一种针对无线传感网中黑洞攻击的检测与防御方法

王 珺[1,2] 朱志伟[2] 刘俊杰[1,2]
(南京邮电大学宽带无线通信与传感网技术教育部重点实验室 南京 210003)[1]
(南京邮电大学通信与信息工程学院 南京 210003)[2]

摘 要 无线传感器网络WSN(Wireless Sensor Networks)被广泛应用于军事、生产、医疗等各个方面,而当下的许多传感器网络都部署在恶劣、开放的环境中,存在各种各样的威胁。黑洞攻击是一种典型的路由攻击,在这种攻击中恶意节点声称自己是剩余能量多、能够一跳到达目的节点的节点或者声称自己就是目的节点,因此很多节点会把要发送的数据发给该恶意节点,而恶意节点吸引数据包后,并不将数据包转发而是丢弃,这就造成传输空洞。针对这种特性,文中提出了一种基于位置信息的诱捕检测算法BTCOLI(Blackhole Attack Detection Algorithm Based on Location Information),以实际不存在的目的节点为诱饵,找到黑洞节点,对其进行身份验证以及位置检测,从而剔除该恶意节点。同时,还提出了相应的防御方案:在网络中加入预共享对称密钥,并提供HMAC(Hash-based Message Authentication Code)消息验证机制,以防止恶意节点加入网络。最后通过搭建NS-2下的仿真平台,验证了该算法在检测率方面的优越性。

关键词 无线传感器网络,路由层攻击,黑洞攻击
中图法分类号 TN915.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.02.016

Detection and Defense Method for Blackhole Attacks in Wireless Sensor Networks

WANG Jun[1,2] ZHU Zhi-wei[2] LIU Jun-jie[1,2]
(Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[1]
(College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[2]

Abstract Wireless sensor networks(WSN) are widely used in military, production, medical and so on. Many sensor networks are deployed in hostile and open environments, so there exist a variety of threats. Blackhole attack is a typical route attack in WSNs. A malicious node claims that it has enough residual energy and it can reach the destination in one hop or claims itself to be the destination node. So the malicious node can attract other nodes to send data to it. But it will discard the packets without forwarding it which results in the "data hole". This paper proposed a new location detection method with trapping method. A non-existent destination node is used as a bait to locate the blackhole nodes. By verifying the identity and position information of the nodes, the malicious nodes can be removed. At the same time, the algorithm adds the pre-shared symmetric key and HMAC(Hash-based message authentication code) message authentication mechanism to prevent malicious nodes from joining the network. The results of simulation based on NS2 platform show that the proposed algorithm is superior to other ones with higher detection ratio.

Keywords WSN, Routing layer attacks, Blackhole attack

1 引言

与传统的有线网络相比,无线传感器网络(WSN)[1]有许多优点:拓扑结构易变化,数据融合能力强大,能耗较低,无需网络基础设施,具有自组织能力,并且能够在条件恶劣的开放环境中自主感知和协作管理,从而丰富了信息的采集、检测和处理的方式。过去针对无线传感器网络的大多数研究假设在一个相对安全的环境中,但是如今许多无线传感网是应用于不受信任的开放环境中,极易受到各种类型的网络攻击[2]。因此,无线传感网的安全问题逐渐演变成为一个热点问题。

黑洞攻击(Blackhole Attack)是WSN中常见的拒绝服务(DoS)攻击类型。路由建立的过程中,恶意节点在收到路由请求分组(Route Request, RREQ)后,会声称自己是高质量、低时延、一跳可到达目的节点的节点或者声称自己就是目的节点,因此很多节点会选择该"恶意节点"作为数据包转发的下一跳节点。在数据传输阶段,黑洞节点作为路由中继节点,在收到报文后,不对其进行转发而是直接丢弃,使得网络中任意两个节点无法通信,相当于在网络中形成了一个"黑洞",黑

到稿日期:2018-01-09 返修日期:2018-05-21 本文受国家自然科学基金(61401234),江苏省高校优势学科工程资助。
王 珺(1975—),女,博士,副教授,主要研究方向为下一代网络技术、传感器网络,E-mail:wang_jun@njupt.edu.cn(通信作者);朱志伟(1991—),男,硕士,主要研究方向为传感器网络的安全性研究;刘俊杰(1994—),男,硕士生,主要研究方向为网络安全技术。

洞攻击的名字也由此而来。黑洞节点可以是新的外部入侵节点,也可以是内部被妥协(Compromised)的节点。黑洞节点的存在严重扰乱了网络通信,图 1 就是一个典型的黑洞攻击,源节点 S 需要与目的节点 D 通信,发起路由请求 RREQ,黑洞节点一般会宣称自己是距离目的节点很近且具有高质量链路、低时延、一跳可达目的节点,从而使其成为路由中继节点,但是在通信过程中黑洞节点 B 直接丢弃数据包而不是转发。

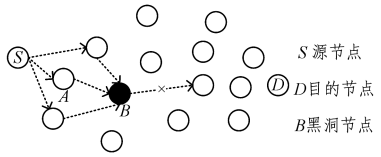

图 1　黑洞攻击

Fig. 1　Blackhole attack

黑洞攻击对网络通信造成了极大危害,并且难以防御,绝大部分无线传感网路由协议[3]没有针对黑洞攻击的安全机制,不能有效防御黑洞攻击。

本文首先介绍了无线传感器网络及其特征,并分析了安全问题严峻的根源;然后详细介绍了无线传感器网络中黑洞攻击的原理和破坏性及其相关工作;接着综合黑洞攻击的特性,提出了一种针对黑洞攻击的检测与防御机制并完成了仿真验证;最后指出下一步的研究方向。

2　黑洞攻击检测的相关工作

2.1　相关工作

Kozma 等[4]提出了 REAct 行为证明审核程序。一旦目的节点分组丢失率超过一定阈值,目的节点立即回复行为反常的反馈包,源节点收到消息包后启动审核程序。行为审核程序利用预先设置的审核节点与布隆过滤器(Bloom Filter)产生行为审核,对比并分析行为结果,寻找发起丢包行为的节点所在的网段。由于布隆过滤器产生的行为证明仅仅包括分组信息,并没有记录路径上转发节点的信息,从而导致源节点无法判断路径上的哪个节点存在反常行为。其次,该方案对多个协同合作的黑洞节点无法起到监测的作用,协同的黑洞节点可以为其他黑洞节点提供行为伪证明,谎称恶意节点存在于另外一条路径上,欺骗系统。

Gupta 等[5]设计了新的路由请求以及路由回复报文来屏蔽黑洞节点。路由回复报文中添加了目的节点的地址信息,该种方式可防止恶意的外部节点在加入网络时不需要获取身份信息。当收到路由回复报文时,节点会检查自身的路由表,在源节点字段相同的情况下,选取路由表中 count 字段较大的报文发送出去,保证节点是合法节点的可能性最大。当回复报文中的序列号不同但却来自于同一个节点时,即表明其中一个报文是黑洞节点所发出的,这时选择下一跳合法度更高的而不是依据报文中的跳数来选择转发某一个报文。该方法依赖于路由表中的转发跳数等统计信息,一旦信任阈值的设置不合理,将造成极大的误判,从而导致该方法的虚警率过大。

Wazid 等[6]对无线传感器网络分簇协议中的黑洞节点进行了检测以及防御。为了发现并隔离黑洞节点,该作者设计了路由认证的消息包,协调器节点向中继节点发送身份认证包,防止恶意节点加入簇中。为了区分节点损坏以及黑洞攻击,中继节点向协调器节点传递数据时需要附带身份认证包,黑洞节点会丢弃数据,但是会回复认证包,当检测到这样的节点即认为该节点是“黑洞节点”,然后隔离黑洞,同时被黑洞节点影响的簇中所有其他节点立即要求加入其他邻居簇。该方法的缺点也很明显,即一旦有正常节点妥协,协调器节点将无法验证该节点的合法性,导致该方法失效。

Aad 等[7]利用信任值来对节点进行监测,网络中的每一个节点自身初始分配一个信用值,同时记录全网所有节点的信任值,对表中节点的信息与可靠性进行综合考虑。该方法需要记录路径上的所有节点,当源节点的数据包能够成功传送至目的节点时,路径上所有节点的信用值会增加;相反,如果数据包没有到达目的节点,则减少路径上所有节点的信用值。该方法的信用阈值难以确定,无法准确定位黑洞节点,路径上的正常节点也经常被误判。

Deng 等[8]将检测算法嵌入路由协议中,提出了下跳节点认证的检测方案。该方案中,节点返回 RREQ 包时需要附带下一跳节点的位置信息。源节点接收到 RREP 包后并不直接进行数据传输,而是需要向附带的地址信息的节点发送 FurtherRequest,查询在该节点与目的节点间是否存在路径。如图 2 所示,当中继节点 E 应答消息包时,需要将其下一跳节点 G 的位置信息附在消息包中回复给源节点。源节点从其他路由寻路并发送消息包给 G 节点,查询该节点是否存在目的节点 D 的路径。如果 G 存在到达目的节点以及回复节点的路径,信任中间回复节点并传输数据包;相反,若 G 没有到达目的节点或者中间回复节点的路径,则广播警报报文,通知全网忽略该节点的消息包。这种方案只对单个运作的黑洞节点起作用,一旦有多个黑洞节点协同工作,此方案就很难检测出黑洞节点。如果节点 E 与节点 G 均为恶意节点,那么向 G 节点发送询问包时,G 会回复其存在到目的节点的路径,源节点会得到虚假回复,导致该方案失效。

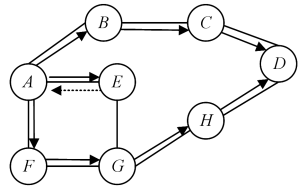

图 2　下一跳节点认证

Fig. 2　Authentication of next hop node

Al-Shurman 等[9]提出冗余路由的方法来防御黑洞攻击,即需要发现 3 种以上到目的节点的不同路径。节点对 ping 数据包采用不同的计数序号的方法,防止丢弃后来到达的数据包。源节点检查回复的数据包,验证节点是安全的还是恶意的,然后再进行数据传输。由于发送节点必须等待所有的冗余数据包到达后才判断路由的真实性,大大增加了网络时延。

2.2　现有方案的不足

已有的各种黑洞攻击的检测机制虽然能一定程度上有效地检测出黑洞攻击的存在,但是经过研究发现仍然存在诸多问题。信任阈值的设置是信誉认证等机制的瓶颈,影响了检测的准确率,冗余路由的出现可以较好地解决该问题,但是路由时延的增加和资源的浪费会影响网络性能。攻击节点有两种出现方式:1)恶意节点向某些正常节点妥协;2)恶意节点冒

充合法节点参与通信。现今大部分解决方案并没有一套完善的体系来应对黑洞节点的以上两种情况。上述有些方法针对 Ad hoc 网络的路由协议进行研究,并不能将其直接应用于资源受限的无线传感器网络中,有些研究用于无线传感器网络时也存在检测率较低、开销过大等问题。文中充分考虑了无线传感器的网络特性,分析了黑洞攻击行为的特性,设计了一种基于地理位置信息的黑洞节点检测及黑洞节点诱捕算法。

3 基于位置信息的黑洞攻击检测算法

3.1 网络模型

该算法的应用模型基于以下假设:

1)网络节点随机分布,通信半径相同,位置固定不变;

2)通信链路是双向对称链路,任意一个节点能够与邻居节点收发消息;

3)网络中的可靠性问题并不在协议考虑之内,消息的丢失和重传将由高层协议来解决;

4)网络中的信标节点可通过直接(如 GPS)或者间接的方式(定位算法)获得自身的地理位置信息。

3.2 基于位置的检测算法思想概述

由上述黑洞节点攻击流程可知,网络在黑洞节点存在的情况下进行路由寻路时,黑洞节点声称自己是高质量、低时延、一跳可到达目的节点的节点或者是目的节点,邻居节点由此选择黑洞节点作为下一跳路由;同时黑洞节点与 sinkhole 攻击不同,sinkhole 节点一般布置在网关附近,而黑洞节点布置在远离基站的位置。因此,由图 1 可知,黑洞节点的实际地理位置离基站往往远大于一跳距离。针对该特性,文中提出一种基于位置信息的检测算法 BADOLI(Blackhole Attack Detection algorithm based on Location Information)。

无线传感器网络不同于一般网络,对于能耗的要求十分苛刻,若为每个节点都部署 GPS 设备,对于大量的传感器节点而言成本太大,文中选取距离无关的 DV-Hop 定位算法[10],该算法无需绝对距离和方位,可以节约成本。但由于算法的原理是基于节点间的最小跳数来实现定位,如果网络已经遭到虫洞攻击,就会影响 DV-Hop 算法的定位精度。虫洞以及黑洞攻击经常成对出现,若在虫洞存在的基础上发起黑洞攻击,将使一些简单有效的检测防御方法失效,从而带来检测、防御上的困扰。因此,本文假设在虫洞攻击存在的情况下对黑洞攻击进行检测,以避免测量的不准确性。虫洞攻击[11]是一种使两个区域的节点互相误认为是邻居的跨区域行为的攻击,在虫洞节点通信半径内的信标节点必将受到影响,所测得的跳数也将会远远小于实际跳数。本节利用虫洞节点存在时出现的几个异常现象,首先提出一种消除虫洞攻击的 DV-Hop 算法,然后利用这个改进的 DV-Hop 算法获取节点信息来实现黑洞节点的检测。

在节点建立路由的过程中,每当某节点收到距离基站一跳可达或者下跳节点就是基站的数据包时,立即启动 3.4 节中改进的定位算法定位黑洞节点的位置。考虑到黑洞节点存在哄骗行为,直接对黑洞节点进行定位可能导致该节点回复虚假的位置信息,从而使测量不准确,因此,需要对收到黑洞节点信息的节点进行定位,即黑洞节点的上一跳节点(如图 1 中的 A 节点)。若该节点与基站距离大于 $2R$,即可知道下一跳节点是黑洞节点,向全网发送警报信息,忽略来自该节点的报文,消除黑洞节点的影响。

3.3 消除虫洞攻击的 DV-Hop 算法

3.3.1 DV-Hop 算法的局限性

因为虫洞攻击会影响 DV-Hop 算法的定位准确性,所以本文根据虫洞特性,提出一种可消除虫洞攻击影响的改进的 DV-Hop 算法。

虫洞攻击一般是在一对节点之间建立一条有线链路或者是一条高质量、低时延的信道。因此,在数据传输的过程中,这更加容易吸引周围的数据包,从而利用这条不安全的“隧道”将从虫洞节点的一端截取到的消息通过协同工作的节点传递到网络的另一端。如果虫洞节点不进行丢弃、篡改等操作,那么该条链路只会加速网络信息的传递。但是一旦该条“隧道”丢弃数据或篡改数据,将会造成数据包的泄漏或破坏;同时,因为私有“隧道”能够造成比实际路径更短的虚假路径,节点之间的路由选择都会被扰乱,最为严重的是当攻击节点断开私有“隧道”之后,节点之间建立的虚假路由信息将会全部失效,在短时间内使得“隧道”周围的节点因负载过重而失效,甚至产生广播风暴。

3.3.2 虫洞节点的检测特性

为了介绍本文提出的算法,定义 $D_R(u)$ 表示以 u 为圆心、半径为 R 的圆周,即一个节点的通信范围。

当网络中存在虫洞节点时,网络可能违背以下两个检测特性,想要进一步提高检测效率亦可增加新的检测特性,本节利用下述两个检测特性可检测出受影响的节点。

1)消息的唯一性:相同的节点无法重复接收邻居节点发送的相同报文。

如图 3 所示,B_3 节点广播一个消息,由于 B_2 在 B_3 的通信范围内,即 $B_2 \in D_R(B_3)$,因此其会接收到 B_3 广播的消息。B_3 的报文同样会被虫洞节点 Y 获取,通过虫洞“隧道”另一端的 X 节点广播出来。因为 B_2 在 X 的通信范围内,所以 B_2 又能收到一次 B_3 的报文,而在正常网络中则不会存在此类现象。需要特别说明以下的一种情况,假设 S_{10},B_3,B_5 任意两点相互都在通信范围内。B_3 转发来自 S_6 的数据包,此时 S_{10} 收到数据包,按照路由算法选择下一跳。假设选择 B_5 作为下一跳,B_5 也转发数据包,此时 S_{10} 又收到了一次数据包。这种情况下,S_{10} 收到的两个报文来自于 B_3 直接发送去的和通过 B_5 转发的,报文中的跳数不同,因而这两个报文并不是同一个报文。

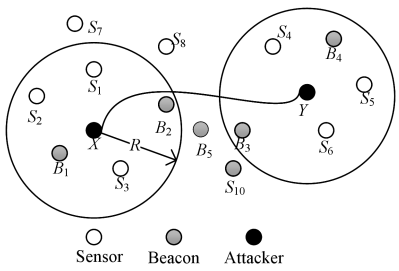

图 3 受虫洞攻击影响的网络

Fig. 3 Network affected by wormhole attacks

2)通信范围有限特性:任何一个节点都不可能与自身通信范围以外的节点通信。

一般情况下,节点不会与自身通信范围以外的节点进行

通信。基于通信范围有限特性的检测方法如下：如图 3 所示，当受到虫洞攻击时，若 B_1 要传递信息，则信息通过虫洞“隧道”$X->Y$ 传递，并经由 Y 广播出去，B_4 会收到 B_1 发送的消息，由于“隧道”两端的节点是不可见的，因此就好像从 B_1 直接传递消息至 B_4。可以得知，若 B_1 直接与超过通信范围的 B_4 进行通信，即可判断受到了虫洞节点的攻击。

由上述的几个特性可以得出定理 1。

定理 1　在 DV-Hop 定位过程中（第一阶段之后每个信标节点即可知道其他信标节点的位置），只要协同工作的虫洞节点的通信范围内分别存在一个及以上信标节点，即可检测出虫洞攻击。

证明：若协同工作的虫洞节点的通信范围内分别存在一个信标节点，且当两个信标节点的距离超过 R 时，将违背通信范围有限性；当两个信标节点距离小于 R 时，将会违背消息的唯一性。推广到多对虫洞节点内存在多个信标节点中，该定理依然可证。

3.3.3　异常节点的筛选

为了减少定位误差，需要使受到影响的节点不参与定位，可采用以下方法实现：当信标节点根据上述两种特性检测到受到虫洞节点的影响时，一旦参与定位将会造成巨大误差。因此，其自身发送休眠消息包，让收到消息包的节点都休眠，即让虫洞节点另一端的节点与自身周围的节点进行休眠。如图 3 所示，B_1 与 B_4 通信时，经过上述两个特性的检测会发现 B_1 节点发送数据包时违背了通信范围有限性，此时可判断其自身受到虫洞攻击的影响。让 B_1 节点发送休眠包，休眠包经过虫洞“隧道”后广播出来，导致 B_3，B_4，S_2，S_3，S_4，S_5，S_6 进入休眠状态；同理，B_4 也会检测到自身受到影响，同样发送休眠包，导致 B_1，B_2，S_1，S_2，S_3，S_4，S_5 进入休眠状态。其余节点仍然按照上述方式工作。由图 3 可知，虫洞节点 X 与虫洞节点 Y 范围内的节点都会进入休眠，即 $D_R(X)\cup D_R(Y)\cup D_R(B_1)\cup D_R(B_2)\cup D_R(B_3)\cup D_R(B_4)$，从而实现了隔离虫洞节点的安全定位。

3.4　基于位置信息的黑洞攻击检测算法（BADOLI）的流程

首先，利用上文介绍的改进的可以消除虫洞攻击影响的 DV-Hop 算法进行安全定位，然后计算节点间的距离。若基站的坐标为 (a,b)，回复其本身是目的节点或者可一跳到达目的节点的上一跳节点 j 的位置为 (x,y)，由式（1）计算出基站与当前位置的距离为：

$$d=\sqrt{(x-a)^2+(y-b)^2} \tag{1}$$

如果 $d>2R$，即可判断宣称自己是目的节点或者可一跳到达目的节点的节点即为黑洞节点，通知全网对其进行隔离。

4　基于位置信息的黑洞节点诱捕认证算法

由于 BADOLI 算法中要求当网络中有节点收到一跳可达目的节点或者目的节点的数据包时即立刻启动 BADOLI 检测算法，大部分正常的路由过程也可能收到正常的一跳可达基站的路由包，此时也需要利用 BADOLI 算法进行检测，这导致了多余的操作，消耗了较多资源。同时，基于距离无关的定位算法由于是通过节点间的连通性和多跳路由计算距离的，并不是直接对两个节点之间的距离进行精确定位，因此存在一定的误差，对距离目的节点较近的正常节点采用该方法，会导致较低的定位精度，从而可能导致误判率增高。因此，本节对文献[12]中的 RBAOM（Resisting Blackhole AODV Mechanism）算法进行改进，提出了一种基于位置信息的黑洞节点诱捕认证算法 BTCOLI（Blackholes Trap Certification of the node based on Location Information），该防御算法引入了身份认证机制，可防止恶意节点冒充合法节点，同时配合 BADOLI 检测算法，可以有效防御内部已妥协节点的黑洞攻击。

4.1　RBAOM 方法的不足

本文针对黑洞攻击，利用信誉机制以及虚拟目的节点的方法进行检测与防御。信誉机制的存在确实可以对黑洞节点起到一定的防范作用，但每个节点对于信誉值、地址表格等数据的存储消耗了一定的空间。trust level 以及 confidence level 的设置增加了网络的时延，trust level 以及 confidence level 阈值的界定困难直接影响了算法的准确度，导致该方法存在一定的局限性。RBAOM 方法基于 AODV 协议，由于该协议可以由中间节点进行回复，因此检测算法的实现比较复杂；同时该路由协议也并不完全适合于能量受限制的无线传感器网络，因此本文不采用 RBAOM 的信誉机制，而是引入 HMAC（Hash-based Message Authentication Code）验证模块。

4.2　HMAC 验证模块

4.2.1　加解密算法概述

密码学中的加密算法有两种，分别为对称密钥加密和非对称密钥加密[13]。相比于非对称密钥，对称密钥具有密钥长度短、加解密速度快、计算复杂度低等优势，因此无线传感器网络中的应用通常采用对称密钥加密算法，也有一些对非对称密钥加密算法的改进方案被运用于 WSN。本文采用对称密钥机制。

4.2.2　散列消息鉴别码

散列消息鉴别码 HMAC 主要基于哈希算法，以一个密钥和消息作为函数的入参，生成一串消息摘要。HMAC 一般用于验证共同享有一个密钥的两个节点之间传输消息的正确性。如果密钥以及消息经过哈希函数的运算后输出的消息摘要不同，那么原始输入必定也不同，满足这种性质的散列函数称为单向散列函数，该函数的安全系数非常高，MD5 和 SHA-1 就是常用的散列函数。HMAC 可与现有的散列函数捆绑使用，想要替换散列函数也很简单，只需去除旧模块，加入新模块即可，HMAC 函数流程如图 4 所示。图 4 也可用式（2）表示：

$$HMAC(K,m)=H((K\oplus opad)\parallel H((K\oplus ipad)\parallel m)) \tag{2}$$

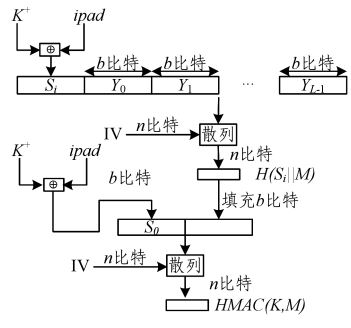

图 4　HMAC 流程

Fig. 4　Process of HMAC

4.2.3　HMAC 验证模块的阐述

因为采用对称密钥，所以需要完善的密钥管理机制。为

了减少开销并降低加解密难度，本文采取全网统一密钥模型的预共享对称密钥机制[14]来实现密钥管理。节点部署过程中，有可信任的第三方为节点存储一对密钥，即全网节点拥有相同的一对密钥。节点经过认证中心的配置后即可加入网络，并且后序的安全性操作可以通过该密钥进行。为了防止密钥被破解或者节点被捕获从而导致密钥泄漏，全局共享密钥在一定周期会更新一次；同时采用双密钥配合两种散列函数使得密钥和消息更加难以被破解，提高了安全性。

认证中心为每个节点分配 K_1，K_2 两把密钥，出于安全性的考虑，采用双重 HMAC 验证，分别对 K_1 密钥以及节点 ID 利用 MD5 进行 HMAC 加密，对 K_2 以及节点 ID 利用 SHA-1 进行 HMAC 加密，安全性同时由 SHA-1 和 MD5 两种算法以及密钥来保证，式(3)即 HMAC 运算形式。这样即使丢失其中一把密钥或者一种算法被破译，也无法破译信息。

$$hmac\_msg = HMAC_{MD5}(K_1, ID) \mid HMAC_{SHA\text{-}1}(K_2, ID) \tag{3}$$

4.3 探测报文的设计

4.3.1 报文设计概述

邻居节点需要利用报文中的节点 ID 以及预先商量好的密钥和散列函数对 HMAC 码进行验证，因此发送报文中需要有 HMAC 码字段，用于存储发送节点的身份认证信息。为了诱捕网络中存在的黑洞节点，需要设置一个虚拟的、网络中不存在的 IP 地址，因此本文设计的探测报文格式如图 5 所示。

类型	节点ID
源节点地址	
目的节点地址（不存在的）	

图 5 探测报文

Fig. 5 Probe message

探测回复报文格式如图 6 所示。

类型	节点ID
源节点地址	
目的节点地址	
HMAC鉴别码	

图 6 回复报文

Fig. 6 Reply message

该报文中“类型”字段如果等于 1 则代表该报文为探测报文，等于 2 则代表该报文为探测回复报文。HMAC 鉴别码：回复探测报文时需要将式(3)的计算结果附在 HMAC 鉴别码字段以供周围节点对其进行身份验证。

4.3.2 HMAC 开销分析

1)计算能耗分析

节点新加入网络或者发送带有伪装目的地址的探测报文后，一旦有节点回复该报文，即需 HMAC 鉴别码对节点的身份进行验证。由 HMAC 的概述可知，HMAC 的执行时间与嵌入的散列函数处理消息所用的时间近似相等，本文在笔记本电脑上对 100 万条 11 位的手机号进行 MD5 加密测试(如果对一条记录进行加密，精度有限，无法显示准确的运算时间)用时为 1.6 s，而采用 SHA-1 进行加密测试的耗时为 1.8 s，这是由于 SHA-1 的循环步骤比 MD5 多且要处理的缓存更大。由于本文的节点只需要对一个节点 ID 进行 HMAC 加密，尽管传感器节点的计算能力稍差(有很多传感器 CPU 处理主频已经达到手机的 CPU 级别)，并不会造成较大的计算时延。SHA-1 和 MD5 两种常用的散列函数的能耗仅为 0.000 65 mJ 和 0.006 mJ，这种数量级的能耗也完全可以用于节点的认证中。

假设 n 代表节点平均邻居数，当一个新节点加入网络时，其周围邻居节点需要对其进行身份验证，因此会消耗 $0.006\,65n$ mJ 左右的能耗。当某一节点收到诱捕报文的回复后，先对其进行身份验证，周围邻居也都会收到此回复报文，因此，也消耗 $0.006\,65n$ mJ 左右的能量。

2)存储空间开销分析

每个节点首先需要存储第三方认证中心分发的两串密钥 K_1 和 K_2，同时要存储解析报文中的 ID 以及 HMAC 字段。因此，需要花费 $2c_1+c_2+c_3$ 字节开销，c_1 代表密钥长度，c_2 代表 ID 字段字节数，c_3 代表 160 bit 的 HMAC 鉴别码。

4.4 BTCOLI 算法概述

为了提高检测效率以及进一步减小开销，本文结合 RBAOM 以及 BADOLI 两种算法，提出了一种基于位置信息的黑洞节点诱捕认证算法 BTCOLI，由于诱捕报文(诱捕节点是指：目的节点是网络中不存在的节点，黑洞节点接收时不进行查表即回复一跳到达该目的节点)的存在，可以只对回复诱捕报文的节点进行检测，减少了对正常路由过程中的节点的判断。该算法的流程如图 7 所示。

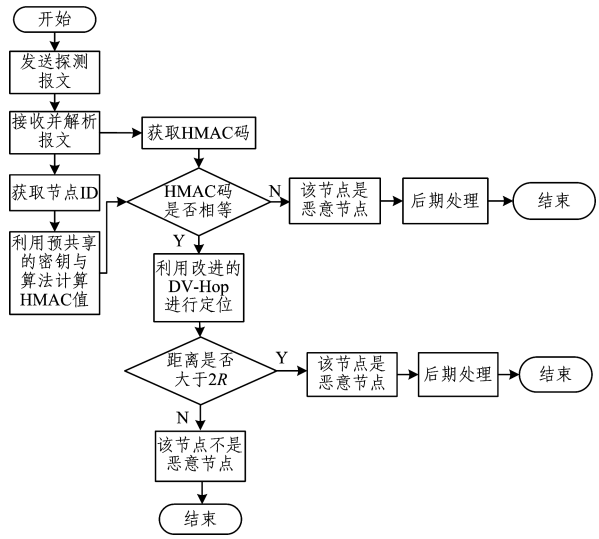

图 7 BTCOLI 算法的流程图

Fig. 7 Flow chart of BTCOLI algorithm

初始化网络时，每个节点由受信任的第三方分发两个密钥 K_1 和 K_2，同时协商所要使用的散列算法(本文中即 SHA-1 和 MD5 算法)用于身份认证过程。节点向周围发送 4.3 节所设计的诱捕探测报文，当收到邻居节点对诱捕探测报文的回复后，首先利用 HMAC 验证模块对回复节点身份进行验证，防止恶意节点冒充合法节点。解析出接收到的回复报文中的 HMAC 码，同时节点本身将报文中的节点 ID、预先分发的密钥和协商的散列算法代入式(3)进行运算，如果运算出的 HMAC 码与报文中解析出的 HMAC 码不同，则表示节点是恶意节点。如果计算出的 HMAC 码与报文中解析出的 HMAC 码相同，则表示该节点可能是正常节点，也可能是已获取了网络密钥的已妥协的黑洞节点，此时需要进行下一步

判断。首先启用改进的消除虫洞攻击的 DV-Hop 定位算法对节点自身进行定位，若计算出的自身节点与目的节点距离超过 $2R$，即可判别下一跳点是黑洞节点，通知全网对黑洞节点进行隔离。

5　仿真验证与性能分析

为了验证 4.4 节中提出的算法的有效性，本文利用 NS-2 仿真工具进行实验仿真，并通过检测成功率、虚警率、分组投递率对所提算法进行评估。

5.1　仿真参数设置

本实验中仿真参数的设置如表 1 所列。

表 1　仿真参数

Table 1　Simulation parameters

参数	参数值
拓扑大小/m^2	500 * 500
攻击节点数目	1～11
通信方式	Constant Bytes Rate(CBR)
仿真时间/s	200
包速率/(pkt/s)	2
分组负载/bytes	512

5.2　仿真结果与分析

本节对提出的 BTCOLI 算法进行仿真分析，以验证本文所提算法在检测成功率等方面的优越性。为了防止单次实验的不确定性，黑洞攻击节点的个数设置为 1～11 个，每种情况下，网络随机布置 500 次，对测量结果进行整理分析。

1）检测成功率和黑洞节点个数的关系

图 8 给出了在相同场景下，BTCOLI 算法、BADOLI 算法和 RBAOM 算法随着黑洞节点个数的增加，其检测成功率的对比图。由仿真结果可知，BADOLI 算法仅仅依据地理位置信息对黑洞节点进行检测；而利用改进的 DV-Hop 算法进行定位时，由于误差的存在，其检测成功率低下，仅仅保持在 55%左右。RBAOM 算法利用诱导报文以及信誉机制对黑洞攻击进行检测，当黑洞节点个数较少时，其由于信誉机制的存在保持了较高的检测率；当黑洞节点个数增加时，误导消息变多，正常节点的信誉阈值以及黑洞节点的信誉阈值的设置受到干扰，黑洞节点无法被检测或者正常节点被误判为黑洞节点，从而导致检测成功率持续下降。所提 BTCOLI 算法舍弃了信誉机制，结合位置信息、诱捕算法以及身份认证确保了黑洞攻击的检测成功率。由仿真结果可知，当黑洞节点不断增加时，本文算法的检测成功率依旧能够保持在 85%左右，能够成功地检测和剔除黑洞节点，保障了网络的正常运行。

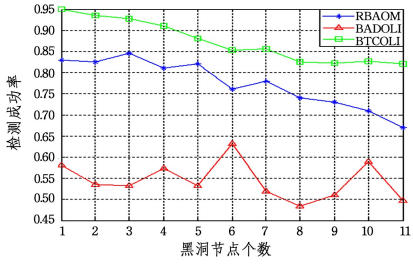

图 8　检测成功率和黑洞节点个数的关系

Fig. 8　Relationship between detection success rate and number of blackhole nodes

2）虚警率和黑洞节点个数的关系

图 9 给出了黑洞节点个数对虚警率的影响。由仿真结果可知，RBAOM 算法利用诱导报文以及信誉机制对黑洞攻击进行检测，当黑洞节点由 1 个增加至 11 个时，漏检率一直在增加，由最初的 0.02 左右持续上升至 0.1，可见信誉机制存在很大弊端。这是因为信誉机制阈值的设置存在不确定性，随着黑洞节点不断增加，伪装报文的个数也不断增加，当某个节点收到回复消息时，就会降低节点的信誉值。一旦正常节点阈值设置不佳即可能导致正常节点信誉值下降至阈值以下，从而被误判为黑洞节点。BADOLI 算法根据黑洞节点的地理位置一般大于一跳这个事实来进行黑洞节点的判断，当利用剔除虫洞节点的 DV-Hop 算法进行节点定位时，误差的存在导致了检测的不稳定性，因此其虚警率一直在 0.055 附近波动。本文所提 BTCOLI 算法在黑洞节点不断增加时，无论黑洞节点是什么形式，其由于采取黑洞行为检测以及身份认证双重保障，虚警率一直很低，不超过 0.02。

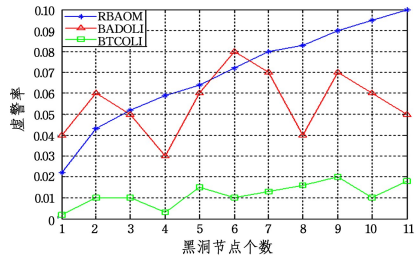

图 9　虚警率和黑洞节点个数的关系

Fig. 9　Relationship between false alarm rate and number of blackhole nodes

3）分组投递率和黑洞节点个数的关系

图 10 给出了黑洞节点个数对分组投递率的影响。在网络初始不存在黑洞节点的情况下，正常网络、RBAOM 以及 BTCOLI 算法均保持着较高的分组投递率，大约在 94%左右。但是当网络中出现黑洞节点并且黑洞节点的个数不断增加时，由于黑洞节点发起黑洞攻击，谎称自己存在一条到目的节点的捷径或者本身就是目的节点，网络流量汇聚于该节点，而黑洞节点丢弃所有的数据包，导致分组严重的丢失现象。

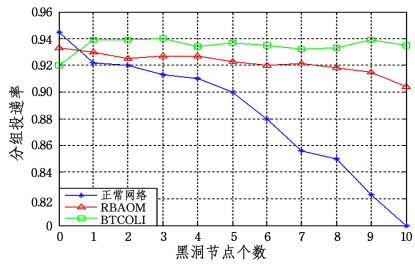

图 10　分组投递率和黑洞节点个数的关系

Fig. 10　Relationship between packet delivery rate and number of blackhole nodes

如图 10 所示，正常网络中，当黑洞节点不断增加时，分组投递率持续降低，增加到 11 个黑洞节点时，分组投递率已经降低到 80%，严重影响了网络的正常运作。RBAOM 算法能够孤立黑洞节点，一定程度上抑制了丢弃报文的恶劣行为，但

检测效率随着黑洞节点的增加而降低,分组投递率仍然存在着一定的下降趋势。本文的 BTCOLI 算法结合黑洞行为检测以及身份认证机制,优化了 RBAOM 中的检测以及防御方式,优化后的黑洞检测和防御机制可以准确地进行黑洞节点的检测和剔除。由图 10 的仿真结果可知,本文算法的分组投递率一直高于 RBAOM 算法以及正常网络,有效地降低了黑洞攻击对网络的影响。

结束语 本文针对传感器网络的黑洞攻击问题及相应的防御方法进行了深入的研究。首先,我们发现虫洞攻击下的 DV-Hop 算法的定位会产生较大的误差,因此提出了一种可消除虫洞节点影响的改进的 DV-Hop 定位算法,同时基于该改进的 DV-Hop 算法提出了基于位置信息的黑洞节点检测算法——BADOLI 算法。为了进一步提高检测效率以及减小开销,将 RBAOM 以及 BADOLI 两种算法相结合,提出了一种黑洞节点诱捕认证算法 BTCOLI,该方案增加了 HMAC 身份认证模块并结合了 BADOLI 算法,可以有效防御外部节点冒充合法节点以及内部妥协节点的黑洞攻击,因而可以提高黑洞节点的检测率、降低误检测率。最后,理论分析和实验仿真验证了所提算法在检测率和投递率方面的优越性。

针对黑洞攻击提出了一种基于位置信息的黑洞攻击的诱捕认证算法,虽然在一定程度上提高了攻击的检测率以及降低了虚警率,但还是存在些许不足,今后的研究还可以从以下几个方向展开:

1)在进行黑洞攻击的检测时,为了进行正常节点位置信息的获取,需要对 DV-Hop 算法进行改进,在消除受到虫洞攻击影响的节点时,致使一些正常节点也进入休眠状态,降低了网络的性能。下一步可以考虑在不影响网络性能的情况下,降低算法的能量开销,减少正常节点的损失。

2)本文中的基于位置信息的黑洞攻击诱捕认证算法 BTCOLI 利用定位算法以及虚假 IP 诱捕的方式等进行黑洞攻击的检测,对于攻击的检测需要进行探测包的发送,在进行探测包的发送时,会增大网络的负担。下一步可以考虑在进行黑洞攻击的检测时保证算法的性能,同时降低网络的开销。

参 考 文 献

[1] 牟思,殷虹,苏醒. 无线传感网络技术与应用[M]. 北京:中国水利水电出版社,2016:1-243.

[2] DAS S,MILLER D R,KAUFMAN Y,et al. Introduction to Wireless Sensor Networks[M]// Wireless Sensor and Mobile Ad-Hoc Networks. New York:Springer,2015:1-18.

[3] ZHANG L. Research on Wireless Sensor Network Routing Protocol Based on Energy Equilibrium[C]// International Conference on Frontiers of Manufacturing Science & Measuring Technology. 2017.

[4] KOZMA W,LAZOS L. REAct:resource-efficient accountability for node misbehavior in ad hoc networks based on random audits [C]// ACM Conference on Wireless Network Security(WISEC 2009). Zurich,Switzerland,2009:103-110.

[5] GUPTA S,KAR S,DHARMARAJA S. BAAP:Blackhole attack avoidance protocol for wireless network[C]// International Conference on Computer and Communication Technology. 2011:468-473.

[6] WAZID M,KATAL A,SACHAN R S,et al. Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network[C]// International Conference on Communications and Signal Processing. IEEE,2013:576-581.

[7] AAD I,HUBAUX J P,KNIGHTLY E W. Denial of service resilience in ad hoc networks[C]// Proceedings of the 10th Annual International Conference on Mobile Computing and Networking. ACM,2004:202-215.

[8] DENG H,LI W,AGRAWAL D P. Routing security in wireless ad hoc networks[J]. IEEE Communications Magazine,2002,40(10):70-75.

[9] AL-SHURMAN M,YOO S M,PARK S. Black hole attack in mobile Ad Hoc networks[C]// Southeast Regional Conference,2004. Huntsville,Alabama,USA,2004:96-97.

[10] SHANG X H. Research on Location Algorithm of Wireless Sensor Network Based on DV-Hop[D]. Jilin:Jilin University,2012. (in Chinese)
尚小航. 基于 DV-Hop 的无线传感器网络定位算法研究[D]. 吉林:吉林大学,2012.

[11] LAZOS L,POOVENDRAN R,MEADOWS C,et al. Preventing wormhole attacks on wireless ad hoc networks:a graph theoretic approach[C]// Wireless Communications and Networking Conference. 2015.

[12] ABDELSHAFY M A, KING P J B. Resisting blackhole attacks on MANETs[C]// IEEE Consumer Communications & Networking Conference. IEEE,2016:1048-1053.

[13] 宋成明,赵文,常浩. 计算机网络安全原理与技术研究[M]. 北京:中国水利水电出版社,2015.

[14] LI J,CHEN X,LI M,et al. Secure Deduplication with Efficient and Reliable Convergent Key Management[J]. IEEE Transactions on Parallel & Distributed Systems,2014,25(6):1615-1625.