.一种基于灰度投影的电子稳像改进算法[J].微电子学与计算机,2008,25(11): 212-215.
- [5] 王明佳,金光,钟平,等.实用电子稳像技术原理及方法[J].光机电信息,2003(2):29-31.
- [6] 刘明,赵跃进,周渝斌.电子稳像中的运动补偿矢量处理方法的研究[J].光学技术,2005, 31(3):457-462.

作者简介:

张国栋 男,(1983-),硕士研究生.研究方向为信号与信息处理.

王明泉 男,(1970-),硕士研究生,教授,博士生导师.研究方向为一维和多维信号与信息处理、分析与重构、现代无损检测技术、测控技术和工业内视技术.

(上接第52页)

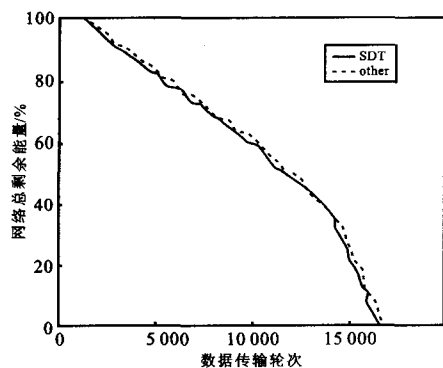


图3 网络节能性比较

点的情况;(2)Sink 不需要完整的被传输数据就能重构信息,允许系统存在部分数据丢失;(3)该方案能在存在妥协节点的情况下有效地抵御偷听、数据篡改和 DoS 攻击.下一步工作要讨论在节点被意外攻陷的情况下,进行一些安全模型的建立,并将这些方案应用到各种类型的传感器网络中.

参考文献:

- [1] 殷新春,徐力杰.WSN 中一种基于数据融合的能量高效分簇路由协议[J].微电子学与计算机,2007,24(9):116-119.
- [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]. SAINT-W, 2003(3):384.
- [5] Ganesan D. Highly-resilient, energy-efficient multipath routing in wireless sensor networks[J]. MobiHoc, 2001(1):251-254.
- [6] Estrin D Tutorial. Wireless sensor networks part IV: sensor network protocols[EB/OL]. [2009-10-11]. <http://nestl.ee.ucla.edu/tutorials/mobicom02/>.

作者简介:

刘宁 男,(1971-),硕士研究生,讲师.研究方向为网络技术、信息安全.