物联网中基于信任抗丢包攻击的安全路由机制

张光华[1,2] 杨耀红[1] 张冬雯[1] 李 军[3]
(河北科技大学信息科学与工程学院 石家庄 050018)[1]
(西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)[2]
(河北师范大学数学与信息科学学院 石家庄 050024)[3]

摘 要 在开放的物联网环境下,节点在路由过程中极易遭到恶意丢包攻击(包括黑洞攻击和灰洞攻击),这将严重影响网络的连通性,并导致网络的数据包投递率下降以及端到端延时增加。为此,在RPL协议的基础上,提出了一种基于信任的安全路由机制。根据节点在数据转发过程中的行为表现,引入惩罚因子来评估节点间的直接信任关系,通过熵为直接信任值和间接信任值分配权重,进而得到被评估节点的综合信任值。利用模糊集合理论对节点间的信任关系进行等级划分,为路由节点选取信任等级较高的邻居节点进行数据转发,而信任等级较低的邻居节点将被隔离出网络。此外,为了避免正常节点由于某些非入侵因素而被当作恶意节点隔离出网络,为这类节点提供一个给定的恢复时间,从而进一步判断是否将其隔离出网络。利用Contiki操作系统及其自带的Cooja网络模拟器对所提方案进行仿真,实验结果表明,在节点数目和恶意节点比例不同时,本方案的恶意节点检测率、误检率、数据包投递率和端到端延时4个指标均有所改善。在安全性方面,本方案的恶意节点检测率和误检率明显优于tRPL协议;在路由性能方面,本方案的数据包投递率和端到端延时明显优于tRPL协议和MRHOF-RPL协议。仿真分析结果充分说明:所提方案不仅能够有效识别恶意节点,而且能够在恶意攻击存在的情况下保持较好的路由性能。

关键词 物联网,信任评估,丢包攻击,恶意检测,RPL协议
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.06.023

Secure Routing Mechanism Based on Trust Against Packet Dropping Attack in Internet of Things

ZHANG Guang-hua[1,2] YANG Yao-hong[1] ZHANG Dong-wen[1] LI Jun[3]
(College of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang 050018, China)[1]
(State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China)[2]
(College of Mathematics and Information Science, Hebei Normal University, Shijiazhuang 050024, China)[3]

Abstract In an open Internet of Things environment, nodes are vulnerable to malicious packet dropping attacks (including black hole attacks and gray hole attacks) in the routing process, which will seriously affect the connectivity of the network and lead to the decrease of packet delivery rate and the increase of end-to-end delay. For this reason, this paper proposed a trust-based secure routing mechanism on the basis of RPL protocol. According to the behavior of the nodes in the data forwarding process, the penalty factor is introduced to evaluate the direct trust relationship between the nodes, the entropy is used to assign weights to the direct trust value and the indirect trust value, so that the comprehensive trust value of the evaluated nodes is obtained. The fuzzy set theory is used to classify the trust relationship between nodes, and the neighbor nodes with higher trust level are selected for the routing node to forward data, while the neighbor nodes with lower trust level are isolated from the network. In addition, in order to prevent normal nodes from being isolated from the network as malicious nodes due to some non-intrusion factors, a given recovery time will be provided to further determine whether to isolate them from the network. This paper used Contiki operating system and its Cooja network simulator to carry out the simulation experiment of this scheme. The results show that the malicious node detection rate, false detection rate, packet delivery rate and end-to-end delay of this scheme are improved when the number of nodes and the proportion of malicious nodes are different. In terms of security, the malicious node detection rate and false detection rate of this scheme are significantly better than tRPL protocol. In terms of routing performance, the packet

到稿日期:2018-08-20 返修日期:2018-11-29 本文受国家重点研发计划项目(2016YFB0800703),国家自然科学基金项目(61572255),河北省高等学校科学技术研究项目(ZD2018236)资助。

张光华(1979—),男,博士,副教授,CCF会员,主要研究方向为网络与信息安全;**杨耀红**(1992—),女,硕士生,CCF会员,主要研究方向为网络与信息安全;**张冬雯**(1964—),女,博士,教授,CCF会员,主要研究方向为网络与信息安全;**李 军**(1976—),男,硕士,讲师,主要研究方向为网络与信息安全,E-mail:9099579@qq.com(通信作者)。

delivery rate and end-to-end delay of this scheme are significantly better than tRPL protocol and MRHOF-RPL protocol. The simulation analysis results fully demonstrate that this scheme can not only effectively identify malicious nodes, but also maintain better routing performance in the presence of malicious attacks.

Keywords Internet of things, Trust evaluation, Packet dropping attack, Malicious detection, RPL protocol

1 引言

物联网(Internet of Things, IoT)[1-2]是一个大规模的异构网络,能够将大量嵌入式设备(智能手机、平板电脑、可穿戴智能设备和智能汽车等)按照约定的协议与互联网连接起来,实现任何物体之间的互联。近年来,随着无线通信、传感器、嵌入式计算等技术的不断发展、成熟,物联网产业快速发展壮大,并已被广泛应用于智能交通、智能电网、智慧城市、智能医疗等领域[3-4]。根据 Gartner 公司的预测[5],到 2020 年,全球物联网设备的数量将达到 250 亿。

物联网在快速发展的同时,其安全也面临着巨大挑战。物联网节点由于大多部署在无人监管的公共场所,因此很容易受到恶意攻击。特别是在路由过程中,具有合法身份的内部节点极易引发丢包攻击。丢包攻击[6]是指在路由发现阶段,恶意节点对外谎称自己有一条极佳的路径到达目的节点,但是只要它接收到数据包,便会将全部或部分数据包丢弃。将恶意节点丢弃接收到的全部数据包这一行为,称为黑洞攻击;将恶意节点丢弃接收到的一部分数据包这一行为称为灰洞攻击。丢包攻击不仅会使网络中的数据包投递率降低,还会增加端到端的延时,更为严重的是,这些被恶意丢弃的数据很可能被攻击者用来进行非法活动,从而对人们的财产及生命安全造成威胁。

为了抵抗丢包攻击,本文提出了一种能够检测和隔离恶意攻击的信任评估模型,并将其应用于低功耗有损网络路由协议(Routing Protocol for Low-Power and Lossy Networks, RPL)。本方案根据节点转发数据包成功与否的行为来评估节点间的直接信任关系。为了快速识别出恶意节点,将惩罚因子引入到直接信任评估中,并通过熵给直接信任值和间接信任值分配权重,以避免主观分配权重给综合信任评估的准确性带来影响,同时结合模糊集合理论对节点间的信任关系进行等级划分,以此为网络选取可信的路由节点进行数据转发,并将识别出的恶意节点隔离出网络;此外,为了避免正常节点由于某些非入侵因素而被误识为恶意节点隔离出网络,将为这类节点提供一段恢复时间,进而判断是否将其隔离出网络。

本文第 2 节介绍相关工作;第 3 节概述 RPL 路由协议;第 4 节详细阐述所建立的信任评估模型;第 5 节介绍加入信任评估模型的 RPL 路由协议;第 6 节给出仿真实验,并对仿真结果进行分析;最后总结全文。

2 相关工作

目前,解决丢包攻击的方法有很多,其中一个行之有效的方法是根据路由节点的数据转发行为,对其进行信任评估,建立信任模型[7],以有效地识别恶意节点,增强网络的安全性和健壮性。

在无线传感器网(Wireless Sensor Networks, WSNs)和移动自组织网(Mobile Ad hoc Networks, MANETs)中,已有大量研究将信任评估应用于恶意节点检测。文献[8-9]提出了一种基于 QoS 信任和社会信任度量的分层信任管理协议,能够有效地处理自私节点和恶意节点。但其使用能量作为参数来计算不同的信任度量,当正常节点被自私节点包围时,将会消耗大量的能量,甚至会将正常节点误识为恶意节点。文献[10]提出了一种适用于医疗传感器网络的信任管理方案,采用成功交互次数、失败交互次数以及老化因子来计算节点信任值,并使用窗口机制处理历史信息,但这种固定的滑动窗口会使那些不活跃的恶意节点难以被检测到。文献[11]提出了一种基于 D-S 证据理论的信任管理策略,该策略为了解决 MANETs 中的黑洞攻击和灰洞攻击提出了两种算法:一种是基于邻居节点观察模型的直接信任值算法,该算法通过对邻居节点的观察获取历史证据并利用 D-S 证据理论得到直接信任值,以此对抗灰洞攻击;另一种是基于邻居推荐模型的间接信任值算法,为了防止诽谤攻击,该算法引入了证据距离来平衡不同邻居节点推荐的信任值,然而,当诽谤节点过多时,该算法会导致网络瘫痪,此外,由于引入了额外的控制分组,该方法具有较高的计算开销和路由开销。文献[12]提出了一种与文献[11]类似的方法,也是根据邻居节点的直接观察和推荐信息来衡量节点信任值,以此区分正常节点、可疑节点和恶意节点,然而,该方法不仅具有与文献[11]类似的局限性,还在假设中限制了灰洞节点的丢包率。

与 WSNs 和 MANETs 相比,将信任评估应用于物联网的研究较少。文献[13]在文献[8-9]的基础上,提出了一种物联网信任管理协议。该协议主要面向社会物联网环境,不适用于广泛的物联网环境。文献[14]对现有的物联网信任管理进行了分类,探索了影响信任关系的信任属性,还提出了一种物联网整体信任管理框架。近年来,将信任管理应用于 RPL 协议的研究陆续被提出。文献[15]引入了分组转发指示 PFI 作为 RPL 协议的信任度量,为了计算 PFI 度量,将每个节点分组发送给邻居节点,并监听这些节点是否转发分组,然后计算该分组成功沿路径传播的概率。然而该方法仅根据节点自身的知识来选择路径,很容易由于节点自身行为不当而选择错误的路径。为了确保 RPL 网络的通信安全,文献[16]利用可信平台模块 TPM 在交换密钥材料之前建立节点间的信任评估模型,但该方案的信任评估仅用于密钥交换安全,而不能用于路由选择和建立。为了弥补文献[16]在路由安全上的缺陷,文献[17]在 RPL 协议中提出了一种基于节点信任的路由度量,然而,该方案仅给出了理论研究,尚未证实其有效性。文献[18-19]提出了一种基于信任的物联网弹性路由机制,将主观逻辑的思想应用于节点间的信任评估,能够有效识别恶意节点,然而其在信任评估中没有考虑来自第三方的推荐信息,这会影响信任评估的完整性和准确性。

上述信任评估方案，一方面是针对 WSNs 和 MANETs 而设计的，在一定程度上通过信任评估来识别恶意节点，并为进一步的研究提供了理论基础，但这些方案不能直接应用于物联网；另一方面是针对物联网而设计的，虽然在一定程度上为建立物联网节点间的信任模型提供了思路，但用于解决恶意攻击（如丢包攻击、Sinkhole 攻击、Wormhole 攻击等）的研究较少。因此，针对物联网中的丢包攻击，本文在 RPL 协议的基础上设计了一种新的信任评估机制，使其能够有效地检测和隔离恶意节点。

3　RPL 协议

RPL 协议是由国际互联网工程任务组（Internet Engineering Task Group Force，IETF）的 ROLL（Routing Over Low power and Lossy networks）工作组设计的一种基于 IPv6 框架的距离矢量路由协议[20]，通常用于物联网的网络层。RPL 协议的拓扑结构类似于树形，被称为面向目的地的有向非循环图（Destination Oriented Directed Acyclic Graphs，DODAG），如图 1 所示。每个 DODAG 中只有一个根节点，通常为边界路由器（Border Router，BR），并且 DODAG 中的每个节点都有许多存储信息，如标识符、父节点列表、已发现的邻居节点列表、Rank 值和其他参数等。RPL 协议使用特定的控制消息和 Trickle 定时器来构建和维护网络拓扑。控制消息包括 3 种：DIO（DODAG Information Object）消息、DAO（DODAG Advertisement Object）消息和 DIS（DODAG Information Solicitations）消息。其中，DIO 消息用于 DODAG 上行链路的发现、创建和维护；DAO 消息用于调节和控制 DODAG 的下行链路；DIS 消息用于发现邻近的 DODAG。

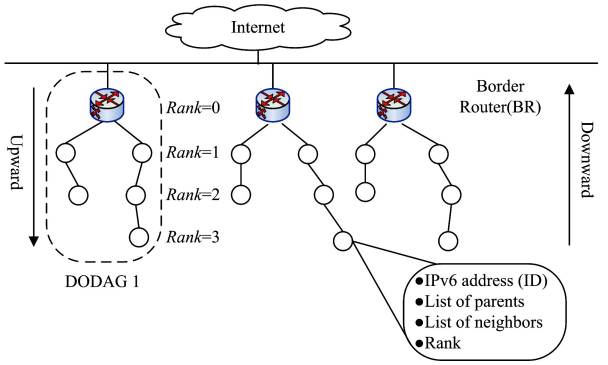

图 1　RPL 网络拓扑

Fig. 1　RPL network topology

在 DODAG 中，每个节点均会被分配一个 *Rank* 值，表示其在图中的位置。Rank 值是由目标函数（Objective Function，OF）通过一些特定的路由度量（如延迟、链路质量、吞吐量等）计算得到的。在 RPL 拓扑中，所有节点的 *Rank* 值必须满足以下两个条件：1）从 BR 到叶节点的 *Rank* 值应该递增，而从叶节点到 BR 的 Rank 值应该递减；2）数据包沿上行链路发送给 BR 或沿下行链路发送给叶节点时，应遵守文献[20]中定义的 *Rank* 值规则。因此，当节点沿上行链路接收数据包时，发送方的 *Rank* 值必须高于该节点，反之，当节点沿下行链路接收数据包时，发送方的 *Rank* 值必须低于该节点。

在 RPL 拓扑构建阶段，BR 会以广播的方式发送 DIO 消息，该消息包含 BR 的 *Rank* 值、DODAG ID、DODAG 版本、OF、Trickle 计时器以及度量等。当某节点接收到来自其邻居节点的 DIO 消息后，将根据 DIO 消息中的信息计算自己的 *Rank* 值，并将其封装在 DIO 消息中广播出去。每个接收到 DIO 消息的节点都会建立一个自己的父节点集合，并将其中路径最佳的父节点作为首选父节点。为了防止 DODAG 环路，每个节点的 *Rank* 值均大于其父节点的 *Rank* 值。然后重复广播和封装 DIO 消息这个过程，直到 DIO 消息到达叶节点为止。一旦网络拓扑构建完成，将根据 Trickle 计时器进行维护。Trickle 定时器主要负责调节控制消息的传输速率。也就是说，在稳定状态下，Trickle 计时器的时间间隔将增加，控制消息的传输速率将减慢；相反，如果网络拓扑发生不一致（如 DIO 消息被更改等），那么 Trickle 计时器的时间间隔将被重置为较低值，并加快控制消息的传输速率。

4　信任评估模型

在网络中，每个节点均需要根据路由协议将数据包转发给下一跳节点，为了避免将数据包转发给恶意节点，本文设计了一种能够检测和隔离恶意节点的信任评估模型。本模型由信任值计算、信任等级评估、信任监控与更新、信任恢复 4 部分组成，其整体设计如图 2 所示。

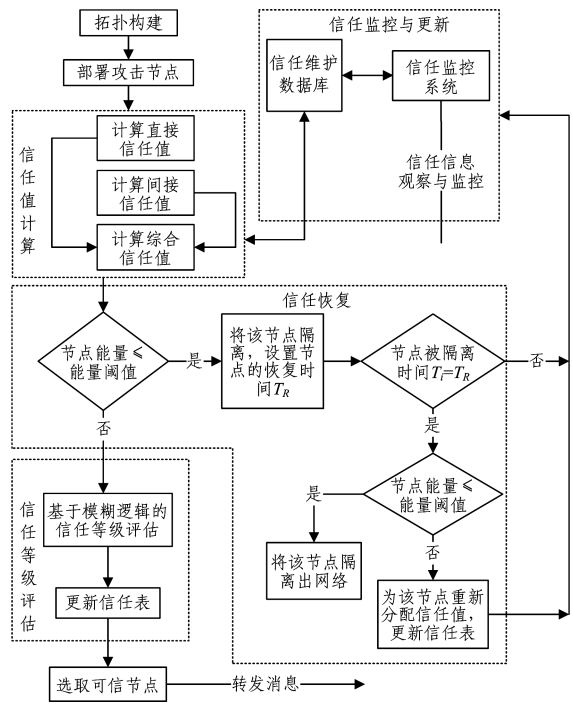

图 2　信任评估模型的整体设计框图

Fig. 2　Overall design block diagram of trust evaluation model

在信任值计算阶段，路由节点根据收集的信任信息分别计算邻居节点的直接信任值和间接信任值，然后将直接信任值与间接信任值分别加权并求和，得到被评估节点的综合信任值。在信任等级评估阶段，采用模糊集合理论将上一阶段得到的节点综合信任值进行区间分类，并选取信任等级较高的邻居节点进行数据转发，将信任等级较低的邻居节点进行隔离。在信任监控与更新阶段，路由节点将观察邻居节点行为，收集相关信任信息，并周期性地更新信任数据库。在信任

恢复阶段，为那些由于非入侵因素而被误识为恶意节点的正常节点提供一段恢复时间，以便其能够再次参与到网络中。与以往应用于 RPL 路由协议的信任评估模型[17-19]相比，本模型增加了信任恢复阶段，这样有助于那些被误识为恶意节点的正常节点重新恢复信任，避免被隔离出网络，从而降低误检率。接下来将详细介绍这 4 部分。

4.1 信任值计算

路由节点为了计算邻居节点的信任值，需收集与该邻居节点相关的信任信息。根据信任信息来源的不同，可将信任值分为直接信任值和间接信任值两种。

4.1.1 直接信任值

直接信任值 T_{ij}^{d} 是指节点 i 通过与邻居节点 j 直接交互数据而获得的信任值，其计算方法[21]如下：

$$T_{ij}^{d}=\frac{PF_{ji}(t)}{PF_{ji}(t)+\beta[PS_{ij}(t)-PF_{ji}(t)]} \tag{1}$$

其中，t 表示对节点 j 进行评估的时间，$PS_{ij}(t)$ 表示节点 i 发送给节点 j 的数据包总数，$PF_{ji}(t)$ 表示节点 j 成功转发来自节点 i 的数据包总数。这 3 个信息均被记录在节点 i 的邻居节点数据包的转发信息表中。另外，$[PS_{ij}(t)-PF_{ji}(t)]$ 代表节点 j 未能转发来自节点 i 的数据包总数，β 表示惩罚权重，可以通过调节 β 达到惩罚恶意节点的目的。

在文献[21]中，惩罚因子 β 的具体取值方法并未详细给出，而是设定为固定值，这样会使得不同信任程度的节点在出现不良行为后，均会受到相同的惩罚，不利于快速降低恶意节点的信任值。为了解决这一问题，本文设置 β 的初始值为 0.01，在后续的评估中，β 的取值与被评估节点当前所处的信任等级有关(4.2 节将给出它们之间的对应关系)，即恶意节点的信任等级越低，被赋予的惩罚因子值就越高，以此逐步降低恶意节点的直接信任值。

4.1.2 间接信任值

间接信任值 T_{ij}^{ind} 是指节点 i 通过广播查询从第三方节点 k(节点 k 为节点 i 和节点 j 共同的邻居节点)获得的关于节点 j 的推荐信息经综合计算得到的信任值。其计算方法如下：

$$T_{ij}^{ind}=\frac{\sum\limits_{k\in N(k)}(T_{ik}^{d}\times T_{kj}^{d})}{\sum\limits_{k\in N(k)}T_{ik}^{d}} \tag{2}$$

其中，T_{ik}^{d} 和 T_{kj}^{d} 分别为节点 i 对邻居节点 k 的直接信任值以及节点 k 对节点 j 的直接信任值；$N(k)$ 表示节点 i 和节点 j 共有的邻居节点集合。

4.1.3 综合信任值

综合信任值 T_{ij} 是指节点 i 通过直接和间接方式得到的关于节点 j 的综合评估信任值，该值是由直接信任值和间接信任值分别加权并求和得到的，如式(3)所示。由于直接信任值和间接信任值在综合信任评估中所占的比重不同，因此为了克服主观分配权重的弊端、提高信任评估的准确性，本文采用信息熵来确定这两种信任值在综合信任值中的权重。信息熵是信息论中的概念，常被用于度量随机事件携带的平均信息量，反映了多个评价指标对待评价对象的影响程度，即评价指标在评价体系中提供有用信息的多寡程度。因此，可采用信息熵来度量直接信任值和间接信任值在综合信任评价中的有效程度，并以此确定这两种信任值各自的权重。

$$T_{ij}=\omega_{ij}^{d}\times T_{ij}^{d}+\omega_{ij}^{ind}\times T_{ij}^{ind} \tag{3}$$

其中，ω_{ij}^{d} 和 ω_{ij}^{ind} 分别表示直接信任值和间接信任值的自适应权重，其计算方法分别如式(4)和式(5)所示：

$$\omega_{ij}^{d}=\frac{1-\frac{H(T_{ij}^{d})}{\log_2 T_{ij}^{d}}}{[1-\frac{H(T_{ij}^{d})}{\log_2 T_{ij}^{d}}]+[1-\frac{H(T_{ij}^{ind})}{\log_2 T_{ij}^{ind}}]} \tag{4}$$

$$\omega_{ij}^{ind}=\frac{1-\frac{H(T_{ij}^{ind})}{\log_2 T_{ij}^{ind}}}{[1-\frac{H(T_{ij}^{d})}{\log_2 T_{ij}^{d}}]+[1-\frac{H(T_{ij}^{ind})}{\log_2 T_{ij}^{ind}}]} \tag{5}$$

其中，$H(T_{ij}^{d})$ 和 $H(T_{ij}^{ind})$ 分别代表直接信任值的信息熵和间接信任值的信息熵。由信息论中的理念可知，$H(T_{ij}^{d})$ 反映了节点 i 对节点 j 直接信任程度为 T_{ij}^{d} 时，节点 i 信任节点 j 的平均不确定性，可由参数 T_{ij}^{d} 和 $1-T_{ij}^{d}$ 来确定，T_{ij}^{d} 表示节点 i 对被评价节点 j 的直接信任程度，$1-T_{ij}^{d}$ 表示节点 i 对被评价节点 j 的质疑程度；同样地，$H(T_{ij}^{ind})$ 反映了节点 i 对节点 j 的间接信任程度为 T_{ij}^{ind} 时，节点 i 信任节点 j 的平均不确定性，可由参数 T_{ij}^{ind} 和 $1-T_{ij}^{ind}$ 来确定。由此可得到 $H(T_{ij}^{d})$ 和 $H(T_{ij}^{ind})$，两者的计算方法如式(6)和式(7)所示[22]：

$$H(T_{ij}^{d})=-T_{ij}^{d}\log_2 T_{ij}^{d}-(1-T_{ij}^{d})\log_2(1-T_{ij}^{d}) \tag{6}$$

$$H(T_{ij}^{ind})=-T_{ij}^{ind}\log_2 T_{ij}^{ind}-(1-T_{ij}^{ind})\log_2(1-T_{ij}^{ind}) \tag{7}$$

4.2 信任等级评估

由于信任不是绝对的概念，所以很难确定节点信任与不信任的界限。为了更加有效地评估节点的可信性，本文采用模糊集合理论，将节点间的信任关系划分为 5 个不同信任等级的信任集合 $V=\{v_1,v_2,v_3,v_4,v_5\}$，其所代表的信任等级分别为“完全不信任”“不太信任”“一般信任”“比较信任”“完全信任”，如表 1 所列。这样不仅有助于选取高质量的可信节点进行安全通信，还有助于检测和隔离恶意节点。

表 1 信任等级划分

Table 1 Trust level division

V	信任等级	范围	β
v_1	完全不信任	[0,0.2]	0.3
v_2	不太信任	[0.2,0.5)	0.2
v_3	一般信任	[0.5,0.7)	0.1
v_4	比较信任	[0.7,0.9)	0.01
v_5	完全信任	[0.9,1)	0.01

为了确定各节点所属的信任等级集合，将 4.1 节计算所得的综合信任值代入隶属函数，并根据最大隶属原则判断出被评估节点所属的信任等级集合。本文采用的隶属函数是对文献[23]中的方法的改进，为了满足本文所提信任等级划分的要求，将原本的 4 组隶属函数修改为 5 组隶属函数，并根据表 1 中的要求，为原有的隶属函数赋予了具体参数值。这 5 个信任等级集合所对应的隶属函数如式(8)－式(12)所示，其中 x 表示被评价节点的综合信任值。图 3 给出了这些信任等级集合所对应的隶属函数曲线，其中，横坐标是根据式(3)得到的被评估节点的综合信任值，纵坐标是根据隶属函数得到的隶属度。由图 3 可以看出，完全不信任等级 v_1 的曲线从 0 开始逐渐降低，并在 0 处取得最大值，而完全信任等级 v_5 的曲线从 0 开始逐渐增加，并在 1 处取得最大值；此外，曲线 v_2，

v_3，v_4 均是在中间值处取得最大值，两侧均逐渐降低，它们对应的中间值分别为 0.4，0.6，0.8。由此可见，对这 5 个隶属函数采用最大隶属原则，便可得到每个被评估节点的综合信任值所属于的信任等级集合。

$$v_1=\begin{cases}0.5\times(1-\dfrac{x-0.2}{x}), & 0.2\leqslant x\leqslant 1\\ 0.5\times(1+\dfrac{0.2-x}{0.2}), & 0\leqslant x<0.2\end{cases} \tag{8}$$

$$v_2=\begin{cases}0.5\times(1-\dfrac{x-0.6}{x-0.4}), & 0.6\leqslant x\leqslant 1\\ 0.5\times(1+\dfrac{0.6-x}{0.2}), & 0.4\leqslant x<0.6\\ 0.5\times(1+\dfrac{x-0.2}{0.2}), & 0.2\leqslant x<0.4\\ 0.5\times(1-\dfrac{0.2-x}{0.4-x}), & 0\leqslant x<0.2\end{cases} \tag{9}$$

$$v_3=\begin{cases}0.5\times(1-\dfrac{x-0.8}{x-0.6}), & 0.8\leqslant x\leqslant 1\\ 0.5\times(1+\dfrac{0.8-x}{0.2}), & 0.6\leqslant x<0.8\\ 0.5\times(1+\dfrac{x-0.4}{0.2}), & 0.4\leqslant x<0.6\\ 0.5\times(1-\dfrac{0.4-x}{0.6-x}), & 0\leqslant x<0.4\end{cases} \tag{10}$$

$$v_4=\begin{cases}0.5\times(1+\dfrac{1-x}{0.2}), & 0.8\leqslant x\leqslant 1\\ 0.5\times(1+\dfrac{x-0.6}{0.2}), & 0.6\leqslant x<0.8\\ 0.5\times(1-\dfrac{0.6-x}{0.8-x}), & 0\leqslant x<0.6\end{cases} \tag{11}$$

$$v_5=\begin{cases}0.5\times(1+\dfrac{x-0.8}{0.2}), & 0.8\leqslant x\leqslant 1\\ 0.5\times(1-\dfrac{0.8-x}{1-x}), & 0\leqslant x<0.8\end{cases} \tag{12}$$

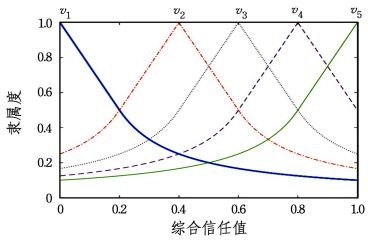

图 3　综合信任值的隶属度

Fig. 3　Membership degree of comprehensive trust value

根据节点信任等级的划分，将信任等级为 v_4 和 v_5 的节点视为可信节点，也就是说这类节点几乎没有恶意行为（设置 $\beta=0.01$，惩罚力度很小），在路由决策中优先选择这类节点。而信任等级为 v_3 的节点可能具有某些恶意行为，因此，仅在信任等级为 v_4 和 v_5 的节点不可用时，才考虑使用信任等级为 v_3 的节点进行数据转发（v_3 是可接受的信任等级阈值）。一般情况下，我们尽可能避免使用信任等级为 v_3，v_2 和 v_1 的节点进行数据转发，其中信任等级为 v_2 和 v_1 的节点是严格不用于数据转发的。

此外，为了防御节点间的共谋攻击，在计算间接信任值时，仅选取信任等级为 v_4 和 v_5 的邻居节点作为推荐节点。

4.3　信任监控与更新

由于节点的行为随着时间的推移而动态变化，因此，信任监控和更新成为了信任评估必不可少的环节。在该环节中，每个节点均在混杂模式下监控邻居节点的数据转发行为，通过直接关系和间接关系收集邻居节点的信任信息，并负责节点信任值的更新。

在更新节点信任值时，如果更新频率过低，则意味着某些不活跃的恶意节点可能被漏检；相反，如果更新频率过高，则可能会占用过多的网络资源（如节点的能量、内存和 CPU 等），从而缩短节点的网络寿命。因此，为了解决这一问题，本模型采用 RPL 路由协议中的 Trickle 定时器来控制节点信任值的更新，以此实现节点信任值的自适应更新。

4.4　信任恢复

由于某些非入侵因素（如供电不足、缓冲区容量不足等），一些正常节点可能为了保留自身资源而拒绝转发数据包，从而表现出自私性，以致于这类节点的信任值变得很低，一旦其信任值低于阈值，该节点将会被当作恶意节点隔离起来。为了解决这个问题，在信任恢复阶段，不对能量偏低的节点进行信任等级评估，而是将其隔离起来观察一段时间 T_R，以便这类节点能够在规定的时间内恢复能量，特别是由电池供电的物联网节点。这类节点如果能够在 T_R 内恢复能量，那么将重新进入网络，否则，将被隔离出网络。

当一个新节点或刚恢复能量的节点进入网络时，为其分配一个信任等级为 v_3 的初始信任值（(0.5+0.7)/ 2=0.6）。没有为该节点分配信任等级为 v_4 和 v_5 的信任值，是为了防止恶意节点利用此机会在网络中更改身份。本文在 4.2 节提到尽可能避免使用信任等级为 v_3，v_2 和 v_1 的节点进行数据转发，因此，只有在特殊情况下（信任等级为 v_4 和 v_5 的邻居节点能量受限或不存在）才会考虑使用新节点或者刚恢复能量的节点进行数据转发。另外，本文没有使用任何特殊的能量模型，而是采用 ContikiRPL 平台上提供的默认能量方案。

5　基于信任抗丢包攻击的 RPL 协议

本文将上述所提的信任评估模型与 RPL 协议相融合，通过信任评估对恶意丢包节点进行检测，将检测出的恶意节点隔离出网络，帮助路由节点选择安全且可靠的首选父节点。算法 1 给出了基于信任的首选父节点的选择算法。本算法使用 RFC6651 中规定的预计传输次数（Expected Transmission count，ETX）作为路由度量[24]，并按照文献[20]的规定来维护节点的 *Rank* 值。

算法 1 的主要设计思想为：1）判断当前节点 i 的两个邻居节点 A 和节点 B（节点 A 和 B 在邻居节点列表中的位置紧邻）是否存在根节点，如果存在，则选取根节点作为首选父节点，否则，进行下一步判断；2）比较节点 A 和节点 B 的 ETX 值和 *Rank* 值，这是 RPL 协议中确定首选父节点和路由决策的正常操作，其中，ETX_Limit 表示首选父节点到达目的节点的最高 ETX 值；3）当节点 A 和节点 B 的 ETX 值均不大于 ETX_Limit 时，选择信任等级较高的节点作为首选父节点，使用 $A.T_{level}$ 和 $B.T_{level}$ 分别表示节点 A 和 B 的信任等级。同

时为了确保不发生环路，当前节点不考虑将 *Rank* 值比其本身大的节点作为父节点。这样，不仅将信任值嵌入到 RPL 路由决策中，而且保持了物联网节点间 *Rank* 值的一致性，从而实现了可信节点的选取和路由决策。

算法 1 基于信任的首选父节点的选择算法

```
输入：Node A，Node B
输出：Preferred_Parent
Begin
1. If (A==Root || B==Root) Then
2.     Preferred_Parent=Root;
3.     Goto RESULT;
4. If (A.ETX>ETX_Limit)&(B.ETX>ETX_Limit)
5.     Preferred_Parent=NULL;
6.     Goto RESULT;
7. If (A.ETX<= ETX_Limit)‖(B.ETX<=ETX_Limit)
8.     Preferred_Parent=A.ETX<B.ETX? A:B;
9.     Goto RESULT;
10. If (A.Rank>Rank_Self)&(B.Rank>Rank_Self)
11.    Preferred_Parent=NULL;
12.    Goto RESULT;
13. If (A.Rank<=Rank_Self)‖(B.Rank<=Rank_Self)
14.    Preferred_Parent=A.Rank<B.Rank? A:B;
15.    Goto RESULT;
16. Preferred_Parent=A.T_level>B.T_level? A:B;
17. RESULT:
18. Return Preferred_Parent;
End
```

此外，算法 2 给出了丢包攻击的检测和隔离算法。如果候选父节点的信任等级不低于信任等级阈值，那么首选父节点将由算法 1 决定；否则，该节点为恶意节点，将被隔离出网络，并重新搜索首选父节点。

算法 2 丢包攻击的检测和隔离算法

```
输入：Potential_ParentList[ ],Preferred_Parent // 来自算法 1
输出：Preferred_Parent
Begin
//检查当前节点数据库中候选父节点的有效性
1. For all j∈Potential_ParentList[ ] do
2.   If (j.T_level>=Threshold_Trust_level)
3.       Return Preferred_Parent; // 按照算法 1
4.   Else
5.       该节点为恶意节点，隔离出网络；
6.       Preferred_Parent=NULL;
7.       重新搜索父节点；
8.   End If
9. End for
10. Return Preferred_Parent;
End
```

6 仿真实验结果及分析

6.1 仿真实验环境及参数设置

本文利用 Contiki 2.7 操作系统及其自带的 Cooja 网络模拟器[25]进行仿真实验，仿真环境设置如下：*N* 个路由节点随机分布在 100 m×100 m 的正方形区域内，随机选取不同比例的节点作为恶意节点，其中恶意节点能够随机发起黑洞攻击和灰洞攻击两种丢包攻击。为了更好地评估本方案，设置了两种网络场景：1）网络中节点数目为 40～120 个（每次递增 20 个），恶意节点比例设置为 10%（随节点数目的增加而增加）；2）网络中节点数目为 60 个，恶意节点比例为 0～25%（每次递增 5%）。此外，在无恶意攻击时，经过多次仿真实验可得到：当节点能量不超过能量阈值时，其能量恢复正常所需的平均时间约为 10 s，因此在仿真中设置信任恢复时间 T_R 为 10 s。具体的参数设置如表 2 所列。

表 2 仿真参数设置

Table 2 Setting of simulation parameters

参数	值
网络拓扑大小/m^2	100×100
节点数目 *N*/个	40～120
根节点数目/个	1
恶意节点比例/	0～25
无线电模型	Unit Disk Graph Medium (UDGM): distance loss
传输半径/m	50
干扰半径/m	55
仿真时间/min	60
信任恢复时间 T_R/s	10

为了检验本方案的有效性，将从恶意节点检测率、误检率、数据包投递率、端到端延时 4 个方面进行分析，并将本方案与 MRHOF-RPL 协议[26]和 tRPL 协议[19]进行比较，同时所有仿真结果取 50 次独立实验结果的平均值。

6.2 网络安全性分析

将信任评估模型应用于路由协议的主要目的是识别出网络中的恶意节点，因此，恶意节点检测率和误检率是分析其安全性能的两个重要指标。恶意节点检测率是指被检测出的恶意节点的数目与全部恶意节点数目的比值。误检率是指正常节点被检测为恶意节点的数目与全部正常节点数目的比值。由于 MRHOF-RPL 协议中没有检测和隔离恶意节点的机制，因此本仿真仅比较 tRPL 协议和本方案。

图 4 和图 5 给出了两种方案在场景 1 中的恶意节点检测率和误检率的对比图。从图 4 可看出，随着网络中节点数目的增加，两种方案的恶意节点检测率均逐渐上升，这是因为它们的检测率均与网络中邻居节点的数目有关，节点数目越多，邻居节点的数目也越多，一旦节点行为不当，便很容易被检测到。另外，随着网络中节点数目的增加，本方案的恶意节点检测率明显高于 tRPL 协议，这是因为本方案在进行信任评估时考虑了邻居节点的推荐信息，更为充分地评估了节点间的信任关系，有利于恶意节点的识别。这在一定程度上也表明了本方案在大规模网络中检测恶意节点的能力更为突出。从图 5 可以看出，随着节点数目的增加，这两种方案的误检率均逐渐降低，其中，本方案的误检率明显低于 tRPL 协议，这是因为本方案考虑了非入侵因素对正常节点的影响，并为这类节点设置了一定的恢复时间，从而减少了正常节点被误识为恶意节点的情况。

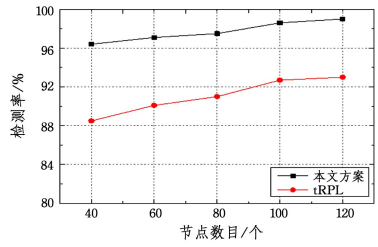

图 4　不同方案在场景 1 中检测率的对比图

Fig. 4　Comparison diagram of detection rate of different schemes in scenario 1

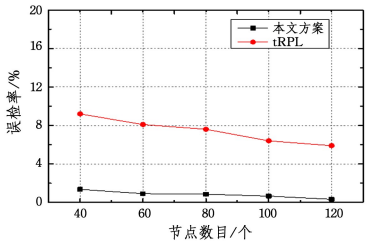

图 5　不同方案在场景 1 中误检率的对比图

Fig. 5　Comparison diagram of false detection rate of different schemes in scenario 1

图 6 和图 7 给出了两种方案在场景 2 中的恶意节点检测率和误检率的对比图。从图 6 可看出，随着恶意节点比例的增加，两种方案的恶意节点检测率均逐渐下降，这是因为恶意节点的比例增加的同时正常节点的比例减少，影响了节点间信任评估的准确性，从而增加了识别恶意节点的难度。其中，恶意节点检测率下降趋势较快的是 tRPL，这是因为 tRPL 在进行信任评估时，没有考虑惩罚因子，致使某些不活跃的恶意节点具有较高的信任值，不易被检测到。从图 7 可以看出，随着恶意节点比例的增加，两种方案的误检率均逐渐增加，其中，本方案的误检率明显低于 tRPL 协议，其原因与前面所述一样，即考虑了非入侵因素对正常节点的影响。

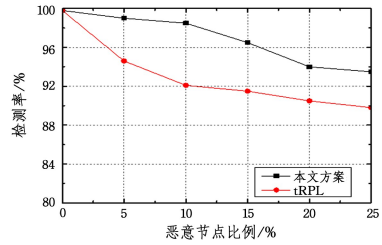

图 6　不同方案在场景 2 中检测率的对比图

Fig. 6　Comparison diagram of detection rate of different schemes in scenario 2

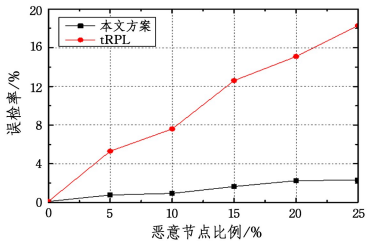

图 7　不同方案在场景 2 中误检率的对比图

Fig. 7　Comparison diagram of false detection rate of different schemes in scenario 2

6.3　路由协议的性能分析

检测恶意节点的主要目的是维持正常的路由过程，因此，在恶意节点存在的情况下，分析不同方案的数据包投递率和端到端延时是十分重要的。数据包投递率是指目的节点接收的数据包总数与源节点发送的数据包总数的比值。端到端延时是指将数据包从源节点传送到目的节点所需的时间。本仿真将对 MRHOF-RPL 协议、tRPL 协议和本方案进行比较。

图 8 和图 9 给出了 3 种方案在场景 1 中的数据包投递率和端到端延时的对比图。由图 8 可以看出，随着节点数目的增加，3 种方案的数据包投递率均略有下降，这是因为在密集的网络中，数据包会由于网络自身原因（如链路故障、数据冲突等）而产生丢包的情况，从而降低数据包投递率。其中，本方案和 tRPL 协议的数据包投递率均高于 MRHOF-RPL 协议，这是因为 MRHOF-RPL 协议中没有防范恶意节点的措施，而本方案和 tRPL 协议均能够在一定程度上检测出恶意节点，并将其隔离出网络。然而，与 tRPL 协议相比，本方案的数据包投递率较高，这表明本方案检测和隔离恶意节点的效果更为显著。从图 9 中可以看出，随着节点数目的增加，3 种方案的端到端延时均增加，这是因为随着节点数目的增加，确定数据包到达目的节点的路由所需的时间也就越长。其中，本方案和 tRPL 协议的端到端延时均低于 MRHOF-RPL 协议，这是因为本方案和 tRPL 协议能够将检测到的恶意节点隔离出网络，从而降低了恶意节点丢包行为对端到端延时的影响。另外，本方案的端到端延时略高于 tRPL 协议，这是因为 tRPL 协议中信任评估的方案较为简单，其产生的计算开销较少，而本方案为了准确地识别出恶意节点，增加了节点间信任评估的细节，因此产生的计算开销略多，从而增加了端到端延时。

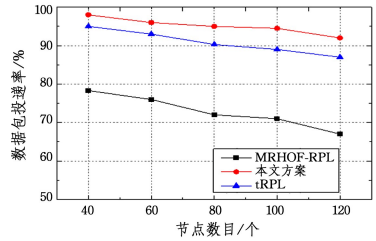

图 8　不同方案在场景 1 中数据包投递率的对比图

Fig. 8　Comparison diagram of packet delivery rate of different schemes in scenario 1

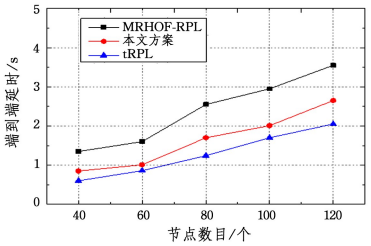

图 9　不同方案在场景 1 中端到端延时的对比图

Fig. 9　Comparison diagram of End-to-End delay of different schemes in scenario 1

图 10 和图 11 分别给出了 3 种方案在场景 2 中的数据包投递率和端到端延时的对比图。从图 10 可以看出，随着恶意节点比例的增加，3 种方案的数据包投递率均不断降低，这是

因为恶意节点比例增加时，数据包被恶意节点丢弃的概率也随之增加，从而降低了数据包投递率。在恶意节点不存在时，3 种方案的数据包投递率均稳定在 99%左右，此时影响数据包投递率的主要因素是网络自身原因引起的丢包等情况。从图 10 中还可看出，随着恶意节点比例的增加，MRHOF-RPL 协议的数据包投递率下降幅度最大，当恶意节点比例为 25%时，MRHOF-RPL 协议的数据包投递率降低到 65%左右，而本方案的数据包投递率仅有小幅度下降，这是因为本方案能够有效识别恶意节点并将其隔离出网络。tRPL 协议虽然也能识别恶意节点，但效果没有本方案明显，因此其数据包投递率的下降幅度也较大。从图 11 可以看出，随着恶意节点比例的增加，3 种方案的端到端延时均不断增加，这是因为恶意节点越多，数据包被丢弃的可能性越大，将数据包传送到目的节点所需的时间也就越长。其中，MRHOF-RPL 协议的端到端延时最长，这是因为它缺少防范恶意攻击的能力。另外，本方案的端到端延时略高于 tRPL 协议，这是因为本方案所采取的恶意节点防范措施比 tRPL 协议略复杂，增加了端到端延时。

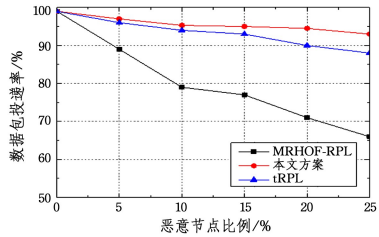

图 10 不同方案在场景 2 中数据包投递率的对比图

Fig. 10 Comparison diagram of packet delivery rate of different schemes in scenario 2

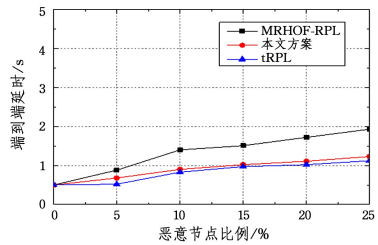

图 11 不同方案在场景 2 中端到端延时的对比图

Fig. 11 Comparison diagram of end-to-end delay of different schemes in scenario 2

结束语 本文针对物联网中的丢包攻击，提出一种利用信任评估来识别恶意节点的策略，并将其应用于 RPL 协议。本方案通过节点间的直接关系和间接关系来评估节点的信任值，并利用模糊集合理论对节点间的信任关系进行等级划分，从而选取可信节点进行数据转发，并将识别出的恶意节点隔离出网络。考虑到某些非入侵因素会使正常节点被误识为恶意节点，将为这类节点提供一段恢复时间，以便其能够重新加入网络。此外，本文从恶意节点检测率、误检率、数据包投递率和端到端延时 4 个方面分析了本方案的安全性和路由性能，实验结果表明本方案不仅能够有效地检测和隔离恶意节点，而且能够在恶意节点存在的情况下，仍保持良好的路由性能。下一步工作将继续优化本方案，使其在保证路由性能的前提下，检测出更多的恶意攻击。

参 考 文 献

[1] ZHANG Y Q,ZHOU W,PENG A N. Survey of Internet of Things Security [J]. Journal of Computer Research and Development,2017,54(10):2130-2143. (in Chinese)
张玉清，周威，彭安妮. 物联网安全综述[J]. 计算机研究与发展，2017,54(10):2130-2143.

[2] LIN J,YU W,ZHANG N,et al. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications[J]. IEEE Internet of Things Journal, 2017,4(5):1125-1142.

[3] ISLAM S M R,KWAK D,KABIR M H,et al. The Internet of Things for Health Care: A Comprehensive Survey [J]. IEEE Access,2017,3:678-708.

[4] KURT M N,YILMAZ Y,WANG X. Distributed Quickest Detection of Cyber-Attacks in Smart Grid [J]. IEEE Transactions on Information Forensics and Security,2018,13(99):1-16.

[5] ALFONSO V,JAMES F H,HUNG L H,et al. Predicts 2015: The Internet of Things[EB/OL]. (2014-12-30) [2018-07-28]. https://www. gartner. com/doc/2952822/predicts-internet-things.

[6] KSHIRSAGAR V H,KANTHE A M,SIMUNIC D. Trust Based Detection and Elimination of Packet Drop Attack in the Mobile Ad-Hoc Networks [J]. Wireless Personal Communications,2018,100(2):311-320.

[7] HAN G,JIANG J,SHU L,et al. Management and Applications of Trust in Wireless Sensor Networks: A survey [J]. Journal of Computer and System Sciences,2014,80(3):602-617.

[8] BAO F,CHEN I R,CHANG M,et al,Hierarchical Trust Management for Wireless Sensor Networks and Its Application to Trust-based Routing [C]// Proceedings of ACM Symposium on Applied Computing. Taiwan: ACM,2011,1732-1738.

[9] BAO F,CHEN I R,CHANG M J,et al. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection [J]. IEEE Transactions on Network & Service Management,2012,9(2): 169-183.

[10] HE D,CHEN C,CHAN S,et al. ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks [J]. IEEE Transactions on Information Technology in Biomedicine,2012,16(4):623-632.

[11] YANG B,YAMAMOTO R,TANAKA Y. Dempster-Shafer Evidence Theory based Trust Management Strategy against Cooperative Black Hole Attacks and Gray Hole Attacks in MANETs [C]// 16th International Conference on Advanced Communication Technology. Pyeongchang: IEEE,2014:223-232.

[12] WANG B,CHEN X,CHANG W. A Light-weight Trust-based QoS Routing Algorithm for Ad Hoc Networks [J]. Pervasive and Mobile Computing,2014,13(2014):164-180.

[13] BAO F,CHEN I R. Trust Management for the Internet of Things and Its Application to Service Composition [C]// 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). San Francisco: IEEE, 2012:1-6.

[14] YAN Z,ZHANG P,VASILAKOS A V. A Survey on Trust Management for Internet of Things [J]. Journal of Network and Computer Applications,2014,42(3):120-134.

[15] KARKAZIS P,LELIGOU H C,SARAKIS L,et al. Design of Primary and Composite Routing Metrics for RPL-compliant Wireless Sensor Networks [C]// 2012 International Conference on Telecommunications and Multimedia (TEMU). Chania: IEEE,2012:13-18.

[16] SEEBER S,SEHGAL A,STELTE B,et al. Towards a Trust Computing Architecture for RPL in Cyber Physical Systems [C]// Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013). Zurich: IEEE, 2013: 134-137.

[17] DJEDJIG N,TANDJAOUI D,MEDJEK F. Trust-based RPL for the Internet of Things [C]// 2015 IEEE Symposium on Computers and Communication (ISCC). Larnaca: IEEE, 2016: 962-967.

[18] KHAN Z A,HERRMANN P. A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things [C]// 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA). Taipei: IEEE, 2017: 1169-1176.

[19] KHAN Z A,ULLRICH J,VOYIATZIS A G,et al. A Trust-based Resilient Routing Mechanism for the Internet of Things [C]// Proceedings of the 12th International Conference on Availability,Reliability and Security (ARES'17). Reggio Calabria: ACM,2017:1-6.

[20] THUBERT P,WINTER T,BRANDT A,et al. RPL:IPv6 Routing Protocol for Low power and Lossy Networks [J]. Internet Requests for Comment,2012,6550(5):853-861.

[21] 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.

[22] ZHOU Z P,SHAO N N. An Improved Trust Evaluation Model Based on Bayesian for WSNs [J]. Chinese Journal of Sensors and Actuators,2016,29(6):927-933. (in Chinese)
周治平,邵楠楠. 基于贝叶斯的改进 WSNs 信任评估模型[J]. 传感技术学报,2016,29(6):927-933.

[23] WU G,DU Z,HU Y,et al. A Dynamic Trust Model Exploiting the Time Slice in WSNs [J]. Soft Computing,2014,18(9):1829-1840.

[24] VASSEUR J P,KIM M,PISTER K,et al. Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks [S/OL]. [2018-07-28]. https://tools.ietf.org/pdf/rfc6551.pdf.

[25] OSTERLIND F,DUNKELS A,ERIKSSON J,et al. Cross-Level Sensor Network Simulation with COOJA [C]// Proceedings. 2006 31st IEEE Conference on Local Computer Networks. Tampa:IEEE,2011:641-648.

[26] QASEM M,ALTAWSSI H,YASSIEN M B,et al. Performance Evaluation of RPL Objective Functions [C]// IEEE International Conference on Computer and Information Technology;Ubiquitous Computing and Communications;Dependable,Autonomic and Secure Computing;Pervasive Intelligence and Computing. Liverpool:IEEE,2015:1606-1613.