第 46 卷 第 7 期 计 算 机 工 程 2020 年 7 月
Vol. 46 No. 7 Computer Engineering July 2020

·网络空间安全· 文章编号：1000-3428(2020)07-0143-07 文献标志码：A 中图分类号：TP393.08

基于信任机制与 Rank 阈值的 RPL 路由协议

李成星，王 珺，徐京明

（南京邮电大学 通信与信息工程学院，南京 210003）

摘 要： RPL 路由协议是物联网环境中的一种轻量级距离矢量路由协议，其容易受到恶意节点攻击，从而导致网络丢包严重，甚至影响节点间的正常通信。为检测并隔离 RPL 路由协议中的 Rank 攻击节点，提出一种基于信任机制与 Rank 阈值的安全 RPL 路由协议 Sec-RPL。引入直接信任值计算方法，利用攻击节点的恶意行为会引起信任值下降这一特性，初步筛选出正常节点及疑似恶意节点，再根据疑似恶意节点的 Rank 值与 Rank 阈值进行比较，将低于 Rank 阈值的疑似恶意节点确定为攻击节点进行隔离，实现最佳路由决策。仿真结果表明，Sec-RPL 路由协议在检测成功率、丢包率及误报率方面均有较好的性能，并且相比 OF0-RPL 和原 RPL 路由协议计算资源消耗更少、安全性更高。

关键词： 物联网；RPL 路由协议；Rank 攻击；信任机制；Rank 阈值

开放科学（资源服务）标志码（OSID）：

中文引用格式： 李成星，王珺，徐京明. 基于信任机制与 Rank 阈值的 RPL 路由协议[J]. 计算机工程，2020，46(7)：143-149，158.

英文引用格式： LI Chengxing，WANG Jun，XU Jingming. RPL routing protocol based on trust mechanism and Rank threshold[J]. Computer Engineering，2020，46(7)：143-149，158.

RPL Routing Protocol Based on Trust Mechanism and Rank Threshold

LI Chengxing，WANG Jun，XU Jingming

（College of Telecommunications and Information Engineering，
Nanjing University of Posts and Telecommunications，Nanjing 210003，China）

【Abstract】 The RPL routing protocol is a lightweight distance vector routing protocol in Internet of Things（IoT），which is vulnerable to Rank attacks，causing normal communication between nodes to be significantly affected by serious network packet loss. In order to detect and isolate the malicious Rank attack nodes in the RPL routing protocol，this paper proposes a security RPL routing protocol based on trust mechanism and Rank threshold，Sec-RPL，which introduces the detection and isolation technology of malicious nodes. Based on the fact that malicious attacks on nodes will lead to a decrease in the trust value，Sec-RPL filters the normal nodes and suspected malicious nodes preliminarily. Then the Rank values of suspected malicious nodes are compared with the threshold of Rank，and the nodes with a Rank value lower than the threshold are isolated as attack nodes to achieve optimal routing decisions. Simulation results show that the Sec-RPL routing protocol has excellent performance in the success rate of detection，packet loss rate，and false alarm rate. Also，it consumes fewer computing resources and has higher security than the OF0-RPL and original RPL routing protocol.

【Key words】 Internet of Things（IoT）；RPL routing protocol；Rank attack；trust mechanism；Rank threshold

DOI： 10.19678/j.issn.1000-3428.0054756

0 概述

物联网是连接电子产品、家用电器等异构设备进行数据交换的网络。随着物联网业务的快速发展，全球物联网设备量正呈几何级增长，但相关的安全技术却没有得到相应提升[1]。考虑到物联网设备的资源有限以及传输链路的不可靠，可将物联网归类于低功耗有损网络（Low-power and Lossy Network，LLN）。针对 LLN 无线链路的不稳定性，IETF ROLL 工作组提出一个 RPL 路由协议[2]。该协议基于 IPv6 和 6LoWPAN 技术，具有强健壮性，使得物联网能够适应快速、频繁的网络拓扑变换。由于 RPL 路由协议在设计之初对网络的安全性关注较少，导致其面临许多威胁，而现如今异构设备的大量增长，更是使得物联网

基金项目： 国家自然科学基金面上项目“面向大规模无线网络感知数据的多标记学习模型与算法”（61571233）。

作者简介： 李成星（1993—），男，硕士研究生，主研方向为物联网安全；王 珺，副教授、博士；徐京明，硕士研究生。

收稿日期： 2019-04-28 **修回日期：** 2019-07-18 **E-mail：** 1017010307@njupt.edu.cn

长期处于不安全的状态,容易受到恶意节点(黑客)的攻击,因此非常有必要对 RPL 路由协议的安全性进行更加深入的研究。

目前,针对 RPL 路由协议中 Sinkhole 攻击、Blackhole 攻击、Rank 攻击等的研究已经逐步开展[3],其中 Rank 攻击是 RPL 协议中最具破坏性的攻击之一。事实上,Rank 值是 RPL 协议中的一个重要参数,表示节点在网络拓扑中相对于根节点的位置,离根节点越近其 Rank 值越小。RPL 协议定义的 Rank 值策略被用于选择最优父节点、决定最佳路由及避免环路,但是其如果被恶意节点操控,就会对网络造成不利影响。在 Rank 攻击[4-5]中,恶意节点基于 Rank 值的改变来通告虚假的最佳路由,从而吸引或迫使邻居节点经过其传输数据。通过此恶意节点路由的数据包会路由到其他串联攻击节点,如黑洞节点或转发节点,从而丢弃数据包或者选择性地将数据包转发到其他目的地,甚至泄露网络的机密信息。可见,Rank 攻击能否成功很大程度上取决于协作能力,例如,结合黑洞攻击与 Sybil 攻击的 Rank 攻击,通过丢弃或伪造路由信息会对网络拓扑造成巨大破坏。本文介绍了 RPL 路由协议的原理及常见的 RPL 路由协议攻击类型,并结合 Rank 攻击的特性,提出一种基于信任的 Rank 攻击检测与隔离的安全 RPL 路由协议。

1 Rank 攻击检测

1.1 RPL 路由协议原理

RPL 路由协议是一种轻量级的距离矢量路由协议。在拓扑形成期间,RPL 路由协议通过传播由根节点发起的控制分组 DODAG 信息对象(DODAG Information Object,DIO)消息来执行向下拓扑的构造[6-7]。节点在收到 DIO 消息后,通过 DIO 消息配置选项中的相关字段来选择和优化 RPL 实例中的路由并回复目的地通告对象(Destination Advertisement Object,DAO)消息确认加入网络,同时将目标函数(Objective Function,OF)中定义的一个或多个度量和约束转换为 Rank 值。新节点可以通过广播 DODAG 信息请求(DODAG Information Solicitation,DIS)来加入现有网络,以便从 RPL 节点请求 DIO 消息。这些消息周期性地进行广播并通过使用 Trickle[8]算法来确定周期,通过上述过程构建的网络拓扑称为 DODAG。

与传统的路由协议不同,RPL 路由协议利用路由度量、路由约束和 OF 等因素来计算最佳路由路径。在路由过程中,RPL 路由协议为网络中运行的每个传感器节点选择一个首选父节点,并且每个子节点都包含父节点的相关信息,如控制和路由信息,这些信息对于路由和网络稳定性具有重要作用。路由决策基于指定的 OF,如跳数、能量最小化和延迟等。

1.2 常见的 RPL 攻击

由于 RPL 设备具有弱安全性,没有防篡改能力,因此攻击者可以捕获节点,提取所有加密信息并利用其在网络中进行合法工作。一旦捕获某个节点,攻击者可在其中注入恶意代码,从而打破一些路由规则。文献[9]针对 RPL 协议的多数现有攻击进行分析,根据攻击目标和手段对攻击进行分类。

本文介绍了 3 种常见的 RPL 路由协议攻击:

1)Sinkhole 攻击[10-11]是最常见的 RPL 攻击之一。在 Sinkhole 攻击中,恶意节点会发布错误的路由消息,并宣称其具有到达特定目的地的最佳路由,从而吸引邻居节点通过该恶意节点传送数据。当恶意节点接收到数据分组时,立即修改网络安全数据在内的各种路由信息,从而使网络拓扑结构复杂化。

2)Blackhole 攻击[12]中的恶意节点会直接丢弃所有通过其的数据,从而隔离网络中的部分节点。选择性转发攻击[10]是 Blackhole 攻击的一个特例,在选择性转发攻击中某些数据包(数据或控制消息)会被选择性地丢弃,从而破坏路由路径并影响网络效率。

3)DODAG 不一致攻击[13]中的恶意节点会篡改 RPL IPv6 报头,导致正常节点对表示数据包预期传输方向的“O”标志位和检测 Rank 错误的“R”标志位处理不当。攻击者节点可以通过发送标志“O”和“R”的数据包直接攻击其父节点,因此指定的数据包将被丢弃,并且 Trickle 定时器将被重置,从而导致通道阻塞和能量耗尽。

在 3 种攻击中,Rank 攻击最具威胁性,因为其可以放大所有攻击的不利影响。Rank 攻击分为增大型 Rank 攻击和减小型 Rank 攻击。通过发布高 Rank 值,攻击者可在 DODAG 中进行更深层次地移动,以便在网络中生成环路。通过发布低 Rank 值,DODAG 的大部分节点将经过恶意 Rank 攻击节点连接到 DODAG 根节点,这样恶意节点就能够窃听、操纵和隔离大部分网络流量。攻击者可以通过不断改变首选父节点来破坏拓扑的稳定性,同时使系统产生高开销、严重的分组冲突并导致整体网络性能恶化。由于减小型 Rank 攻击危害性更大,因此本文重点研究减小型 Rank 攻击。图 1、图 2 是 Rank 攻击前后的网络拓扑图示例,其中使用 OF0 目标函数[14]。

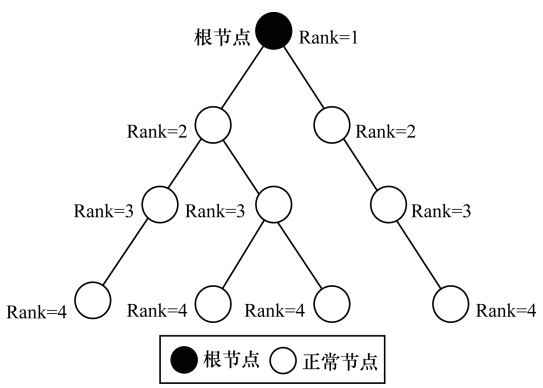

图 1 正常的 DODAG 网络拓扑

Fig. 1 Network topology of normal DODAG

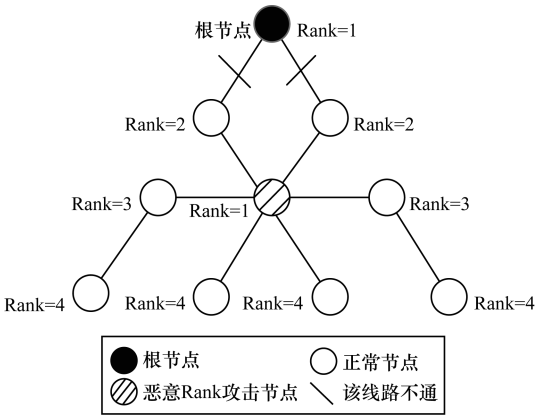

图 2　Rank 攻击下的 DODAG 网络拓扑

Fig. 2　Network topology of DODAG under Rank attacks

1.3　现有 Rank 攻击检测方法存在的问题

虽然目前已提出许多解决 RPL 路由协议中 Rank 攻击的方法,但是这些方法均存在各种问题,并不适用于资源受限的物联网。

文献[12]提出一种 VeRa 安全机制,针对减小型 Rank 攻击,引入 Rank 验证的概念。恶意节点通过复制靠近根节点或者特定 Rank 值的邻居节点的 Rank 值来执行 Rank 攻击。在 VeRa 机制中,通过实现单向哈希链方法防止攻击节点获得比其原始 Rank 值更低的 Rank 值,同时确保从 DODAG 根节点到邻近节点的 Rank 值严格递增。但是该机制存在较大漏洞,不能检测出恶意节点伪造 Rank 进行恶意活动。

文献[15]通过在 DODAG 的根节点中查找 Rank 值不一致来检测攻击节点。如果节点的 Rank 值低于其父节点,则 DODAG 根节点将该节点判断为攻击节点,因为 RPL 协议的 Rank 策略规定父节点的 Rank 值必须低于其子节点的 Rank 值。在第一个模块中,DODAG 根节点请求每个节点报告各自的 Rank 值和邻居节点的 Rank 值。当每个节点接收到该请求后,以其邻居和父级别节点进行响应。在第二个模块中,DODAG 根节点分析收集的数据并检测攻击节点。DODAG 根节点通过比较其自身的 Rank 值与其邻居节点报告的 Rank 值来检查每个节点的 Rank 值不一致情况。如果 Rank 值的差异大于预定阈值,则 DODAG 根节点判断该节点是攻击节点。但文献[15]方法存在两个问题:1)误检率高;2)DODAG 根节点必须向每个节点报告攻击节点的信息,但是在存在攻击节点的情况下此类信息是否可信并不确定。

文献[16]提出一种 TRAIL 安全机制。通过在每个父节点中查找 Rank 值不一致来检测攻击节点。子节点向其父节点 A 告知自身 Rank 信息,父节点 A 将包含子节点 Rank 信息和自身 Rank 信息的消息转发给父节点 A 的上级父节点 B。上级父节点 B 通过检查 Rank 值是否满足以下两个条件来验证节点的可靠性:1)消息中子节点的 Rank 值高于父节点 A 的 Rank 值。2)父节点 A 的 Rank 值位于消息中子节点的 Rank 值和上级父节点 B 的 Rank 值之间。如果不满足这两个条件,则父节点将其子节点视为攻击节点。TRAIL 机制也存在一个问题,子节点可能选攻击者节点作为其父节点,因为子节点无法辨别该父节点是否为攻击节点,所以文献[17]提出一种安全父节点的选方法,以确保子节点从候选父节点中选出合适的父节点。但是该策略不能有效抵御 Blackhole 攻击,同时在子节点选择父节点时可能会排除正常的最优父节点,选择次最优父节点,从而使得每条路径的跳数变大,造成系统资源消耗增加。

文献[18]提出一种基于信任的 Sec-Trust 机制,用于检测和隔离 Rank 攻击和 Sybil 攻击。通过节点间基于时间的分组交换计算以评估节点的可信行为,可信度低于特定阈值的节点被判定为恶意节点。该机制仅使用推荐信任,但却未考虑间接推荐的不确定性,同时其划分的 5 个信任级别不太合理,不能有效识别出恶意节点,因此造成较高的误判率。

上述检测方法虽然能在一定程度上检测出 Rank 攻击,但是依然存在各种问题。本文考虑到物联网环境下传感器节点资源受限的特性,充分分析 Rank 攻击行为特性,设计一种结合信任阈值和 Rank 阈值的 Rank 攻击检测与隔离方法。

2　基于信任机制的 Rank 攻击检测与隔离方法

2.1　网络模型

本文方法使用的网络模型基于以下假设:

1)仅适用于静态网络,节点随机分布,所有节点通信半径相同,在仿真期间节点能量充足。

2)每个节点都以混杂模式运行,因此可以监测邻居数据分组的传输。

3)随着时间的推移,每个节点间的有效通信(分组转发成功率)会反映出节点的攻击性质。

2.2　基于贝叶斯的信任计算

2.2.1　信任引入

在社交网络中,信任是一个常被提及的概念。信任可以定义为委托人委托受托人所做的事情,然后对受托人进行评价确定其信任程度。该定义在计算机通信领域同样适用。在传感器网络中,信任是一个复杂的概念,是指对传感器节点可靠性、完整性、安全性等特性的期望。在一个节点与另一个节点直接或间接的通信中,节点的信任是一个可以观察到的有限量化过程,节点的累积信任值用来定义节点的信誉。节点间的协作在信任关系中至关重要,因为这些关系决定了网络的可拓展性、可靠性等性能。

文献[19]研究表明在资源受限的传感器节点中,使用密码学及传统协议中的交换和分发密钥来创建和形成信任,其在物联网中已被证明是不现实的。基于密码机制的路由方案使用加密、认证等技

术,对节点的计算能力要求较高,极大地增加了通信资源消耗。而基于信任的路由方案中节点计算量小,只需利用相邻节点之间的交互行为来计算得到信任值,通信开销较低,适用于资源受限的物联网设备。

经过理论分析及大量实验验证,贝叶斯方法是一种有效的信任评估方法,其基于主体概率进行信任度计算,得到的信任度较主观,并根据对象的经验和认知对相关信息进行综合分析。因此,本文引入贝叶斯方法进行信任值计算。

2.2.2 直接信任值计算

直接信任是指一个节点对其直接连接邻居的信任,即其对发送请求的处理可靠性和能力[20]。本文将节点的直接信任定义为节点之间成功交互的可能性,以确定节点到正确目的地的分组转发行为,如图 3 所示。

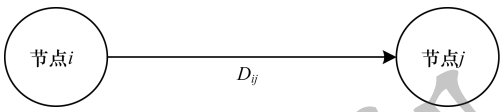

图 3 直接信任示意图

Fig. 3 Schematic diagram of direct trust

文献[21]提出的 RFSN 模型是无线传感器网络中最具代表性的贝叶斯信任管理模型。该模型通过贝叶斯方法拟合信誉分布与 Beta 分布,得到的节点信誉服从 Beta 分布,即 $\text{reputation}_{ij} \sim \text{Beta}(\alpha_{ij}+1, \beta_{ij}+1)$,其中,$\text{reputation}_{ij}$表示节点 i 关于节点 j 的信誉分布,α_{ij}和β_{ij}分别表示节点 j 转发来自节点 i 的成功数据包数目和失败数据包数目。本文采用基于贝叶斯的 RFSN 模型下信誉分布的数学期望来表示节点 i 对节点 j 的直接信任值 D_{ij},即节点 j 能否真实转发来自节点 i 的分组的可能性,如式(1)所示:

$$D_{ij}=E(\text{Beta}(\alpha_{ij}+1,\beta_{ij}+1))=\frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \tag{1}$$

由于计算节点信任值的目的是根据信任值检测并隔离网络中的恶意节点,而基于 Beta 分布的信任方案没有考虑到恶意节点给网络带来的影响,因此在网络存在 Rank 及其他攻击的情况下,会对信任值计算带来较大影响。为解决该问题,本文引入惩罚因子 λ,表示对行为不当(转发数据包失败)节点的惩罚权重,从而对上述直接信任值计算公式进行改进。

节点最初的信任值为 0.5,表示尚不明确节点是否可信。由于 λ 表示附加给任何行为不当节点的惩罚权重,因此 λ 初始值设定为 0.1,而惩罚增量设定为 λ 初始值的一半(0.05),即 $\lambda=\lambda_i+0.05$。如果评估一个节点时,其一旦表现出恶意行为,那么 λ 便增加 0.05,会逐渐降低行为不当节点的信任值并迅速检测出恶意节点,同时需将其与路由决策进行隔离。

综上所述,直接信任值的计算公式可以修正为:

$$D_{ij}=\frac{\alpha_{ij}+1}{\alpha_{ij}+\lambda\beta_{ij}+2} \tag{2}$$

需要注意的是,虽然直接信任值可以通过对恶意行为的统计和计算得到,但是恶意节点可能会通过伪装使得其恶意行为难以被检测到。在这种情况下,恶意节点通过伪造身份信息伪装成正常节点,一个节点采用多个身份,使得受害者将数据包发送给攻击者,造成网络混乱,为其他恶意节点创造操作机会,此类攻击称为 Sybil 攻击。由上文可知,当 Rank 攻击与 Sybil 攻击相结合时丢弃或伪造路由信息,会对网络拓扑造成巨大破坏,因此在未来的工作中将对 Sybil 攻击作进一步研究。

2.2.3 信任值更新

节点的信任值是变化的,有的恶意节点会在一开始表现为正常节点,因此信任值需要随时间的变化进行更新,但是信任值更新频率较低意味着可能无法捕获到某些节点的恶意行为,造成整个网络的混乱。相反地,如果信任更新太频繁,则可能会过多占用节点能量及存储器和 CPU 等网络资源,从而最终导致传感器节点过早死亡。在信任更新阶段,每个节点基于直接信任值来收集直接邻居的信任信息。在更新节点的信任值时,采用定期更新信任值的方法,基于给定的时间,周期性地重新计算当前的信任值,同时恶意节点伪造其 Rank 值造成网络中出现不一致现象,从而导致 Trickle 计时器重置其更新周期,即重置 DIO 消息的发送周期[5-6]。关于 Trickle 计时器的相关描述,可详见 RFC 6550、RFC 6206 标准[2,8]。

2.3 Rank 阈值计算

因为信任值的计算是一个动态过程,仅根据节点信任值来辨别 Rank 攻击是不够的,并且信任阈值的设置也是一个难题,所以本文考虑结合 Rank 攻击时恶意节点的 Rank 值规律特性进行检测。由上文介绍可知在 Rank 攻击中,恶意节点通过改变其 Rank 值来通告虚假的最佳路由,使其成为该通信范围内的虚假首选父节点,从而吸引邻居节点通过其传输数据。为排除该恶意节点,在父节点选择阶段,当存在多个候选父节点时可选择次最优父节点为其父节点,然后排除可能是恶意节点的最优首选父节点,因此需要设置一个合理的 Rank 阈值,排除低于该阈值的节点。阈值计算公式如式(3)所示:

$$T_i=R_{\text{ave}}-R_{\max}\times K \tag{3}$$

其中,T_i 表示 Rank 阈值,R_{ave}表示邻居节点的平均 Rank 值,$R_{\max}$表示邻居节点的最大 Rank 值,K 为[0,0.5]中的一个恒定参数。

如果参数 K 值太小,则阈值 T_i 相对而言会很大,这样虽然能排除恶意节点,但也会误排除多数正常节点,从而大幅增加系统的误报率。如果参

数 K 值太大，则阈值 T_i 相对而言会很小，这样不仅不能排除恶意节点，而且会导致节点选择攻击节点作为其父节点，使得网络中每个节点到根节点的跳数增加，因此需要对阈值范围内的候选父节点进行筛选。需要注意的是式(3)在节点数很少时不具参考价值，但在物联网环境下无需考虑该情况，因为攻击节点无法收集大量数据包，而本文考虑的是节点数量很多的情况。

在本文方法中，根据节点转发数据包成功与失败的次数这一指标计算出节点间的信任值，并根据相应的 Rank 阈值对候选父节点进行筛选，使得高于阈值的节点可以继续与其他节点进行安全通信，而低于阈值的节点被判定为恶意节点并被隔离。两种方法的结合提高了检测准确率，降低了系统误判率，并且由于 RPL 协议标准中指出当拓扑重构时节点 Rank 值不像其他链路或节点指标一样快速变化，因此为本文 Rank 阈值计算方案提供了相关理论依据。

2.4　Sec-RPL 路由协议

根据上文对原 RPL 路由协议进行改进，形成基于信任的 Rank 攻击检测与隔离 RPL 路由协议，称为 Sec-RPL。而 Contiki 系统下基于 OF0 目标函数的 RPL 路由协议，称为 OF0-RPL。Sec-RPL 路由协议实现过程如图 4 所示。

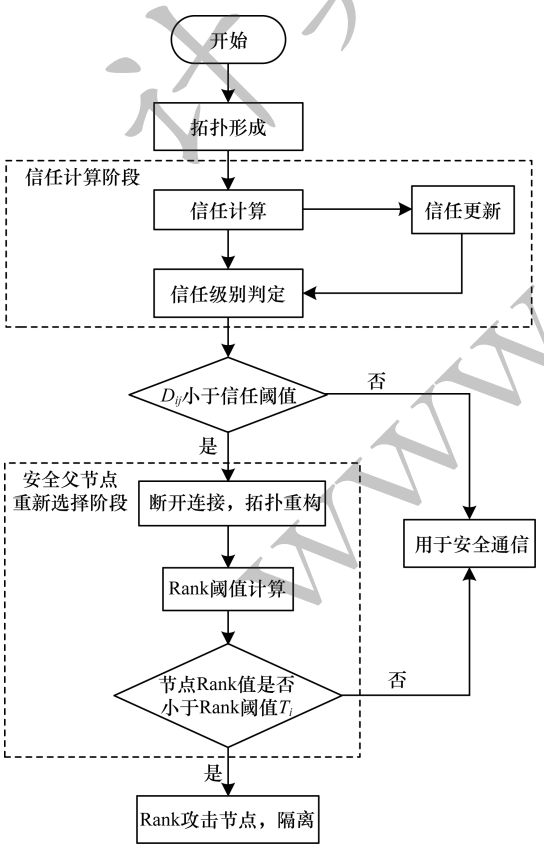

图 4　Sec-RPL 路由协议实现过程

Fig. 4　Implementation process of Sec-RPL routing protocol

通过节点间相关广播消息的不断发送，网络拓扑 DODAG 构建完成。此时，信任机制开始运作，根据节点之间转发数据包成功与失败的次数来计算对应的信任值并周期性更新该值。当网络中的疑似恶意节点不断导致数据包转发失败时，使得邻居节点对疑似恶意节点的信任值越来越低，直到低于设定的某个信任阈值，那么邻居节点便断开与疑似恶意节点的连接并进行拓扑重构。根据减小型 Rank 攻击的特性可知，Rank 攻击节点必须有一个较低的 Rank 值才能吸引周围的邻居节点通过恶意节点来传送数据。因此，通过仿真可以得到一个合理的 Rank 阈值并隔离低于该阈值的节点。

Sec-RPL 路由协议中对节点恶意行为的容忍度较低，一旦发现节点的恶意行为，相应的惩罚因子便会增加 0.05，使恶意行为对信任值的影响变大。恶意节点的信任值越来越低，当低于预先设定的安全通信信任值时，便会被认为是低信任节点。然后，通过 Rank 阈值对恶意节点进行筛选，检测并隔离 Rank 攻击节点，从而极大降低系统误判。

3　仿真验证与性能分析

为验证 Sec-RPL 路由协议的性能，本文利用 Contiki 3.0 实验平台下的 Cooja 仿真工具进行实验仿真，在节点混杂模式下收集路径中的分组转发信息，并将其作为计算 Rank 攻击数和误报率等性能指标的依据，然后对 Sec-RPL 路由协议进行评估。仿真参数设置如表 1 所示。

表 1　仿真参数设置

Table 1　Setting of simulation parameters

参数名称	参数值
覆盖范围/m^2	70 × 70
节点数	30
恶意节点数	1 ~ 3
传输范围/m	50
路由协议	RPL 和 Sec-RPL
链路损失模型	UDGM
目标函数	OF0
攻击准备时间/s	5
仿真时间/min	40

3.1　参数 K 的确定

由上文对 K 值的分析可知，K 值不是越大越好，也不是越小越好，K 应该取一个合适的值，使得成功排除攻击节点的概率最高同时所有节点到根节点的总跳数最小，从而保证系统能量消耗在理论上最少。由于本文方法中 Rank 阈值计算过程与信任计算过程相对独立，因此先通过 Contiki 3.0 的 Cooja 模拟器进行模拟实验确定 K 值。

将根节点固定在坐标原点位置，随机部署正常

节点和攻击节点并分别进行仿真实验。图 5 显示在 K 的每个取值下,分别统计并计算其 100 次实验成功排除攻击节点的概率及平均总跳数,其中成功排除恶意节点的概率表征节点的误检率及漏检率,K 值过小,会将正常节点错误地判定为恶意节点,即误检率;K 值过大,会将恶意节点误判为正常节点,即漏检率。因此,本文用成功排除恶意节点的概率表示误检率和漏检率。由仿真结果可以看到,当 K 值超过某个阈值时,随着恶意节点由 1 个增加到 3 个,成功排除概率逐渐降低,由此可知 K 值对仿真结果影响较大。

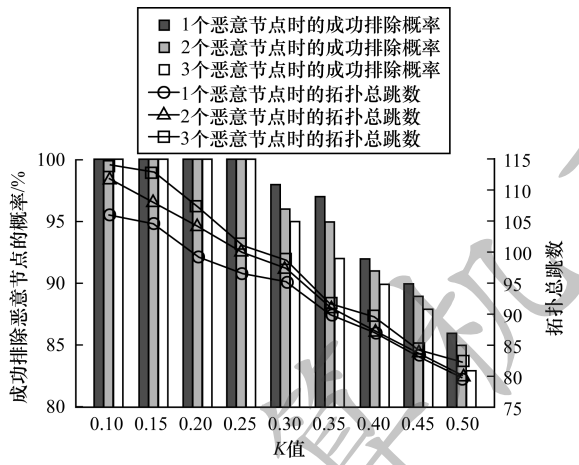

图 5 不同 K 值下成功排除恶意节点的概率和拓扑总跳数

Fig. 5 The probability of successfully excluding malicious nodes and the total number of topological hops under different K values

根据上述实验数据可以看出,当 $K=0.25$ 时,系统对恶意节点的成功排除概率最高且到根节点的平均总跳数最小,此时误检率和漏检率均达到最低,阈值计算公式具体如下:

$$T_i = R_{\text{ave}} - R_{\max} \times 0.25 \tag{4}$$

3.2 Sec-RPL 和 OF0-RPL 路由协议性能比较

3.2.1 Rank 攻击实施

在 Rank 攻击实施过程中,恶意节点保持合法行为约 5 s,这一时间足够完成拓扑构建,之后恶意节点通过在每个 Trickle 定时器周期内广播虚假的低 Rank 值来开始其攻击。恶意节点声称具有到根节点更优的路径来吸引其邻居节点,从而创建未优化的路径。RPL 协议标准规定 Rank 值以向下方式增加,以防止路由循环和未优化的路由。未经优化的路径使 RPL 每隔一段时间就进行本地修复和全局修复[2],极大地减少了 RPL 网络生命周期并耗尽节点能量。

3.2.2 攻击节点检测与隔离

根据 RFC 6550[2] 中的定义,在拓扑形成阶段,根节点通过发送包含了网络基本信息的 DIO 消息给其通信范围内的其他节点,构建 DODAG 的拓扑结构。DIO 消息中包含实例身份标志、有向无环图的版本号、有向无环图的标志值、簇头节点 Rank 值、路由协议工作模式、有向无环图的配置信息、路由条件以及根节点、邻居节点的 IP 地址等。因此,每个 DIO 消息中包含的网络基本信息是一致的,其中每个节点都有一个 IPv6 地址作为标志符(ID)、一个父节点列表、一个邻居列表、一个 Rank 值和其他参数。将潜在父节点 i 发送的 DIO 消息与邻居列表中保存的 DIO 消息相比较,通过判断子节点的潜在父节点的 DIO 消息与子节点的邻居列表所保存的 DIO 消息是否一致进行攻击检测。

图 6 展示了在仿真期间网络遭受的 Rank 攻击次数随时间的变化情况。网络在 5 s 时受到 Rank 攻击,刚开始的攻击次数很多,随着仿真的进行,系统根据计算得到的 Rank 阈值和设置的信任阈值辨别出恶意节点并将其剔除,因此检测到的攻击次数逐渐减少。这证明了 Sec-RPL 路由协议对于 Rank 攻击的检测与隔离具有较好的效果,能有效防御 Rank 攻击。

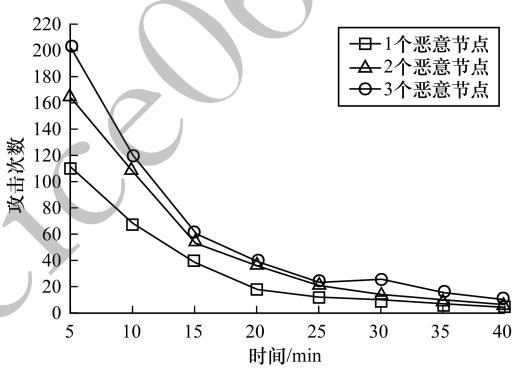

图 6 Sec-RPL 检测的 Rank 攻击次数

Fig. 6 Number of Rank attacks detected by Sec-RPL

3.2.3 性能分析

图 7 展示了 OF0-RPL 和 Sec-RPL 路由协议在 Rank 攻击下各节点的丢包率比较。可以看出,OF0-RPL 路由协议的丢包率明显高于 Sec-RPL 路由协议。由于 OF0-RPL 路由协议存在安全方面的漏洞,因此导致其遭受 Rank 攻击时,网络性能急剧恶化,表现为丢包率居高不下,而 Sec-RPL 路由协议结合了信任机制和 Rank 阈值,既保证了检测准确性,又降低了 Rank 攻击下节点的丢包率。由仿真结果可知,当恶意节点数量增加到 3 个时,Sec-RPL 路由协议在 Rank 攻击下的丢包率有所增加,但系统仍能保持一个较低的丢包率。随着时间的变化,Sec-RPL 能够成功检测和剔除恶意 Rank 攻击节点,维护网络正常运行。

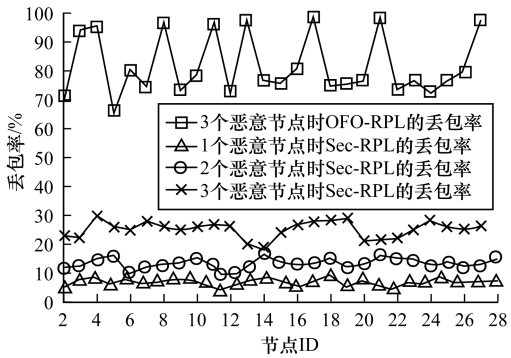

图 7　OF0-RPL 和 Sec-RPL 在 Rank 攻击下节点丢包率比较

Fig. 7　Comparison of node packet loss rate between OF0-RPL and Sec-RPL under Rank attacks

4　结束语

本文提出一种基于信任机制与 Rank 阈值的 RPL 路由协议 Sec-RPL。通过检查节点之间分组转发成功与失败的次数计算节点间的信任值,并结合节点 Rank 阈值评估节点行为及隔离网络中的恶意节点,从而实现最佳路由决策。仿真结果表明,Sec-RPL 路由协议相比 OF0-RPL 路由协议计算资源消耗较小,相比原 RPL 路由协议安全性较高,并且对于 RPL 路由协议面临的 Blackhole 攻击、选择转发攻击等也具有一定的检测效果。本文虽然针对 RPL 路由协议提出一种基于信任的 Rank 攻击检测与隔离方法,在一定程度上加强了系统安全性能,同时降低了误检率及漏检率,但仍存在计算资源消耗较高的问题,因此下一步将对 Sec-RPL 路由协议进行功能扩展,使其能更高效地检测与隔离 RPL 攻击,此外还将量化节点能耗,通过节点信任值计算最小化网络整体能耗,使 Sec-RPL 路由协议更适用于快速发展的物联网环境。

参考文献

[1] ZHANG Yuqing, ZHOU Wei, PENG Anni. 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] BRANDT A, HUI J, KELSEY R, et al. RPL: IPv6 routing protocol for low-power and lossy networks: RFC 6550[S]. Fremont, USA: IETF, 2012.

[3] KALYANI S, VYDEKI D. Survey of rank attack detection algorithms in Internet of things[C]//Proceedings of 2018 International Conference on Advances in Computing, Communications and Informatics. Washington D. C., USA: IEEE Press, 2018: 2136-2141.

[4] REHMAN A, KHAN M M, LODHI M A, et al. Rank attack using objective function in RPL for low power and lossy networks[C]//Proceedings of 2016 International Conference on Industrial Informatics and Computer Systems. Washington D.C., USA: IEEE Press, 2016: 1-10.

[5] LE A, LOO J, LASEBAE A, et al. The impact of rank attack on network topology of routing protocol for low-power and lossy networks[J]. IEEE Sensors Journal, 2013, 13(10): 3685-3692.

[6] ZHU Lin, GAO Deyun, LUO Hongbin. Research of RPL protocol of wireless sensor network[J]. Computer Technology and Development, 2012, 22(8): 1-4. (in Chinese)
朱琳,高德云,罗洪斌. 无线传感器网络的 RPL 路由协议研究[J]. 计算机技术与发展,2012,22(8):1-4.

[7] YU Ke, WANG Huifeng. Study and improvement of RPL routing protocol[J]. Computer Engineering, 2018, 44(3): 103-108. (in Chinese)
俞柯,王慧锋. RPL 路由协议的研究与改进[J]. 计算机工程,2018,44(3):103-108.

[8] LEVIS P, CLAUSEN T, HUI J, et al. The Trickle algorithm: RFC 6206[S]. Fremont, USA: IETF, 2011.

[9] MAYZAUD A, BADONNEL R, CHRISMENT I. A taxonomy of attacks in RPL-based Internet of things[J]. International Journal of Network Security, 2016, 18(3): 459-473.

[10] WALLGREN L, RAZA S, VOIGT T. Routing attacks and countermeasures in the RPL-based Internet of things[J]. International Journal of Distributed Sensor Networks, 2013, 9(8): 1-11.

[11] WEEKLY K, PISTER K. Evaluating sinkhole defense techniques in RPL networks[C]//Proceedings of the 20th IEEE International Conference on Network Protocols. Washington D. C., USA: IEEE Press, 2012: 1-6.

[12] DVIR A, HOLCZER T, BUTTYAN L. VeRA—version number and rank authentication in RPL[C]//Proceedings of the 8th International Conference on Mobile Ad-Hoc and Sensor Systems. Washington D. C., USA: IEEE Press, 2011: 709-714.

[13] SEHGAL A, MAYZAUD A, BADONNEL R, et al. Addressing DODAG inconsistency attacks in RPL networks[C]//Proceedings of 2014 Global Information Infrastructure and Networking Symposium. Washington D. C., USA: IEEE Press, 2014: 15-19.

[14] THUBERT P. Objective function zero for the Routing Protocol for Low-power and lossy networks (RPL): RFC 6552[S]. Fremont, USA: IETF, 2012.

[15] RAZA S, WALLGREN L, VOIGT T. SVELTE: real-time intrusion detection in the Internet of things[J]. Ad Hoc Networks, 2013, 11(8): 2661-2674.

[16] PERREY H, LANDSMANN M, UGUS O, et al. TRAIL: topology authentication in RPL[C]//Proceedings of 2016 International Conference on Embedded Wireless Systems and Networks. New York, USA: ACM Press, 2013: 59-64.

(下转第 158 页)

(上接第 149 页)

[17] IUCHI K, MATSUNAGA T, TOYODA K, et al. Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network[C]//Proceedings of the 21st Asia-Pacific Conference on Communications. Washington D. C., USA: IEEE Press, 2015: 14-24.

[18] AIREHROUR D, GUTIERREZ J A, RAY S K. SecTrust-RPL: a secure trust-aware RPL routing protocol for Internet of things[J]. Future Generation Computer Systems, 2019, 93: 860-876.

[19] ESCHENAUER L, GLIGOR V D, BARAsS J. On trust establishment in mobile ad-hoc networks[C]//Proceedings of International Workshop on Security Protocols. Berlin, Germany: Springer, 2004: 47-66.

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

[21] GANERIWAL S, BALZANO L K, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks, 2008, 4(3): 1-37.

编辑　陆燕菲