IEEE802.15.4e标准的安全多跳时间同步协议设计

杨 伟 王 沁 万亚东 何 杰
(北京科技大学计算机与通信工程学院 北京 100083)

摘 要 IEEE802.15.4e是工业物联网中最新的MAC层标准,其采用时间同步技术实现高可靠、低功耗的无线网络。由于时间同步机制是工业无线网络中的核心支撑技术,因此其往往成为攻击者的首选攻击目标。针对IEEE802.15.4e标准的多跳时间同步协议存在安全性不足的问题,提出了一个多跳时间同步安全策略SMTSF。SMTSF安全策略主要采用基于异常的入侵检测算法、基于信任模型的多路径时间同步方法和加密与认证等关键技术,有效保障了节点之间安全地进行多跳时间同步。在基于入侵检测的算法中,边界路由器对节点的Rank值进行规则验证,可以有效检测出时间同步树攻击;同时设计了轻量级防火墙来抵御来自互联网的恶意主机攻击。在基于信任模型的多路径时间同步方法中,通过建立节点之间的信任模型来保障网络中节点可以找到一条安全多跳同步路径。仿真结果表明,SMTSF能有效检测时间同步树攻击并抵御捕获攻击。

关键词 IEEE802.15.4e,安全,时间同步,工业物联网
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.03.0038

Design of Secure Multi-hop Time Synchronization Protocol for IEEE802.15.4e

YANG Wei WANG Qin WAN Ya-dong HE Jie
(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract IEEE802.15.4e is the latest MAC layer standards for the industrial Internet of things, which enables highly reliable and ultra-low power wireless networking through time synchronization technique. Because time synchronization is a core fundamental technology for industrial wireless network, it often becomes an attractive target for attac-kers. This paper proposed a secure multi-hop time synchronization mechanism called SMTSF for IEEE802.15.4e. SMTSF mainly adopt anomaly-based intrusion detection algorithm, multi-path approach based on trust modeling, encryption and authentication technologies to secure multi-hop time synchronization. In the process of anomaly-based intrusion detection algorithm, the border router nodes verify the rank value of other nodes in the network which can effectively detect time synchronization tree attack. A mini-firewall based on packet filtering can stop intrusion attempts from the Internet. The multi-path approach based on trust modeling can find a secure path to the root node by establishing trust model between nodes. Simulation experiments show that SMTSF can detect time synchronization tree attack and defend against compromise attack.

Keywords IEEE802.15.4e, Secure, Time synchronization, Industrial Internet of things

物联网被认为是继计算机、互联网之后信息技术领域的又一次重大变革,它"通过信息传感设备,按照标准的通信协议,实现任何物品在任何时间任何地点的互联互通"[1]。物联网可以广泛应用在工业控制、环境监测、智慧城市以及智能交通等领域[2-3],其中以工业无线技术为核心的工业物联网是目前物联网领域中的主流发展方向之一。IEEE802.15.4e[4]是工业物联网中最新的MAC层标准,可以更好地支持工业和商业的应用,如过程自动化、工厂自动化、定位和追踪等,并且其可以与IETF制定的物联网标准如6LoWPAN[5]和RPL[6]进行连接。IEEE802.15.4e标准的关键技术是时间同步信道跳频(Time Synchronization Channel Hopping, TSCH):采用时间同步技术协调网络中的节点状态(发送、接收或休眠),避免了节点空闲监听,降低了节点能量消耗,从而延长了网络寿命;采用跳频技术让节点在不同的时隙使用不同信道,增强节点抵抗周围环境中无线干扰和多径干扰的鲁棒性[7]。在工业无线网络中,使用时间同步信道跳频技术可以实现在极低的

到稿日期:2016-02-23 返修日期:2016-06-20 本文受国家"八六三"高技术研究发展计划基金项目(2014AA041801-2),360开放实验室课题资助。

杨 伟(1987—),男,博士生,主要研究方向为无线传感器网络安全,E-mail:ustbyangwei@139.com;王 沁(1961—),女,博士,教授,主要研究方向为无线传感器网络与嵌入式系统;万亚东(1982—),男,博士,讲师,主要研究方向为无线传感器网络安全;何 杰(1983—),男,博士,讲师,主要研究方向为无线传感器网络安全。

功耗下达到 99.9%的可靠性[8]。目前，工业无线标准 WirelessHART 和 ISA100.11a 均采用了 IEEE 802.15.4e 标准的时间同步信道跳频技术。

与传统网络相比，工业无线网络对安全性提出了更高的要求。2010 年出现的震网病毒(Stuxnet)是第一个专门针对工业控制系统的恶意代码，包括中国、伊朗和印尼等多个国家地区的工业控制网络均因遭受该病毒的攻击而无法正常运行。由于时间同步是工业无线网络中的核心支撑技术，因此其往往成为攻击者的首选攻击目标。一旦网络的时间同步机制被破坏，将导致网络跳频、资源分配、路由转发和数据融合等依赖时间同步机制的应用不能正常运行。

然而 IEEE802.15.4e 标准[4]的时间同步协议在设计之初主要关注同步精度和能耗问题，缺乏安全方面的考虑。研究表明[9-10]，针对时间同步协议的攻击多种多样，如篡改同步时间包、延时攻击、时间同步树攻击以及捕获攻击等。Sun 等人[11]针对 TPSN 时间同步协议存在安全性不足的问题提出了 TinySeRSync 安全时间同步协议；尹香兰等人[12]针对 FTSP 时间同步协议受到恶意攻击的现象，提出一种基于单向链的轻量级安全时间同步协议 LiteST。由于 IEEE802.15.4e 标准的时间同步协议与 TPSN 和 FTSP 时间同步协议存在较大区别，且 IEEE802.15.4e 标准主要适用于工业无线网络，对网络安全性要求更加苛刻，因此以上安全时间同步协议均无法应用于 IEEE802.15.4e 标准。

本文主要研究 IEEE802.15.4e 标准的安全多跳时间同步协议。首先介绍无线传感器网络(WSN)中安全多跳的时间同步协议的相关研究；然后分析 IEEE802.15.4e 标准的时间同步协议，指出 IEEE802.15.4e 标准的多跳时间同步协议存在的安全问题，并提出一个多跳时间同步安全策略 SMTSF，其主要包括基于异常的入侵检测算法、基于信任模型的多路径时间同步方法和加密与认证等关键技术；最后通过仿真实验验证 SMTSF 能有效检测时间同步树攻击并抵御捕获攻击。

1 相关研究

Huang 等人[9]指出了 FTSP 时间同步协议存在篡改发送时间攻击、篡改包序列号攻击、假冒节点标识攻击和叛徒攻击，并提出了时间黑名单滤波器、包序列号黑名单滤波器、时钟偏差率滤波器和时间波动滤波器来抵御以上攻击，同时采用 TelosB 硬件平台及 TinyOS 操作系统搭建一个安全时间同步原型系统来验证以上防御方法的有效性。

Sun 等人[11]指出了 TPSN 时间同步协议存在延时攻击、虫洞攻击、女巫攻击以及捕获攻击等，然后提出了 TinySeRSync 安全时间同步协议，将加密和认证等安全机制加入到时间同步协议中以抵御恶意的外部攻击，如采用信息完整性认证来防止修改时间同步值攻击，在通信包中加入时间信息来抵抗重放攻击并通过估计端到端延迟来抵御 Pulse-Delay 攻击。

尹香兰等人[12]针对 FTSP 时间同步协议受到恶意攻击的现象，提出一种基于单向链的轻量级安全时间同步协议 LiteST，其能够防御篡改或延迟时间同步包、外部虫洞等外部攻击，并能容忍内部攻击节点发送错误时间信息。

Ganeriwal 等人[13]对 TPSN 时间同步协议的安全性进行了分析，指出了其可能遭受各种外部和内部攻击，其中最重要的是延时攻击；然后将信息完整性认证等安全机制融入时间同步协议中，提出了安全的单跳时间同步协议(SPS)和安全的组同步协议(SGS)，并在 MICA2 硬件平台上验证了 SPS 协议在最大延时攻击情况下其时间精度基本保持不变，且 SGS 协议可以有效抵御内部攻击。

2 IEEE802.15.4e 标准的时间同步协议

在 IEEE802.15.4e 网络中，时间被分成许多时隙，每个时隙有足够长的时间让一对节点交换数据包，但是节点需要在精确的时间发送和接收数据包。槽帧(slotframe)是多个时隙的组合，它是周期性重复的。图 1 为一个槽帧长度为 101 的时隙通信示意图。每一个时隙都有绝对时隙号(ASN)，它表示网络从开始形成经过的时隙数目。所有节点共享 ASN，节点 A 和 B 在时隙 1 通信，节点 B 和 D 在时隙 2 通信，节点 A 和 C 也在时隙 2 通信，但是它们使用不同的信道，互不干扰。

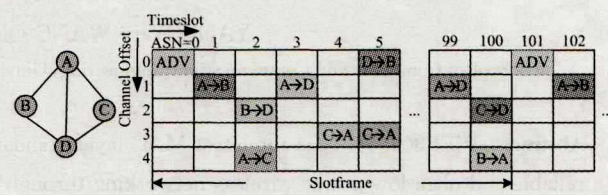

图 1 IEEE802.15.4e 网络的时隙-信道分配矩阵模型示意图

2.1 单跳时间同步

IEEE802.15.4e 标准采用时间同步信道跳频技术，其同步机制与传统 WSN 时间同步算法有很大区别，它采用时隙模板同步机制，包括 ASN 同步和 Device-to-Device 同步两部分。

节点在入网过程中需要进行 ASN 同步，具体过程如下：全功能设备周期性地发送广播 EB 包，EB 包中有足够的信息让节点加入和同步网络，节点接收到广播信息后，从广播信息中提取 ASN 值，并在下一个时隙自增。ASN 值在 IEEE802.15.4e 网络中的作用主要有两个：1)节点在每一个时隙处于什么状态都应该依据资源的调度，ASN 的值被用来计算节点何时应处于发送或接收状态；2)IEEE802.15.4e 标准提出信道跳频的技术，让节点在不同时隙使用不同信道，以增强节点抵抗周围环境中无线干扰和多径干扰的鲁棒性，而具体使用哪个信道则通过 ASN 的值计算。

Device-to-Device 同步用于节点加入网络后邻居节点之间时间的对齐。传感器节点一般通过硬件晶振来计时，如选择频率为 32.768kHz 的晶振，由于晶振存在时间偏移现象，典型的两个晶振存在 30ppm 偏移，即在 1s 的时间范围内两个晶振跑偏的时间差最大可以达到 60us，为了保持两个节点的时间一致性，其需要周期性重同步。Device-to-Device 同步的具体方式包括两种：Frame-based 同步和 Ack-based 同步。

(1)Frame-based 同步方式

Frame-based 同步方式如图 2 所示。

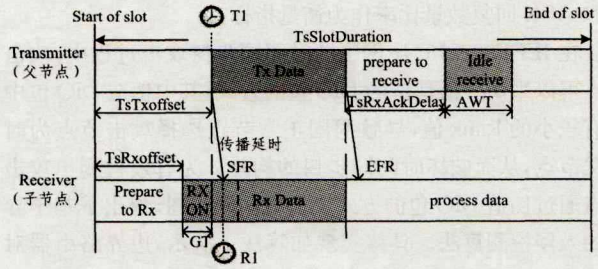

图 2　Frame-based 同步方式

父节点在时隙模板的预定时间发送同步包给子节点，其首先等待 TsTxoffsetms 时间（典型 2ms），在这段时间内配置射频和准备发送数据，在这个时间点将数据包的前导码发送出去，子节点在时隙开始首先等待 TsRxoffsetms 时间打开射频。考虑到子节点可能不完全同步父节点，提前打开射频，这段时间称为保护时间（Guard Time，GT）。经过很短的传播延迟（典型 2us），子节点收到父节点的前导码，射频芯片前导码引脚产生一个高电平给微控制器，子节点记录下当前的时间，然后可以计算与父节点的时间偏差，并调整自己的同步周期长度。

（2）Ack-based 同步方式

Ack-based 同步方式如图 3 所示。

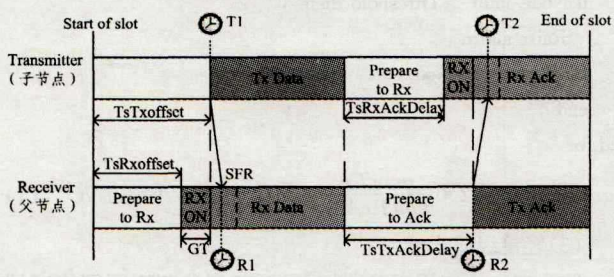

图 3　Ack-based 同步方式

子节点向父节点发起时间同步请求，其在时隙模板的 TsTxoffsetms 时间后准确地将时间同步包发送出来，父节点收到同步包的前导码后打时间戳并计算其与子节点的时间偏差；然后父节点计算偏差并将这个值填到 ACK 包中，等待 TsTxAckDelayms 后发送 ACK 包；子节点接收到 ACK 包后获得时间偏差，并调整自己的同步周期长度。

2.2　多跳时间同步面临的安全问题

IEEE802.15.4e 标准定义了节点如何与时间父节点进行时间同步，但是没有指出节点如何选择时间父节点以及节点如何进行多跳时间同步。IETF 6TiSCH 工作组推荐使用 RPL 路由协议生成时间同步树[14]，离根时钟源比较远的节点可以通过时间同步树逐层进行同步。RPL 是物联网 IPv6 路由协议，其通过使用目标函数和度量构建有向非循环图（DODAG），每个节点都拥有路由父节点。6TiSCH 工作组建议使用路由父节点作为其时间父节点，其能带来两方面的好处：1）DODAG 是有向非循环图，可以有效避免多跳时间同步中循环；2）DODAG 通过 RPL 路由协议建立与维护，不需要额外的能量开销来构造时间同步树。

IEEE802.15.4e 标准的多跳时间同步仍然面临多种安全问题，主要包括时间同步树攻击、捕获攻击和篡改时间同步包攻击[9]。由于采用 RPL 路由协议生成时间同步树，攻击者可以通过伪造 DIO 包攻击的方式破坏时间同步树的构建。捕获攻击是 WSN 中最有害的攻击之一。由于 IEEE802.15.4e 网络中节点资源大都受限，并且没有防篡改保护，当节点遭受捕获攻击后，攻击者可以读到节点存储的所有数据甚至改变节点行为，并且还可以拿到网络密钥，成功通过信息验证而不会被认为是攻击者。当一对节点通过多跳路径进行同步时，一个捕获节点可以带来任意误差，导致路径上所有节点的时间同步受到影响。多跳时间同步过程包含了多个单跳时间同步，假如单跳时间同步包没有进行加密或完整性认证，由于无线信号的广播特性，其容易被攻击者监听，同时攻击者可能对同步包进行伪造或篡改，造成单跳时间同步不正确，从而导致多跳时间同步受到破坏。

3　多跳时间同步安全策略 SMTSF

针对 IEEE802.15.4e 标准的多跳时间同步过程中存在多种安全漏洞，提出了一个多跳时间同步安全策略 SMTSF，其可以有效保障节点之间安全地进行多跳时间同步。SMTSF 主要采用了基于异常入侵检测技术、基于信任模型的多路径时间同步方法和加密与认证等关键技术。如图 4 所示，低功耗有损网络（LLN）由大量资源受限的无线传感器节点组成，节点之间通过单跳或多跳方式进行时间同步，然后通过边界路由器将采集数据发送到互联网中的服务器。传感器节点运行标准工业物联网协议栈，主要包括 MAC 层 IEEE802.15.4e 协议、路由层 RPL 与 6LoWPAN 协议、传输层 UDP 协议和应用层 CoAP 协议。SMTSF 采用混合部署方式，在普通节点上部署一些简单入侵检测模块，在边界路由器上部署信息收集模块、入侵检测的分析引擎模块和轻量级防火墙。其中，入侵检测和多路径同步模块运行在协议栈路由层，能有效抵御时间同步树攻击和捕获攻击；加密与认证协议运行在 MAC 层，能有效抵御监听和篡改时间同步包攻击；部署在边界路由器上的轻量级防火墙可以保护 LLN 网络免受来自互联网的攻击；通过采用多层次、全方位部署策略，可以保障 LLN 网络中节点安全地进行多跳时间同步。

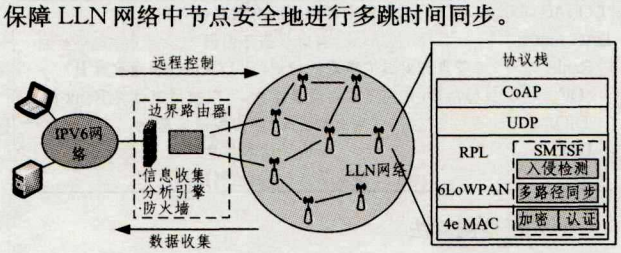

图 4　多跳时间同步安全策略 SMTSF 示意图

3.1　基于异常的入侵检测算法

在 IEEE802.15.4e 网络多跳的时间同步形成的过程中，首先采用 RPL 路由算法构建分层的时间同步树，网关节点作为全网的时钟源并处于最顶层，然后簇头和现场节点按照时间同步树依次进行时间同步。针对攻击者在时间同步树构建过程中进行攻击，提出了基于异常的入侵检测算法来检测时间同步树攻击，并设计了一个轻量级防火墙来保护 IEEE802.15.4e 网络免受来自互联网的攻击。

采用何种方式部署实时入侵检测系统是一个非常关键的问题。边界路由器的计算能力和存储能力比较强大，并且不用考虑能耗问题。边界路由器主要包括 3 个模块：1)信息收集，其收集网络节点 DIO 包信息；2)入侵检测的分析引擎，其通过对收集数据进行分析来发现各种攻击；3)轻量级防火墙，其主要用来抵御来自互联网的非法主机攻击。在资源受限的节点中主要部署信息采集模块，节点采集到相关信息后将实时发送到边界路由器。

(1)信息收集

信息采集模块是入侵检测过程中的一个关键模块。IEEE802.15.4e 网络的多跳时间同步树采用 RPL 路由协议构建。RPL 路由协议通过使用目标函数和度量构建有向非循环图(DODAG)，实现多跳转发数据包，其基本术语如表 1 所列。RPL 路由协议使用 DIO 包构建向上路由，即节点收到邻居节点广播 DIO 包后选择父节点，其中 Rank 值的大小是一个重要依据。边界路由器主要收集网络中节点及其邻居信息的 Rank 值，其可以通过周期性发送请求包来实现，请求包由 Gateway ID，RPL Instance ID，DODAG ID，DODAGVersion Number 字段构成，其大小为 6 个字节。网络中节点收到请求包后回复响应包，响应包主要包括 Node ID，DODAG ID，Rank，ParentID 和邻居节点信息，具体信息如图 5 所示，邻居节点信息包括邻居节点个数、邻居节点 ID 和邻居节点 Rank。由于 RPL 路由协议支持节点上传信息到边界路由器，因此在信息采集模块收集数据的过程中可以不用发送请求包，而是等待节点周期性地将响应包上传上来，从而降低网络通信量，减少能量消耗，但这需要在节点上设置相应的发送机制。

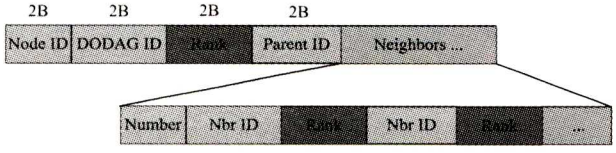

图 5 信息采集模块中节点响应包的结构图

表 1 RPL 路由协议的基本术语

术语	解释
DODAG	面向目的地的有向非循环图
DAG root	有向非循环图根
Rank	节点相对其它节点的位置(从 DODAG 根角度考量)
OF	目标函数(定义了路由度量指标，可以被用来计算 Rank 值)
DIO	信息对象发布(路由控制信息)
DAO	目的地通告信息
DIS	请求信息(路由控制信息)

(2)入侵检测算法

IEEE802.15.4e 网络的时间同步树由 RPL 路由协议构建。RPL 路由协议使用 ICMPv6 控制包来交换路由信息，其通过父节点广播 DIO 信息来构建 RPL DODAG 图，子节点周期性地发送 DAO 包给边界路由器。在 RPL DODAG 图中，节点的 Rank 值的大小是有规律的，子节点 Rank 值大于父节点 Rank 值。以节点 P 和节点 C 为例，节点 P 是节点 C 的父节点，则 Rank(C)＝Rank(P)＋ RankIncrease，其中 RankIncrease 与 RPL 路由协议定义了 OF0 函数相关。OF0 函数将链路质量、丢包率以及时间延迟等参数作为衡量指标，实际使用中 RankIncrease 的计算过程如式(2)所示，其主要将发包数量和 ACK 回复数量比率作为衡量指标。

在 IEEE802.15.4e 网络的时间同步树攻击过程中，攻击节点可以采用广播伪造的 DIO 包的方式，其中伪造 DIO 包中含有较小的 Rank 值，导致周围正常节点选择攻击节点为时间父节点，从而破坏时间同步树的构建。为有效检测出攻击节点通过伪造 DIO 包的方式攻击时间同步树，提出了基于异常的入侵检测算法。具体实现如算法 1 所示，边界路由器对收集信息进行数据分析，当节点 Rank 值小于其父节点 Rank 值与 MinHopRankIncrease 的和时(其中 MinHopRankIncrease 是 RPL 路由协议中规定的最小 Rank 增量)，表示出现异常。为了进一步提高检测率，设置了门限值 Threshold，当检测到同一个节点出现异常次数超过 Threshold 时就发出报警信息，并将该节点加入黑名单。

算法 1 SMTSF 中入侵检测的算法

```
Require: N—A list of nodes in the IEEE802.15.4e network
  for Node in N do
    if Node.rank <Node.parent.rank+MinHopRankIncrease then
                    Node.fault=Node.fault+1
      end if
    end for
  for Node in N do
    if Node.fault >Threshold then
      Raise alarm
    BlackList.add(Node)
    end if
end for
```

$$RankIncrease=2*\frac{numTx}{numTxAck}*MINHOPRANKINC \quad (1)$$

(3)轻量级防火墙

防火墙主要应用于互联网领域，起到分割不同网络区域的作用，从而根据设定的规则允许或禁止部分主机对内网进行访问，其可以是一套专门的硬件设备，也可以是一个软件，如 Windows 系统防火墙是通过软件实现的。在 WSN 中防火墙应用不是很多，主要原因如下：1)WSN 对能耗要求苛刻，防火墙应用会增加能量开销；2)目前 WSN 大都是孤立网络，没有与互联网进行互联互通，面临来自互联网的威胁相对较少。然而，IEEE802.15.4e 网络是面向物联网领域的，其通过上层路由协议与互联网进行互联互通，而互联网中攻击现象层出不穷，以 DOS 攻击为例，由于互联网主机比资源受限节点功能更强，其破坏力更大，因此需要为 IEEE802.15.4e 网络设计轻量级防火墙。

为更好地保护 IEEE802.15.4e 网络免受来自互联网的攻击，设计一个轻量级防火墙。其主要包括以下 3 方面功能：1)通过包过滤机制禁止特定主机 IP 访问 IEEE802.15.4e 网络，防止互联网中恶意主机对 IEEE802.15.4e 网络进行破坏；2)IEEE802.15.4e 网络内部节点协同发现有恶意的外部主机访问时，可以禁止其访问；3)提供安全审计功能。由于边界路由器位于 IEEE802.15.4e 网络与互联网中间，并且其有较强的计算能力和存储能力，因此将轻量级防火墙部署在边界路由器上。轻量级防火墙的具体实现算法如算法 2 所示，Host 代表来自互联网的主机，Source 代表来自 IEEE802.15.4e

网络的内部节点；设置两个过滤器 GlobalFilter 和 LocalFilter，其中 GlobalFilter 通过管理员手动设置，将互联网中某些危险 IP 段禁用，LocalFilter 是通过 IEEE802.15.4e 网络内部节点举报的。外部 Host 访问 IEEE802.15.4e 网络时先通过 GlobalFilter 过滤，然后经过 LocalFilter，通过映射关系判断有无新节点举报，若存在则记录下来，当超过了门限值 Threshold 则将其添加到 GlobalFilter，并将其从 LocalFilter 中删除。

算法 2　轻量级防火墙的算法

```
Require: Host—The host in the Internet
Require: Source—The node in the IEEE802.15.4e network
Require: GlobalFilter—some hosts need to filter based on IP rule
Require: LocalFilter— A map mapping an external host to a set of
IEEE802.15.4e
    Network nodes. The set describes some nodes that have reported
    that
    Specific external host.
  if Host in GlobalFilter then
    return filter the Host
  end if
  if Host in LocalFilter then
    Filter = LocalFilter.get(Host)
    {Add new Source to the list of nodes reported the Host}
    Filter.add(Source)
    if Filter.size() ≥ Threshold then
      GlobalFilter.add(Host)
      LocalFilter.remove(Host)
    end if
  end if
```

3.2　基于信任模型的多路径时间同步方法

捕获攻击(Compromise Attack)严重威胁着 IEEE802.15.4e 标准中正常的多跳时间同步。为有效抵御该类攻击，提出了基于信任模型的多路径时间同步方法。该方法通过建立节点与节点之间的信任模型，在构建多跳路径时绕过那些不受信任的节点，使得节点可以找到一条安全路径同步到根节点上。如图 6 所示，节点 10 通过一条多跳路径与节点 1 同步。假如节点 10 选择 Path_1，捕获节点 3 将破坏它们的正常时间同步。当节点 10 选择 Path_2 或者 Path_3 时，其可以成功绕过捕获节点进行正常时间同步。但是如何从多条路径中选择一条安全路径将是一个挑战，本文提出了基于信任模型的方法来解决这个问题。

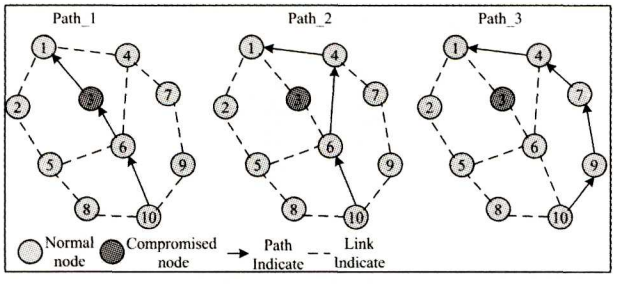

图 6　基于多路径的时间同步方法

(1)信任模型的建立

信任模型就是对网络中节点之间的信任关系进行量化，通过信任值来判断节点是否是攻击节点。当节点有多个邻居节点时，可以选择信任值最高的节点作为下一跳，从而绕过攻击节点。节点信任值的来源主要有两个方面：1)数据包转发的比率 $rate1=\frac{numTx\_K}{numTx\_A}$，其反映的是节点的合作关系，$numTx\_A$ 表示节点 A 发送数据包的总数，$numTx\_K$ 表示通过节点 K 转发的数据包数量；2)数据包转发的成功率 $rate2=\frac{numTx\_K\_ACK}{numTx\_K}$，其中 $numTx\_K$ 表示通过节点 K 转发的数据包数量，$numTx\_K\_ACK$ 表示节点 K 回复 ACK 的数量。

节点的信任值可以表示为 $T^d=\theta_1 T^w+\theta_2 T^r$，其中 θ_1，$\theta_2\in[0,1]$，$\theta_1+\theta_2=1$。本文借鉴了文献[15]的信任模型，引入了时间因子来描述信任值 T^w 和 T^r，其中 T^w 如式(2)所示，T^r 如式(3)所示。节点 A 每隔一段时间观察节点 K 的行为，$G_A(t_j)$ 代表节点 A 的观察时刻，其中 $j=1,2,\cdots,I$；$G_A(t_c)$ 代表当前计算时刻；$rate1$ 代表数据包转发的比率，$rate2$ 代表数据包转发的成功率，β 是遗忘因子且 $\beta\in[0,1]$。

$$T^w=P\{A:K,rate1\}=\frac{1+\sum_{j=1}^{I}\beta^{G_A(t_c)-G_A(t_j)}numTx\_K}{2+\sum_{j=1}^{I}\beta^{G_A(t_c)-G_A(t_j)}numTx\_A} \tag{2}$$

$$T^r=P\{A:K,rate2\}=\frac{1+\sum_{j=1}^{I}\beta^{G_A(t_c)-G_A(t_j)}numTx\_K\_ACK}{2+\sum_{j=1}^{I}\beta^{G_A(t_c)-G_A(t_j)}numTx\_K} \tag{3}$$

(2)多路径时间同步方法

基于信任模型机制可以绕开或避免攻击节点，但是由于路径上的节点存在失效情况(如因电压过低而无法工作)，仅选出一条安全的路径可能导致同步失败，因此需要考虑在一定传输概率下选择合适的路径数目以达到多跳时间同步。节点建立到根节点的同步路径时，首先找到多个下一跳邻居节点，然后通过自身计算的信任值来选择值得信任的下一跳节点进行包传递，直到最后选择了一条可以信任的路径进行多跳时间同步。定义 P_M 为时间同步包通过多路径成功到达根节点的概率，P_S 为单跳传输可靠性；若节点到根节点的跳数为 n，时间同步包通过多跳成功传输的概率为 P_S^n，则在 Num_Path 跳路径情况下时间同步包不能到达根时钟源的概率是 $(1-P_S^n)^{Num\_Path}$，其与 $1-PM$ 是等价的，因此可以推导出式(4)，其表示要成功通过多跳方式进行同步需要选择 Num_Path 条路径。

$$Num\_Path=\frac{\lg(1-P_M)}{\lg(1-P_S^n)} \tag{4}$$

(3)加密与认证方法

多跳时间同步过程通常由多个单跳时间同步组成。假如单跳时间同步过程遭受到监听或篡改攻击，造成单跳节点之间时间同步不正确，从而导致多跳时间同步受到影响。为了有效保证两个单跳节点之间能够安全地进行时间同步，需要对同步信息进行加密和完整性认证。

IEEE802.15.4e 标准提供三级安全性，包括无安全、使用控制清单 ACL 和采用 AES-128 的对称加密算法。采用 AES-128 的对称加密算法分为很多等级，包括仅加密 ENC、仅认证 MIC 和加密与认证 ENC-MIC。目前许多低功耗2.4G

射频模块支持 AES-128 硬件加密和信息完整性认证，通过写命令方式将射频模块设置到相应加密或认证模式。密文计算过程如式(5)所示，其中 *Plaintext* 表示明文，*Ciphertext* 表示密文，*Counter* 为计数器，*key* 表示密钥；完整性认证过程如式(6)所示，若认证码的位数是 32 位，则取 X_n 的高位 4 个字节。采用加密或完整性认证方法可以大大提高时间同步的安全性，如 TinySeRSync[11] 和 SPS[13] 安全时间同步协议均采用了该方法，但是由于其操作会带来额外的能量开销，因此需要在安全性与能耗两方面平衡考虑。

$$Ciphertext_i = E(key, Counter_i) \oplus Plaintext_i, i=0,1,\cdots,n \tag{5}$$

$$\begin{aligned} X_0 &= E(key, Plaintext_0 \oplus IV) \\ X_i &= E(key, Plaintext_i \oplus X_{i-1}), i=1,2,\cdots,n \end{aligned} \tag{6}$$

4 实验设计与结果分析

为了验证多跳时间同步安全策略 SMTSF 的性能，搭建了基于 OpenWSN 平台的仿真实验。OpenWSN 由美国加州大学伯克利分校研发，它是第一个完成 IEEE802.15.4e 标准并且完全开源的软件平台，能够很好地支持 6LoWPAN，RPL 和 CoAP 标准。OpenWSN 平台提供的基于离散事件的仿真器 OpenSim 不但可以对 IEEE802.15.4e 网络进行仿真，还可以精确地对节点的时钟进行模拟。OpenSim 是一个基于代码级的仿真器，其仿真效果基本上等同于真实节点。如图 7 所示，仿真节点连接在事件总线上，其通过多生产者-多消费者通信机制进行消息传递，OpenSim 提供了仿真节点需要的 SimEngine，MoteHandler，BspBoard，HwCrystal 和 Bsp-Radio 等功能模块。

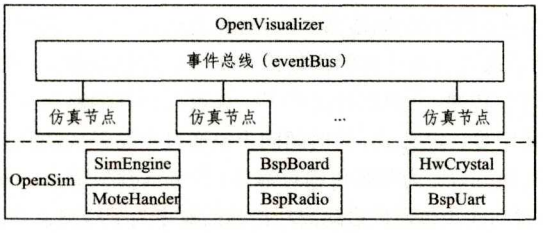

图 7 OpenWSN 仿真平台软件架构图

4.1 基于入侵检测的时间同步树构建的仿真

为了验证基于异常入侵检测的时间同步树构建的性能，采用 OpenSim 仿真器进行了仿真实验。仿真环境包含 21 个节点，包含攻击节点。攻击节点与正常节点一样，周期性地发送 EB 包、KA 包、DIO 包和 DAO 包，但是其广播的 DIO 包的 Rank 值是被伪造的，其小于自身计算得到的 Rank 值。RPL 路由协议采用 ICMPv6 控制信息来交换路由图信息，其通过广播 DIO 信息来构建 RPL DODAG 图。在 RPL DODAG 图中，节点的 Rank 值大小是沿着时间同步树依次增加的，图 8 中节点 1、节点 2、节点 5、节点 13 和节点 19 的 Rank 值的关系是 Rank(1)<Rank(2)<Rank(5)<Rank(13)<Rank(19)；子节点 Rank 的计算如式(1)所示，它通过接收父节点 DIO 包，获取父节点的 Rank 值，然后在其基础上增加 RankIncrease。

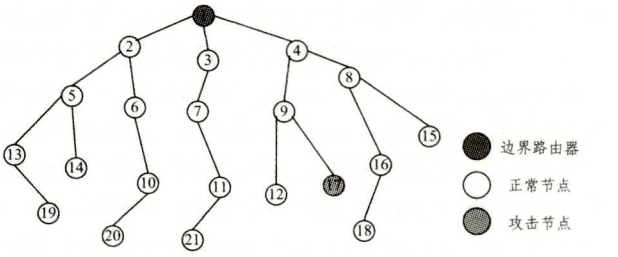

图 8 无攻击情况下的时间同步树结构图

图 9 所示为攻击情况下的时间同步树构建拓扑图。仿真节点 17 变成攻击节点，其广播伪造 DIO 包，DIO 包中 Rank 值比正常情况下的小，在正常情况下，其选择仿真节点 9 作为父节点，其 Rank 值大小为：Rank(17)=Rank(9)+RankIncrease；然而仿真节点 17 伪造 Rank 值，使得 Rank(17)<Rank(9)，周围邻居节点 11 和节点 12 接收到包含更小 Rank 值的 DIO 包时，将选择攻击节点 17 作为父时钟源；此时，边界路由器通过基于 Rank 异常的入侵检测算法能够发现该类攻击行为，因为仿真节点 9 是仿真节点 17 的父时钟源，然而其 Rank 值却大于子节点 17 的，这与 RPL 路由协议规定不一致，因此其能成功检测出仿真节点 17 是攻击节点。

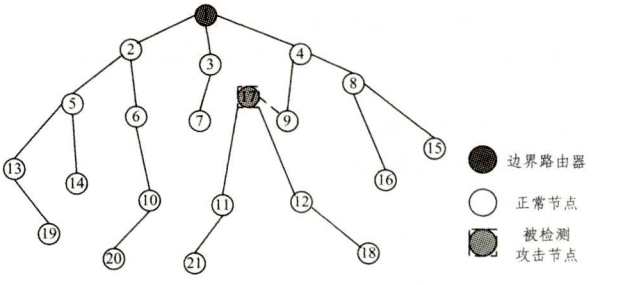

图 9 攻击情况下的时间同步树结构图

图 10 所示为不同攻击节点数目下入侵检测算法的检测率随时间变化的情况。在仿真过程中，攻击节点数目 m 的大小为 1，2 或 3。攻击节点周期性地广播伪造的 DIO 包，其中伪造 DIO 包中含有较小的 Rank 值。网络中节点通过信息采集模块来监听网络 DIO 包的信息，然后将其发送到边界路由器，边界路由器通过入侵检测算法判断有无攻击节点。从图 10 看出，仿真实验运行 5 分钟、攻击节点数目为 1 时具有很高的检测率，可以达到 91%，但是攻击节点比较多时检测率不高，因为有些攻击节点未被检测出来；随着检测时间的增加，检测率有明显上升，当运行时间为 20 分钟时，检测率均可以达到 90%左右。

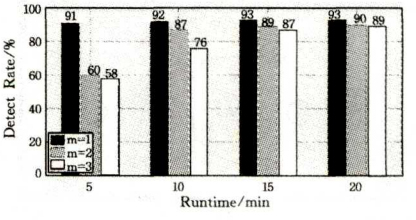

图 10 入侵检测算法的检测率随时间变化的情况

4.2 基于信任模型的多路径时间同步仿真

仿真实验由 60 个节点组成，每个仿真节点包含 32.768 kHz 晶振模型，其时钟漂移在[−30ppm，+30ppm]之间随机选择，设置每个仿真节点的最大邻居节点数为 10；在 Open-

WSN 仿真网络的时间同步过程中，使用 EB 包和 KA 包进行同步，EB 包的同步周期设置为 10s，KA 包的同步周期设置为 5s，网络的时隙大小为 15ms，遗忘因子 β 的大小为 0.9。在使用 OpenSim 进行仿真时，假设根时钟源是可信的，其余的节点可能受到恶意节点的攻击，如篡改或伪造同步包；对于每个仿真节点，其周围邻居中的恶意节点个数 t 可以为 0，1，2 和 3；当 $t=0$ 时，节点的周围邻居中没有恶意节点，其与正常时间同步一样；当节点受到恶意节点攻击后，导致同步丢失，其将不再重新入网，被认为丢同步。

图 11 所示为网络同步率随着恶意节点个数的变化图。当 $t=0$ 时，即无恶意节点的情况下，在原始同步协议和 SMTSF 下均有 95%以上的节点同步；然而随着恶意节点数目的增加，原始同步协议的网络节点同步率下降非常快，当 $t=4$ 时仅有 65%的节点同步到网络。相比较而言，安全的多跳时间同步策略 SMTSF 下降速度比较慢，当 $t=4$ 时网络同步率接近 85%，网络同步率提高了 15%以上，这主要是由于其选择了一条安全路径进行同步从而绕开了恶意节点。

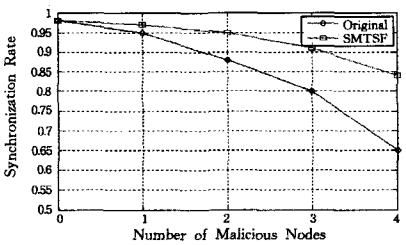

图 11　网络同步率随恶意节点个数的变化情况

图 12 示出了节点平均同步误差随着恶意节点个数的变化情况。当 $t=0$ 时，在原始同步协议和 SMTSF 下的平均同步误差值都小于 100us，同步精度很高；然而随着恶意节点数目的增加，原始同步协议和 SMTSF 下的平均同步误差都增大，但原始同步协议下的同步误差更容易受到恶意节点的影响。当 $t=4$ 时，原始同步协议下的平均同步误差超过 200us，而此时安全的多跳时间同步策略 SMTSF 下的误差为 150us 左右，同步精度提高 33%，表明 SMTSF 可以有效抵御恶意节点攻击，从而降低同步误差。同步误差影响网络同步周期的大小，同步误差越小，节点同步周期越长，从而网络功耗越低。

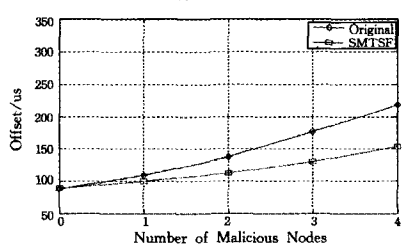

图 12　平均同步误差随恶意节点个数的变化情况

结束语　针对 IEEE802.15.4e 标准的多跳时间同步过程中存在多种安全漏洞，提出了一个多跳时间同步安全策略 SMTSF。SMTSF 主要采用了基于异常入侵检测技术、基于信任模型的多路径时间同步方法和加密与认证等关键技术。在基于异常的入侵检测算法中，采用集中式和分布式相结合的部署方式将入侵检测模块部署到边界路由器和资源受限节点上，实时采集 IEEE802.15.4e 网络中节点 DIO 包信息，然后在边界路由器上对网络中节点的 Rank 值进行规则验证，以有效检测时间同步树攻击；并设计包过滤机制的轻量级防火墙用于抵御来自互联网的恶意主机攻击。在基于信任模型的多路径时间同步方法中，建立节点与节点之间的信任模型，从而在构建多跳路径时绕过那些不受信任的节点，使得节点可以找到一条安全路径同步到根节点上。采用硬件支持加密与认证方法，以有效抵御监听和篡改时间同步包攻击。最后通过仿真实验验证了 SMTSF 能有效检测时间同步树攻击并抵御捕获攻击。

未来的主要工作是在真实无线传感器节点上部署多跳时间同步安全策略 SMTSF，并将其应用到实际工业物联网中。

参 考 文 献

[1] INFSO D. 4 Networked Enterprise & RFID INFSO G. 2 Micro & Nanosystems, in co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future[R]. Version 1.1, 2008.

[2] MIORANDI D, SICARI S, DE PELLEGRINI F, et al. Internet of things: Vision, applications and research challenges[J]. Ad Hoc Networks, 2012, 10(7): 1497-1516.

[3] ATZORI L, IERA A, MORABITO G. The Internet of Things: A survey[J]. Computer Networks, 2010, 54: 2787-2805.

[4] IEEE 802.15.4e-2012: IEEE Standard for Local and Metropolitan Area Networks-Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1[S]. New York: LAN/MAN Standards Committee, 2012.

[5] KUSHALNAGAR N, MONTENEGRO G, SCHUMACHER C. IPv6over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals: RFC 4919[R]. New York: Internet Engineering Task Force, 2007.

[6] WINTER T, HUBERR P, BRANDT A, et al. RPL: IPv6 routingprotocol for low-power and lossynetworks: RFC 6550[R]. New York: Internet Engineering Task Force, 2012.

[7] WATTEYNE T, LANZISERA S, MEHTA A, et al. Mitigating Multipath Fading through Channel Hopping in Wireless Sensor Networks[C]// 2010 IEEE International Conference on Communications (ICC). 2010: 1-5.

[8] DOHERTY L, LINDSAY W, SIMON J. Channel-specific wireless sensor network path data[C]// Proceedings of 16th International Conference on Computer Communications and Networks, 2007(ICCCN 2007). IEEE, 2007: 89-94.

[9] HUANG D J, TENG W C, YANG K T. Secured flooding time synchronization protocol with moderator[J]. International Journal of Communication Systems, 2013, 26(9): 1092-1115.

[10] YANG W, WANG Q, QI Y, et al. Time Synchronization Attacks in IEEE802.15.4 e Networks[C]// 2014 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI). IEEE, 2014: 166-169.

[11] SUN K, NING P, WANG C. TinySeRSync: secure and resilient time synchronization in wireless sensor networks[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006: 264-277.

（下转第 194 页）

用的随机数 N 相同，由引理 1 可知，所对应的 Γ_i（$1\leqslant i\leqslant m-1$）相同。综合以上两个条件可知，图 1 和图 2 这两次加密过程中前 $m-1$ 个分组的加密过程完全相同，因此所得到的密文 C_i 对应相同，即 $C'=(C_1\parallel\cdots\parallel C_{m-1})$。

在 Step2 中，因为 P 的最后一个明文分组只有 $n-1$ 位（不是满分组），根据第 1 节对参数 Λ 的介绍可知，$\Lambda'=\phi_\gamma(m)$，又因为 Step1 中 $\Gamma_m=\phi_\gamma(m)$，因此 $\Gamma_m=\Lambda'$。

由 Step1 可知：$C_m=\pi(\Gamma_m\oplus P_m)$。

由 Step2 和 $Format(x,n)$ 的填充原理得：

$$\begin{aligned}Tag'&=\pi(\Lambda'\oplus(First_{n-1}(C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\parallel 1)\oplus sum')\\&=\pi(\Lambda'\oplus(First_{n-1}(C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\parallel 1)\oplus P_m\oplus C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\end{aligned}$$

假设 $P_m\oplus C_1\oplus C_2\oplus\cdots\oplus C_{m-1}$ 的最后一位为 1，那么根据 iPMAC 模式的结构原理可知：

$$\begin{aligned}Tag'&=\pi(\Lambda'\oplus(First_{n-1}(C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\parallel 1)\oplus sum')\\&=\pi(\Lambda'\oplus(C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\oplus P_m\oplus C_1\oplus C_2\oplus\cdots\oplus C_{m-1})\\&=\pi(\Lambda'\oplus P_m)\end{aligned}$$

因为 $\Gamma_m=\Lambda'$，所以 $Tag'=\pi(\Gamma_m\oplus P_m)=C_m$。

$C_1\oplus C_2\oplus\cdots\oplus C_{m-1}$ 的最后一位为 1 的概率为 0.5，因此该伪造攻击成功的概率为 0.5，共使用一次解密访问。证毕。

因为 iPMAC 和 VPMAC 具有相同的结构特点，所以以上攻击方法同样适用于 VPMAC。

结束语 针对 iPMAC 模式的结构特点提出伪造攻击。iPMAC 的输入使用可变参数 Γ 和 Λ，在一定程度上增强了模式的安全性。控制随机数 N 不变，利用 Γ 和 Λ 在一定情况下相等这一特点提出攻击，使得可变参数相互抵消，得到一组新的有效对应关系（明文，密文，标签）。通过一次解密模块访问，即可实现对 iPMAC 的伪造攻击，成功伪造的概率为 0.5。因为 iPMAC 和 VPMAC 使用相同的加密模型，所以本文提出的伪造攻击过程同样适用于 VPMAC。

参 考 文 献

[1] GILBERT E, MACWILLIAMS F, SLOANE N. Codes which detect deception[J]. Bell System Technical Journal, 1974, 53(3): 405-424.

[2] PRENEEL B, VAN P Oorschot. MD-x MAC and building fast MACs from hash functions[C]// Advances in Cryptology-Crypto 95 Proceedings. Lecture Notes in Computer Science, Vol. 963, D. Coppersmith ed., Springer-Verlag, 1995.

[3] "Secure Hash Standard". Federal Information Processing Standards Publication 180-1[J]. Us Dept of Commerce/nist National Technical Information Service, 1995.

[4] WANG P, FENG D G. To construct the MAC based on block cipher [J]. Graduate School of Chinese Academy of Sciences Journa, 2005, 22(6): 746-750. (in Chinese)
王鹏，冯登国. 基于可调分组密码的 MAC 构造[J]. 中国科学院研究生院学报，2005，22(6)：746-750.

[5] ISO/IEC 9797-1. Information technology-security techniques message authentication code (MACs)-part 1: Mechanism using a block cipher[S]. International organization for standardization. geneve, swizerland, 1999.

[6] BLACK J, ROGAWAY P. A block-cipher mode of operation for parallelizable message authentication[M] // Lecture Notes in Computer Science 2332: Advances in cryptology-eurocrypt. 2002: 384-397.

[7] SARKAR P. Pseudo-random functions and parallelizable modes of operations of a block cipher[J]. IEEE Transactions on Information Theory, 2010, 56(8): 4025-4037.

[8] CAESAR-competition for authenticated encryption: security, applicability, and robustness[OL]. http://competitions.cr.yp.to/caesar.html.

[9] NASOUR B, JAVAD A, MOHAMMAD R. A single query forgery on avalanchev1[R]. Cryptographic Competitions Mailing List, 2014.

[10] GUY B. Forgery on stateless cmcc[OL]. http://eprint.iacr.org.

[11] CHAKRABORTY D, NANDI M. Attacks on the authenticated encryption mode of operation PAE[J]. IEEE Transaction on Information Theory, 2015, 61(10): 5636-5642.

[12] BRINCAT K, MITCHELL C. New CBC-MAC forgery attacks [C]// varadharajan, V, Mu, Y. (eds.) ACISP 2001. LNCS, Springer, Heidelberg, 2119: 3-14.

[13] CHEN J, HU Y P, WEI Y Z. A random message forgery attack on PMAC and TMAC-V[J]. Chinese Journal of Computers, 2007, 30(10): 1827-1832. (in Chinese)
陈杰，胡予濮，韦永壮. 随机消息伪造攻击 PMAC 和 TMAC-V[J]. 计算机学报，2007，30(10)：1827-1832.

[14] CHAO S D, ZHANG Z L, TIAN H, et al. Improved PMAC and security analysis[J]. Computer Engineering and Applications, 2009, 45(21): 77-78. (in Chinese)
晁仕德，张绍兰，田华，等. 改进的 PMAC 及安全性分析[J]. 计算机工程与应用，2009，45(21)：77-78.

（上接第 181 页）

[12] YIN X L, QI W D. LiteST: a lightweight secure time synchronization protocol for wireless sensor networks [J]. Journal on Communations, 2009, 30(4): 74-85. (in Chinese)
尹香兰，齐望东. LiteST：一种无线传感器网络轻量级安全时间同步协议[J]. 通信学报，2009，30(4)：74-85.

[13] GANERIWAL S, PÖPPER C, ČAPKUN S, et al. Secure time synchronization in sensor networks[J]. ACM Transactions on Information and System Security (TISSEC), 2008, 11(4): 23.

[14] THUBERT P, WATTEYNE T, PALATTELLA M R, et al. IETF 6TSCH: Combining IPv6 Connectivity with Industrial Performance[J]. Seventh International Conference on Innovative Mobile & Internet Services in Ubiquitous Computing, 2013, 395(6): 541-546.

[15] LUO J, LIU X, FAN M. A trust model based on fuzzy recommendation for mobile ad-hoc networks[J]. Computer Networks, 2009, 53(14): 2396-2407.