无线传感网数据安全采集方案研究

汪 燕,李玲娟
(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日益广泛的使用,其数据的安全已成为许多领域重点关注的问题。文中以解决无线传感器网络的数据安全采集问题为目标,设计了一种无线传感器网络的数据安全采集方案。该方案针对分层的无线传感器网络,对所有的采集数据进行加密,并采用构造数据凭证的方法检测出丢失数据的个数,以防止对无线传感器网络的攻击。文中对数据安全性和丢失数据检测率的分析结果表明:所提出的方案综合考虑了数据的安全性、真实性和时效性,抗攻击能力强,整体效率高。

关键词:无线传感网;安全采集;凭证;加密
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2013)02-0229-04
doi:10.3969/j.issn.1673-629X.2013.02.059

Research on Safe Data Acquisition Scheme for WSN

WANG Yan,LI Ling-juan
(College of Computer,Nanjing University of Posts and Telecommunications,Nanjing 210003,China)

Abstract:With the increasing applying of wireless sensor network,its data security has been focused in many fields. It aims at resolving the problem of safety data capture in wireless sensor network,and has designed a scheme for it. The scheme is based on hierarchical wireless sensor network. In order to prevent attacks on wireless sensor networks,the scheme encrypts all the acquisition data and detects the number of lost data by means of constructing data certificate. The results of analyzing security and the rate of finding the lost data show that the proposed scheme synthetically considers security,authenticity and timeliness of the data,and has high anti-attack ability and high integrated efficiency.

Key words:wireless sensor network;security acquisition;certificate;encryption

0 引 言

无线传感网(Wireless Sensor Network,WSN)将客观世界的一些物理信息和网络传输结合在一起,提供更直接、更有效、更真实的信息,扩展了人们的信息获取能力。WSN 在军事及公共安全、环境监测和交通管理等领域有着广泛的应用[1]。无线传感网的节点一般由数据采集、数据处理、数据传输和电源组成[2]。在大多数的非商业应用中,如环境监测、森林防火、候鸟迁徙跟踪等应用中,安全问题并不是一个非常紧要的问题。然而,在用于商业上的小区无线安防网络、军事上的敌控区监视敌方的军事部署等的无线传感网中,数据的采集、数据传输过程、甚至节点的物理分布都要保密。

收稿日期:2012-06-19;**修回日期**:2012-09-23
基金项目:国家"973"重点基础研究发展计划项目(2011CB302903)
作者简介:汪 燕(1988-),女,江西景德镇人,硕士研究生,主要研究方向为信息安全及其应用;李玲娟,教授,主要研究方向为数据挖掘、信息安全、分布式计算。

1 相关工作

无线传感网的安全问题越来越被重视[3]。数据的安全是相关研究中重要的课题。文献[4,5]中,提出了在分层的无线传感网的传感器节点与汇聚节点中增加一个中间节点即存储节点,负责缓存数据,处理查询并响应数据。文献[6]中将安全多方的思想运用到无线传感网,通过邻居节点的信息保证数据的保密性和完整性,但是文献中没有考虑到邻居节点全部丢失的情况,同时关联证据的上传会浪费网络的许多带宽和能量。文献[7]提出了使用一种通过特殊编码技术保护数据的保密性和完整性的方案,保证了存储节点响应汇聚节点查询时返回所有满足条件的数据,但是该文献没有考虑到截断攻击将编码数据完全丢失的情况,由于数据的丢失可能来自于截断攻击和通信故障,所以只通过编码不能有效地判断数据丢失的来源。在文献[8]中提到安全信息聚合,保证在数据的聚合过程中不出现数据丢失的情况。与文中的研究目标一样都考虑到数据的安全采集,及防止数据丢失,但是安全信息聚合用到了数据的聚合,其中的通信开销和计算

开销都比较大,不适合普通一般采集的应用。文献[9]研究的无线传感网则采用了数据中心化的结构。文中将借鉴文献[4~8]的思想展开进一步的研究。

2 具有存储节点的分层 WSN

1)具有存储节点的分层 WSN 结构。

分层的无线传感网采用基于分簇的层次型组网模式。节点分为普通节点和汇聚节点(Sink),前者采集的数据先发送到后者进行汇聚,最后通过互联网或卫星到达管理节点[10]。由于受到成本的限制,传感器节点的处理能力、存储能力、通信能力相对较弱,如果簇内的每个节点都直接与汇聚节点通信,易使汇聚节点成为网络瓶颈,造成数据冲突。为此,文中针对文献[4,5]的具有存储节点的分层 WSN 进行研究,拓扑结构如图 1 所示。

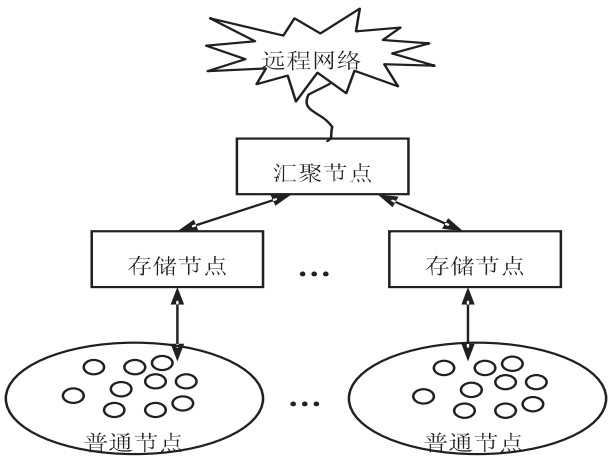

图 1 具有存储节点的分层无线传感网拓扑结构

普通节点负责采集数据,并周期性地传送数据给存储节点。存储节点负责存储数据,在汇聚节点发出数据查询请求时,存储节点响应请求,返回要查询的数据给汇聚节点。下文提及的分层无线传感网均指这种引入了存储节点的分层无线传感网。

2) 分层 WSN 的安全问题。

上述具有存储节点的分层无线传感网中,由于存储节点缓存了尚未传给汇聚节点的采集数据,一旦受到攻击者控制,当汇聚节点查询数据时,受攻击的存储节点不返回或只返回部分数据,产生的影响远远大于普通节点被控制的情况。因此,文中主要考虑如何防止对存储节点的攻击,即考虑如何防止攻击者获取和破坏存储节点存储的采集数据。

3 分层 WSN 的数据安全采集方案

3.1 设计思路

文中主要研究分层无线传感网的安全数据采集,且主要针对基于时间的范围查询应用。例如,普通节点每 1s 采集一次数据,以每 1min 为周期将采集的数据传送给存储节点。

主要设计思路如下:普通节点周期地向存储节点发送数据,发送前先进行数据加密,而且不仅发送自己采集的数据,还把用自己周期内采集的数据个数生成的数据凭证发给存储节点,作为数据丢失的证据。当有数据丢失时,汇聚节点可以通过查看该证据,了解到数据丢失的情况。无线传感器网络的存在一定的信道丢失率,根据文献[11,12],该丢失率在 5% ~10%,若数据丢失的比率明显高于信道丢失率,汇聚节点有理由判断可能存在截断攻击。

3.2 具体方案

1)初始化阶段。

为了保证数据的安全,防止采集的数据泄露给存储节点和其他普通节点,必须先对普通节点采集的数据进行加密,再将其转发给存储节点存储。

文中使用基于主密钥的密钥分配,汇聚节点先随机选择主密钥 k,通过计算 $\mathrm{hash}(k,s_i)$,每个普通节点生成共享密钥。例如,$k_{i,t}$ 表示节点 i 在 t 时间内的加密密钥,为了进一步提高安全性,通过 $k_{i,t+1}=\mathrm{hash}(k_{i,t},t+1)$ 生成下一时序的加密密钥。通过这种处理,就算某个节点遭到攻击,也不会影响邻居节点的安全性。

假设在节点部署前已经完成了基于主密钥的密钥分配。在无线传感网部署后,假定短时间内所有的节点都是可信的。在这段时间内,所有节点需完成无线传感网的初始化工作,所有普通节点和存储节点广播 hello 报文,传感器节点通过收到的 hello 报文确定自己的存储节点。

2) 数据提交阶段。

初始化后,普通节点开始采集数据,并周期地向存储节点转发数据。转发的数据不仅包括节点采集到的数据,还包括数据的凭证。转发的内容如下:

si storage node: $\mathrm{E}_{ki,t}(\mathrm{data})$; $h_{i,t}$; $\mathrm{num}_{i,t}$

其中,$\mathrm{E}(\cdot)$ 为对称加密运算,$h_{i,t}$ 是数据报文,$\mathrm{num}_{i,t}$ 是个数凭证。

数据提交阶段各步骤如下:

第一步:采集数据提交,每个传感器节点将一个存储周期内的数据提交给自己的存储节点。在数据提交前,需要对采集的数据进行预处理。首先,在一个存储周期结束时,产生一个位标识 $v_{i,t}$,用来标识存储周期 t 内的采集数据分布,例如 $v_{i,t}=101010$ 表示存储周期内有 6 个采集点,1,3,5 采集点分别有数据产生,而 2,4,6 没有采集到数据。其次,在一个存储周期结束时,产生一个个数标识 $\mathrm{count}_{i,t}$,用来标识周期内采集到的数据个数。最后,将位标识、个数标识、采集数据一起加密得到:

$E_{ki,t}(\text{data}) = E_{ki,t}(v_{i,t}, \text{count}_{i,t}, \text{data}_1, \text{data}_2, \cdots)$

在数据采集时,有一个特殊情况需要考虑,如果节点在一个周期内没有采集到数据,则以标签 $\text{Lable}_{i,t} = E_{ki,t}(i,t,v_{i,t})$ 的形式上传。

第二步:为了验证数据的完整性,检测数据是否被篡改,需要计算数据报文 $h_{i,t}$,作为汇聚节点验证数据完整性的证据,$h_{i,t}$ 由 $\text{hash}(i,t,v_{i,t},k_{i,t})$ 生成。

第三步:为了判断截断攻击,还需生成个数凭证 $\text{num}_{i,t}$,这样处理的目的是在有数据丢失的情况下,可以通过个数凭证计算出丢失的程度,从而判断截断攻击的可能。num 的处理如图 2 所示。

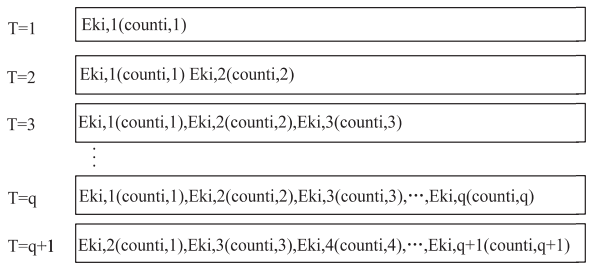

图 2　num 生成过程图

当 $T = t$ 时,$\text{num}_{i,t}$ 的数据如图 3 所示。

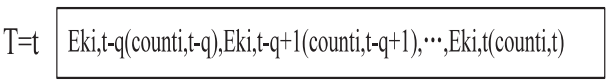

图 3　$\text{num}_{i,t}$ 的数据

即 s_i 节点在周期 t 内的 $\text{num}_{i,t}$ 为 $\{E_{ki,t-q}(\text{count}_{i,t-q}), E_{ki,t-q+1}(\text{count}_{i,t-q+1}), \cdots, E_{ki,t}(\text{count}_{i,t})\}$

3) 数据查询阶段。

文中针对基于时间的范围查询。汇聚节点发出查询请求后,存储节点响应查询,并提交数据,即:

sink　storage node: rangequery = $\{t, [a,b]\}$

storage node　sink: $E_{ki,t}/\text{Lable}_{ki,t}$; $h_{i,t}$; $\text{num}_{i,t}$

汇聚节点的处理过程如下:

第一步:对收到的 $E_{ki,t}/\text{Lable}_{ki,t}$ 进行解密,$D(E_{ki,t})/D(\text{Lable}_{ki,t})$ 得到 $v_{i,t}$ 和 $\text{count}_{i,t}$ 及采集数据,其中 $D(\cdot)$ 表示解密。

第二步:汇聚节点将通过解密得到的 $v_{i,t}$ 求 $h_{i,t} = \text{hash}(i,t,v_{i,t},k_{i,t})$,与实际收到的 $h_{i,t}$ 比较,验证数据是否被篡改,若 $h_{i,t}$ 不同则发出篡改攻击的预警,根据节点所属的存储节点来定位攻击的来源。

第三步:将解密得到的 $\text{count}_{i,t}$ 分别求和,求出采集数据的个数总和 $\sum_{\text{count}} = \sum \text{count}_{i,t}$。

第四步:若汇聚节点没有得到某个节点的数据,汇聚节点发送查询 $t+1$ 时刻的数据,当 $t+1$ 周期内的数据存在时,查看 $\text{num}_{i,t+1}$ 中的 $E_{ki,t}(\text{count}_{i,t})$,通过解密 $D(E_{ki,t}(\text{count}_{i,t}))$ 可以得到 t 时刻数据丢失的个数 $\text{out}_{i,t}$。若 $t+1$ 周期内的数据没有响应,则查看 $t+2$ 周期内的数据,同样进行如上操作。依次操作,若到 $t+q$ 时,还是没有数据响应,则让存储节点确认该节点是否已停止工作,若正常工作可以判断有截断攻击的可能,发出数据截断攻击的警报。

第五步:对所有的丢失个数求和得到 $\sum_{\text{out}} = \sum \text{out}_{i,t}$。则丢失率为:

丢失率 $= (\Sigma_{\text{out}}/(\Sigma_{\text{count}}+\Sigma_{\text{out}})) * 100\%$

通过信道丢失率 5% ~ 10%,判断截断攻击的可能。如果超过信道丢失率则产生数据截断攻击的报警,并根据节点所属的存储节点定位攻击来源。

4　方案性能分析

4.1　安全性分析

传感器节点对采集的数据都进行了预处理,即采集数据通过基于主密钥的加密方式,对数据进行了加密处理,保证了数据不能被存储节点或其他普通节点获得。同时,考虑到采集到的数据和采集个数也都是敏感信息,所以位标识和数据凭证作为数据的一部分需要进行加密才能上传。由于文中采用的加密机制是基于时间的密钥,每个周期内采用的密钥都与下一周期不同,即使攻击者破解了某个周期的密钥,也不能攻击其他周期内的加密数据。而且每个节点采用的密钥不同,即使攻破了某个节点的密钥,也不会影响其他节点的安全性。因此,在文中设计的方案中,攻击者不能从正常的节点获取采集数据和其他加密数据,达到了安全目的。

文中同时考虑了数据的真实性和时效性,由于被攻击了的存储节点可能篡改数据,因此在提交的数据中同时包含了数据报文,用来检测数据是否被伪造,验证数据的真实性及其完整性。在某种情况下,攻击者可能会用过去失效的数据来冒充实时的数据,由于提交的数据中包含数据的周期 t 的信息,即标记了数据的采集周期信息,所以失效的信息很容易被汇聚节点检测出来。

还有一类攻击是截断攻击,即被攻击了的存储节点不提交或只提交部分节点的采集数据给汇聚节点。针对这类攻击,文中通过生成数据凭证的方法来检测丢失的数据,具体分析见下节。

4.2　丢失数据检测性能分析

在文中的方案中,由于上报的数据有数据凭证,当节点 t 时刻数据丢失时,可以通过查看 $t+1 \sim t+q$ 周期内的数据凭证,获得 t 时刻丢失的数据个数。假设每个节点数据能正确上传的概率为 p,则丢失的数据可检测出来的概率 P_{find} 为

$$P_{\text{find}} = 1 - (1-p)^q$$

图 4 显示了不同 p 和不同 q 值下,对丢失数据的检

测率。

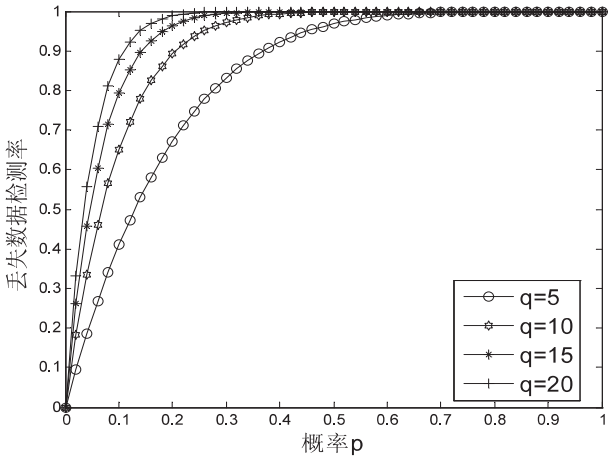

图 4 丢失数据检测率

由图 4 可知,当 $q = 5$,p 大于 0.7 时,丢失数据被检测的概率接近 1;甚至当 $q = 20$ 时,p 大于 0.3 丢失的数据都能被检测出来。由于无线传感网的信道丢失率范围是 5% ~ 10%,所以文中设计的方案提供了丢失数据的高检测率。

5 结束语

文中研究了分层无线传感网的安全数据采集问题,设计了一种有效的解决方案,并分析了方案的有效性。文中在 WSN 的数据安全采集及存储方面做了有益的研究工作,可供进一步研究参考。

参考文献:

[1] 李玲娟,丁 亮. 无线传感网中多跳路由算法的研究[J]. 计算机技术与发展,2010,20(6):55-58.

[2] 任丰原,黄海宁,林 闯. 无线传感器网络[J]. 软件学报,2003,14(7):1282-1290.

[3] 孙利民. 无线传感网[M]. 北京:清华大学出版社,2005:179-183.

[4] Ratnasamy S,Karp B,Shenker S,et al. Data-centric storage in sensornets with GHT,a geographic hash table[J]. Mobile Networks and Applications,2003,8(4):427-442.

[5] Desnoyers P,Ganesan D,Li H,et al. PRESTO:a predictive storage architecture for sensor networks[C]//Proceeding of HOTOS'05. Santa Fe,NM,USA:[s. n.],2005:23-28.

[6] 赵 洋. 安全多方计算及其应用协议研究[D]. 成都:电子科技大学,2009.

[7] Sheng B,Li Q. Verifiable Privacy-preserving RangeQuery in Two-tiered Sensor Networks[C]//Proceedings of Infocom' 08. Phoenix,AZ,USA:[s. n.],2008:46-50.

[8] He W,Liu X,Nguyen H,et al. PDA:Privacy-preserving Data Aggregation in Wireless Sensor Networks[C]//Proceeding of Infocom'07. Anchorage,Alaska,USA:[s. n.],2007:2045-2053.

[9] Shao M,Zhu S,Zhang W,et al. pDCS:Security and privacy support for data-centric sensor networks[J]. IEEE Transactions on Mobile Computing,2009,8(8):1023-1038.

[10] 周 伟. 基于分簇的无线传感器网络关键技术研究[D]. 上海:上海大学,2011.

[11] 张招亮,陈海明,黄庭培,等. 无线传感器网络中一种抗无线局域网干扰的信道分配机制[J]. 计算机学报,2012,35(3):504-517.

[12] Wan C Y,Campbell A T,Krishnamurthy L. PSFQ:A Reliable Transport Protocol for Wireless Sensor Networks[J]. IEEE Journal on Selected Areas in Communications,2005,23(4):862-872.

(上接第 224 页)

[3] Wang Yunjia, Fu Yongming. On 3D Geo-visualization of a Mine Surface Plant and Mine Roadway[J]. Geo-spatial Information Science,2007,10(4):287-292.

[4] Rossmann M. Planning,Simulation and Real-time Depiction of Coal-mining Processes Using a "Virtual Reality" System[J]. Glueckauf Mining Reporter,2003(1):27-31.

[5] 张荣立,何国纬,李 铎. 采矿工程设计手册[M]. 北京:煤炭工程出版社,2003:2473-2474.

[6] 钱一达. 采矿分项工程设计实用手册[M]. 北京:北京矿业出版社,2006:753-754.

[7] 徐志强,杨邦荣,王李管,等. 巷道实体的三维建模研究与实现[J]. 计算机工程与应用,2008,44(6):202-205.

[8] Sunday D. About Planes and Distance of a Point to a Plane [EB/OL]. [2012-05-25]. http://softsurfer. com/Archive/algorithm_0104/algorithm_0104. htm#Planes.

[9] 戴晓明,朱 萍. 平面散乱点三角剖分分治算法的实现[J]. 计算机技术与发展,2006,16(1):11-12.

[10] 孙中昶,卢秀山,田茂义. 矿山巷道 3 维建模算法研究及实现[J]. 测绘学报,2009,38(3):250-253.

[11] 郝长胜,孙宝雷,王瑞智. 基于 OpenGL 的矿山巷道建模算法应用研究[J]. 现代矿业,2010(11):8-10.

[12] 孙家广. 计算机图形学[M]. 第 3 版. 北京:清华大学出版社,1998:369-371.

[13] 张 宏,温永宁,刘爱利,等. 地理信息系统算法基础[M]. 北京:科学出版社,2006.

[14] 赵 陌. 计算可视化的一个快速三维旋转算法[J]. 系统仿真学报,2008,20(4):938-943.

[15] 龚沛曾,陆慰民,杨志强. Visual Basic 程序设计教程[M]. 北京:高等教育出版社,2000.

无线传感网数据安全采集方案研究

作者： 汪燕， 李玲娟
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)： 2013(2)