控制与决策
Control and Decision

一种基于多跳确认和信任评估的选择性转发攻击检测方法

尹荣荣， 张文元， 杨绸绸， 李曦达

引用本文:
尹荣荣, 张文元, 杨绸绸, 等. 一种基于多跳确认和信任评估的选择性转发攻击检测方法[J]. 控制与决策, 2020, 35(4): 949–955.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2018.0608

文章编号: 1001-0920(2020)04-0949-07 DOI: 10.13195/j.kzyjc.2018.0608

一种基于多跳确认和信任评估的选择性转发攻击检测方法

尹荣荣[1,2†], 张文元[1,2], 杨绸绸[1], 李曦达[1]

(1. 燕山大学 信息科学与工程学院，河北 秦皇岛 066004;
2. 燕山大学 河北省特种光纤与光纤传感重点实验室，河北 秦皇岛 066004)

摘 要: 针对无线传感器网络中的选择性转发攻击行为,提出一种基于多跳确认和信任评估(MHA-TE)的选择性转发攻击检测方法. MHA-TE方法利用基于源节点的请求响应形式的多跳确认方案,通过源节点发送请求包、中间节点回复响应包的方式确定路径中产生恶意丢包行为的节点,进而将被检举出的恶意节点作为信任评估的参数更新标准,运用Bate分布建立信任评估模型分析各个节点的交互情况,确定路径中各节点的信任值,并将更新后的信任值与对应的信任值阈值比较,进行恶意节点的判定. 该方法结合多跳确认和信任评估的优势,能够解决路径上多恶意节点误警率高和静态信任阈值适应性差以及检测率低的问题. 仿真实验结果表明,相比于Two-hops方法、MLCM方法和ITEM方法,MHA-TE方法不仅能够有效检测恶意节点,具有较高的检测率和较低的误警率,而且可以在很大程度上降低网络开销.

关键词: 无线传感器网络；选择性转发攻击；攻击检测；多跳确认

中图分类号: TP393.08 **文献标志码:** A

A selective forwarding attacks detection approach based on multi-hop acknowledgment and trust evaluation

YIN Rong-rong[1,2†], *ZHANG Wen-yuan*[1,2], *YANG Chou-chou*[1], *LI Xi-da*[1]

(1. School of Information Science and Engineering，Yanshan University，Qinhuangdao 066004，China；2. The Key Laboratory for Special Fiber and Fiber Sensor of Hebei Province，Yanshan University，Qinhuangdao 066004, China)

Abstract: Considering the selective forwarding attacks behavior, based on multi-hop acknowledgment and trust evaluation (MHA-TE), a selective forwarding attacks detection method is proposed in wireless sensor networks. MHA-TE method using the multi-hop acknowledgment mechanism based on request response patterns from the source node. Through the source node send the request packets and the middle nodes reply to the response packets, the nodes which generate malicious packets loss behavior in the path are confirmed. Then using the malicious nodes as the standard of update parameters in trust evaluation mechanism, the data exchange among nodes is analyzed by the Bate distribution trust evaluation model. And the each node's trust value is obtained. Finally, by comparing the updated trust value with the corresponding trust value threshold, the determination of the malicious nodes is performed. By combining the best of both multi-hop acknowledgment and trust evaluation, these problems such as the high false alarm rate of multiply malicious nodes in the path, low adaptability of static trust value threshold and low accuracy detection rate can be solved. Compared with Two-hops, MLCM and ITEM methods, the simulation results show that the MHA-TE can detect the malicious nodes effectively with higher detection rate and lower false alarm rate, and also can reduce the network overhead to a large extent.

Keywords: wireless sensor network；selective forwarding attack；attack detection；multi-hop confirmation

0 引 言

随着无线传感器网络(wireless sensor networks, WSNs)不断深入的研究和发展,其安全问题成为新的研究热点. WSNs面临许多外部和内部的攻击[1],选择性转发攻击是多种内部攻击中危害最严重的攻击形式之一,它会导致连续的丢包行为[2]. 为了增强其隐蔽性,恶意节点通常表现得与正常节点一样,会选择性地丢弃有价值的数据包,导致基站不能及时收到完整准确的信息[3-4],从而造成网络失效甚至瘫痪. 因此,发现并剔除网络中产生选择性转发攻击的恶意节点,对确保网络的安全至关重要.

目前,研究者已经给出很多针对选择性转发攻

收稿日期: 2018-05-08；**修回日期:** 2019-04-28.
基金项目: 国家自然科学基金项目(61802333)；河北省高等学校科学技术研究项目(QN2018029).
†通讯作者. E-mail: yrr@ysu.edu.cn.

击恶意节点的检测方案,其中多跳确认方案受到广大学者的关注. Balakrishnan等[5]提出了TWOACK机制,通过3个连续节点对恶意行为进行判断,设路径中3个连续节点为N_1、N_2和N_3,N_3每收到一个数据包都会发送1个TWOACK包经过N_2到达N_1,若N_1没有收到TWOACK包,则向源节点检举恶意链路N_2-N_3,然而该方案加剧了网络消息的冲突和碰撞. 为了解决此弊端,Liu等[6]提出了2ACK确认机制,在N_3接收到大量数据包后,选择接收到的部分数据包发送对应的TWOACK包. Shakshuki等[7]提出了EAACK机制,当源节点发送数据包时,等待一个时间阈值,若没有收到基站发送的ACK包,则启动SACK方案. 上述多跳确认机制都能避开产生丢包的链路,但缺点是不能检测出具体的恶意节点. 针对具体恶意节点的检测问题,Kang等[8]提出了EAACK2机制,当源节点接收到检举报告,不会立刻相信该报告,而是启动MRA模式,该方案能够检测到部分恶意节点. 俞波等[9]提出了CHEMAS机制,Young等[10]提出了CADE机制,CHEMAS和CADE的优势是当检测路径中有一个恶意节点时,恶意节点的检测率较高,但当路径上存在合谋攻击或多个恶意节点时,恶意节点的误警率较高. Hai等[11]提出了Two-hops方案,考虑节点合谋导致的丢包,引入两种恶意因素α和β,该方案可以避免合谋攻击,但没有解决路径上存在多个恶意节点的检测问题.

信任评估模型是一种可以识别多恶意节点的有效检测方案. Feng等[12]提出的AODV方案通过节点相互合作完成信息的传递,适用于检测不连续的恶意节点,忽略了相邻恶意节点合谋的情况. 蔡绍滨等[13]提出的云信任模型通过构造信任云模型求得信任值,该方法能够解决路径上两个相邻节点间合谋的不足,但未能很好地解决入侵识别的敏感度与入侵容忍之间的矛盾. 肖云鹏等[14]提出了轻量云模型MLCM方案,可以解决入侵识别的敏感度与入侵容忍之间的矛盾,但需要多次信任值的求解,信任评估的误差较大. 冯健昭等[15]提出的β分布和肖德琴等[16]提出的高斯分布均通过直接信誉和间接信誉加权求和得出每个节点的信任值,最后与信任阈值进行比较,这两种方案虽然只需要确定一个信任阈值,但是该静态信任阈值不能满足网络适应性,正常节点被判定为恶意节点的比率较高. Zawaideh等[17]提出了基于公平信任的恶意节点检测和隔离方案,该方案使用修改后的邻居权重信任确定算法,可以有效提升正常节点被误判为恶意节点的准确率,但是需要经过不断更新信誉列表才能逐渐找出恶意节点,静态信任阈值的问题依然存在. Ozcelik等[18]提出了一种混合入侵检测系统,根据各节点观察其邻居节点的活动,计算其邻居的功能信誉值,该方案可以集中检测恶意节点,但引起了主观权重局限性,而且信任值仍然比较单一. 周治平等[19]提出的ITEM方案是基于贝叶斯和熵的信任评估模型,该模型在一定程度上克服了主观分配权重带来的局限性,但是静态信誉值的问题并未解决.

综上所述,已有多跳确认方案大多可以找出路径中的恶意链路,且对路径中单一恶意节点的检测率较高,但多跳确认方案的请求响应机制多通过基站发送请求包,而中间节点向基站回复响应包来进行恶意节点的识别,该方式应对路径中出现多个恶意节点时,请求包会被接近基站的恶意节点所丢弃,导致请求包不能到达接近源节点的恶意节点,使得误警率较高. 以往信任评估模型大多通过监测和评估邻居节点的行为计算其邻居节点的信任值,并通过结合直接信任值和间接信任值来确定每个节点的综合信任值,然后与已知静态信任阈值比较,虽然能够识别多个恶意节点,但静态阈值在不同场景下的适应性较差,且需要较多的监测节点,对节点要求较高. 为此,本文通过融合多跳确认方案和信任评估模型,可以解决路径上多恶意节点误警率高和静态信任值阈值适应性差、检测率低的问题,同时还可以节约网络开销.

基于上述考虑,本文提出一种基于多跳确认和信任评估(multi-hop acknowledgment and trust evaluation, MHA-TE)的选择性转发攻击检测方法,利用多跳确认的请求响应机制确定产生丢包行为的节点,在此基础上通过构建Bate分布模型分析各个节点的交互情况得出信任值,比较各个节点的信任值和相应的信任值阈值,最后判断出恶意节点. 该方法融合了多跳确认和信任值模型的优势,解决了路径上多恶意节点检测率低、多信任值误差大、静态信任阈值适应性差、对节点要求高的问题.

1 基于多跳确认和信任评估的选择性转发攻击检测方法

本节详细介绍所提出的基于多跳确认和信任评估的选择性攻击检测方法,通过该方法可以检测出数据传递过程中丢包的恶意节点,并将发现的恶意节点剔除出网络.

1.1 包格式定义

包格式的定义可将不同形式的包区分开来,主要有数据包、请求包、响应包和ACK包,为检测方案中包的形成和仿真中传递包的大小提供依据.

数据包是部署在检测环境中的节点遇到突发事件由源节点产生的包,经过多跳传递到基站,DstID为目的节点ID, SreID为生成包的源节点ID, Packet_ID为转发信息的中间节点的ID, Payload为数据包承载的信息片段, $\mathrm{MAC}_{\mathrm{K(S\text{-}BS)}}$ 为源节点与基站共享密钥生成的MAC码(利用位置绑定ID密钥技术为数据包生成的签名摘要,防止恶意节点编造、撰改包信息),内容为 $\mathrm{MAC}_{\mathrm{K(S\text{-}BS)}}\{\mathrm{SreID, Packet\_ID, Payload}\}$.

请求包由源节点产生,与数据包发送方向一致,作用是为了查看路径上节点的存储内存中是否有数据包的信息, R 为随机选取的一个数, H_i 表示源节点到请求包经过的节点的跳数,每经过一跳, H_i 加1.

响应包由存储内存中有数据包信息的节点发出,沿相反路径传递到源节点. 若节点存储内存中没有数据包信息,则该节点发送一个伪造的响应包到源节点会被源节点很容易地识别出来,这样相当于更轻易地"暴露"自己为恶意节点. Note_ID为产生响应包的ID, Next_lostpacket_ID 为产生响应包的节点检举的下一跳丢包节点ID; $\mathrm{MAC}_{\mathrm{K(I-BS)}}$ 为对应的中间节点与基站共享密钥生成的MAC码,内容为 $\mathrm{MAC}_{\mathrm{K(I\text{-}BS)}}\{\mathrm{Packet\_ID, Note\_ID, Payload}\}$, $\mathrm{MAC}_{\mathrm{K(I\text{-}BS)}}$ 中Packet_ID和Payload是数据包中Packet_ID和Payload字段.

ACK包是由基站产生的包,沿着与数据包发送的相反方向发送到源节点, $\mathrm{MAC}_{\mathrm{K(BS\text{-}BS)}}$ 是由基站自己的密钥生成的MAC码,内容为 $\mathrm{MAC}_{\mathrm{K(BS\text{-}BS)}}\{\mathrm{Packet\_ID, Dst\_ID, Payload}\}$, 与 $\mathrm{MAC}_{\mathrm{K(I\text{-}BS)}}$ 一样, $\mathrm{MAC}_{\mathrm{K(BS\text{-}BS)}}$ 中Packet_ID和Payload是数据包中的Packet_ID和Payload字段.

1.2 检测方案

本文所提出的检测方法包含两个过程,先通过多跳确认机制找出路径中被检举的节点,再将该节点作为信任评估模型中参数更新的评估标准,从而确定产生丢包的恶意节点,融合这两种方法解决在多跳确认方案中存在多恶意节点误警率高和信任评估模型中存在静态信任值阈值适应性差的问题.

1.2.1 请求响应机制

当特定事件发生时,源节点 S 会产生一个数据包,同时建立一个计时器,该数据包沿着路径向基站BS传递. 在时间阈值 T_0 内,如果源节点收到目的节点发送的ACK包,则说明源节点产生的数据包已经安全到达目的节点;如果恶意节点伪造ACK包发送到源节点,则源节点会根据 $\mathrm{MAC}_{\mathrm{K(BS-BS)}}$ 码很快识别出来发送ACK的节点为恶意节点. 如果源节点没有收到目的节点发送的ACK包,则源节点会沿数据包传输的路径发送请求包,中间节点接收到请求包后按原路径相反的方向发送响应包到源节点,正常节点在收到请求包后,会发送响应包给源节点,而对于恶意节点,节点直接将数据包丢弃,所以恶意节点产生不了响应包,即路径中最后产生响应包的节点为恶意节点的上一跳节点. 节点间根据同步机制,在一定时间内如果未收到来自上一跳节点的响应包,则产生响应包传递到源节点,否则,节点只是转发上一跳节点的确认包. 若源节点在计时器设定的时间阈值 T_m 内没有收到响应包,则判定源节点的邻居节点为恶意节点. 设 δ 为邻居节点间的最大传输延迟,中间节点 i 设置的计时器时间为

$$T_i = 2 \times \delta \times (H_m - H_i). \tag{1}$$

其中: H_i 为源节点到第 i 个节点的跳数, H_m 为源节点到目的节点的跳数. 区别于传统的基于基站发送请求包的方案,这里通过源节点发送请求包、中间节点回复响应包给源节点的机制,能够减少请求包在转发路径上被多个恶意节点丢弃的概率.

1.2.2 信任评估模型

为了进一步提升恶意节点的检测率,减小对正常节点的误警率,将1.2.1节中被检举出的恶意节点作为本节信任评估的参数更新标准. 引入贝叶斯信任评估模型,根据源节点收到的响应包判断传输路径中各个节点的交互情况,其模型核心描述如下: θ 表示源节点通过交互得到的节点 N_i 为正常节点的概率, α 表示交互成功的次数, β 表示交互失败的次数,该交互情况可以用Beta分布描述. 经过大量 n 次交互得到的期望结果是 $\alpha \sim n\theta, \beta \sim n(1-\theta)$,有

$$\lambda = \frac{\alpha}{\alpha + \beta}. \tag{2}$$

为进一步降低较旧的证据在信任评估中所占的权重值,引入衰减因子 μ,使得 $\alpha = \mu\alpha + s, \beta = \mu\beta + f$, $0 \leqslant \mu \leqslant 1$, s 为交互成功次数, f 为交互失败次数.

经过大量 n 次交互后得到节点的信任表,信任表中信任值 $\lambda_i \leqslant \lambda_0$ 的节点为恶意节点. λ_i 为经过 n 次交互得到的节点 i 的信任值; λ_0 为信任阈值,由 n 次交互得到的各个节点信任值的均值来反映,有

$$\lambda_0 = \sum_{i=1}^{N} \frac{\lambda_i}{N}. \tag{3}$$

信任阈值 λ_0 随着信息交互情况的变化而变化,相比于静态信任值阈值,该动态信任值阈值可保证网络在不同场景下的准确度,网络适应性更好,误警率更低.

综上,基于源节点的请求响应机制和动态信任阈值的信任评估模型的融合,克服了多跳确认方案面对

传输路径上多个恶意节点检测率低的问题和信任评估方案网络适应性差、对节点要求高的问题,进一步提升了传输路径上恶意节点的检测率,降低了对正常节点的误警率,同时减少了网络开销.

1.2.3 检测流程

综合第1.2.1节和第1.2.2节的内容,可以得到整个检测方法的流程如图1所示.

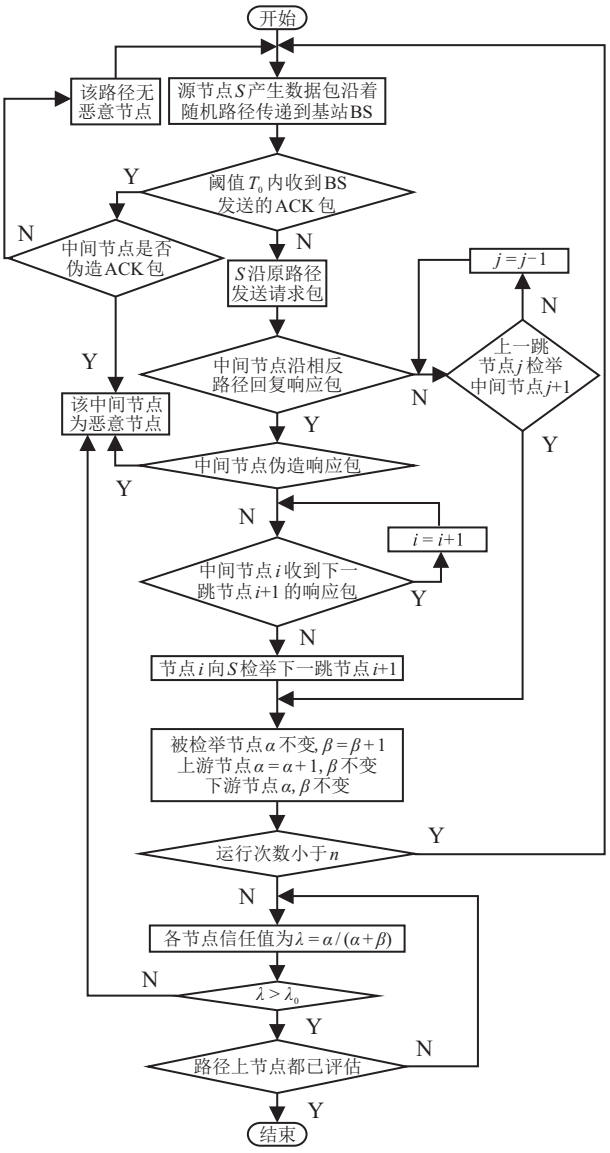


图1 基于请求响应和信任评估的检测流程

2 仿真分析和结果

该部分对所提出的检测方案进行性能仿真评估. 假定300个传感器节点随机地分布在200 m×200 m的区域,随机选取网络中20个节点组成一条路径传送数据. 假定事件源生成100个事件包,由源节点经过该路径传递到基站,随机设置路径上0~30%的节点为恶意节点,恶意节点会随机发起选择性转发攻击,为了模拟更真实的场景,不仅考虑恶意节点的丢包行为,还考虑由于信道原因造成的丢包. 为了考察恶劣的信道环境对检测率的影响,设信道丢包率在0~15%之间变化,将整个实验重复进行200次,取实验结果的平均值,具体仿真参数如下:仿真区域S为200 m×200 m,两节点间最大延迟δ为0.2 s,节点数N为300,节点初始能量E_{init}为0.5 J,节点半径R为15 m,传输和接收能耗E_{elec}为50 nJ/bit,事件包数num为100,放大器功耗ε_{amp}为10 pJ(bit/m^2).

2.1 网络安全分析

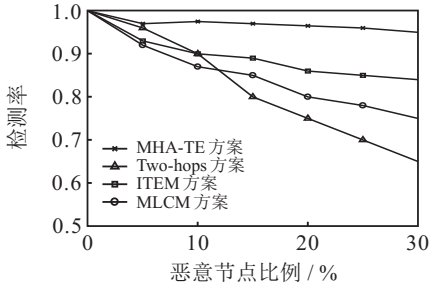
检测率和误警率是分析网络安全性能的两个重要指标,影响这两个重要指标的因素有恶意节点丢包率、恶意节点比例(恶意节点占路径总数的比例)和信道丢包率. 通过分析和评估这3个因素对检测率和误警率造成的影响来验证本文方案对选择性转发攻击的检测能力. 将本文MHA-TE方案与Two-hops方案[11]、MLCM方案[14]和ITEM方案[19]进行对比,分别讨论恶意节点丢包率在10%和20%下,随着恶意节点比例和信道丢包率的变化,4种方案的检测率和误警率的仿真结果.

2.1.1 检 测 率

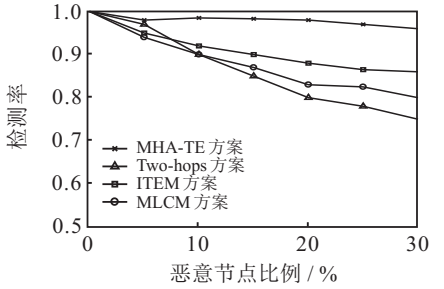
检测率即检测概率,它是检测到的恶意节点数与全部恶意节点数的比值. 在无信道丢包率的情况下,考察4种方案恶意节点丢包率、恶意节点比例对恶意节点检测率的影响,结果如图2(a)和图2(b)所示. 然后,在恶意节点比例(占路径节点总数的30%)一定时,考察恶意节点丢包率、信道丢包率对恶意节点检测率的影响,结果如图2(c)和图2(d)所示.

由图2(a)和图2(b)可见,4种方案的恶意节点检测率都随恶意节点比例的增加而减小,即随着路径上恶意节点数的增加,4种方案对于恶意节点检测的误差越来越大,但MHA-TE方案的检测率始终高于其他3种方案,因为MHA-TE方案的多跳确认机制可以很好地识别出伪造的ACK包和响应包的恶意节点,且针对篡改和丢弃数据包的节点都进行了恶意节点的识别,而其他3种方案不能识别出篡改数据包的恶意节点. 同时,MLCM方案信任值的多次求解导致误差较大,从而检测率低于ITEM方案. 另外,在恶意节点比例较低时,Two-hops方案的检测率要高于ITEM方案和MLCM方案,随着恶意节点比例增加,MLCM方案和ITEM方案的检测率高于Two-hops方案,可见Two-hops方案可以很好地识别路径中的单个恶意节点,但是对于路径中存在多个恶意节点的状况,检测率较低.

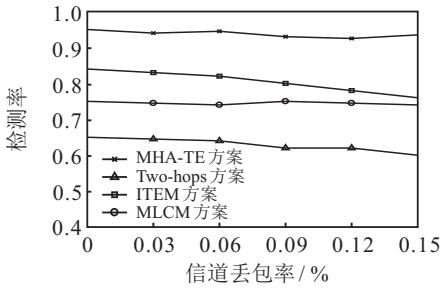
由图2(c)和图2(d)可见,随着信道丢包率的增加,MHA-TE方案的恶意节点检测率最高,Two-hops



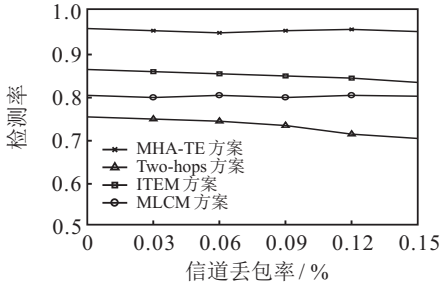
(a) 恶意节点比例对检测率影响 (恶意节点丢包率10%)



(b) 恶意节点比例对检测率影响 (恶意节点丢包率20%)



(c) 信道丢包率对检测率影响 (恶意节点丢包率10%)



(d) 信道丢包率对检测率影响 (恶意节点丢包率20%)

图 2　检测率仿真结果

方案的检测率最低. 这是因为MHA-TE方案的动态信任评估模型可以将多跳确认机制提供的所有丢包节点都进行很好地甄别,因此不会漏掉产生丢包的恶意节点,而Two-hops方案和ITEM方案因为检测机制的单一,对于恶意节点的检测效果较差,MLCM方案虽然结合了信任模型和云模型,但是多信任值求解的误差导致检测率较低. 同时,MLCM方案的检测率变化较小,因为该方案解决了信道引起的敏感度矛盾的问题,对于信道导致的丢包率影响较小. 此外,图2(c)中,ITEM方案的检测率变化最明显,因为ITEM方案的静态信任值阈值导致其在恶劣环境中的检测率下降得最快. 图2(d)中,Two-hops方案的检测率变化得最明显,因为随着信道环境的恶劣化,Two-hops方案被丢弃的恶意因素警告包增加,源节点收到的恶意因素的警告包减少,检测率降低.

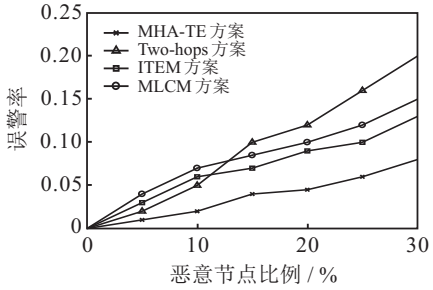
综合图2可以看出,4种方案的检测率都随着恶意节点丢包率的增加呈增加趋势,因为恶意节点的丢包率越高,恶意节点对网络产生的影响越大,被检测出来的概率越大. 同时,本文方案MHA-TE解决了Two-hops方案路径上多恶意节点检测率低、ITEM方案静态信任阈值网络适应性差和MLCM方案多信任值求解误差大的问题,无论恶意节点比例还是信道丢包率对检测率的影响都小于其他3种方案.

2.1.2　误 警 率

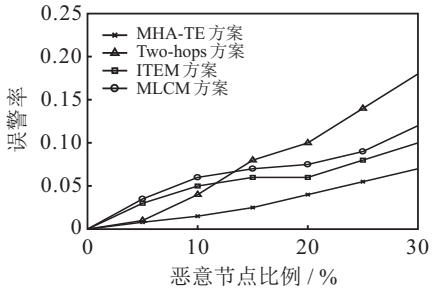
误警率是指被误检的节点占网络中所有被检测节点总数的比例,其中误检包括正常节点被检测成恶意节点以及恶意节点被检测为正常节点的状况. 当没有信道丢包率时,考察4种方案恶意节点丢包率、恶意节点比例对误警率的影响,如图3(a)和图3(b)所示. 然后,在恶意节点比例(占路径节点总数的30%)一定时,考察恶意节点丢包率、信道丢包率对误警率的影响,结果如图3(c)和图3(d)所示.

由图3(a)和图3(b)可见,随着恶意节点比例的增加,4种方案的误警率均呈上升趋势. 这是因为随着路径中恶意节点数量的增加,将恶意节点判断为正常节点的几率增加. 但MHA-TE方案总体上较其他3种方案误警率低,这是因为MHA-TE方案利用基于源节点的请求响应机制减少了请求包和警告包被丢弃的可能,使得信任评估机制能准确识别恶意节点,而其他3种方案不能很好地识别出篡改数据包的恶意节点,导致网络的误警率较高. 同时,ITEM方案比MLCM方案的误警率要低,因为ITEM方案利用熵来对高度可信的节点赋予较大的权重减小了节点的误判. 另一方面,在恶意节点比例较低时,ITEM方案和MLCM方案的误警率比Two-hops方案的误警率高,因为ITEM方案的静态信任值会导致网络适应性较差,MLCM方案的多信任值的计算会增加误差. 随着恶意节点比例的增加,Two-hops方案的误警率比ITEM方案和MLCM方案高,这是因为Two-hops方案多恶意节点检测率低的特性导致其恶意节点被认为是正常节点的概率增加.

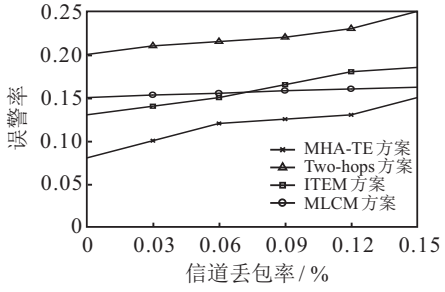
由图3(c)和图3(d)可见,随着信道丢包率的增加,MHA-TE方案与其他3种方案相比误警率较低,因为MHA-TE方案可以识别被恶意节点篡改的数据包,



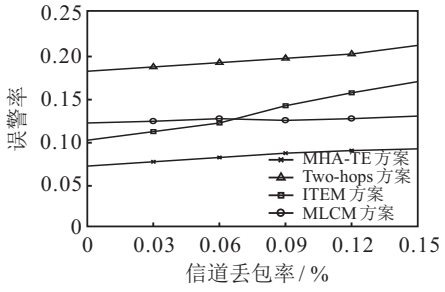
(a) 恶意节点比例对误警率影响
(恶意节点丢包率10%)



(b) 恶意节点比例对误警率影响
(恶意节点丢包率20%)



(c) 信道丢包率对误警率影响
(恶意节点丢包率10%)



(d) 信道丢包率对误警率影响
(恶意节点丢包率20%)

图 3 误警率仿真结果

而其他3种方案不能识别被篡改的数据包. Two-hops方案的误警率最高,因为Two-hops方案存在面对多恶意节点检测率低的弊端,这导致其将恶意节点判定为正常节点的比例增加. MLCM方案的误警率变化最小,因为该方案解决了由于信道引起的敏感度的问题,受信道丢包率的影响较小. 图3(c)中,MHA-TE方案的误警率增加得比其他3种方案更快,因为MHA-TE方案在恶意节点丢包率较小时,由于信道丢包率的影响,正常节点被认为是恶意节点的比例增加. 图3(d)中,MHA-TE方案的误警率上升得比其他3种方案更小,这是因为MHA-TE方案融合了多跳确认机制和信任评估模型的优势,对于恶意节点的识别更加精确. 同时,ITEM方案的误警率比Two-hops方案的误警率增加得快,这是因为ITEM方案静态阈值的设定导致网络适应性差,误警率变化较大.

综合图3可以看出,4种方案的误警率都随着恶意节点丢包率的增加呈下降趋势,因为恶意节点的丢包率越高,恶意节点对网络产生的影响越大,被误检的概率越小. 同时,本文MHA-TE方案无论随着恶意节点比例的变化还是信道丢包率的变化,性能都优于其他3种方案,说明MHA-TE方案通过融合多跳确认机制和信任值评估模型,网络适应性较高,在不同的应用环境中对恶意节点识别的准确率较高.

2.2 网络能耗分析

为分析本文检测方案的能耗,下面通过使用网络开销将本文MHA-TE方案与Two-hops方案、MLCM方案及ITEM方案进行比较,随着仿真周期的增加,3种方案网络开销的对比如图4所示.

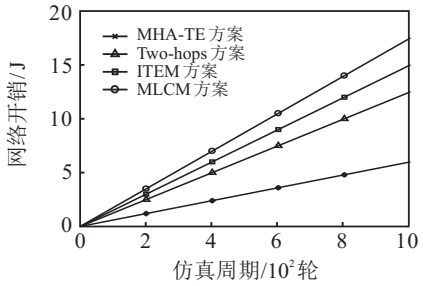


图 4 网络消耗能量的变化趋势

由图4可见,随着仿真周期的增加,4种方案的网络开销均呈上升趋势,但是本文方案的网络开销要比其他3种方案低,因为本文方案没有用到监测节点,同时在基于源节点的请求响应机制中,恶意节点丢掉数据包后,源节点会发送请求包,恶意节点前一个节点会回复响应包,恶意节点到基站的这些中间节点没有消耗能量,大大节省了网络开销. 而Two-hops方案、MLCM方案和ITEM方案都需要监测节点的实时监控,增加了大量的网络开销. MLCM方案的网络消耗最高,因为除了监测节点需要不断的监控外,还需要通过云模型多次计算信任值,大大地增加了网络的开销. 随着仿真周期的增加,ITEM方案比Two-hops方案的网络消耗高,这是因为ITEM方案需要大量的监测节点进行邻居节点的监控,而Two-hops方案只需要几个监测节点进行监控,减少了能量的消耗.

3 结 论

本文针对无线传感器网络中的选择性转发攻击行为,提出了一种基于多跳确认和信任评估模型的选

择性转发攻击检测方法. 本文主要的创新性工作体现在: 1) 提出了基于源节点的请求响应形式的多跳确认方案; 2) 提出了利用响应包来判断各个节点的交互情况, 进而更新信任表中各个节点的信任值形式的信任评估模型; 3) 与传统的检测方法不同, 本文的检测方法融合了多跳确认方案和信任评估模型, 解决了路径上多恶意节点误警率高和静态信任阈值适应性差、检测率低的问题, 同时有效地节约了网络开销. 下一步工作将研究针对合谋的选择性转发攻击的检测方法, 进一步增强系统的总防御能力.

参考文献(References)

[1] Zhou H, Wu Y, Feng L, et al. A security mechanism for cluster-based WSN against selective forwarding[J]. Sensors, 2016, 16(9): 1-6.

[2] Sert S A, Fung C, George R, et al. An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks[C]. Fuzzy Systems. Naples: IEEE, 2017: 1-6.

[3] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and counter measures[J]. Ad Hoc Networks, 2003, 1(2/3): 293-315.

[4] Reddy Y, Durand J, Kafle S. Detection of packet dropping in wireless sensor networks[C]. Seventh International Conference on Information Technology. Las Vegas: IEEE, 2010: 879-884.

[5] Balakrishnan K, Deng J, Varshney P K. TWOACK: Preventing selfishness in mobile ad hoc networks[C]. Wireless Communications and Networking Conference. New Orleans: IEEE, 2005: 2137-2142.

[6] Liu K J, Deng J, Varshney P K. An acknowledgment-based approach for the detection of routing misbehavior in MANETs[J]. IEEE Transactions on Mobile Computing, 2007, 6(5): 536-550.

[7] Shakshuki E M, Kang N, Sheltami T R. EAACK-A secure intrusion detection System for MANETs[J]. IEEE Transactions on Industrial Electronics, 2013, 60(3): 1089-1098.

[8] Kang N, Shakshuki E M, Sheltami T R. Detecting forged acknowledgements in MANETs[C]. Advanced Information Networking and Applications(AINA). Singapore: IEEE, 2011: 488-494.

[9] 俞波, 杨珉, 王治. 选择传递攻击中的异常丢包检测[J]. 计算机学报, 2006, 29(9): 1542-1552.
(Yu B, Yang M, Wang Z. Identify abnormal packet loss in selective forwarding attacks[J]. Chinese Journal of Computers, 2006, 29(9): 1542-1552.)

[10] Young K K, Hwaseong L, Kwantae C, et al. CADE: Cumulative acknowledgement based detection of selective forwarding attacks in wireless sensor networks[C]. Convergence and Hybrid Information Technology. Busan: IEEE, 2008: 416-422.

[11] Hai T H, Huh E N. Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge[C]. Network Computing and Applications. Cambridge: IEEE, 2008: 325-331.

[12] Feng T, Xiong F, Chen G. Effects of atmosphere visibility on performances of non-line-of-sight ultraviolet communication systems[J]. Optik - International Journal for Light and Electron Optics, 2008, 119(13): 612-617.

[13] 蔡绍滨, 韩启龙, 高振国. 基于云模型的无线传感器网络恶意节点识别技术的研究[J]. 电子学报, 2012, 40(11): 2232-2238.
(Cai S B, Han Q L, Gao Z G. Research on cloud trust model for malicious node detection in wireless sensor network[J]. Acta Electronica Sinica, 2012, 40(11): 2232-2238.)

[14] 肖云鹏, 姚豪豪, 刘宴兵. 一种基于云模型的WSNs节点信誉安全方案[J]. 电子学报, 2016, 44(1): 168-175.
(Xiao Y P, Yao H H, Liu Y B. A WSNs node reputation security scheme based on cloud model[J]. Acta Electronice Sinica, 2016, 44(1): 168-175.)

[15] 冯健昭, 肖德琴, 杨波. 基于分布的无线传感器网络信誉系统[J]. 计算机应用, 2007, 27(1): 111-113.
(Feng J Z, Xiao D Q, Yang B. Reputation system for wireless sensor networks based on distribution[J]. Computer Applications, 2007, 27(1): 111-113.)

[16] 肖德琴, 冯健昭, 周权. 基于高斯分布的传感器网络信誉模型[J]. 通信学报, 2008, 29(3): 47-53.
(Xiao D Q, Feng J Z, Zhou Q. Gauss reputation framework for sensor networks[J]. Journal on Communications, 2008, 29(3): 47-53.)

[17] Zawaideh F, Salamah M, Al-Bahadili H. A fair trust-based malicious node detection and isolation scheme for WSNs[C]. Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS). Amman: IEEE, 2017: 1-6.

[18] Ozcelik M M, Irmak E, Ozdemir S. A hybrid trust based intrusion detection system for wireless sensor networks[C]. Networks, Computers and Communications (ISNCC). Marrakech: IEEE, 2017: 1-6.

[19] 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.
(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.)

作者简介

尹荣荣 (1985−), 女, 副教授, 博士, 从事无线传感器网络容错控制等研究, E-mail: yrr@ysu.edu.cn;

张文元 (1991−), 男, 硕士生, 从事无线传感器网络路由协议的研究, E-mail: 312161117@qq.com;

杨绸绸 (1974−), 女, 副研究员, 从事无线传感器网络可靠性分析评价等研究, E-mail: ccyang@ysu.edu.cn;

李曦达 (1977−), 女, 副教授, 博士, 从事无线传感器网络资源优化等研究, E-mail: lixida@ysu.edu.cn.

(责任编辑: 郑晓蕾)