文章编号:1001 - 893X(2011)01 - 0061 - 07

基于 D - S 的时钟同步竞争安全算法*

王 波, 吕俊伟, 于振涛

(海军航空工程学院 控制工程系, 山东 烟台 264001)

摘 要:针对物联网时钟同步安全研究的不足,提出了一种时钟同步安全算法。首先,基于投票竞争的理念,给出了时钟同步安全算法过程;然后,为了解决此过程中涉及到的网络通信延迟不确定难题,提出了基于 D - S 理论的解决方法;最后,进行了仿真测试实验,结果表明在网络通信延迟不确定情况下,所提同步算法能容忍内部节点攻击,提高了时钟同步的安全性。

关键词:物联网;时钟同步;D - S 理论;安全;投票竞争;通信延迟

中图分类号:TN393 **文献标识码**:A doi:10.3969/j.issn.1001 - 893x.2011.01.013

A New Security Algorithm for Clock Synchronization Based on D - S Theory

WANG Bo, LV Jun-wei, YU Zhen-tao

(Department of Control Engineering, Naval Aeronautical and Astronautical University, Yantai 264001, China)

Abstract: The Internet of Things is the research hot spot, and clock synchronization is a key technology for Internet of Things. Internet of Things will involve political, economic and military security, and the security of its clock synchronization has attracted much attention. Aimed at the lack of the research of clock synchronization security, this paper presents a new algorithm for clock synchronization security. Firstly, based on the idea of voting and feedback, the course of this clock synchronization algorithm is given. Then, to solve the problems caused by communication delay in algorithm process, a solution based on D - S theory is proposed. Finally, the test experiment is performed and the results show that the proposed clock synchronization algorithm can improve the security of the clock synchronization.

Key words: Internet of Things; clock synchronization; D - S theory; security; competition; communication delay

1 引 言

物联网是世界信息产业的下一次浪潮,在国民经济、国家安全等领域发挥了重大作用[1-3]。

狭义上的物联网指连接物品到物品的网络,实现物品的智能化识别和管理;广义上的物联网则可以看作是信息空间与物理空间的融合,将一切事物数字化、网络化,在物品之间、物品与人之间、人与现实环境之间实现高效信息交互方式,并通过新的服务模式使各种信息技术融入社会行为[2]。

物联网旨在将所有物品通过各种信息传感设备与互联网连接起来以实现智能化信息采集、识别和管理。因此,可以认为物联网是互联网应用和服务的延伸和扩展[2]。

物联网将涉及到我国各行各业,许多重要设施

* **收稿日期**:2010 - 09 - 19;**修回日期**:2010 - 11 - 29
基金项目:国家高技术研究发展计划(863 计划)创新研究基金资助项目(2010AAJ133)
Foundation Item: The National High - Tech Research and Development Program (863 Program) of China (No.2010AAJ133)

设备将联接到物联网上,因此物联网将关系到国家的安全,它的安全性远比互联网要求高,其研究已成为我国的战略课题[3]。

时钟是信息空间与物理空间中的基本参量,在物联网的很多应用中,例如节点的状态判断、节点的相互协同以及节点的数据融合等,物联网的时钟同步起着重要的作用[4-6]。因此,时钟同步技术已成为物联网的关键技术之一。

在安全方面,敌方可以通过破坏物联网时钟同步过程,使我国重要的设备设施无法正常运行。因此,物联网时钟同步安全的研究具有重要的理论和实际意义。

物联网中的安全问题之一是如何防御网络内部的妥协节点攻击。目前的研究还存在一定不足,这可以从三方面来说明:

(1)目前国内外有关物联网的研究已明朗起来,人们关注热点主要集中在传感器、射频识别(RFID)、云计算及普适服务等领域,研究成果也较多,文献[2]对这些进行了较好的综述。但作为物联网许多应用的支撑技术之一,时钟同步问题却没有得到完整的论述和深入研究,研究成果匮乏;

(2)物联网是以互联网为基础的,时钟同步在互联网中已经得到了深入研究,取得了很好的成果,并成功应用到实际中,其中典型的是 NTP 协议[7-9],其全称为 Network Time Procotol,即网络时钟协议。它的具体实现方案是在网络上指定若干时钟源网站,为用户提供授时服务。NTP 协议规定了简单的认证机制,可以一定程度上抵御外部恶意节点攻击,但却无法防御网络内部的妥协节点攻击[7];

(3)目前传感器网络是个活跃的研究领域,可以认为物联网包含传感器网,传感器网是物联网实现数据信息采集的一种末端网络[1]。

传感器网络中的时钟同步引起了人们的极大重视,目前已有多种针对传感器网络的时钟同步安全算法,出现了不少研究成果[4-5]。但是这些算法在讨论安全性的同时都关注时钟同步中的开销问题,没有着重考虑网络通信延迟的不确定难题。因此,以互联网为基础的物联网无法借签传感器网络时钟同步安全算法。

物联网的建设在我国日益受到重视,研究我国物联网时钟同步安全算法的客观要求越来越强烈。因此,针对物联网时钟同步安全研究的不足,本文提出了一种面向物联网的时钟同步安全算法。仿真测试实验结果表明,与所对比的安全时钟同步算法相比,文中所提同步算法能容忍在网络通信延迟不确定情况下的内部节点攻击,提高了时钟同步的安全性。

2 竞争的安全算法过程

在互联网,为了保证时钟同步的安全性,常设置若干台时钟服务器,使时钟参考源成冗余布置。客户端可以与多台时钟服务器进行同步,通过选择算法淘汰错误的时钟服务器[7]。

虽然物联网是互联网的延伸,但因为物联网比互联网庞大,其中的节点众多,所以物联网如果采用这种互联网的时钟同步安全算法,将使网络通信以及时钟服务器负担加重。因此,互联网的时钟同步安全算法并不适用于物联网。

本文提出的时钟同步安全算法是基于投票机理的,即判断某一时钟服务器是否安全是由其它服务器的投票来确定;在同步过程中,客户端在确认安全的时钟服务器后,就可与时钟服务器进行时钟同步。

具体的算法过程如下:

(1)准备投票条件

1)取 $i=1$;

2)时钟服务器 i 发布“准备投票条件”;

3)取 $j=1$;

4)$j\neq i$,若 $j=i$,$j=j+1$;

5)时钟服务器 i 启动针对时钟服务器 j 的虚拟时钟,并利用 NTP 算法[3]求取与时钟服务器 j 时钟差值;

6)若 $j=n$(n 为时钟服务器总数),$i=i+1$,返回第 2 步;

7)若 $j\neq n$,$j=j+1$,返回第 4 步。

(2)投票

1)取 $i=1$;

2)时钟服务器 i 计算接收的时钟差值,选出时钟差超出范围的时间服务器,并向其投票;

3)若 $i\neq n$(n 为时钟服务器总数),$i=i+1$,返回第 2 步;

(3)统计票数并判断

1)取 $i=1$;

2)时钟服务器 i 统计自身得到的票数;

3)若票数超出规定值,则标记服务器自身为不安全时钟;

4)若 $i\neq n$(n 为时钟服务器总数),$i=i+1$,返

回第 2 步;

(4)客户端时钟同步

1)客户端选择一时钟服务器;

2)客户端确认时钟服务器是否安全;

3)若时钟服务器是安全的,则利用 NTP 同步算法[7]进行同步;

4)若时钟服务器是不安全的,则记录下此时钟服务器,以避免下个同步周期选中,并重新选择另一时钟服务器。

3　基于 D－S 的安全性判断

上述时钟同步安全算法是利用时钟差值来判断时钟服务器节点的安全性,这在理想条件下是可行的。但在实际情况中,由于网络延迟的不确定性影响,影响了同步结果[8-9]。因此,时钟差并不能准确反映节点的安全性,因此需要寻找新的安全性判断方法。

D－S 证据理论在不确定性表示、量测和合成方面有着特有的优势,在解决各领域的不确定问题上日益得到广泛应用。因此,可用它来判断时钟服务器节点的安全性。

基于 D－S 证据理论判断时钟服务器节点的安全性,分为 3 个步骤[10-12]。

3.1　识别框架的建立

DS 证据理论是建立在识别框架上的。设 Θ 表示 T 所有可能取值的一个论域集合,且所有在 Θ 内元素间是互不相容的,则 Θ 就是 T 的识别框架[10]。

定义节点安全性判断的识别框架为

$$\Theta = \{t_1, t_2, t_3, \cdots, t_n, \alpha\} \tag{1}$$

式中,$t_i = 1,2,3,\cdots,n$ 是时间服务器 i 利用 NTP 同步算法计算出的其它服务器的时间信息,α 是不确定的命题。

3.2　证据信任度求取算法

DS 证据理论要求证据在识别框架上对所有命题产生一个信任度即 BBA。若 Θ 是一识别框架,函数 $m:2^{\Theta}\rightarrow[0,1]$ 在满足下列条件[10]:

$$m(\Phi) = 0 \tag{2}$$

$$\sum_{t\subseteq U} m(t) = 1 \tag{3}$$

式中,$m(t)$ 为各个时间服务器节点的时间信息 t 在证据下的信任度 BBA。这里选择用于判断节点安全性的证据有时钟偏移量、路径延迟和路径延迟变化,其对应信任度 $m_i(t)$ 的求取算法下面分别介绍。

(1)时钟偏移量证据信任度 $m_1(t)$

如果 NTP 时钟服务器是按网络拓扑结构进行优化布置的,它们的网络流量和路径同时发生大变化的可能性不大,因此其时钟偏移大多在真实值附近。因此,时钟偏移量证据信任度 $m_1(t)$ 的求取算法公式可表示为

$$\begin{cases} m_1(t_i) = \dfrac{\varepsilon_i}{\varepsilon} \times w_1 \\ \varepsilon = \displaystyle\sum_{i=1}^{n} \varepsilon_i \\ \varepsilon_i = \displaystyle\sum_{j=1, j\neq i}^{n} \frac{1}{|\theta_i - \theta_j|} \end{cases} \tag{4}$$

式中,θ_i 和 θ_j 分别为对应时间服务器 i 和 j 的时间偏移。

(2)路径延迟证据信任度 $m_2(t)$

按照最小时延原理,路径延迟越小,时间同步误差减少的可能性越大。因此,路径延迟证据信任度 $m_2(t)$ 的求取算法公式可表示为

$$\begin{cases} m_2(t_i) = \dfrac{\beta_i}{\beta} \times w_2 \\ \beta = \displaystyle\sum_{i=1}^{n} \beta_i \\ \beta_i = 1/\delta_i \end{cases} \tag{5}$$

式中,δ_i 为对应时间服务器 i 的路径延迟。

(3)路径延迟变化证据信任度 $m_3(t)$

按照最小时延原理,相对最小路径延迟,若路径延迟变大,同步误差增大的可能性越大。因此,路径延迟变化证据信任度 $m_3(t)$ 的求取算法公式可表示为

$$\begin{cases} m_3(t_i) = \dfrac{\eta_i}{\eta} \times w_3 \\ \eta = \displaystyle\sum_{i=1}^{n} \eta_i \\ \eta_i = \dfrac{1}{\delta_i - \delta_{im}} \end{cases} \tag{6}$$

$$\sum_{i=0}^{3} w_i = 1 \tag{7}$$

式中,δ_{im} 为对应时间服务器 i 的目前最小路径延迟;w_i 为 3 个时钟证据 BBA 算法的比例系数,它们的和为 1。

3.3　NTP 时间源证据合成

利用 Dempster 合成规则,对 3 个时钟证据的信任度 $m_i(t)$ 进行合成,合成公式可描述为

$$\begin{cases} m_i = \dfrac{\eta_i}{\eta} \\ \eta_i = m_1(t_i) + m_2(t_i) + m_3(t_i) \\ \eta = \sum_{i=0}^{m} m_1(t_i) + m_2(t_i) + m_3(t_i) \end{cases} \tag{8}$$

通过证据合成得到识别框架中各个服务器时间信息的信任度 $m(t)$。若某一时间服务器的信任度 $m(t)$低于预先设定的一个门限 ζ,就可以判定该时间服务器不安全。

4 仿真实验

4.1 仿真实验系统

因为实际互联网的不可控性,无法在实际网络中分析验证文中所提安全算法,所以本文采用网络通信延迟设置和网络仿真两种方法作为实验手段[13-14]。网络仿真软件为 OMNeT++,用它来建立网络通信模型[15-16]。

搭建的仿真实验系统如图 1 所示。图中,Source 为网络信号源,产生具有自相似特征的网络流量[15];Sink 接收信息,处理办法是将接收消息直接删除,从而模拟一个完整的通信过程[16];NTP 时间服务器实现 NTP 协议,内含有一个高恒稳晶振。为了便于模拟网络路径延迟,时间服务器内含有一个延迟程序;监控主机用来设置时钟服务器的延迟时间、时钟服务器的时钟,以及观察时钟服务器的安全性判断结果;网络设备为交换机(Switch),它对接收到的消息复用,然后排队经过 buffer,最终分路回到网络中。

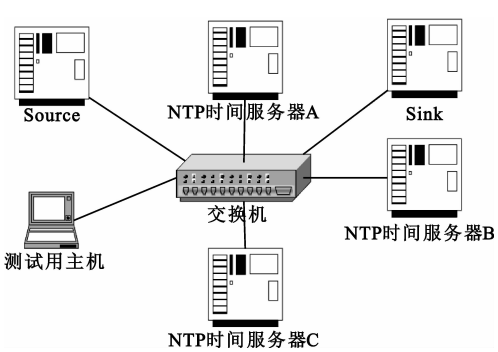

图 1 仿真实验系统示意图

Fig.1 Schematic diagram of simulation system

4.2 实验过程

本文所提安全算法的难点是解决网络通信延迟对算法的影响问题。

为了进行分析比较,实验时还测试了同样条件下基于 NTP 协议的安全性。

4.2.1 设置通信延迟的实验过程

通信延迟参数设置如表 1 所示。

表 1 通信延迟设置参数

Table 1 Set parameters of communication delay

序号	时间服务器发送延迟/ms	时间服务器接收延迟/ms
1	20	20
2	40	40
3	20	40
4	40	20

因子参数设置:$W_1 = 0.42, W_2 = 0.10, W_3 = 0.48$。

为了便于实验与分析实验结果,时间服务器的时钟在每次实验中为固定不变的。服务器时钟参数:正确时钟为 0 分 0 秒 0 毫秒,错误时钟为 0 分 0 秒 20 毫秒。时钟误差上限参数为5 ms,信任度判定门限 $\zeta = 0.36$。

实验过程如下:

(1)Source 和 Sink 停止工作;

(2)设置时钟服务器 A、B 和 C 均为正确时间;

(3)设置时钟服务器 A 和 B 的时间延迟为表 1 第一行情况,时钟服务器 C 的时间延迟为表 1 第二行情况;

(4)时钟服务器基于 NTP 算法和基于 D-S 算法,判断时钟服务器安全性,并上报监控主机,如表 2 第一行所示;

(5)分别设置时钟服务器 A、B 和 C 的时间延迟为表 1 第三和第四行情况;

(6)时钟服务器基于 NTP 算法和基于 D-S 算法,判断时钟服务器安全性,并上报监控主机,如表 2 第二行所示;

(7)设置时钟服务器 A、B 为正确时间,C 为错误时间;

(8)设置时钟服务器 A 和 B 的时间延迟为表 1 第一行情况,时钟服务器 C 的时间延迟为表 1 第二行情况;

(9)时钟服务器基于 NTP 算法和基于 D-S 算法,判断时钟服务器安全性,并上报监控主机,如表 2 第三行所示;

(10)分别设置时钟服务器 A、B 和 C 的时间延迟为表 1 第三和第四行情况;

(11)时钟服务器基于 NTP 算法和基于 D – S 算法,判断时钟服务器安全性,并上报监控主机,如表 2 第四行所示。

4.2.2　网络仿真的实验过程

网络流量对通信延迟的影响十分明显,会影响安全算法的结论。仿真过程为:

(1)网络信号源 Source 在网络中生成自相似网络流量,模拟真实的网络流量模型。信号源发出信息包长度不同以及周期不同,网络流量也不同[14,16];

(2)信号源向网络中发出一定长度的分组包,经过交换机 Switch 等网络设备发送到 NTP 时钟服务器等网络节点,最后分组包被 Sink 模块接收;

(3)NTP 时钟服务器对于信号源发来的流量消息和其它消息不做处理。NTP 时钟服务器基于 NTP 算法和基于 D – S 算法,判断时钟服务器安全性,并上报监控主机。

网络仿真参数:网络交换机处理速度10 Mbit/s,信号源信息包长度分别为0 byte、1 500 byte和3 000 byte,周期为2 ms,同步周期为60 s,仿真时间3 600 s。

服务器时钟参数仍为:正确时钟为 0 分 0 秒 0 毫秒,错误时钟为 0 分 0 秒 20 毫秒;不失一般性,设置时钟服务器 A 和 B 的时钟为正确时钟、C 的时钟为错误时钟。时钟误差上限参数仍为5 ms,信任度判定门限仍为 $\zeta = 0.36$。

4.3　实验结果

4.3.1　设置通信延迟的实验结果

设置通信延迟的实验结果如表 2 所示。

表 2　设置通信延迟的实验结果

Table 2 The result of set communication delay experiment

实验条件	时钟服务器安全判断	
	基于 NTP 竞争判断	基于 D – S 竞争判断
时钟服务器时钟均正确、路径对称	安全	安全
时钟服务器时钟均正确、路径不对称	不安全	安全
时钟服务器 C 时钟错误、路径对称	不安全	不安全
时钟服务器 C 时钟错误、路径不对称	不安全	不安全

由表 2 可以看出,基于 NTP 的竞争判断不易消除网络延迟对安全性判断的影响,而基于 D – S 竞争判断克服了基于 NTP 判断的不足,能正确识别出不安全的时钟服务器。这是因为 NTP 算法有个重要的前提条件,就是网络传输的往返路径是对称的。不对称的路径对 NTP 计算结果影响是很大的,使基于 NTP 竞争的安全判断得出错误的结果[7-8]。

因此,基于 D – S 的时钟同步竞争安全算法能够保证在一定错误同步报文时钟同步的安全性。

4.3.2　网络仿真的实验结果

网络仿真的实验结果如表 3 所示,仅列出了信号源的信息包长度为1 500 byte的情况,表中 A、B 和 C 分别指时钟服务器 A、B 和 C,T 和 F 分别代表时钟服务器安全和不安全。

表 3　网络仿真的实验结果

Table 3 The result of the network simulation experiment

序号	基于 NTP 竞争判断			基于 D – S 竞争判断		
	A	B	C	A	B	C
1	T	T	F	T	T	F
2	T	F	F	T	T	F
3	T	T	F	T	T	F
⋮		⋮			⋮	

基于 NTP 竞争和基于 D – S 竞争的安全的判断结果统计如表 4 所示。其中,判断错误是指把不安全的时钟服务器 C 判断为安全,或把安全的时钟服务器 A 和 B 判断为不安全;相反的判断则是正确的安全判断。

表 4　实验结果的统计

Table 4 The statistics of results

信号源包长度/byte	基于 NTP 竞争判断		基于 D – S 竞争判断	
	错误次数	正确次数	错误次数	正确次数
0	0	60	0	60
1 500	6	54	1	59
3 000	38	22	9	51

由表 4 可知:

(1)信息源信息包短时,网络流量小,网络延迟小,基于 NTP 竞争和基于 D – S 竞争算法都能正确判断内部妥协攻击节点;

(2)随着信息源信息包长度增加,网络流量增大,网络延迟且不确定性随之增大,容易使网络传输的往返路径产生不对称,破坏了 NTP 算法的前提条件,因此,基于 NTP 竞争的错误判断次数也增加;

在大流量下,基于 NTP 竞争的安全判断仍然有

正确的次数,原因在于网络延迟是随机的,即使网络延迟增加,但往返路径仍有对称的情况或有最小延迟的情况出现[7];

(3)随着网络流量增大,虽然两种算法错误判断次数都增加,但基于 D-S 竞争算法的错误判断次数远低于基于 NTP 竞争算法的错误判断次数。这说明前者能很大程度上克服网络延迟不确定性的影响。

总之,相比基于 NTP 竞争的安全算法,基于 D-S 竞争的安全算法能大幅提高识别错误时钟服务器的能力,也就提高了抵御内部攻击节点发送错误同步报文的能力。

5 结束语

为了防御物联网内部妥协节点对时钟同步的攻击,本文提出了一种时钟同步安全算法,给出了算法过程,并利用 DS 理论解决了网络通信延迟不确定的难题。通过仿真实验结果可以得出如下结论:

(1)文中所提时钟同步安全算法能容忍在网络通信延迟不确定情况下的内部妥协节点攻击,与所对比的安全时钟同步算法相比,大幅提高了时钟同步的安全性;

(2)随着网络流量增大,网络延迟及其不确定性增大,文中所提时钟同步安全算法性能也将降低,即出现错误的判断结果,但与所对比的安全时钟同步算法相比,降低幅度小得多;

(3)虽然随着网络延迟及其不确定性增大,文中所提时钟同步安全算法出现了错误的判断,但错误的次数较少。下一步,可以通过滤波或智能判断等技术工作消除这些错误的判断。

联网时钟同步安全对于我国物联网建设具有重要意义,但目前相关研究成果匮乏。本文提出的物联网时钟同步安全算法对今后的研究具有一定的借鉴作用。

参考文献:

[1] 宁焕生, 张瑜, 刘芳丽,等. 中国物联网信息服务系统研究[J]. 电子学报, 2006(12A): 2514-2517.
NING Huan-sheng, ZHANG Yu, LIU Fang-li, et al. Research on China Internet of Things' Services and Management [J]. Acta Electronica Sinica, 2006(12A): 2514-2517. (in Chinese)

[2] 孙其博. 物联网:概念、架构与关键技术研究综述[J]. 北京邮电大学学报,2010(3):1-9.
SUN Qi-bo. Internet of Things: Summarize on Concepts, Architecture and Key Technology Problem[J]. Journal of Beijing University of Posts and Telecommunications, 2010(3): 1-9. (in Chinese)

[3] 沈苏彬, 范曲立, 宗平,等. 物联网的体系结构与相关技术研究[J]. 南京邮电大学学报(自然科学版), 2009,29(6):1-11.
SHEN Su-bin, FAN Qu-li, ZONG Ping, et al. Study on the architecture and associated technologies for internet of things[J]. Journal of Nanjing University of Posts and Telecommunications, 2009, 29(6): 1-11. (in Chinese)

[4] 李凤保, 蒋义援, 潘泽友. 无线传感器网络时钟同步技术综述[J]. 仪器仪表学报, 2006, 27(1): 355-358.
LI Feng-bao, JIANG Yi-yuan, PAN Ze-you. Survey on time synchronization in wireless sensor networks[J]. Chinese Journal of Scientific Instrument, 2006, 27(1): 355-358. (in Chinese)

[5] 杨宗凯, 赵大胜. 无线传感器网络时钟同步算法综述[J]. 计算机应用, 2005(5): 1170-1172.
YANG Zong-kai, ZHAO Da-sheng. Survey of time synchronization algorithms in wireless sensor network[J]. Computer Applications, 2005(5): 1170-1172. (in Chinese)

[6] 杨春明, 屈玉贵, 赵保华. 一种新的动态无线传感器网络中的安全时同步算法[J]. 小型微型计算机系统, 2008, 29(7): 1353-1356.
YANG Chun-ming, QU Yu-gui, ZHAO Bao-hua. Novel Protocol for Secure Clock-synchronization in Dynamic Wireless Sensor Networks[J]. Journal of Chinese Computer Systems, 2008, 29(7): 1353-1356. (in Chinese)

[7] RFC 1305,The Network Time Protocol (NTP)[S].

[8] 沈燕芬. 用于网络时间同步的 NTP 协议[J]. 现代计算机, 2004, 18(5): 54-56.
SHEN Yan-fen. NTP of network clock synchronization[J]. Modern Computer,2004, 18(5): 54-56. (in Chinese)

[9] 徐怡山, 陶克, 贺鹏. NTP 时间同步性能研究[J]. 三峡大学学报, 2004, 26(6): 47-49.
XU Yi-shan, TAO Ke, HE Peng. Study of Performance for NTP Time Synchronization[J]. Journal of China Three Gorges University, 2004, 26(6): 47-49. (in Chinese)

[10] Zeng Cheng. Open frame dempster-shafer theory and its application in data fusion[D]. Beijing: Beijing Institute of Technology, 2005.

[11] Josang A. The Consensus Operator for Combining Beliefs [J]. Artificial Intelligence,2002,141(1):157-170.

[12] LUO H, YANG SL, FU C, et al. A new evidence combination rule based on the support degree of focal element[C]//Proceedings of the 4rd International Conference on Fuzzy Systems and Knowledge Discovery. Haikou: IEEE, 2007:432-437.

[13] 李明国, 宋海娜, 胡卫东. Internet 网络时间协议原理与实现[J]. 计算机工程, 2002, 28(2): 37-39.

LI Ming－guo, SONG Hai－na, HU Wei－dong. Principle and Implementation of Internet Network Time Protocol[J]. Computer Engineer, 2002, 28(2): 37－39. (in Chinese)

[14] 黎文伟, 张大方, 谢高岗,等. 基于通用 PC 架构的高精度网络时延测量方法[J]. 软件学报, 2006, 17(2): 275－284.
LI Wen－wei, ZHANG Da－fang, XIE Gao－gang, et al. A High Precision Approach of Network Delay Measurement Based on General PC[J]. Jounral of Software, 2006, 17(2): 275－284. (in Chinese)

[15] 于会游,周春晖,许希斌. 分组通信网络时钟同步研究及性能仿真[J]. 计算机仿真,2009(5):173－177.
YU Hui－you, ZHOU Chun－hui, XU Xi－bin. Simulation Analysis of Time Synchronization in Packet Networks[J]. Computer Simulation, 2009 (5):173－178. (in Chinese)

[16] Giorgi G, Narduzzi C. Modeling and Simulation Analysis of PTP Clock Servo[C]//Proceedings of 2007 Internation IEEE Symposium on Precision Clock Synchronication (ISPCS), for Measurement, Control and Communication. Vienna, Austria: IEEE, 2007: 155－161.

作者简介:

王　波(1966－),男,山东烟台人,2007 年获博士学位,现为高级工程师,主要研究方向为传感器与网络、时钟同步;

WANG Bo was born in Yantai, Shandong Province, in 1966. He received the Ph.D. degree in 2007. He is now a senior engineer. His research interests include sensors and networks, clock synchronization.

吕俊伟(1960－),男,山东烟台人,2003 年获博士学位,现为教授、博士生导师,主要研究方向为图像处理、传感器与网络;

LV Jun－wei was born in Yantai, Shandong Province, in 1960. He received the Ph.D. degree in 2003. He is now a professor and also the Ph.D. supervisor. His research interests include image processing and sensors networks.

于振涛(1984－),男,山东寿光人,博士研究生,主要研究方向为传感器网络。

YU Zhen－tao was born in Shouguang, Shandong Province, in 1984. He is currently working toward the Ph.D. degree. His research direction is sensors networks.

Email: shouguangyzt@163.com