软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(Suppl.(1)):126−133

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

具有容错性的无线传感器网络时间同步协议*

秦绍华[1,2+], 陈冬岩[1]

[1](山东大学 控制科学与工程学院,山东 济南 250061)

[2](山东师范大学 物理与电子科学学院,山东 济南 250014)

Fault-Tolerant Time Synchronization Protocol for Wireless Sensor Networks

QIN Shao-Hua[1,2+], CHEN Dong-Yan[1]

[1](School of Control Science and Engineering, Shandong University, Ji'nan 250061, China)

[2](College of Physics and Electronics, Shandong Normal University, Ji'nan 250014, China)

+ Corresponding author: E-mail: qsh@sdu.edu.cn, http://control.sdu.edu.cn/

Qin SH, Chen DY. Fault-Tolerant time synchronization protocol for wireless sensor networks. *Journal of Software*, 2012,23(Suppl.(1)):126−133 (in Chinese). http://www.jos.org.cn/1000-9825/12014.htm

Abstract: Time synchronization protocol is an important part of wireless sensor networks. Many applications and communication protocols of wireless sensor networks are built on the basis of an accurate synchronized timing. The previous time synchronization protocol for wireless sensor networks focuses on how to improve the accuracy and reduce related energy consumption, but now the security problem of time synchronization protocol in wireless sensor networks is catching people's attention. This paper designs a new fault-tolerant time synchronization protocol (FTTSP) for wireless sensor networks with random weighting estimation, based on the analysis for the attack to time synchronization protocol for wireless sensor networks. Simulation results show that the protocol has good intrusion detection capability and fault tolerance to malicious synchronization information.

Key words: wireless sensor network, time synchronization, fault-tolerant

摘 要: 时间同步协议是无线传感器网络的重要组成部分,许多无线传感器网络的应用和通信协议都是建立在准确同步的基础之上的.以往的无线传感器网络时间同步协议专注于如何提高同步时间的精确性和减少相关的能量消耗,而现在无线传感器网络时间同步协议的安全问题越来越受到人们的重视.在对无线传感器网络时间同步协议受到的攻击类型进行分析的基础上,利用随机加权平均算法设计了一种具有容错能力的新型无线传感器网络时间同步协议——FTTSP(fault-tolerant time synchronization protocol).仿真结果表明,该协议具有良好的入侵检测能力和对恶意同步信息的容错能力.

关键词: 无线传感器网络;时间同步;容错

无线传感器网络(wireless sensor networks,简称 WSNs)是由部署在监测区域内的大量廉价微型传感器节点,通过无线通信方式形成的一种多跳的自组织网络系统[1,2].广泛应用于军事侦察、工业控制、物流、智能建筑等领域.时间同步协议是无线传感器网络中重要的组成部分,许多无线传感器网络的应用,例如目标跟踪、数据收集和定位等都需要网络节点之间具有统一的时间.同时,许多基于时间的无线传感器网络的通信协议也是建

* 收稿时间: 2012-05-05; 定稿时间: 2012-08-17

立在精确时间同步的基础之上的,例如许多基于 TDMA 的 MAC 协议.传统的时间同步协议致力于解决时间同步的精确度问题,以及如何利用最少的能量和通信代价取得时间同步,对于时间同步协议的安全性问题重视不够.无线传感器网络节点的计算和存储资源有限,使其不能使用复杂的安全协议,而无线传感器网络分布的广泛性和无线通信的特点,又使其极易受到恶意节点的攻击,特别是对于节点被捕获的攻击形式更是难以防范,因此,无线传感器网络的安全问题受到越来越广泛的关注[3−5].对于时间同步协议来说,其安全性受到破坏,不仅仅是单个包错误的问题,而且会导致节点时间的偏移,进而影响无线传感器网络基于时间同步的应用和通信协议的运行[6].因此,如何提高无线传感器网络时间同步协议的安全性是关系到无线传感器网络能否可靠运行的一个根本问题.

在无线传感器网络中,一般通信协议并不能完全保证信息的安全,而且对时间同步信息的攻击具有自己的特殊性,因此,如何提高时间同步协议的抗攻击性,以及在时间同步信息受到攻击的环境中,如何使得时间同步协议能够容错运行,是本文研究的重点.

本文的贡献主要有:

(1) 采用分布式算法,设计了一个具有容错能力的无线传感器网络安全时间同步协议.

(2) 利用节点晶振频率在短时间内稳定的特性,以估计值与实际值的偏差作为判据,对恶意同步信息的攻击行为进行检测.

(3) 采用随机加权平均的数据融合算法对接收到的来自不同节点的同步信息进行数据融合,减少恶意同步信息对于节点同步算法的影响,达到容错效果.

本文第 1 节介绍目前无线传感器网络时间同步协议安全方面的研究进展,然后分析无线传感器网络时间同步协议面临的主要安全问题,并对本协议需要用到的数学理论进行介绍.第 2 节主要对本协议的结构和运行机制进行介绍.第 3 节利用仿真实验对本协议的入侵检测机制和容错性能进行验证.最后总结全文.

1 相关工作

1.1 已有的时间同步协议

由于无线传感器网络的特殊性,传统的网络时间同步协议并不适用于无线传感器网络,目前典型的无线传感器网络时间同步协议主要有 RBS(reference broadcast synchronization)[7],TPSN(timing-sync protocol for sensor networks)[8]和 FTSP(flooding time synchronization protocol)[9].这些时间同步协议主要致力于解决如何提高时间精确度问题,其安全性存在许多漏洞.文献[10]对其安全性进行了分析.文献[11−14]对于无线传感器网络时间同步协议的安全性进行了关注,但这些协议都是基于层次结构的参考节点时间同步模型,利用门限值对比同步信息偏移量来检测攻击,当参考节点失效时,协议便无法运行.文献[15]利用分布式算法解决了这一问题,但其对于时间的估计是用简单的算术平均算法,而不能根据观测值的偏移量对数据进行有效地估计.

1.2 无线传感器网络的时间攻击类型

无线传感器网络由于其分布的广泛性和节点资源的受限性,极易受到攻击,无线传感器网络受到的攻击行为可以分为物理攻击、数据攻击和资源攻击等.这些攻击行为都会对无线传感器网络产生影响,进而干扰时间同步协议的运行.本文主要从时间同步协议的角度对攻击类型进行研究.

(1) 时间同步信息包的丢失.由于节点被损坏,或通信被干扰,都会造成时间同步信息包的丢失.这将使节点在同步周期内不能接收到同步信息,降低节点时间同步的准确度.

(2) 时间同步信息包的更改.当节点被捕获,或恶意节点成功加入网络,这些节点会发送错误的时间同步信息包,收到并信任这些同步信息的节点会造成本节点的时间同步错误.

(3) 时间同步信息包的延迟.恶意节点可以采取拥塞通信信道、重放同步信息等方法增大时间同步信息包到达接收节点的延迟,造成时间同步协议的失败.

可见,针对时间同步协议的攻击主要造成同步信息的缺失和错误,增大节点时间同步的偏差,信息加密措施

可以保证信息包的完整性和机密性,但是,对于信息的时间准确性却难以保证,而且加密信息的新鲜性也是建立在节点时间同步的基础上的.特别是节点被捕获时,时间同步信息包的安全性很难得到保证.因此,需要建立具有安全机制的时间同步协议,特别是在时间同步信息包错误的情况下,如何使得时间同步协议能够容错运行,这是本文研究的重点问题.

1.3 时钟同步模型

在无线传感器网络中,每个节点依靠计算本地晶振的振荡次数来计时,节点 i 的时间模型可以表示为

$$C_i(t)=\alpha_i t+\beta_i \tag{1}$$

其中,$C_i(t)$为节点的本地时间,α_i 为时钟偏移率,t 为物理时间,β_i 为本地时间与物理时间的偏移量.由于晶振的振荡频率会受到晶振本身物理特性和周围温度的影响,其时间的精确度并不是很高,因此,节点需要周期性地接收时间同步信息,对本地时间进行调整.本文所提到的时间同步协议基于 ICTS(interactive convergence time synchronization)[16].

ICTS 利用时间同步信息消除本地节点和邻居节点之间的时间偏移量来达到全网时间同步.假设节点 s 为运行时间同步算法的节点,其邻居节点数为 n_s, $T_i(i=1,2,...,n_s)$ 为邻居节点同步信息发送时间,T_s 为同步信息接收时间,则两节点时间偏移量为 $\Delta_{s,i}=T_s-T_i$.接收到足够多邻居节点信息后,节点 s 可以通过以下算法校准其时间:

$$C_s'(t)=C_s(t)+\frac{1}{n_s+1}\sum_{i=1}^{n_s}\Delta_{s,i} \tag{2}$$

ICTS 采用算数平均的方法来计算本地节点和邻居节点的时间偏差值,当某个节点由于受到攻击,使其发送时间出现较大偏移时,会使本地校准时间同样产生大的偏移,而且这个偏移量会在网络中扩散,进而影响整个网络的时间同步.因此本文对接收到的同步信息进行数据融合,采用随机加权平均算法来消除不正确同步信息对协议的影响.

1.4 随机加权平均

随机加权信息融合算法是参数估计中的一种基本算法,其基本思想是:对各传感器所提供的测量信息进行加权,并根据信息的有用程度在线调整各传感器的权值,使各个传感器的加权因子尽可能合理,以便获得最优融合结果[17].相比于算数平均,它可以有效地利用多个传感器的信息,使估计结果达到最优.

假设有 N 个传感器,其方差为 δ_i^2 (i=1,…,N),传感器测得的值为 x_i (i=1,…,N),则根据随机加权平均算法,其估计值为

$$x=\sum_{i=1}^{N}v_i x_i \tag{3}$$

其最优随机加权因子为

$$v_i=\frac{1}{\delta_i^2\sum_{i=1}^{N}\frac{1}{\delta_i^2}} \tag{4}$$

1.5 最小均方误差方法

在时间同步协议中,接收方依据时间同步包中发送方的时间调整自己的时间,因此发送方的时间准确性直接影响时间同步的精度.但是,发送方的时间往往受到多种因素的影响,因此,时间同步协议中通常运用多次接收的时间同步包的信息,采用最小均方误差方法对时间同步包的发送时间进行修正.为简化运算,文献[18]采用递归算法的最小均方误差方法对发送时间进行修正.设 y_i 为同步时间包的发送时间,x_i 为同步时间包的接收时间, $\hat{y}_i$ 为节点对发送时间的估计值,i(i=1,…,n)为接收次数,则

$$\hat{y}_i=b_1x_i+b_o.$$

设

$$RSS=\sum_{i=1}^{n}\gamma^{n-i}(y_i-\hat{y}_i)^2=\sum_{i=1}^{n}\gamma^{n-i}(y_i-b_1x_i-b_0)^2,$$

其中,$\gamma(0<\gamma<1)$ 为遗忘系数.

要使 RSS 取得极小值,则 $\frac{\partial RSS}{b_1}=0,\frac{\partial RSS}{b_0}=0$, 即

$$b_0\sum_{i=1}^{n}\gamma^{n-i}+b_1\sum_{i=1}^{n}\gamma^{n-i}x_i=\sum_{i=1}^{n}\gamma^{n-i}y_i,$$

$$b_0\sum_{i=1}^{n}\gamma^{n-i}x_i+b_1\sum_{i=1}^{n}\gamma^{n-i}x_i^2=\sum_{i=1}^{n}\gamma^{n-i}x_iy_i.$$

为了能够采用递归算法,我们定义

$$S_{1,n}=\sum_{i=1}^{n}\gamma^{n-i};\quad S_{x,n}=\sum_{i=1}^{n}\gamma^{n-i}x_i;\quad S_{y,n}=\sum_{i=1}^{n}\gamma^{n-i}y_i;\quad S_{xy,n}=\sum_{i=1}^{n}\gamma^{n-i}x_iy_i;\quad S_{x^2,n}=\sum_{i=1}^{n}\gamma^{n-i}x_i^2,$$

则可以得到:

$$\begin{aligned}S_{1,n}&=\gamma S_{1,n-1}+1,\\ S_{x,n}&=\gamma S_{x,n-1}+x_n,\\ S_{y,n}&=\gamma S_{y,n-1}+y_n,\\ S_{xy,n}&=\gamma S_{xy,n-1}x_n\ y_n,\\ S_{x^2,n}&=\gamma S_{x^2,n-1}+x_n^2.\end{aligned}$$

这样,上述方程可以改写为

$$b_0S_{1,n}+b_1S_{x,n}=S_{y,n},\ \ b_0S_{x,n}+b_1S_{x^2,n}=S_{xy,n}.$$

解方程可得:

$$b_0=\frac{S_{x,n}S_{xy,n}-S_{x^2,n}S_{y,n}}{S_{x^2,n}-S_{x^2,n}S_{1,n}},\ \ b_1=\frac{S_{x,n}S_{y,n}-S_{1,n}S_{xy,n}}{S_{x^2,n}-S_{x^2,n}S_{1,n}}\tag{5}$$

2 FTTSP 协议

2.1 FTTSP协议结构

本协议采用分布式算法,节点通过减少相互之间的时间偏移量最终达到时间同步.其协议结构可以分为攻击检测、本地时间校准、加权系数生成 3 部分,如图 1 所示.

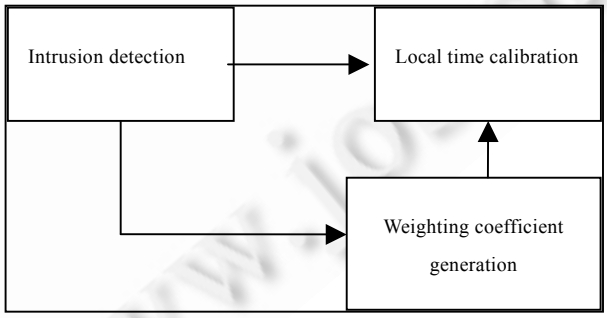

Fig.1 Protocol structure

图 1 协议结构

2.1.1 入侵检测

在正常情况下,节点时间和物理时间之间是一种线性关系,设同步信息包中发送方时间为 y_i,同步信息包接

收时间为 x_i 由公式(1)得:

$$y_i = \alpha_y t_i + \beta_y,\ x_i = \alpha_x t_i + \beta_x,$$

i(i=1,…,n)为同步次数,则

$$\frac{y_i - y_1}{x_i - x_1} = \frac{\alpha_y (t_i - t_1)}{\alpha_x (t_i - t_1)} = \frac{\alpha_y}{\alpha_x},$$

$$y_i = \frac{\alpha_y}{\alpha_x}(x_i - x_1) + y_1 = \frac{\alpha_y}{\alpha_x} x_i + y_1 - \frac{\alpha_y}{\alpha_x} x_1.$$

令 $b_1 = \frac{\alpha_y}{\alpha_x}, b_0 = y_1 - \frac{\alpha_y}{\alpha_x} x_1$, 则有

$$y_i = b_1 x_i + b_0.$$

利用最小均方误差方法,可以根据历史同步信息对发送时间进行估计:

$$\hat{y}_i = \hat{b}_1 x_i + \hat{b}_0 \approx y_i,$$

其中,

$$\hat{b}_0 = \frac{S_{x,n} S_{xy,n} - S_{x^2,n} S_{y,n}}{S_{x^2,n} - S_{x^2,n} S_{1,n}},\ \hat{b}_1 = \frac{S_{x,n} S_{y,n} - S_{1,n} S_{xy,n}}{S_{x^2,n} - S_{x^2,n} S_{1,n}}.$$

当同步信息包受到攻击后,其发送时间必然会产生偏离,不再与物理时间呈线性关系,即

$$y_i' = \alpha_y t_i + \beta_y + \varepsilon = y_i + \varepsilon,$$

其中,ε为恶意攻击包中发送时间的偏离值,则

$$\hat{y}_i - y_i' \approx y_i - y_i' = \varepsilon.$$

因此,我们可以用发送时间的估计值与发送时间的差值作为检测同步信息包是否受到攻击的判据,当 $\hat{y}_i - y_i' > \Delta$ 时,我们认为此同步信息是不可信的.

2.1.2 本地时间校准

当节点接收到多个邻居节点的同步信息后,同步协议运用 ICTS 算法进行时间校准,即

$$x_i'(t) = x_i(t) + \frac{1}{n_s + 1} \sum_{j=1}^{n_s} (y_{ji} - x_i).$$

ICTS 算法采用算数平均来处理偏移量,不能有效地利用多个节点的同步信息,当恶意同步信息包的发送时间偏移量小于检测门限值时,入侵检测机制会认为其可信,但是这个偏移量依然会对节点的时间同步造成影响,如果恶意同步信息持续以小于检测门限值的偏移量增长,就会产生累计效应,最终使节点同步失败.因此,我们需要采用随机加权方法对公式(2)进行修正,以产生对同步时间的最佳校准,即

$$x_i'(t) = x_i(t) + \sum_{j=1}^{n_s} v_j (y_{ji} - x_i) \tag{6}$$

其中,加权系数为

$$v_j = \frac{1}{\delta_j^{\,2} \sum_{j=1}^{N} \frac{1}{\delta_j^{\,2}}} \tag{7}$$

2.1.3 加权系数生成

随机加权方法中加权系数的选择至关重要,由公式(7)可知,加权系数是由发送时间的方差决定的,如何确定这个方差是我们需要考虑的问题.

根据数学知识我们知道,发送时间的方差为

$$\delta_j^{\,2} = \sum_{i=1}^{n} (\hat{y}_{ji} - \bar{y_j})^2,$$

其中 $\hat{y}_{ji}$ 为节点 j 的第 i 次估计值,$\bar{y}_j$ 为节点 j 多次估计值的均值.

但是这个值是节点 j 发送时间统计意义上的方差,表征的是统计意义上的多次估计值相对均值的偏移量.不能有效地反映同步信息受到攻击时引起的偏差,因为这种偏差具有突发性.因此,我们认为,用单次估计值与标准时间的偏移更能反映同步信息受到攻击的程度.同时我们观察到,当网络处于稳定状态时,本地节点的校准时间能够很好地反映标准时间.同时,即使受到干扰,本地节点的校准时间也是一种缓慢的变化.而且在一个受到攻击的网络环境下,本地节点的校准时间也是唯一可以相信的时间源.因此,我们取本地节点的校准时间作为标准时间,来估计发送时间的方差.即

$$\delta_j^2 = (\hat{y}_{ji} - x_i)^2,$$

其中,x_i 为本地节点第 i 次校准时间值.

2.2 协议运行机制

本地节点周期性地接收邻居节点的时间同步信息,对每个同步信息包中的发送时间进行估计,用估计值与实际值的偏差作为判据进行入侵检测,当差值大于门限值时,判定这个同步信息包为恶意攻击同步信息,丢弃这个包,当连续收到同一节点的恶意攻击同步信息时,将此节点列入黑名单,并向上层协议发出报警信息.当差值小于门限值时,判定此信息可用,用估计值和本地校准时间计算其加权系数.当接收完所有邻居节点时间同步信息后,本地节点运行时间校准程序,对本地时间进行校准,本次同步结束.

3 FTTSP 协议评价

我们用 Matlab 对 FTTSP 协议同步时间算法做了仿真实验,以检测同步协议对于恶意同步信息的入侵检测和容错性能.网络环境设计为:本地节点从 3 个邻居节点周期性地接收同步信息包,由于节点本身计时误差和传输过程中存在的不确定性,同步信息中的发送时间 y_i 与物理时间存在误差 e_i,本地节点接收到同步信息后,根据每个邻居节点的累计发送时间,用最小均方误差算法对本次的发送时间进行估计,得到发送时间的估计值 $\hat{y}_i$,本地节点融合 3 个邻居节点的发送时间估计值,得到本地节点的时间校准值 $x_i'(t)$.

3.1 入侵检测性能

为验证同步协议入侵检测的性能,我们假设节点 2 在 40 分钟时,由于节点被捕获或者是同步信息包被更改,使得同步信息包的发送时间发生较大偏离,如图 2 所示,可见,此时的观测值严重偏离物理时间,而根据节点累计观测值得到的估计值,却并未发生显著变化,两者的差值 $\hat{y}_i - y_i' > \Delta$,可以有效地检测到恶意同步信息的入侵,当攻击消失后,节点的估计值具有较好的线性,可以有效地消除同步信息中的正常误差.可见,本算法不但可以有效地检测入侵,而且在正常网络环境下,还可以有效地消除同步误差,提高时间同步的精度.

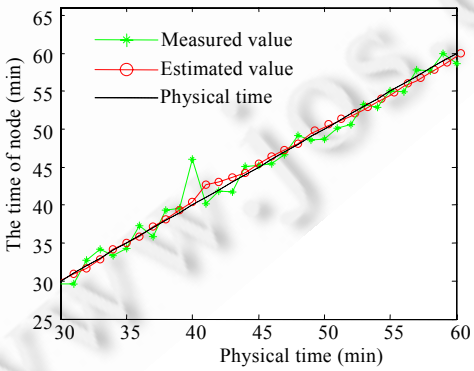

Fig.2 Intrusion detection actions under attack of node synchronization information

图 2 节点同步信息受到攻击时入侵检测机制动作

3.2 容错性

当攻击使得同步信息的偏移量呈缓慢增长时,如图 3 所示,发送时间的估计值和观测值的差距并不是很大,即 $\hat{y}_i - y_i' < \Delta$, 这时,入侵检测机制不能有效地发挥作用,但是,随着时间的累积,这种偏移会逐渐增大,最终造成估计值也随之产生偏移,如果本地节点依然采用算数平均的算法,这个异常的偏移量必将使得本地节点的同步误差加大,可见这种攻击更具隐蔽性,但随着时间的累积,同样会对时间同步协议造成破坏.

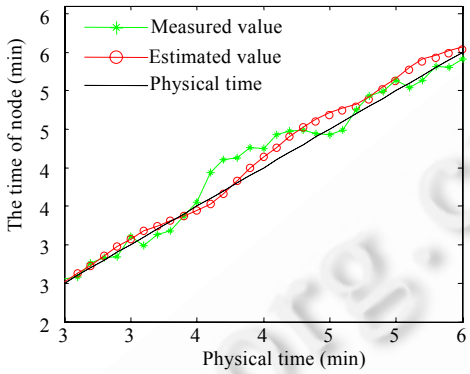

Fig.3 Estimated value under hidden attack of node synchronization information

图 3 节点同步信息受到隐蔽攻击时的估计值

本协议根据估计值的波动情况,采用随机加权的方法,可以有效地应对这种隐蔽性攻击.当节点估计值偏离本地校准值较大时,可以相应地减少其权值,降低其对本地校准时间的影响.如图 4 所示,节点 2 受到攻击,缓慢增加偏移量,结果节点 2 的估计值偏移逐渐增大,但是得益于随机加权的融合算法,本地节点的时间校准值并未发生偏离,显示出了较好的容错性能.

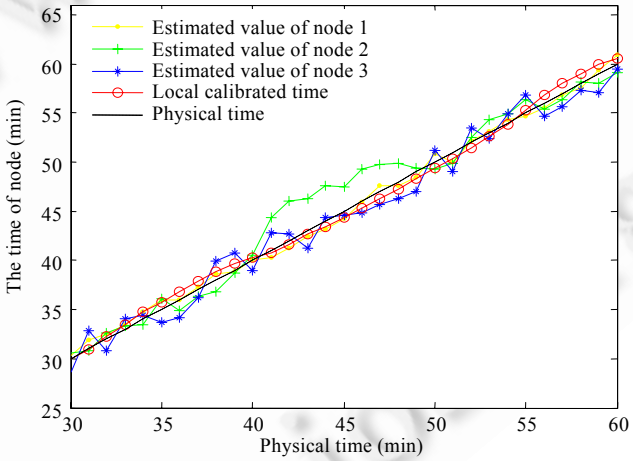

Fig.4 Local calibrated time under hidden attack of node synchronization information

图 4 节点同步信息受到隐蔽攻击时本地时间校准效果

4 总 结

本文针对无线传感器时间同步协议存在的安全问题,基于数据融合的思想,采用随机加权的方法,设计了一种具有容错机制的无线传感器时间同步协议,同时,在协议中加入入侵检测机制,在时间同步信息受到恶意攻击时能够进行报警,而且,由于采用最小均方误差的方法对观测值进行估计,能够有效地消除时间同步协议运行时产生的偶然误差,提高时间同步的精度.

References:

[1] Akyildiz IF, Su WL, Sankarasubramaniam Y, *et al*. A survey on sensor networks. IEEE Communications Magazine, 2002, 8(1):102−114.

[2] Ren FY, Huang HN, Lin C. Wireless sensor networks. Journal of Software, 2003,14(7):1282−1291. http://www.jos.org.cn/1000-9825/20030713.htm

[3] McKnight-MacNeil E, Rentel CH, Kunz1 T. Behavior of clock-sampling mutual network synchronization in wireless sensor networks: Convergence and security. Wireless Communications and Mobile Computing, 2010,10(1):158−170.

[4] Kalita1 HK, Kar A. Wireless sensor network security analysis. Int'l Journal of Next-Generation Networks (IJNGN), 2009,11(1): 1−10.

[5] Healy M, Newe T, Lewis E. Security for wireless sensor networks: A review. IEEE Sensors Applications Symp., 2009,80−85.

[6] Boyle D, Newe T. Securing wireless sensor networks: Security architectures. Journal of Networks, 2008,3(1):65−77.

[7] Estrin EJ, Fine D. Grained network time synchronization using reference broadcast. In: Proc. of the 15th Symp. on Operating Systems Design and Implementation (OSDI). 2002. 147−163.

[8] Ganeriwal S, Kumar R, Srivastava MB. Timing-Sync protocol for sensor networks. In: Proc. of the SenSys 2003: The 1st Int'l Conf. on Embedded Networked Sensor Systems. 2003. 138−149.

[9] Maroti M, Kusy B, Simon G, Ledeczi A. The flooding synchronization protocol. In: Proc. of the 2nd ACM Conf. on Embedded Networked Sensor Systems (SenSys). 2004. 39−49.

[10] Manzo M, Roosta T, Sastry S. Time synchronization attacks in sensor networks. In: Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks. ACM Press, 2005. 107−116.

[11] Ganeriwal S, Capkun S, Han CC, Srivastava MB. Secure time synchronization service for sensor networks. In: Proc. of the WiSe 2005: The 4th ACM Workshop on Wireless Security. 2005. 97−106.

[12] Song H, Zhu S, Cao G. Attack-Resilient time synchronization for wireless sensor networks. In: Proc. of the MASS 2005. 2005. 765−772.

[13] Sun K, Ning P, Wang C. TinySeRSync: Secure and resilient clock synchronization in wireless sensor networks. IEEE Journal on Selected Areas in Communications, 2006,24(2):395−408.

[14] Sun K, Ning P, Wang C. Fault-Tolerant cluster-wise clock synchronization for wireless sensor networks. IEEE Trans. on Dependable Secur. Comput., 2005,2(1):177−189.

[15] Hu X, Park T, Shin KG. Attack-Tolerant time-synchronization in wireless sensor networks. In: Proc. of the IEEE INFOCOM 2008. 2008. 448−456.

[16] Lamport L, Melliar-Smith P. Synchronizing clocks in the presence of faults. Journal of the Association for Computing Machinery, 1985,32(1):52−78.

[17] LI W, He PJ, Gao SS. Applying random weighted information estimation to implementing a new fusion algorithm formulti-sensors. Journal of Northwestern Polytechnical University, 2010,28(5):674−678 (in Chinese with English abstract).

[18] So HSW, Nguyen G, Walrand J. Practical synchronization techniques for multichannel MAC. In: Proc. of the MobiCom 2006. 2006. 134−145.

附中文参考文献:

[2] 任丰原,黄海宁,林闯.无线传感器网络.软件学报,2003,14(7):1282−1291. http://www.jos.org.cn/1000-9825/20030713.htm

[17] 李伟,何鹏举,高社生.多传感器加权信息融合算法研究.西北工业大学学报,2010,28(5):674−678.

秦绍华(1973－),男,山东济南人,博士生,主要研究领域为无线传感器网络,认知无线电.

陈冬岩(1972－),男,博士,教授,博士生导师,主要研究领域为无线传感器网络,嵌入式系统.