Journal of Computer Applications
计算机应用,2018,38(3):682 -687
ISSN 1001-9081
CODEN JYIIDU
2018-03-10
http://www.joca.cn

文章编号:1001-9081(2018)03-0682-06
DOI:10.11772/j.issn.1001-9081.2017092214

# 物联网中基于信任抗 On-off 攻击的自适应安全机制

张光华[1,2],杨耀红[2*],庞少博[2],陈振国[3]
(1.综合业务网理论及关键技术国家重点实验室(西安电子科技大学),西安 710071; 2.河北科技大学 信息科学与工程学院,石家庄 050000;
3.华北科技学院 河北省物联网数据采集与处理工程技术研究中心,河北 三河 065201)
(* 通信作者电子邮箱 hbyangyaohong@163.com)

**摘 要**:为了降低静态安全机制中不必要的数据源认证开销和防御信任阈值机制中存在的 On-off 攻击,在物联网(IoT)环境下提出了一种基于信任的自适应安全机制。首先,根据节点在信息交互中的行为表现建立节点间的信任评估模型,进而给出节点总体信任值的度量方法;然后,对于总体信任值高于信任阈值的节点,采用基于信任的自适应检测算法实时地检测这些节点总体信任值的变化情况;最终,中继节点根据自适应检测的结果决定是否验证接收到的消息。仿真实验结果和分析表明,该机制降低了中继节点的能量开销,同时对物联网中的 On-off 攻击起到较好的防御作用。

**关键词**:物联网;On-off 攻击;信任评估;自适应安全;能耗
**中图分类号**:TP393.1 **文献标志码**:A

# Adaptive security mechanism for defending On-off attack based on trust in Internet of things

ZHANG Guanghua[1,2], YANG Yaohong[2*], PANG Shaobo[2], CHEN Zhenguo[3]
(1. *State Key Laboratory of Integrated Services Networks (Xidian University), Xi'an Shaanxi* 710071, *China*;
2. *College of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang Hebei* 050000, *China*;
3. *Hebei Engineering Technology Research Center for IoT Data Acquisition and Processing, North China Institute of Science and Technology, Sanhe Hebei* 065201, *China*)

**Abstract:** To reduce the unnecessary overhead of data source authentication in static security mechanism and defend the On-off attack in trust threshold mechanism, an adaptive security mechanism based on trust was proposed in the Internet of Things (IoT). Firstly, the trust evaluation model was built according to node behavior in information interaction, further the measure method for total trust value of nodes was given. Then, for the nodes whose total trust values were higher than the trust threshold, the trust-based adaptive detection algorithm was used to detect the changes of the total trust values of these nodes in real time. Finally, the relay nodes determined whether to authenticate the received message according to the returned result of adaptive detection algorithm. The simulation results and analysis show that the proposed mechanism reduces the energy overhead of relay nodes, and plays a better role in defense against On-off attacks in IoT.

**Key words:** Internet of Things (IoT); On-off attack; trust evaluation; adaptive security; energy consumption

## 0 引言

物联网(Internet of Things, IoT)[1-2]实际上是一个大型的异构网络,它将大量终端设备(射频识别(Radio Frequency Identification, RFID)设备和传感器等)通过感知技术连接到互联网中,实现任何物体之间的智能化通信,几乎不需要人为干预就能完成日常任务。然而,物联网中的这些设备常常暴露在公共场合,通过无线传输信道进行通信,因此很容易受到恶意攻击[2-4],这就给物联网的安全带来了巨大的挑战;同时,物联网中的各节点均是能量有限的,故不能一味地提高网络的安全性,而忽略网络中节点的能量消耗问题;因此,既保证物联网所需的安全环境又能够减少节点能量的消耗,成为了国际研究界关注的热点。

为了减少物联网中各节点的能耗,同时又保留一定的安全措施,自适应安全[5-6]的概念就被提出了。自适应安全的优势在于能够根据安全威胁等级动态地调整安全措施,从而减少不必要的能量消耗。文献[7]为泛在移动网络和 Green IT(Green Information Technology)提出了基于自治和信任系统的自适应安全模型,该模型削减了一些安全措施,每个节点只传送必要的数据包。文献[8]为无线传感器网络的多跳能量采集提出了按需访问控制的自适应安全机制,节点可利用基站来发布其当前的安全措施,这有助于发送节点依据其安全需求选择合适的接收节点。文献[9]提出了物联网中的动态信任模型,其中安全措施的调整取决于路由度量中节点的置信度(丢包率、介质访问冲突等)。然而,这些自适应安全机制大多是由节点的能量等级来触发的,缺少有效的风险评估,这很有可能使恶意节点利用网络安全措施的削减而发起恶意攻击。

**收稿日期**:2017-09-13;**修回日期**:2017-10-07;**录用日期**:2017-10-10。 **基金项目**:国家自然科学基金资助项目(61572255);中国博士后科学基金资助项目(2015M582622);2016 年河北省物联网数据采集与处理工程技术研究中心开放课题(2016KF05)。

**作者简介**:张光华(1979—),男,河北石家庄人,副教授,博士,CCF 会员,主要研究方向:信任管理、网络安全; 杨耀红(1992—),女,河北邢台人,硕士研究生,主要研究方向:网络安全; 庞少博(1992—),男,河北承德人,硕士研究生,主要研究方向:网络安全; 陈振国(1976—),男,山东冠县人,副教授,博士,主要研究方向:物联网安全。

对于自适应安全中存在的安全风险,信任评估[10-11]是一种较好的解决方法。信任评估能够有效防御网络节点的内部攻击,已被广泛用于检测那些已经通过加密和认证屏障的恶意攻击。目前,采用信任评估解决物联网节点内部攻击的方式很多,主要是针对诽谤攻击[12]和共谋攻击[13]等一般性攻击,对于节点表现时好时坏的 On-off 攻击研究较少,主要原因是: 1) 在 On-off 攻击中,恶意节点存在 on 和 off 两种状态。在 on 状态时,节点表现不正常,具有攻击性; 在 off 状态时,节点和正常节点一样,表现正常。恶意节点不断地在 on 状态和 off 状态间交替转换,这就导致 On-off 攻击的 on 状态与 off 状态很难被预测到,不利于防御者找到 On-off 攻击规律进行防护。2) On-off 节点的信任值降低的速度很慢但增加的速度却很快,信任阈值机制很难发现 On-off 节点的存在。文献[14-15]均针对 On-off 攻击的特点提出了快速降低节点信任值和缓慢恢复节点信任值的方法,但都需要消耗节点大量的能量。文献[16]提出了物联网中分布式信任管理框架,该机制通过信任分配方法来自动鉴别物联网中的恶意节点,从而防止可能发生的 On-off 攻击,但该方案是通过直接观察节点行为而得到各节点信任值,没有考虑邻居节点的推荐信息。文献[17]提出了一种基于信任和能量意识的路由补救算法,解决了 On-off 攻击在消息转发过程中造成的丢包问题。虽然,上述这些方案均给出了解决 On-off 攻击的思路,但是这些方法并不适用于解决基于信任阈值的自适应安全中存在的 On-off 攻击。此外,信任评估机制一般只用于解决节点自私性和节点内部攻击问题,很少用于完成加密服务。

综上所述,现有的自适应安全缺乏有效的风险评估,而信任评估机制多用于解决节点的内部攻击,很少用于辅助加密和认证机制。因此,在给定的数据源认证机制的前提下,本文提出了物联网环境下基于信任的自适应安全机制以及一种检测 On-off 攻击的自适应检测算法,能够在节省中继节点的能量开销的同时防御 On-off 攻击的发生。此外,本方案能够对数据源认证机制起到较好的辅助作用。

## 1　信任评估模型

本方案所考虑的是一个资源受限的异构网络,在网络中,正常节点会合法地将消息发布到网络中,而一些恶意节点会在网络中非法地发布任何消息( 包括真实消息和虚假消息) 。为了防止恶意节点在网络中注入虚假消息或者篡改消息,传统静态安全机制的做法是在合法节点所发布的消息中添加消息认证码,以便于中继节点进行数据源认证,确保数据的完整性,尽可能地拒绝虚假消息。虽然该方法可以通过数据源认证来防止虚假数据的注入和消息被恶意篡改,但是中继节点需要验证收到的全部消息,这将造成大量的资源浪费,因此传统静态安全机制并不适用于动态且低功耗的物联网环境。

为了避免恶意节点在物联网中注入虚假消息或者篡改消息,同时又降低中继节点的能量消耗,本文将在中继节点对接收到的消息进行数据源认证前,采用基于信任的评估方法全面地评估发送节点的可信度,避免不必要的认证开销。该方法将节点的直接经验值、直接观察值和邻居推荐值这三个信任值分别加权并求和,得到节点的总体信任值。中继节点会通过比较发送节点的总体信任值与信任阈值之间的大小,进而判断是否验证该消息,这样便可减少中继节点进行不必要数据源认证的次数,降低中继节点的能源浪费。这里的发送节点既可以是源节点也可以是中继节点。为了便于下文中的描述,将信任阈值设置为 $t$。

**定义 1**　总体信任值是指直接经验值、直接观察值和邻居推荐值这三种信任值的合成,即主体 $A$ 对客体 $B$ 的综合信任评价。节点 $P_i$( 主体) 对节点 $P_j$( 客体) 的总体信任值,记为 $T_{ij}$。

节点总体信任值 $T_{ij}$ 的计算方法,如式( 1) 所示。总体信任值 $T_{ij}$ 是实数,其取值为 $0 \leqslant T_{ij} \leqslant 1$。其值为 0,则表明节点 $P_i$ 完全不信任节点 $P_j$; 其值为 1,则表明节点 $P_i$ 完全信任节点 $P_j$。

$$T_{ij} = \alpha E_{ij} + \beta O_{ij} + \gamma R_{ij} \tag{1}$$

其中: $E_{ij}$、$O_{ij}$、$R_{ij}$ 分别代表节点的直接经验值、直接观察值、邻居推荐值。$\alpha$、$\beta$、$\gamma$ 分别表示这三个信任值的权重因子,它们满足以下两个条件: 其一,$0 < \gamma \leqslant \beta < \alpha < 1$; 其二,$\alpha + \beta + \gamma = 1$。总体信任值 $T_{ij}$ 是节点 $i$ 对节点 $j$ 的综合信任程度,由直接经验值 $E_{ij}$、直接观察值 $O_{ij}$ 和邻居推荐值 $R_{ij}$ 分别加权并求和得到。直接经验值 $E_{ij}$ 来自于实体间的直接交互,是主体对客体的直接感知,最为可靠; 直接观察值 $O_{ij}$ 来自于主体对客体与其他实体进行信息交互时行为表现的观察,是主体对客体的间接感知,较为可靠; 邻居推荐值 $R_{ij}$ 来自于第三方实体的间接推荐,容易受到恶意推荐实体的攻击,可靠性较差。因此,在总体信任值的计算过程中,$\alpha$ 的取值最大,$\beta$ 的取值次之,$\gamma$ 的取值最小( $\gamma$ 的最大值不超过 $\beta$ 的最小值) ,而各个权重因子的具体大小由实际网络的应用要求确定。本方案将采用递归的方法计算节点的直接经验值、直接观察值和邻居推荐值这三个信任值,具体计算方法如下。

1) 直接经验值。

**定义 2**　直接经验值是指通过实体间的直接交互经验而得到的主体 $A$ 对客体 $B$ 的信任值。节点 $P_i$( 主体) 对节点 $P_j$( 客体) 的直接信任值,记为 $E_{ij}$。

直接经验值 $E_{ij}$ 的大小与发送节点 $P_j$ 发送的消息能否通过中继节点 $P_i$ 的数据源认证有关。如果来自节点 $P_j$ 的消息通过了中继节点 $P_i$ 的数据源认证,这会对 $E_{ij}$ 产生一个积极的影响; 如果中继节点 $P_i$ 接收到的来自节点 $P_j$ 的消息没有通过验证,则会对 $E_{ij}$ 产生一个消极的影响。一般情况下,如果发送节点 $P_j$ 的总体信任值 $T_{ij}$ 高于信任阈值 $t$,但节点 $P_j$ 发送了错误消息,那么造成这一现象的主要原因通常是节点 $P_j$ 的能量受到限制。

为了对节点的能量状况进行分类,本文中,用 $c$ 表示节点能量受限的临界值,$c_i$ 表示节点 $P_i$ 的自身能量。若 $c_i < c$,则表明节点 $P_i$ 的能量受到限制; 若 $c_i < c_j$,则表明节点 $P_i$ 的能量受限程度高于节点 $P_j$ 的能量受限程度。

直接经验值 $E_{ij}$ 的计算方法,如式( 2) 所示。直接经验值 $E_{ij}$ 的当前值取决于前一个直接经验值 $E_{ij}'$ 和新产生的经验值。如果中继节点 $P_i$ 接收到来自节点 $P_j$ 的消息通过了数据源认证,那么新产生的经验值为 1; 如果中继节点 $P_i$ 接收到来自节点 $P_j$ 的消息没有通过验证,但节点 $P_j$ 满足 $T_{ij} > t$ 和 $c_j < c$,即节点 $P_j$ 到目前为止仍为可信节点,但其能量受到限制,被迫成为妥协节点,那么新产生的经验值为 $a(0 < a < E_{ij}')$; 否则,新产生的经验值为 0。很明显,当节点 $P_j$ 的能量受到限制时,中继节点 $P_i$ 对节点 $P_j$ 新产生的经验值会降低,同时,$E_{ij}$ 的

值也会随之降低,进而导致总体信任值 $T_{ij}$ 也会降低。因此,一个可信节点在能量受限后,若持续转发不能通过中继节点验证的消息,那么也会变成不可信节点。$\eta^e$ 是一个权重因子,其取值为 $0 < \eta^e < 1$,目的是保持 $E_{ij}$ 的值在实数 0 ~ 1,并能够对前一个直接经验值 $E_{ij}'$ 和新产生的经验值都产生影响。

由式(2)可知,当 $\eta^e$ 的值较小时,$E_{ij}$ 的取值更依赖于新产生的经验值,而 $E_{ij}'$ 对 $E_{ij}$ 的影响则较小。例如:$E_{ij}'$ 和 $E_{ij}$ 这两个经验值间隔的时间较长,或者消息延时超过规定时间,这均将导致 $E_{ij}$ 与 $E_{ij}'$ 之间几乎没有联系,此时,$E_{ij}$ 的值则完全取决于新产生的经验值。

$$E_{ij} = \eta^e E'_{ij} + (1 - \eta^e) \times \begin{cases} 1, & \text{消息通过了认证} \\ a, & \text{消息未通认证且 } T_{ij} > t \text{ 且 } c_j < c \\ 0, & \text{其他} \end{cases} \quad (2)$$

2) 直接观察值。

**定义 3** 直接观察值是指主体 $A$ 通过直接观察客体 $B$ 与其他实体之间进行信息交互时的行为表现而获得的信任值。节点 $P_i$(主体)对节点 $P_j$(客体)的直接观察值,记为 $O_{ij}$。

在物联网中信息通过无线方式传输,各个节点均可以洞察到其通信范围内其他节点信息交互过程中的状况,也就是说,中继节点 $P_i$ 可以直接观察到发送节点 $P_j$ 在信息交互中的表现,并能够根据节点 $P_j$ 表现的好坏获得相应的直接观察值 $O_{ij}$。一般来说,当接收到的消息通过了数据源认证时,中继节点应该转发此消息并且不对消息内容作任何修改。同样地,当接收到的消息没有通过数据源认证时,中继节点通常不会转发这样的消息,但是如果中继节点转发了此类消息,中继节点也应该不对消息内容作任何修改。如果中继节点更改了接收到的消息内容并且转发出去,那么其他节点对该中继节点的直接观察值将会降低。

在本文中,用 $Retrans_{ji}(m)$ 表示节点 $P_j$ 转发节点 $P_i$ 的消息的状况。如果节点 $P_j$ 转发了来自节点 $P_i$ 的消息 $m$ 且不对其消息内容作任何修改,那么 $Retrans_{ji}(m)$ 的值为 1;如果节点 $P_j$ 没有转发来自节点 $P_i$ 的消息 $m$,那么 $Retrans_{ji}(m)$ 的值为 0;如果节点 $P_j$ 转发了来自节点 $P_i$ 的消息 $m$,但修改了其消息内容,那么 $Retrans_{ji}(m)$ 的值为 -1。

直接观察值 $O_{ij}$ 的计算公式,如式(3)所示。直接观察值 $O_{ij}$ 的当前值是由上一个直接观察值 $O_{ij}'$ 和新产生的观察值所决定的。如果节点 $P_j$ 能够准确无误地转发了来自节点 $P_i$ 的消息,那么新产生的观察值为 1;如果节点 $P_j$ 的能量受到限制,且没有转发来自节点 $P_i$ 发送的消息,那么新产生的观察值为 $b(0 < b < O_{ij}')$;如果节点 $P_j$ 的能量充足但它也不转发来自节点 $P_i$ 的消息,或者节点 $P_j$ 转发了接收到的消息(既包含来自节点 $P_i$ 的消息也包含来自其他节点的消息),但修改了其消息内容,那么新产生的观察值为 0。其中 $\eta^o$ 是一个权值因子,其取值为 $0 < \eta^o < 1$。

$$O_{ij} = \eta^o O'_{ij} + (1 - \eta^o) \times \begin{cases} 1, & Restrans_{ji} == 1 \\ b, & c_j < c \text{ 且 } Restrans_{ji} == 0 \\ 0, & Restrans_{ji} == 0 \text{ 且 } c_j > c \text{ 或 } Restrans_{jx} == -1 \end{cases} \quad (3)$$

3) 邻居推荐值。

**定义 4** 邻居推荐值是指通过第三方实体的间接推荐,主体 $A$ 获得的关于客体 $B$ 的信任值。节点 $P_i$(主体)获得的关于节点 $P_j$(客体)的邻居推荐值,记为 $R_{ij}$。

邻居推荐值 $R_{ij}$ 是由节点 $P_j$ 的邻居节点发送给中继节点 $P_i$ 的推荐信息计算而得的,$R_{ij}$ 的计算方法,如式(4)所示。$R_{ij}$ 的当前值是由两部分所决定的,即前一个邻居推荐值 $R_{ij}'$ 和节点 $P_i$ 新获得的关于节点 $P_j$ 的推荐信息 $r$。新产生的推荐信息 $r$ 和 $\eta^r$ 的取值分别为 $0 \leqslant r \leqslant 1$,$0 < \eta^r < 1$,其中 $\eta^r$ 是权重因子。

$$R_{ij} = \eta^r R'_{ij} + (1 - \eta^r) r \quad (4)$$

假设节点 $P_k$ 是节点 $P_j$ 的邻居节点,那么邻居节点 $P_k$ 所发送的关于节点 $P_j$ 的推荐信息 $r$ 是由节点 $P_k$ 对节点 $P_j$ 的直接经验值 $E_{kj}$ 和直接观察 $O_{kj}$ 分别加权并求和得到的。$r$ 的计算公式,如式(5)所示。其中 $\eta$ 是一个权重因子,其值为 $0 < \eta < 1$,用于权衡 $E_{kj}$ 和 $O_{kj}$ 这两个值。

$$r = \eta E_{kj} + (1 - \eta) O_{kj} \quad (5)$$

## 2 抗 On-off 攻击的自适应安全机制

### 2.1 基于信任阈值的自适应安全机制

为了节省中继节点的能量消耗,在消息传输的过程中,中继节点一般不会对接收到的所有消息都进行数据源认证,只会认证那些需要认证的消息。最简单的自适应安全机制就是设定一个信任阈值,将节点的总体信任值与信任阈值作比较,进而判断是否验证该消息。在该方案中,当发送节点的总体信任值高于信任阈值时,中继节点将默认该节点是完全可信的,不再对该节点传来的消息进行数据源认证;当发送节点的总体信任值低于信任阈值时,中继节点才会对该节点传来的消息进行数据源认证。该方案虽然降低了中继节点执行数据源认证所产生的能量开销,但存在着一个很严重的安全漏洞,即总体信任值超过信任阈值的节点并不一定都是可信节点,也可能是恶意节点。

假如一个恶意节点 $P_j$ 为了赢得其他节点的信任,会故意在信息交互中表现良好,一旦它取得了某个中继节点(假定是节点 $P_i$)的信任,将只发送错误的数据包给这个中继节点 $P_i$,但是由于恶意节点 $P_j$ 与中继节点 $P_i$ 之间的总体信任值 $T_{ij}$ 大于信任阈值 $t$,中继节点 $P_i$ 会默认来自节点 $P_j$ 的消息都是可靠的,并不对其消息进行验证。如此以来,中继节点 $P_i$ 对恶意节点 $P_j$ 的直接经验值 $E_{ij}$ 就不会改变。另外,如果恶意节点 $P_j$ 一直与节点 $P_i$ 之外的其他节点在信息交互过程中均保持良好的表现,那么中继节点 $P_i$ 对恶意节点 $P_j$ 的直接观察值 $O_{ij}$ 也就不会改变;甚至中继节点 $P_i$ 收到的关于恶意节点 $P_j$ 的邻居推荐信息也都是积极的,这就意味着 $R_{ij}$ 不会改变。同样,恶意节点 $P_j$ 与中继节点 $P_i$ 之间的总体信任值 $T_{ij}$ 也将不变。长此以往,恶意节点 $P_j$ 将只对中继节点 $P_i$ 发送错误信息,中继节点 $P_i$ 也会对恶意节点 $P_j$ 发送的消息不加认证地传送,这不仅会使目的节点作出错误的判断,而且会消耗网络资源。上述这种恶意攻击就是 On-off 攻击,它能够轻易地逃脱信任阈值的检测。由此可见,仅通过简单的信任阈值机制判决是否对接收到的消息进行数据源认证,无法抵御恶意节点的 On-off 攻击。为了解决这一问题,本文在信任阈值机制的基础上,提出了抗 On-off 攻击的自适应安全机制。

### 2.2　抗 On-off 攻击的自适应安全

为了检测总体信任值超过信任阈值的节点中是否存在恶意节点,本文提出了基于信任的自适应检测算法,具体算法流程如图 1 所示。本算法的主要思想是当总体信任值 $T_{ij}$ 小于给定的信任阈值 $t$ 时,系统直接返回 false; 如果总体信任值 $T_{ij}$ 超过了给定的信任阈值 $t$, 系统将会周期性地返回 false,但这个周期是随机变化的。其中,信任阈值 $t$ 作为自适应检测算法初步判断中继节点是否对接收到的消息进行数据源认证的分界值,若被设置得过高,则会起不到节约中继节点能量的作用; 若被设置得过低,则无法检测出恶意节点的 On-off 攻击。因此,信任阈值 $t$ 需根据实际网络的应用要求确定。

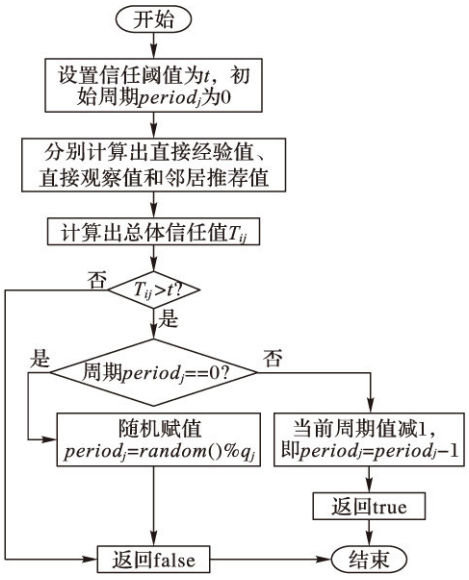



图 1　基于信任的自适应检测算法

Fig. 1　Trust-based adaptive detection algorithm

本算法能够实时地检测已经赢得中继节点 $P_i$ 信任的节点( 比如是节点 $P_j$) 行为,其以随机的方式给发送节点 $P_j$ 分配一个检测周期 $period_j = random() \% q_j$,设节点 $P_j$ 的初始检测周期值为 0。其中,$q_j$ 是一个与节点 $P_j$ 能量有关的值,节点能量 $c_j$ 越高,$q_j$ 的值就越大。这是因为节点 $P_j$ 有充足的能量时,其妥协的可能性就较小,所以系统返回 false 的时间应该长一些,也就是节点 $P_j$ 被检测的周期应该长些或者检测节点 $P_j$ 的频率应该低些。当检测周期结束时,如果节点的总体信任值 $T_{ij}$ 超过信任阈值 $t$ 且系统返回了 false,那就表明中继节点 $P_i$ 接收到的消息是非法的,也表明发送节点 $P_j$ 有可能是恶意节点并取得了中继节点 $P_i$ 的信任。这样的检测结果将导致 $q_j$ 的值减小,缩短对发送节点 $P_j$ 的检测周期,增加数据源认证次数,进而判断节点 $P_j$ 是否频繁转发错误消息。

本算法不定期地返回 false,对总体信任值超过信任阈值的节点进行随机的数据源认证,有助于进一步确定节点 $P_j$ 是否是恶意节点,从而防御恶意节点的 On-off 攻击。如果节点 $P_j$ 的总体信任值高于信任阈值并且被证明长时间发送错误信息,那么中继节点 $P_i$ 将停止观察节点 $P_j$ 的行为且停止收发关于节点 $P_j$ 的推荐信息,但是中继节点 $P_i$ 将继续保留关于节点 $P_j$ 的直接经验信息,以便于提防该节点再次恢复信任。事实上,如果中继节点 $P_i$ 一直验证恶意节点 $P_j$ 的消息,并观察节点 $P_j$ 的行为和收发关于节点 $P_j$ 的推荐信息,这样会导致采用本方案所消耗的能量多于采用传统静态安全机制所消耗的能量,因此,在本方案中,对于此类节点,中继节点将只保留该节点的直接经验值。

本方案中,中继节点在接收到消息后,会根据自适应检测算法的返回值,决定是否验证接收到的消息,具体操作流程如图2 所示。中继节点 $P_i$ 接收到来自节点 $P_j$ 的消息后,首先通过自适应检测算法,依据返回值决定是否验证该消息。如果返回值为 true,那么中继节点 $P_i$ 将不对接收到的消息进行验证,并会把该消息发送给下一跳节点; 如果返回值为 false,中继节点将会对接收到的消息进行验证。如果该消息通过了验证,那么中继节点 $P_i$ 将会把该消息发送给下一跳节点; 如果该消息没有通过验证,中继节点 $P_i$ 将会丢弃该消息。

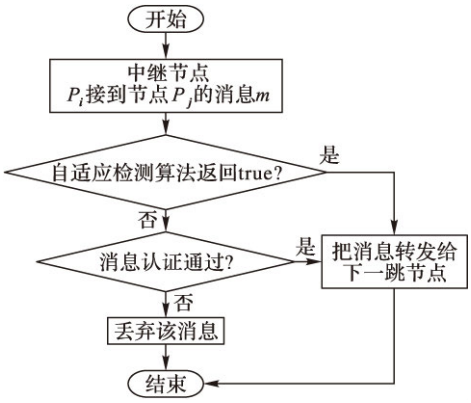



图 2　中继节点处理接收到的消息的过程

Fig. 2　Process of a relay node processing received messages

## 3　仿真实验与结果分析

### 3.1　仿真环境设置

本文采用 Contiki 操作系统下的 Cooja 网络仿真器[18] 进行仿真实验,结合 tinyDTLS ( Datagram Transport Layer Security) 库[19] 采用 HMAC MD5 算法产生消息认证码并进行数据源认证。仿真所用的网络拓扑结构如图 3 所示,图中黑色节点表示根节点,其他颜色及形状不同的节点表示它们的供电方式不同,白色节点表示采用电池供电,双环形节点表示该节点能够进行能量收集( 如: 太阳能供电) ,灰色节点表示由线路供电。在该网络拓扑中根节点会通过中继节点周期性地发送消息给末端节点,末端节点也会通过中继节点周期性地反馈消息给根节点。

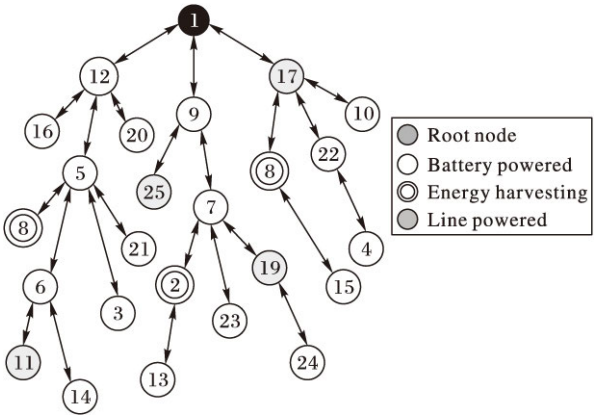



图 3　网络拓扑

Fig. 3　Network topology

在仿真中,设置 $q_j$ 为从 0 ~ 10 的整数。在仿真过程中不考

虑信息延时情况，那么在当前信任值中前一个信任值和新产生的信任值同等重要，故设置权重因子 $\eta^e$、$\eta^o$、$\eta^r$ 均为 0.5。为了防止直接经验值比重过高而不能全面评估节点总体信任值，因此，$\alpha < \beta + \gamma$；同时又满足 $0 < \gamma \leqslant \beta < \alpha < 1$，故设置权重因子 $\alpha$、$\beta$、$\gamma$ 分别为 0.4、0.3、0.3。因为正常节点误传消息的概率很低，所以在仿真过程中忽略正常节点由于误传消息而导致总体信任值下降的情况。在上述条件下，通过仿真实验得到网络拓扑中所有节点在无恶意攻击的情况下，总体信任值趋于平稳时的最小值约为 0.9。为了防御恶意节点的 On-off 攻击，提高网络安全性，需选择总体信任值较高的节点通过自适应检测算法的初步筛选，因此，仿真中设置信任阈值 $t$ 为 0.9。

### 3.2 仿真结果分析

#### 3.2.1 能量开销分析

本仿真采用 Cooja 仿真器中的 energest. h 库函数对中继节点的能量消耗情况进行分析，它能够通过比较中继节点的整体执行时间来衡量节点的能量消耗情况。在相同时间内节点的整体执行时间越短，其能量消耗就越少，节点的寿命就越长。图 4 是在恶意邻居节点数目不同的情况下，中继节点 5 在 5 min( 300 s) 内采用本方案与采用传统静态安全机制所用执行时间的比较。中继节点 5 有 5 个邻居节点，且这些邻居节点均给它发送数据包。

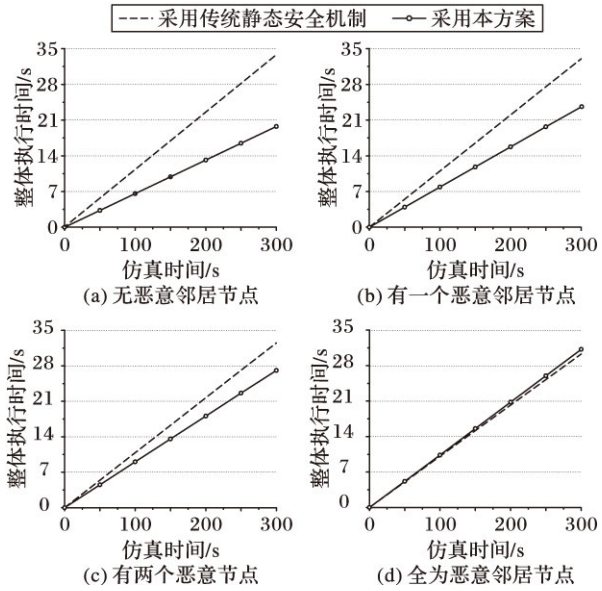



图 4 节点 5 在恶意邻居节点数目不同时所用整体执行时间

Fig. 4 Overall execution time of node 5 with different number of malicious neighbor nodes

由图 4 可见，节点的整体执行时间与仿真时间近乎成正比。为了便于衡量采用本方案与采用传统静态安全机制，节点能量消耗状况的差别，本文定义了一个参数 $\tau = tan_1 / tan_2$，其中，$tan_1$ 表示采用本方案节点的整体执行时间的正切值，它表示采用本方案单位时间内，节点整体执行时间的多少；$tan_2$ 是采用传统静态安全机制节点的整体执行时间的正切值。参数 $\tau$ 意味着采用本方案的节点寿命是采用传统静态安全机制节点寿命的 $\tau$ 倍。由图 4( a) 可得，当中继节点 5 的邻居节点中无恶意节点时，$\tau$ 的值约为 1.7，这表明中继节点 5 采用本方案比采用传统静态安全机制减少了 41.18% 的能量消耗。即便有一些邻居节点是恶意节点，那么中继节点 5 在采用本方案的情况下仍然比采用传统静态安全机制的情况下消耗的能量少。由图 4( b) 和图 4( c) 可得，当有一个恶意邻居节点时，$\tau$ 的值约为 1.4，当有两个恶意邻居节点时，$\tau$ 的值约为 1.2。不过，当所有邻居节点都是恶意节点时，中继节点 5 将对所有邻居节点传来的消息进行数据源认证，因此采用本方案与采用传统静态安全机制能量消耗情况基本一致，不过，从图 4( d) 中可以看出，采用本方案节点的能量消耗略微高于采用传统静态安全机制的能量消耗，这是因为本方案在刚开始的时候，计算总体信任值产生能量消耗。

本文还对网络中其他节点的能量消耗进行了评估，其能量消耗状况与图 4 所示的情况相似，不过 $\tau$ 值是不同的。经过比较，发现 $\tau$ 的取值与中继节点单位时间内接收到的数据包数量多少有关。表 1 总结了 5 min 内几个不同节点在无恶意邻居节点时 $\tau$ 值的情况。从表 1 中可以看出，在无恶意邻居节点时，节点 12 所接收到的数据包数量最多，它的 $\tau$ 值超过了 2，表明采用本方案所消耗的能量低于采用传统静态安全机制所消耗能量的一半。另外，当一些邻居节点妥协时，$\tau$ 的值是介于 1 与表中所给出的值之间的。由此可见，与传统静态安全机制相比，当中继节点单位时间内接收到的数据包越多时，采用本方案中继节点节省的能量就越多。

**表 1 不同节点在无恶意邻居节点时的 $\tau$ 值情况**

Tab. 1 $\tau$ value of different nodes with no malicious neighbor node

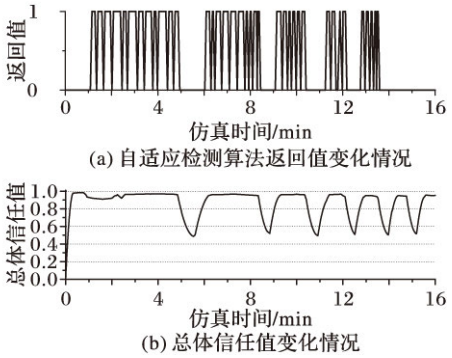
| 节点序号 | 接收到数据包的数目 | $\tau$ 值 |
|---|---|---|
| 24 | 11 | 1.00 |
| 6 | 58 | 1.06 |
| 17 | 181 | 1.38 |
| 9 | 252 | 1.60 |
| 12 | 600 | 2.01 |

#### 3.2.2 安全性分析

为了验证本方案的安全性，假设被信任的节点存在 On-off 攻击。图 5 展示了接收节点受到 On-off 攻击过程中，总体信任值与自适应检测算法返回值的变化情况，图中用 1 表示自适应检测算法返回值是 true，用 0 表示自适应检测算法返回值是 false。在仿真过程中，节点 6 是接收节点，节点 5 是具有 On-off 攻击的发送节点。由图 5 可以看出，当节点 5 的总体信任值高于信任阈值时，自适应检测算法会以随机的方式返回 false，并对来自节点 5 的消息进行数据源认证，然而，节点 5 不知道系统什么时候返回 false，也就无法确定所发送的消息能否避免数据源认证。

与以往的自适应安全机制相比，本方案能够通过实时追踪节点行为，有效地防御恶意节点的 On-off 攻击。即使节点 5 试图恢复信任并发送正常消息，自适应检测算法也会给节点 5 分配一个较小的检测周期，因为节点 5 已经被怀疑具有 On-off 攻击。如果节点 5 长期表现良好，那么检测周期也会逐渐增加。虽然，进行 On-off 攻击的恶意节点总是在发送正常消息与错误消息之间转换，但是自适应检测算法能够以随机的方式返回 false，对接收到的消息进行数据源认证，这会让恶意节点找不到系统返回 false 的规律，无从防备，从而达到

防御 On-off 攻击的目的。




(a) 自适应检测算法返回值变化情况

(b) 总体信任值变化情况

图 5　节点 6 受到 On-off 攻击时总体信任值和自适应检测算法返回值的变化情况

Fig. 5　Change of total trust value and change of returned value by adaptive detection algorithm, when node 6 is attacked by On-off attack

## 4　结语

为了给开放式的物联网提供一个安全且低功耗的环境，本文提出了一个适用于物联网的基于信任的自适应安全机制。本机制将信任评估与自适应安全相结合，中继节点可以根据自适应检测算法的返回值，进而判断是否验证接收到的消息。仿真实验结果表明本方案在降低中继节点的能量开销的同时，对 On-off 攻击起到一定的防御作用。由于本方案在进行信任评估时，没有考虑邻居节点的诽谤攻击，下一步工作将在此方案的基础上，考虑不可信的推荐消息进一步优化信任评估模型，此外，还会将本方案进一步扩展到有损网络或者其他拓扑结构的网络。

**参考文献** (References)

[1] GUO J, CHEN I R, TSAI J J P. A survey of trust computation models for service management in Internet of things systems [J]. Computer Communications, 2017, 97(C): 1 – 14.

[2] WANG P, ZHANG P. A review on trust evaluation for Internet of things [C]// MobiMedia '16: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications. Brussels: ICST, 2016: 34 – 39.

[3] SICARI S, RIZZARDI A, GRIECO L A, et al. Security, privacy and trust in Internet of things: the road ahead [J]. Computer Networks, 2015, 76(C): 146 – 164.

[4] WHITMORE A, AGARWAL A, XU L D. The Internet of things — a survey of topics and trends [J]. Information Systems Frontiers, 2015, 17(2): 261 – 274.

[5] AROUCHA C, ABDELOUAHAB Z, LOPES D, et al. Adaptive security mechanism: a study on the different approaches to mobile devices [J]. Journal of Information Sciences and Computing Technologies, 2015, 2(2): 147 – 153.

[6] GHOSH S, SEETHARAMAN S. Mechanism for adaptive and context-aware inter-IoT communication [C]// ANTS 2015: Proceedings of the 2015 IEEE International Conference on Advanced Networks and Telecommunications Systems. Piscataway, NJ: IEEE, 2016: 1 – 6.

[7] EL-MALIKI T, SEIGNEUR J M. Security adaptation based on autonomic and trust systems for ubiquitous mobile network and green IT [EB/OL]. [2017-04-02]. http://iaria.org/conferences2013/awardsUBICOMM13/ubicomm2013-a6.pdf.

[8] MAURO A D, FAFOUTIS X, DRAGONI N. Adaptive security in ODMAC for multihop energy harvesting wireless sensor networks [J]. International Journal of Distributed Sensor Networks, 2015, 2015(3): 1 – 10.

[9] FERNANDEZ-GAGO C, MOYANO F, LOPEZ J. Modelling trust dynamics in the Internet of things [J]. Information Sciences, 2017, 396(8): 72 – 82.

[10] MOUSA H, MOKHTAR S B, HASAN O, et al. Trust management and reputation systems in mobile participatory sensing applications: a survey [J]. Computer Networks, 2015, 90(C): 49 – 73.

[11] HE D, CHAN S, GUIZANI M. User privacy and data trustworthiness in mobile crowd sensing [J]. IEEE Wireless Communications, 2015, 22(1): 28 – 34.

[12] JIANG J, HAN G, WANG F, et al. An efficient distributed trust model for wireless sensor networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(5): 1228 – 1237.

[13] BHARGAVI S, GORANTHALA V P. The impact of collusion attacks in WSN with secure data aggregation system [J]. Neuropathology, 2015, 31(6): 648 – 653.

[14] 房卫东，石志东，单联海，等. 一种基于 BETA 分布抗 On-off 攻击的信任机制[J]. 系统仿真学报，2015，27(11)：2722 – 2728. (FANG W D, SHI Z D, SHAN L H, et al. Trusted scheme for defending On-off attack based on BETA distribution [J]. Journal of System Simulation, 2015, 27(11): 2722 – 2728.)

[15] 李姗姗. 基于监督机制的 WSN 安全数据融合算法设计[D]. 沈阳：东北大学，2011：19 – 40. (LI S S. Design of secure data aggregation algorithm based on monitoring mechanism in WSN[D]. Shenyang: Northeastern University, 2011: 19 – 40.)

[16] MENDOZA C V L, KLEINSCHMIDT J H. Mitigating On-off attacks in the Internet of things using a distributed trust management scheme [J]. International Journal of Distributed Sensor Networks, 2015, 2015(11): 1 – 8.

[17] 胡蓉华，董晓梅，王大玲. 一种信任和能量意识的 WSN 补救路由算法[J]. 控制与决策，2016，31(3)：435 – 440. (HU R H, DONG X M, WANG D L. A trust and energy aware remedy routing algorithm for wireless sensor networks [J]. Control and Decision, 2016, 31(3): 435 – 440.)

[18] THOMSON C, ROMDHANI I, AL-DUBAI A, et al, Cooja Simulator Manual [EB/OL]. (2016-06) [2017-04-11]. https://www.researchgate.net/publication/304572240-Cooja-Simulator-Manual.

[19] BERGMANN O. Tinydtls: a library for datagram transport layer security [EB/OL]. (2016-02-11) [2017-04-18]. https://sourceforge.net/projects/tinydtls/.

The work is partially supported by the National Natural Science Foundation of China (61572255), the China Postdoctoral Science Foundation (2015M582622), the Open Fund of Hebei Engineering Technology Research Center for IoT Data Acquisition and Processing in 2016 (2016KF05).

**ZHANG Guanghua**, born in 1979, Ph. D., associate professor. His research interests include trust management, network security.

**YANG Yaohong**, born in 1992, M. S. candidate. Her research interests include network security.

**PANG Shaobo**, born in 1992, M. S. candidate. His research interests include network security.

**CHEN Zhenguo**, born in 1976, Ph. D., associate professor. His research interests include Internet of things security.