1.介绍

无线传感器网络已广泛应用于远程环境监测和目标跟踪等领域。然而，以往的研究大多只考虑了WSN专用于单个感知任务的情况。由于数据和控制平面的紧密耦合，这种特定于应用的WSN容易产生高的工作成本、低的服务重用和硬件回收困难[15,34,60]。为了解决上述问题，研究人员将软件自定义网络(SDN)[29]和OpenFlow[36]的概念引入到传统的WSNs中，提出了软件自定义无线传感器网络(SDWSNs)[16,60]和相应的传感器流。

传感器流表抽象层是底层物理层，由一组SDWSN传感器节点组成，这些节点根据它们的传感器流表转发数据包。控制层与转发层分离，包含逻辑集中控制器，通过南向接口SensorFlow控制传感器节点。控制器还通过向北的应用程序接口(API)向应用层提供路由、安全性和其他服务。应用层根据从控制层获得的网络工作状态，实现灵活的管理策略，如位置服务、状态服务、负载均衡、拓扑管理等。

在本文中，我们将重点讨论最后两个关键问题。在安全方面，由于sdwsn引入了逻辑集中控制，实现了数据与控制平面[19]的分离，使得来自传统wsn的安全威胁进一步扩大。以选择性转发攻击为例，一旦恶意节点收到数据包，它们可能会丢弃某些类型的数据包，而不是将其全部转发到下一跳[23,41]。在SDWSNs中，传感器节点同时扮演“主机”和“交换机”的角色。因此，如果选择性转发节点发起内部攻击，如丢包等，将严重影响SDWSNs的正常运行。另一方面，SDWSNs继承了SDN架构[39]的问题。由于所部署环境的能量和能力有限，很容易对SDWSNs进行一些新的SDN攻击[28,39]。新流攻击[56]是一个典型的代表。它通过频繁地向控制平面发送新数据包而导致控制单元单点故障。以上两种攻击都可以看作是恶意转发行为。

大多数最先进的研究都集中在架构和应用程序优化上，SDWSNs中的安全问题仍处于起步阶段，并没有得到足够的重视[28]。 现有的安全性研究通常采用一些加密方法来同时考虑安全威胁[19]，架构[8]或服务[27]。 然而，这些基于密码学的机制在内部攻击的阻力方面不能很好地发挥作用[20]。 有效的传统WSN信任管理解决方案[25]主要基于耦合架构，如果不考虑SDWSN的解耦架构，也无法直接适应SDWSN。

能量约束是无线传感器网络中存在的另一个关键问题[10,54,62]。 SDWSN中的能耗也应该高度优化，因为集中控制平面需要经常收集拓扑信息以达到全局视图，这可能导致高能源成本[21,54]。 如今，SDWSN的资源利用越来越受到关注。 已经提出了许多节省路由，可靠性和网络寿命的节能方案[15,53,54]。 但是，它们主要用于安全的网络环境而不受攻击。 到目前为止，很少有SDWSN研究考虑安全性和能源问题。

在本文中，我们考虑SDWSN部署方案，如图1（b）所示。 该场景包括应用服务器，控制器，汇聚节点和许多SDWSN传感器节点。 控制器选择某些传感器节点作为聚合点（AP）来聚合报告消息[13]。 AP用于节省能量和带宽资源，还可以避免攻击者在控制路径上。 基于上述架构，我们为SDWSN提出了一种节能信任管理和路由机制（ETMRM）。 考虑到恶意转发攻击的存在，我们的目标是有效地收集网络拓扑信息并实现集中式网络管理。 据我们所知，ETMRM是第一个通过考虑安全性和能源方面来研究SDWSN的信任管理和路由机制的论文。 本文的主要贡献概括如下：

1. 我们基于扩展的SensorFlow表实现轻量级本地信任监控和评估方案，并基于扩展报告消息提出集中式信任管理机制。 通过将丢弃规则插入其邻居节点的访问控制流表，可以轻松地将内部攻击节点与网络隔离
2. 我们提出了一种节能报告消息聚合方案，以减少控制开销，最小化总报告能耗，并保证SDWSN中的控制流量传输。 通过考虑节点的全局信任级别，剩余能量级别和传输能量消耗，将AP的选择公式化为整数非线性规划（INLP）问题。
3. 我们提出了一种集中信任路由机制，共同考虑路径上节点的全局信任值和剩余能量，以保证SDWSN中的数据流量传输。
4. 我们已经实现了我们的方案的原型，实验结果表明ETMRM有效地检测和响应内部网络攻击。 与相关工作SDN-WISE相比，所提出的方案还提高了分组传送率，减少和平衡能量消耗，延长了网络寿命，并且降低了控制开销。

本文的其余部分安排如下。 第2节提供了相关工作的调查。 第3节描述了两种恶意转发攻击，并概述了我们的网络安全体系结构。 ETMRM在节点和控制器级别的信任管理和信任路由机制分别在第4节和第5节中描述。 第6节介绍了实验结果和相应的分析。 最后，第7节总结了这项工作。

2.相关工作

*2.1. 软件定义的传感器网络*

许多以前的SDWSN研究已经在架构，通信协议和网络管理方面完成[6,14,16,18,38]。 罗等人。 [34]和De Gante等人。 [12]提出了使用SensorFlow的SDWSN架构，并展示了SDN架构在无线传感器网络中的优势，例如节能和拓扑发现。 Galluccio等。 [16]介绍SDN-WISE，一种用于无线传感器网络的有状态SDN解决方案。 有状态的SDN-WISE减少了传感器和控制器之间交换的信息量，并使传感器节点可编程。 Miyazaki等人提出的系统。 [37]，曹等人。 [6]和Bera等人。 [4]证明了网络管理的灵活性和简单性。 支持SDN的无线传感器网络架构已应用于各种无线场景，如智能家居[55]，智能城市传感[32]，智能物联网（IoT）[40]，工业无线传感器网络[33]等。

能效是SDWSN的另一个吸引人的特征。 Zeng等人利用SDWSN传感器节点的动态可配置特性。 [60]在多任务SDWSN中提出了一种节能的传感器激活策略，具有保证的传感质量。翔等人。 [54]提出了一种用于SDWSN的能量偏好路由算法。他们选择具有较高剩余能量和更好位置的控制节点作为集群，然后使控制节点协调集群内节点以完成不同的任务。为了减轻信息收集的高能源成本，黄等人。 [21]设计用于环境监测应用的认知SDWSN原型。该原型使用强化学习来执行值冗余过滤和负载平衡路由，旨在提高能效和适应性。但是，上述工作主要有利于定期数据收集应用程序。王等人。 [52]提出了一种基于SDN的睡眠调度算法来管理WSN的能量消耗。廖等人。 [53]提出了一种基于多维能量空间的节能算法，以降低无线传感器网络的能量成本。王等人。 [50]在无线多跳网络中呈现SDN路由，其基于节点的剩余能量和全局拓扑视图生成最短路径。仿真结果表明，当流量负载达到一定值时，与现有算法（OLSR，AODV）相比，这种集中式路由机制可以延长网络生命周期。然而，这些节能机制假设网络是完全安全的，在当前严峻的网络情况下无法承诺。

2.2 SDWSN的安全

如今，SDWSN设计不当，仍面临许多挑战[28]，特别是安全问题[39]。一方面，SDN范式的固有特性为SDWSN带来了许多优势。集中安全措施可以在控制层和应用层上实现，不受资源限制，可以使用全局视图轻松识别恶意活动[39]。另一方面，由于解耦架构和逻辑集中控制器的引入，例如对控制平面通信和转发设备的攻击，将引入一些新的威胁[19]。此外，考虑到无线传感器网络的固有问题，例如计算和资源限制，这些新的安全威胁甚至可能导致严重的问题。然而，大多数研究人员更关注SDWSN的架构或应用方面，SDWSNs的安全性很少受到关注[28,39]。通过研究为软件定义的物联网（SDIoT）设计的机制[47]，可以反映安全问题。 Kalkan和Zeadally [26]提出了一项关于SDN技术如何为物联网环境提供安全性的全面调查。他们将文献归类为基于加密，基于网络和基于流量的解决方案。基于加密的解决方案专注于环境的加密属性，以确保安全性。 Chakrabarty和Engels [8]以及Choi和Kwak [9]提出了基于SDN的物联网安全架构，可以提供身份验证，访问控制，完整性，机密性和其他系统安全服务。虽然这些加密和身份验证安全机制可以抵御外部攻击者，但它们无法抵御来自受感染节点的内部攻击[20]。基于网络的解决方案在分层结构中使用簇头。冈萨雷斯等人。 [17]构建基于SDN和集群的新安全网络架构。在每个域中，簇头可以将路由功能和安全规则分发给每个边缘控制器。但是，它保持在架构级别，需要评估性能优势。对于基于流量的解决方案，关键方法是根据从流量流中收集的信息来检测和防止攻击。为了防御SDIoT中的新流攻击，Xu等人。 [56]通过重用控制平面上的异步消息，提出了一种具有低成本监控方法的智能安全机制。同样，Bull等人。 [5]提出了一种基于自适应流的安全机制，用于使用SDN网关的物联网设备。该机制执行流量模式的动态分析，并有效地检测基于TCP和ICMP洪水的攻击。但是，SDIoT的网络规模通常限于一跳，不需要担心来自中间节点的攻击。特别是，作为基于加密的解决方案，Khan和Hameed [27]提出了一种基于SDN的物联网框架，用于提供安全服务。 SDN控制器中的信任模块基于从其邻居节点接收的意见来计算服务请求者的信任值。该方案显示了集中信任计算的理论可行性。但是，他们并不认为底层攻击者可能会损害信任收集过程。其绩效评估也需要完成。

2.3 SDN和WSN中的信任方案

SDN，WSN和传统网络中的信任和安全措施已得到充分研究[31,43,44,58]，例如入侵检测，安全路由和安全数据。 SDN安全机制的反馈控制通常包括三个阶段：收集网络统计数据，检测网络中的异常或入侵，以及插入流规则来保护网络[43]。然而，与SDN相比，SDWSN传感器节点的能量和计算资源是有限的。因此在设计安全结构时必须考虑控制平面的可靠性，计算和通信开销[19]。作为基于密码学的安全机制的重要补充，传统无线传感器网络的信任管理和信任路由方案可以有效地抵御内部攻击者，提高系统的安全性，可靠性和公正性[20,25]。但是，它们通常基于耦合控制和数据平面[28]。每个节点以分布式方式做出信任决策和路由[23]。每个节点都是“自己世界的中心”[48]。这与SDWSN的集中管理无异。因此，并非所有SDN和WSN解决方案都可以组合并适应SDWSN模型[28,39]。为了保证真正安全的SDWSN，安全性必须固有地构建在SDWSN架构中[39]。在[38]中，讨论了传统无线传感器网络的一些集中式网络管理方法。其中之一，Hunkeler等。 [22]提出了一种智能，可管理，高效且可靠的互联网工作架构（IMPERIA），这是一种用于大规模无线传感器网络的集中管理架构。 IMPERIA表明，无线传感器网络管理的集中方法是分布式协议的有效替代方案。为了降低能耗并提高无线传感器网络的可靠性，Sharma和Jena [45]使用聚类和多路径技术设计了一种节能路由策略。该策略基于通过将更多责任转移到接收器来减少传感器节点上的负载的原理。这类似于SDWSN的概念。 Tajeddine等人。 [46]设计CENTERA，一种基于集中信任的高效路由协议，具有适用于WSN的认证方案。该系统中的每个节点周期性地将其邻居列表及其分组转发经验发送到基站（BS）。使用加密机制，路径上的每个节点都解密并验证来自源节点的签名。然后，BS基于其分组转发率来评估每个节点的可信度。 CENTERA可防止重播，修改和冒充攻击。然而，正如[1]中所分析的那样，CENTERA无法完全抵御已经拥有密钥和身份验证信息的受感染合法传感器节点发起的内部攻击。 CENTERA中的节点也不够智能，无法做出隔离行为不当节点的决策。每个中间节点处的加密和解密还在路由发现期间引起过多的计算和能量开销。此外，CENTERA并非专为SDWSN设计。由于固定的上行链路和下行链路路径，网络灵活性受到限制。当存在恶意转发攻击者时，它没有考虑邻居信息收集过程的安全[28,39]和能效[54]问题。

3. ETMRM概述

在本节中，我们首先讨论两种恶意转发攻击。 然后，介绍了我们提出的架构的设计目标。 最后，我们概述了提议的ETMRM方案。

3.1。 对SDWSN的恶意转发攻击

3.1.1。 选择性转发攻击

传感器节点具有有限的通信能力和低计算资源。因此，每个节点都是一个弱势实体，很容易受到攻击者的攻击[49]。如图2（a）所示，在多跳无线网络中，选择性转发攻击是受到攻击的节点通过恶意丢弃转发数据包的子集而发起的威胁，从而恶化网络的数据包传输率[41]。如果攻击者丢弃某些类型的数据包，则称为Greyhole攻击;如果攻击者丢弃所有数据包，则称为Blackhole攻击[23,58]。与WSN相比，受损节点对SDWSN的正常运行更有害。如图2（a）所示，在集中控制SDWSNs中，

•如果攻击者丢弃了收到的数据包，则会损坏数据流量的传输。

•如果攻击者丢弃了收到的报告数据包，则控制器无法接收这些节点的最新状态并验证它们是否仍然存活。因此，控制器将被错误地更新错误的网络拓扑视图，然后做出错误的路由决策。

•如果攻击者放弃规则请求或响应数据包，请求者将不会设置流规则并成功处理传入的数据包。当一定数量的节点受到损害时，网络的运行将陷入瘫痪。

在传统的WSN信任机制中，基于看门狗，MAC层重传率和ACK方法[23]，这些选择性转发攻击可以通过相应的信任排序规则消除不信任节点在一定程度上得到解决[58]。但是，如2.3节所述，这些信任机制主要依赖于来自每个节点的分布式信任决策，并且由于解耦特性和集中管理而无法直接适应SDWSN。

3.1.2 新流量攻击

如图2（b）所示，由于不匹配的数据包将被发送到控制器，攻击者可以通过向其邻居节点注入新数据包来启动新流攻击[56]。邻居节点无法区分合法和非法流量，然后将新的数据包以Packet-In（规则请求）格式封装给控制器。通过这种方式，攻击可以轻易地将大量恶意流量编入网络，并消耗整个网络的大量带宽和能量。不幸的是，与WSN相比，认证和反重放保护方案无法完全防止SDWSN中的这种攻击。这是因为受损节点可以通过使用其合法身份充斥新数据包来轻松启动攻击。此外，SDWSN的控制平面不如SDN的控制平面强。当SDWSN的控制链路拥塞时，正常的网络操作将被破坏，大多数服务将被终止。通过故意将大量恶意流量转发到邻居节点，此攻击也可被视为恶意转发攻击。 SDWSN的相应措施需要考虑传感器节点的有限能力和资源。

3.2。 设计目标

我们的ETMRM旨在同时实现以下目标：

高安全性： 能效：为了消除副作用并保证定期拓扑信息收集的安全性，需要提出一种节能报告消息安全聚合方案，以减少控制开销，保护控制流量的传输。

3.3。 系统总览

为了清楚地理解信任，我们采用如下信任定义[24]。

定义1.（信任）。 信任被定义为一个传感器节点根据先前的行为观察将特定动作放在另一个节点上的信任 等级。 信任值用于反映传感器节点是否愿意并且能够在WSN中正常行动。 如图3所示，在ETMRM中，信任可以分为本地信任和全球信任。 本地信任基于对直接沟通的观察。 它反映了两个邻居节点之间的信任关系。 全局信任由集中信任系统根据从整个网络收集的本地信任信息计算。 它反映了对控制器视图中每个节点的信任评估。

通常，ETMRM在节点和控制器级别利用网络功能。 在节点级，我们将SDWSN传感器节点不仅视为简单的SDN转发交换机，还将其视为具有自身安全功能的单个主机。 每个节点都可以利用扩展的SensorFlow表轻松监控和记录其邻居节点的转发和性能行为。 因此，基于过去成功和不成功的交互，每个节点可以通过轻量级 获得其邻居节点的通信信任值。 然后，通过对通信信任值和性能信任值进行整合，可以得到每个邻居节点的本地信任值。 为了消除本地直接信任[24]中的不准确性，本地信任值将作为网络拓扑报告消息[13,16]的一部分发送到控制器，这使控制器能够构建网络的安全视图。

在控制器级，控制器首先基于收集的信任信息计算每个节点的全局信任值，并进行异常值检测。 全局信任值小于阈值的节点将被视为不受信任的节点（标记为恶意删除攻击者或新流攻击者）。 通过 为了节省能量和带宽资源并且还保护控制流量的传输，将选择具有大信任值和高剩余能量的某些传感器节点作为AP来聚合拓扑报告分组。 最后，考虑到传感器节点的剩余能量和信任级别，控制器可以联合建立可信路由。

4。ETMRM设计：节点级别

在本节和以下部分中，我们将分别描述ETMRM在节点级别和控制器级别的信任管理过程。 首先列出了ETMRM中使用的假设和符号。 然后介绍信任监控，评估和报告流程。

4.1。 假设和符号

对于ETMRM架构，我们做出以下假设：

•网络是静态的并且是随机部署的。 每个传感器节点都有唯一的标识符。 所有传感器节点都是同质的。

•汇聚节点和控制器始终受信任，并且具有无限的能量和计算能力。

•需要时，可以通过加密技术验证来自控制器的消息或流规则。 每个节点都可以与控制器共享对称密钥，以避免伪造消息。

•链路是对称的，网络足够密集，因此每个传感器节点可以在其无线电范围内具有多个单跳邻居节点。

•好的

表1中列出了本节中使用的表示法，其中“表示法”列包含变量的名称，其定义显示在“定义”列中。

4.2。 信任记录

本文中使用的拓扑示例如图4（a）所示。网络中有九个节点，其中节点E和D是AP，节点A是攻击者。控制器位于汇聚节点中。我们将在节点E的视图中解释流表的主要组件。

如图5所示，我们使用行为记录扩展SDWSN的流表。表0用于实现访问控制。攻击者的数据包将立即被丢弃。我们将SensorFlow的流表拆分为数据流表和控制流表，以便分别处理数据和控制流量。 Total计数器表示从规则建立时间到现在的匹配数据包总数。我们使用新的Interval计数器进一步扩展数据和控制流表中的计数器。对于每个流条目，间隔计数器代表t期间相应匹配分组的数量。 Data \_ S，Ctrl \_ S，Data \_ U和Ctrl \_ Ucounters分别表示每个流条目的成功或不成功转发的数据包的数量。

4.2.1。 通讯记录

在两个传感器节点之间的通信期间，当处理该流的每个分组时，将更新匹配的流条目的相应计数器。如果下一个\_ hop neighbor节点不是流的目标节点，则该节点将侦听每个数据包的转发行为。我们以数据流表的第二个流表项（表1）为例。如图4（a）所示，当节点N E已经经由N B向N C发送N G的分组时，N E的信任系统将监视N B的转发行为。假设，每个节点可以通过共享的双向无线信道进行通信，并以混杂模式运行[30]。如果NE听到NB正确转发了该数据包，则数据*Data* \_S将被添加1.如果NE在节点NB的预定时间内没有听到该数据包的重传，或者没有该数据包的数据包输入消息由于规则未命中，或者如果窃听数据包是非法制造的（通过比较附加到数据包的有效负载）[30]，它会认为这种交互不成功并添加数据*Data* \_ U 1.我们可以看到这个在每个t期间实现转发记录。在每个间隔结束时，Interval计数器的数量将被添加到Total计数器，然后将被清除为0.控制流表以相同的方式工作，除了一些控制包类型，例如Beacon，Broadcast转发计数器是不必要的。

4.2.2。 表现记录

对于新流攻击，如2.2节和2.3节所述，可以通过身份验证或反重放保护机制检测和过滤那些伪造身份的数据包。 但是，他们无法抵抗具有合法身份的这些恶意数据包。 因此，我们设计了一个数据包输入记录表，以防御来自这些受损节点的新流攻击。

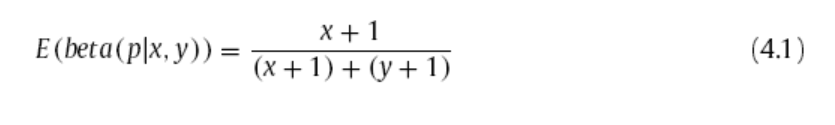
当节点N E从其邻居N A接收新流并且新分组的源地址是N A时，这将导致N E生成一个发给控制器的发送 请求。 然后节点N E将表3中相应的间隔计数器加1，如图5所示。 这实现了邻居节点的分组发送行为的统计。 类似地，在每个周期t结束时，该值也被添加到Total计数器然后被清除为0.考虑到一些节点可能具有大量监视和传输任务，控制器可以将白名单分发到它们的邻居节点以避免误报。

4.3。 本地信任评估

如图3所示，本地信任(LT ij)由通信信任(CT ij)和表现信任(PT ij)组成。考虑到数据流量和控制流量在网络运行中发挥着不同的作用，将通信信任分为相应的数据和控制流量转发信任，分别为CTD ij和CTC ij。如图4 (b)所示，每个节点在每个 t的末尾计算其邻居节点的局部信任值，如下所示。

4.3.1。沟通信任

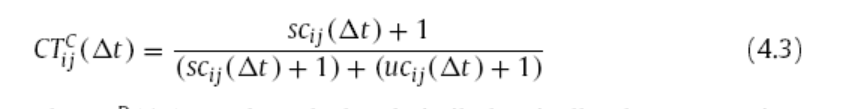
对于节点N i, CT ij (t)反映了它的邻居N j在最后t中的转发诚实度。为了计算该信任值并考虑资源受限的SDWSN节点，我们使用了一种流行的轻量级信任管理机制——贝叶斯信任模型[58]。如式(4.1)所示，贝叶斯理论利用概率命运函数(p | x, y)的期望E ((p | x, y))来得到声誉得分。p表示二进制事件(x, y)和0≤p≤1的后验概率。x和y分别表示积极和消极的相互作用。这个后声誉值E (beta (p | x, y))被解释为未来的最大可能性。



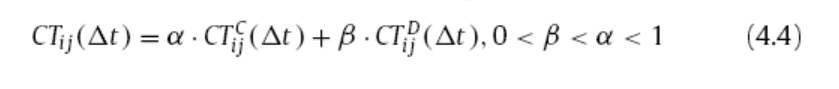
在接下来的部分中，我们以控制流量转发信任的计算为例。对于节点N i s的邻居节点N j，通过搜索流N j需要转发的控制流，可以得到每个t中sc ij (t)成功交互的次数。这包括其下一跳 nj但nj不是目标地址。我们使用一个流条目集fej 来重新发送它们。利用扩展区间计数器，由式(4.2)可得sc ij (t)。用同样的方法可以得到不成功相互作用uc ij (t)的次数。



因此，在交互成功和失败的基础上，由式(4.3)推导出相邻节点j在最后t时刻的CT C ij (t)。



CT D ij (t)的计算方法与此类似。最后,沟通信任CT ij过去t (t)可以通过式(4.4),加权因子α和β和α+β= 1。设置α大于β,因为控制数据包的损害比普通数据包更严重。



4.3.2。表现信任

正如3.1节所讨论的，一些受攻击的节点可能不会丢弃其邻居的数据包，而是向它们发送了太多的恶意数据包(new-flow attack)。因此，PT ij (t)用于测量在最后一个t期间的转发性能。对于节点N 的邻居N j，利用图5所示的分组记录表，由式(4.5)计算性能信任PT ij (t)。Fτ是一个节点可以从一个邻居在t时间 接收新流的最大数量,。它能适应实际的网络工作环境。inl j是对应区间计数器的值，其默认值为1。

发送的新流越多，计算值就越低。当invl j达到Fτ/ 2和N j不在白名单,安全系统的节点Ni将数据包发送警告它的邻居节点N j。如果节点nj仍然发送新流，且PT ij (t) < 1，则节点将向控制节点发送攻击报告。



* 4.3.3。本地信任

将通信信任和表现信任两种转发信任进行集成，利用式(4.6)计算本地信任值LT ij (t)。在现有的工作中，信任值可以是0到1(4字节)之间的实数，也可以是0到10(0.5字节)之间的整数。正如[30]中所讨论的，这对于无线传感器网络来说是至关重要的，因为无线传感器网络的内存有限，传输和接收能力也有限。为了减少内存和传输开销，我们将它设置为0到100之间的无符号整数。它只需要1字节的内存空间，不会丢失太多的精度。



LT ij (t)反映了节点N i的意见对节点N j的信任评价，可用于预测未来节点N j的行为。通过重复这些计算，我可以得到它的所有邻居节点的本地信任值。其他节点也可以以同样的方式执行，以获得它们自己的计算。

* 4.4。信任的报告

4.1.1。新报告消息

通过对转发行为的观察计算本地信任。如果两个节点之间没有直接通信，则无法计算本地信任。此外，如果受到无线干扰或恶意攻击的影响，可能会偏离实际值[24]。在传统的WSNs中，一些基于声誉的信任管理模型将其他邻居节点的推荐信息引入到信任评价中[3,20]。虽然这些方法可能在一定程度上纠正了本地信任，但是它们很容易受到周围恶意恶意攻击节点的影响。此外，收集和人工老化的许多建议需要额外的能源消耗。为了提高资源效率，减少信息交换的开销，我们取消了[30]中提出的每个节点之间的反馈。从集中管理策略的角度来看，这些本地信任值将被报告给控制器，以获得更准确的全局信任值。如图6所示，我们在节点发送给控制器的SDN WISE报告消息中添加了邻居信任信息字段。对报告消息的这个小修改将避免引入额外的传输开销。

4.4.2. 简单报告

在SDWSNs的集中控制中，控制器在存在恶意转发攻击的情况下，如何有效地从网络中收集报表消息是控制器面临的关键挑战。一种简单的方法是让所有节点向整个网络广播报告消息。我们称之为简单广播。另一种方法是在SDN-WISE[16]中使用网络拓扑发现(TD)协议。控制器定期通过接收器节点广播TD数据包。这个包包含控制器的标识。它到接收器的当前距离初始化为0。当节点N i接收到距离sink较近的邻居节点nj的TD数据包时，它会将nj更新为下一个跳向控制器的节点，并将这个TD数据包的信息广播出去。完成拓扑发现后，每个节点都可以通过下一跳向控制器报告其当前邻居列表。我们将这种方法命名为简单报告。定期清除SDN-WISE的邻居列表。所以这个过程需要定期执行。

* 1. 开销分析

通过上述信任记录、信任评估、信任报告的过程，传感器节点完成对相邻节点的信任观察、计算，最后将信任信息报告给控制器。

在信任记录过程中，数据和控制流表可能需要额外的内存空间来存储扩展的计数器。如图5所示，对于每个数据或控制流条目，它只需要另外两个间隔计数器(Dat a \_s, Dat a \_u)或(Ctrl \_s, Ctrl \_u)。针对SDWSNs的低速率网络环境，每个间隔计数器至少可以是8位(1字节)。因此，考虑到一般的流表至少有O (n 20)字节[16]，其中n是流条目的数量，这个额外的O (n 2)字节不会占用太多内存。

在信任评价过程中，不需要进行复杂的数学计算。因此，它适合于资源和能力有限的SDWSN环境。然而，在信任报告阶段，这些报告方法面临以下两个主要问题。

1. 高能源消耗。很明显，简单的广播方式会在报道阶段引发一场广播风暴。在每个拓扑发现期间，还必须向整个网络广播简单的报告方案。为了传递报告消息，它将消耗平均O (N h)传输时间，其中h是到控制器的平均跳数。他们的通信开销和能源成本相当高
2. 高丢包率。这两种方式都不能保证当存在恶意转发攻击时，所有的报告消息和其他控制流量都会到达控制器。它们可能在开始时工作得很好，或者在受损节点很少的时候工作得很好。然而，随着攻击者的增加，传输过程变得不可控制，网络流量的传输率将急剧下降。

因此，为了克服以上问题，我们将提出一种降低通信和能源成本的解决方案，同时保证控制流量的交付。

1. ETMRM设计:控制器级

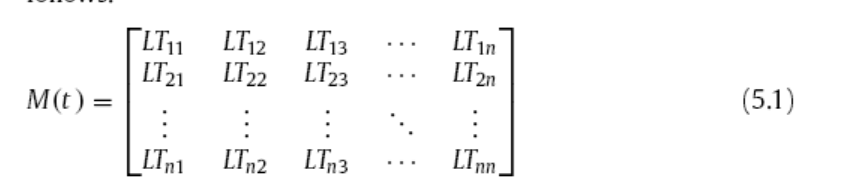
在本节中，我们将在控制器级描述ETMRM的信任管理和信任路由过程。我们首先列出本节中使用的符号。然后引入集中式信任评价模型，提出了一种高效节能的报告消息聚合机制，解决了上述两个关键问题。最后，设计了信任隔离方案和信任路由方案。

5.1。符号

表2列出了本节中使用的符号。

5.2。集中式的信任评价

在网络的初始阶段，没有攻击者，或者攻击者很少。因此，控制器可以在每个t结束时通过简单的广播或报告机制收集具有本地信任值的网络拓扑信息。控制器构建网络图G = (V, E)其中V为节点集，E为边集，| V |为传感器节点数。然后构造局部信任矩阵M (t)。



LT ij是节点ni到相邻节点nj的本地信任值，其中i, j [1, N]， N = | V |。为了保持公平性，放弃了对自己的信任价值LT ii。M (t)的列向量LT ij > 0,我们获得一组本地信任值包含意见节点N j s邻居节点N, s j = {LT ij, LT kj,···, LT mj}。因此，在全局视图中，计算节点nj的一种直接方法是对sj的值求平均值，如式(5.2)所示。



然而，正如在[41,42]中所讨论的，这个平均声誉值T j很容易受到恶意攻击的提升或降级的影响。为了识别和分离这些虚假的信任意见，人们提出了许多WSNs的离群点检测机制[61]。在这里，我们采用了一种通用的方法，就像在[41]中预先设置的方法一样。基于最初的平均值T j,标准差σj信托集合S计算j。



标准差阈值相比στ[41],如果σj≤στ,我们认为信任推荐N j从它的邻居节点是一致的,我们有全球信任值T j = T。另一方面，对节点nj的信任建议是可疑的，可能与恶意攻击相结合。最大偏差的LT ij将被删除，然后从剩下的值里面重新计算信任值T j，直到σj≤στ。然后，我们有tj = tj。考虑到强大的存储和计算能力，控制器中的全局信任值T j是介于[0,1]之间的实数。

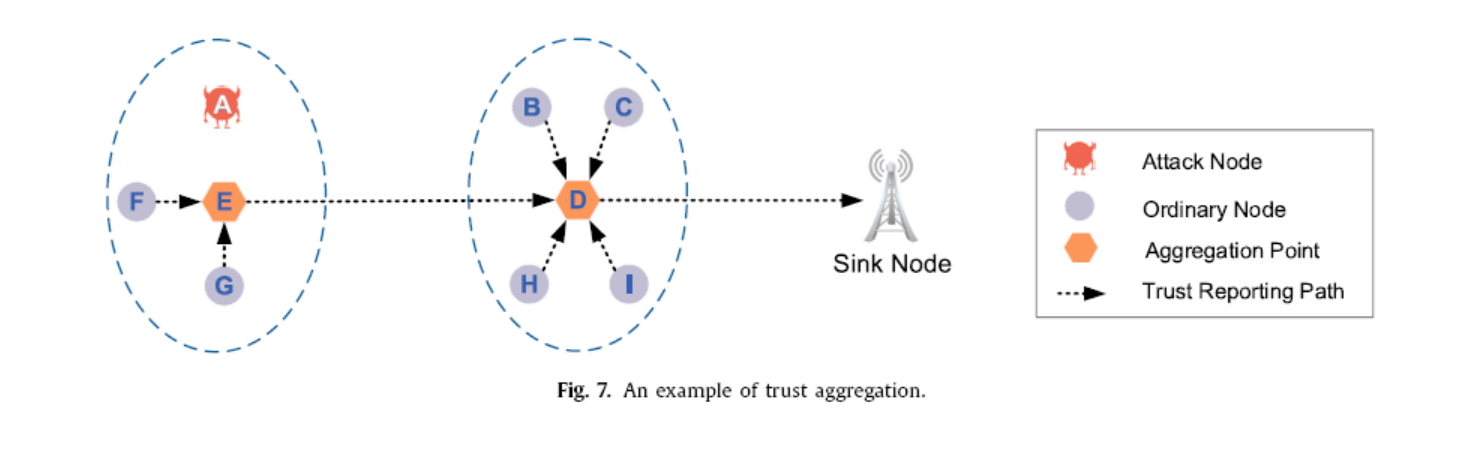
如果T j小于一定信任阈值Tτ,N j将判断恶意节点。如果控制器接收到许多来自N j的新流请求和来自其邻居节点的某些指控，那么它将成为一个新流攻击者。否则，它将是一个选择性的包转发攻击者。在正常的网络管理中，无论攻击类型如何，它都被视为不可信节点，不被考虑。

5.3。信任聚合

如4.5节所述，简单的广播和报告方法可能导致严重的能源消耗和高丢包率问题。此外，随着攻击者的增加，网络流量将变得不可控制。为保护控制流量的传输，平衡网络能耗，延长网络寿命，提出了一种适用于SDWSNs的节能报告消息聚合(ERMAS)方案。

5.3.1。聚合问题构想

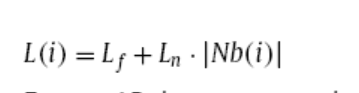
AP选择问题:给定一个存在恶意转发节点的网络，找到作为汇聚点的节点子集，目标是最小化报告能耗，同时保证报告交付。



为了说明这一点，我们给出了一个基于图4所示网络拓扑结构的ERMAS实例。如图7所示，将均匀的传感器节点分别划分为普通节点和APs节点。普通节点具有相同的通信半径。在信任报告阶段，普通节点需要将它们的邻居报告消息连同信任信息发送到它们的APs。APs是具有较高剩余能量和可信度的传感器节点。与为基于SDN的智能电网[51]设计的APs类似，APs也用于辅助普通节点与控制器之间的信息交换。但是与WSNs[30]中常见的集群不同，APs不需要分配任务，也不需要向域内的成员提供信任反馈。

APs首先对邻居节点的报告消息进行聚合，然后将其发送给控制器。为了估算两个节点之间通信的能耗，ERMAS中可以采用自由空间无线电台模型(d2功耗)、多径衰落信道模型(d4功耗)[54]、传感器节点的真实数据表等能耗模型。因此，在报告阶段，普通节点E ON (i)的能耗可由式(5.4)计算。L (i)由一个固定长度的报告包头lf加上它的邻居列表的长度得到。邻居列表的长度由一个邻居信息长度L n乘以当前邻居编号| Nb (i)|计算。Etx为发送每比特所消耗的能量。





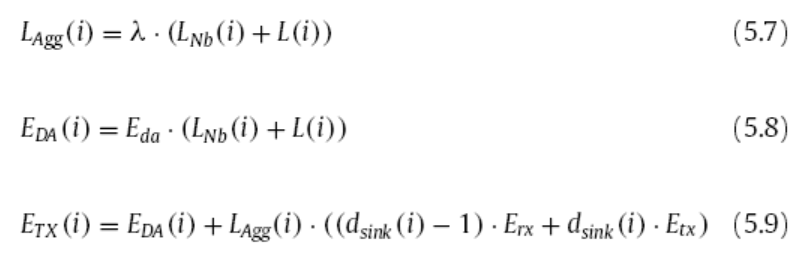
对于AP，在汇聚过程中，其能量消耗E AP (i)与接收和传输能量相结合，如式(5.5)所示。



其接收能耗E RX (i)与其所有邻居节点报告消息lnb (i)的长度近似相关，由式(5.6)计算得到。

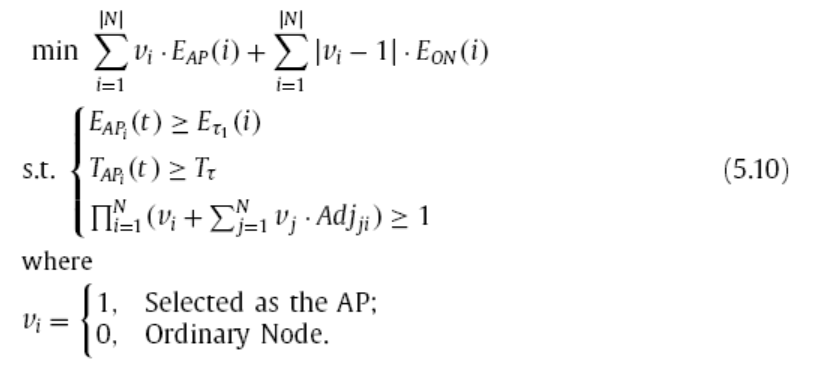


用它的报告消息聚合和报告它的邻居节点的报告消息可以减少数据包的大小和转发的次数。通过Eqs计算了聚合数据包长度和数据聚合能耗。(5.7)及(5.8)。λ为ap节点的压缩率，Eda为压缩1bit的能量然后将汇总的报表包通过d sink (i)乘以传输发送到sink, d sink (i) 1乘以接收通过中继APs发送到汇聚。



由式(5.9)可知，总传输能量消耗E TX (i)可由AP i的数据汇聚能量成本和AP在汇聚路径上的传输能量消耗之和来计算。

最后，优化目标如式(5.10)所示，我们的目标是找到合适数量的高质量APs，以最大限度地降低整个网络的报告能耗。不同位置的APs能耗不同。我们设置阈值（AP节点i在t时刻的剩余能量阈值 = \*节点i的邻居节点在t时刻的平均剩余能量），它的平均剩余能量水平依赖与它的邻居节点。由于节点能量的消耗，节点能量随时间的增长而自适应调整。考虑到安全问题，亚太地区不仅应该拥有更高的剩余能源，而且应该拥有更大的全球信任价值。随后，最后一个约束意味着所有的正常节点要么在AP集中，要么与AP集中的一些邻居节点相邻。这种关系用于确保所有的普通节点(受损节点除外)都能被AP覆盖。



当网络规模较大时，直接求解上述整数非线性规划问题比较困难。候选AP集可以减少可行节点的搜索范围。在当前时刻t，如果节点N i具有比平均水平更高的剩余能量和更大的全局信任值，则节点N i是候选AP。此外，考虑到控制器具有无限的计算能力，可以采用多种启发式算法来解决上述问题。例如，为了研究软件定义嵌入式系统中的任务调度问题，Zeng等人[59]将任务完成时间最小化问题作为一个混合整数非线性规划(MINLP)问题来考虑。针对这一复杂问题，提出了一种三阶段启发式算法。在[2]中可以找到更多的解决方案。

5.3.2。聚合点的责任

在设置阶段，控制器将使用源路由方案所选的APs。然后APs广播由控制节点签署的选举公告。当普通节点N i接收到多个广播通知并被多个AP覆盖时，它将选择剩余能量最高的AP，成为其AP成员。然后N i向它所选的AP发送一个join-in消息，该AP将设置与聚合相关的流规则。其他控制消息，如规则请求，普通节点也可以转发到它们的APs来聚合和转发它们。由于攻击者没有入侵网络，且在攻击开始时没有节点受到攻击，只要ERMAS选择可信的APs，就可以保证报告消息和其他控制流量的传递。事实上，攻击者有可能会破坏AP。这将导致控制流量的丢失。在这种情况下，受攻击的AP将利用本地信任评估机制被其邻居节点快速检测到。每个邻居节点将执行以下步骤:

如果它直接连接到汇聚节点或被多个APs覆盖，它将向汇聚节点或那些APs交付信任报告。

如果它有到控制节点的下一跳，它将向下一跳节点交付信任报告。如果它无法到达控制节点，则只广播信任报告。如果它有办法到达控制节点并从其他节点接收信任报告，它将帮助它们转发报告。

控制器将利用接收到的报告信息替换此恶意AP。还可以为每个AP域分配额外的影子聚合点(Shadow Aggregation Points, SAPs)，以监视所选AP的输入和输出流量。

此外，与普通节点相比，APs承担了更多的聚合报表消息和转发规则请求和响应包的责任，因此APs的能耗将大于普通节点。在这里，我们讨论两种方法来避免APs能源的过度消耗。首先，控制器根据APs的报告消息不断地监视APs的剩余能量。当AP剩余能量小于相邻节点平均剩余能量的一定程度时，控制器利用当前图G和ERMAS对AP进行局部旋转。控制节点部分地替换了相应的APs。另一种方法是，当控制节点观察到某些APs具有较低的剩余能量时，它进行全局AP旋转。

5.4。信任隔离

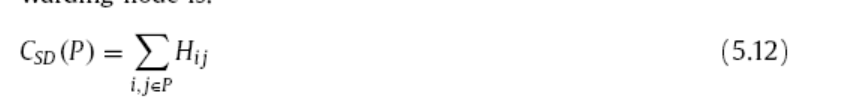
与分布式信任机制不同，该控制器对全局信任评估检测到的不可信传感器节点进行集中响应。如果恶意节点是一个普通节点，控制器需要发送像< src \_ ad dr = j, action = drop >到它的邻居节点这样的drop规则。但是，如果控制器只是向整个网络发送广播，或者向每个受影响的节点发送多个单播，就会浪费大量的能量，无法保证传输。提出了一种降低AP广播能耗的最小AP广播机制。以一个不受信任的节点nj为例，利用图G和全局信任评价方法，建立了它的受害者邻居集VN (nj)，这些都是正常节点，每个AP s邻居集Nb (AP i)。将选择AP广播集B (AP i)，其中| B (AP i)|成员最少，覆盖所有受害邻居节点，如下所示。

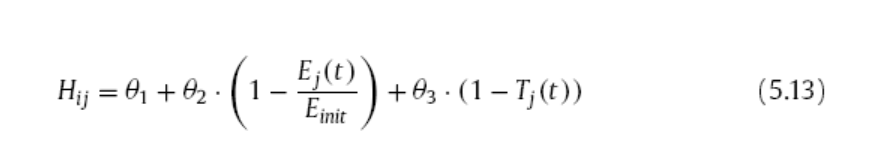


这些控制消息将由控制器签名并发送到集合B (AP i)中的APs。集合中的APs将广播签名消息，然后这些受害邻居节点将drop规则插入到它们的访问控制流表中，如图5所示。它们还将清除数据和控制流表中的规则，以避免将数据包转发给攻击者。一旦攻击者是AP节点，控制器就会执行与ERMAS类似的额外的本地AP旋转。如果上述解决方案失败，控制器将作为最坏的情况进行整个网络广播。

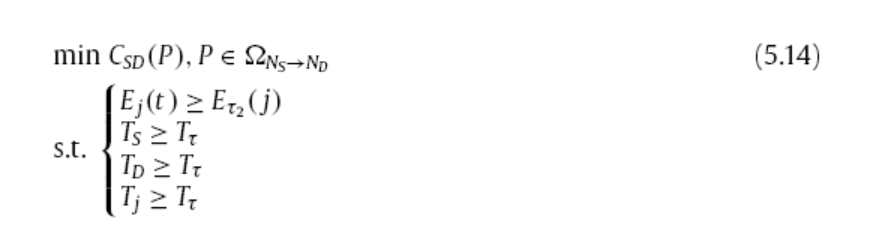
5.5。信任的路由

当源节点N S希望与目标节点N D交流,但它不知道路径节点N D,或它不知道如何处理一个从它的邻居节点到ND新的合法流,它通过Aps将规则请求消息发送到控制节点。控制节点接收规则请求时,它首先检查是否请求者是一个潜在的新的流攻击者,然后决定是否执行安全路由算法。高可信节点将保证数据包的交付。剩余能量越高的节点转发数据包的能力越强。因此，在本工作中，我们考虑路径上节点的信任值和剩余能量，设计了一种安全可靠的路由机制。对于从N S到N D的候选路由路径P，用Eqs计算其路径代价C SD (P)。(5.12)和(5.13),H ij是一个单结合度量函数从路径节点N i N j和<θ1、θ2θ3 >是规模的系数每个因素的影响。可以看出，nj的信任值越大，剩余能量越大，则H ij越小，选择节点nj作为转发节点的可能性越大。





如式(5.14)所示，路由确定问题表示为选择路由代价最小的路径。由于节点在关键位置的能量消耗较快，节点应满足能量约束条件，以保证路由路径的可靠性。我们设置阈值Eτ2 (j) =τ2·E v g (j)τ2可以自适应地调整位置。和节点的全局信任值低于阈值Tτ将被忽略。



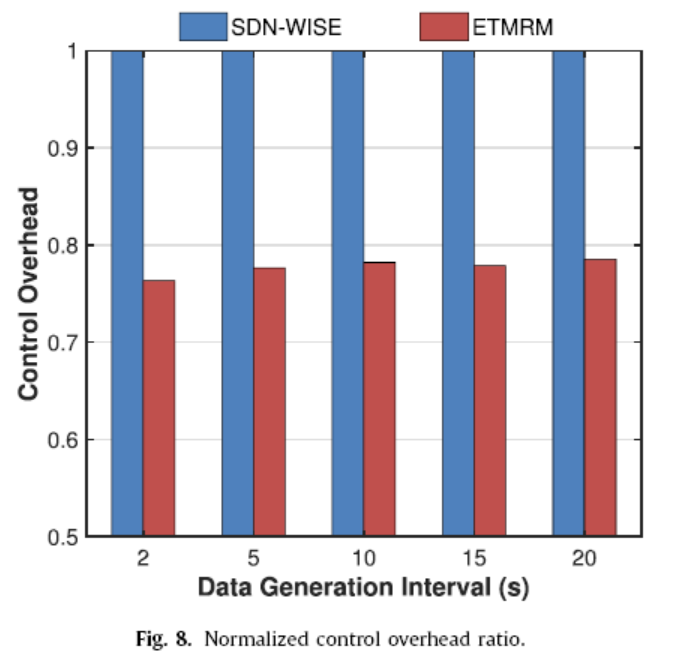
为了解决这个问题，如算法1所示，我们首先去掉不满足上述约束的节点，得到约简后的网络图G。每一个环节的权重都是间接计算出来的。最后，利用Dijkstra算法求出G中的最小路由代价路径。路由路径的构建可以通过将控制消息基于之前选择的APs发送到源节点ns来构建。控制消息可以像SDN中的OpenFlow一样简单地包含下一个跳节点。此外，与源路由机制一样，它还可以维护完整的转发节点，以减少请求的数量。在这里，我们采用前者来遵循开流的原则。当网络安全形势恶化时，也会使用后者。

6. 实验

6.1。实验设置

基于SDN-WISE项目[7]，实现了一个ETMRM原型系统。每个SDWSN节点都使用一个基于轻量级贝叶斯的可信模型。数据平面采用改进后的Cooja平台实现，该平台是由Contiki 2.7[11]中提出的一种面向物联网和WSNs的开源操作系统，并与控制器提供通信接口。该控制器运行在配备英特尔(R)核心(TM) i7-6770HQ CPU和32GB DDR4内存的台式计算机上。将ETMRM的集中式信任评估、隔离、路由和聚合机制作为新的模型在控制器中实现。我们进行了几个仿真实验来测试我们的解决方案在大规模网络下的性能。为了模拟无线传感器网络设备的实际能耗，我们使用横河WT310数字电能表测量了德州仪器CC2530在1 dBm输出功率下的能耗。测量结果与其他实验参数如表3所示。我们随机地在网络中部署100个初始能量相同的传感器节点。节点向同一网络中的其他节点随机发送数据包。我们将数据包生成间隔设置在2到25秒之间，以评估ETMRM和SDN-WISE在不同工作负载下的性能。我们使用伪随机机制为两种方案生成相同的目标地址。首先，我们比较了ETMRM和SDN-WISE在正常网络环境下的控制开销、网络寿命和能量分布等方面的性能。此外，针对不同的选择性转发攻击和新流攻击的攻击者数量，我们根据包投递率、检测率、能耗等指标，将ETMRM与SDN-WISE进行了比较。

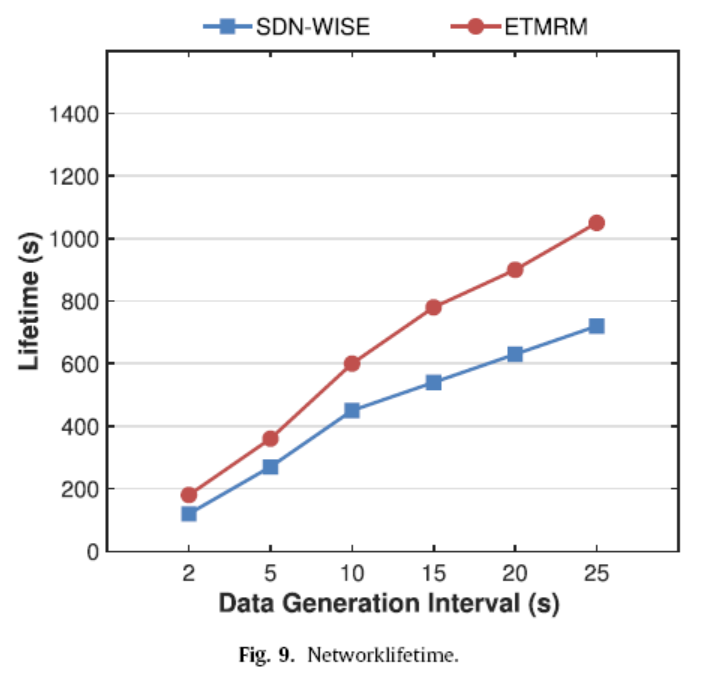
6.2。控制开销



控制开销由控制包与网络中所有包的比值来定义。两种方案的归一化控制开销比如图8所示。在不同的数据生成间隔下，与SDN-WISE相比，ETMRM平均减少了22.3%的控制开销。换句话说，对于相同数量的数据包，ETMRM生成的控制数据包比SDN-WISE少。这是由于SDN-WISE需要通过整个网络工作单独交付每个节点的每个报告、请求或响应包。另一方面，ETMRM聚合网络中的定期报告消息和其他控制包，并通过有效的AP路径交付它们。从而减少了网络中控制包转发的数量。控制开销越小，传输过程中的控制能耗也就越小。这也有利于网络生存期。

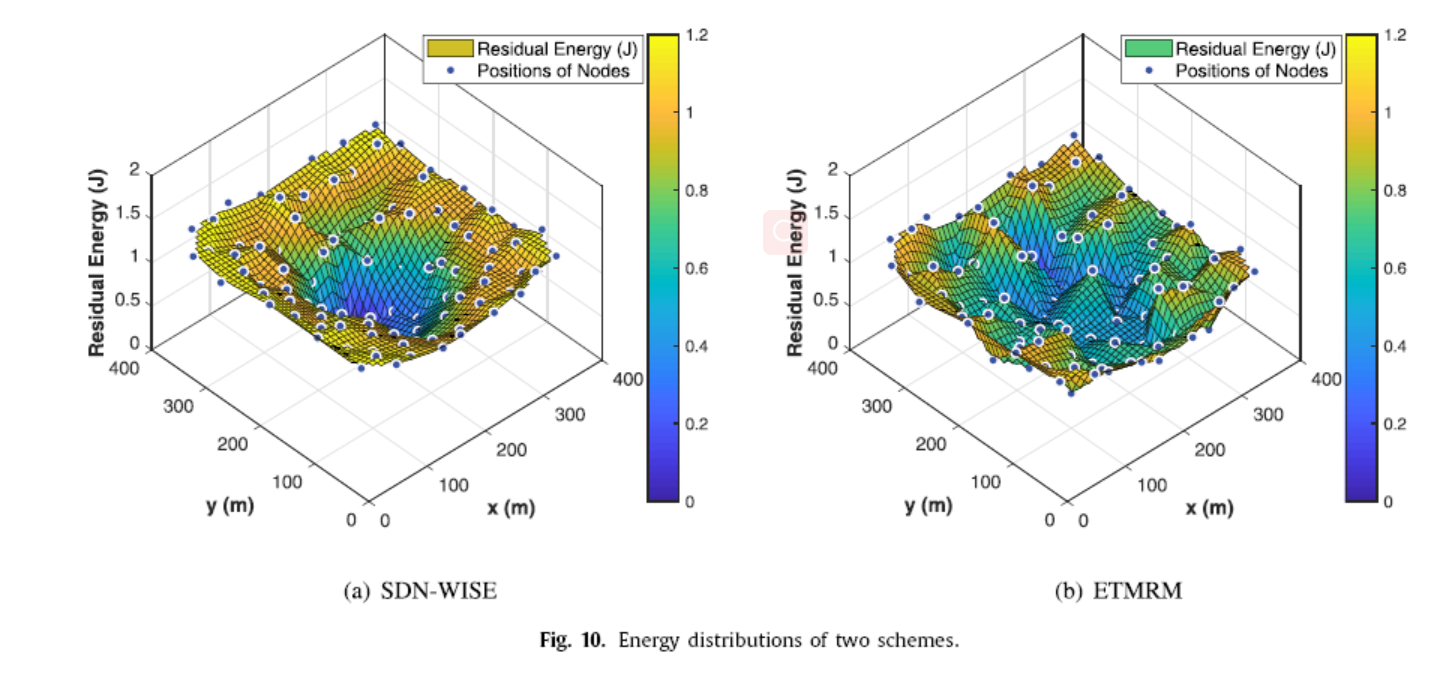
6.3。网络生命周期

耗尽能量的传感器节点将会死亡。网络的生存期定义为第一个节点死亡时间。图9为两种方案在不同数据流量下的网络寿命。数据传输、接收、聚合和备用功耗基于表3中列出的参数。可以看出，当数据间隔较小时，两种方案的网络生存期都较小。这是因为频繁发送数据包也会导致大量来自中间节点的控制流量。关键点上的节点会很快耗尽能量。但是，随着数据间隔的增加，我们可以看到ETMRM的生存时间逐渐优于SDN-WISE。这是因为ETMRM的ERMAS大大降低了控制开销，节省了传输开销。AP旋转机构平衡APs的能耗。此外，该控制器利用全局视图的优点，绕过关键位置的低剩余能量节点，实现了能量感知路由，降低了节点的开销，节约了节点的能量。因此，与SDN-WISE相比，ETMRM的网络寿命延长了33.3%，达到了50%。



6.4。能量分布

如图10 (a)所示，汇聚节点附近存在一个较大的能量孔，节点剩余能量最低。这是因为SDN-WISE的传感器节点需要通过控制路径向控制器发送周期性报告消息等控制数据包。控制器附近的节点被迫转发这些数据包，这将很快消耗掉它们的能量。而在ETMRM中，能量消耗比SDN-WISE更加均衡，如图10 (b)所示，其原因是剩余能量较高的APs将承受这些转发压力，通过聚集控制流量来降低能量消耗。此外，控制器的监控机制可以及时调整这些剩余能量较低的APs。能量感知路由方案还减少了汇聚点附近低剩余能量节点的转发任务，节约了节点的能量。因此，能量孔在一定程度上被揭示出来。



6.5 选择转发攻击

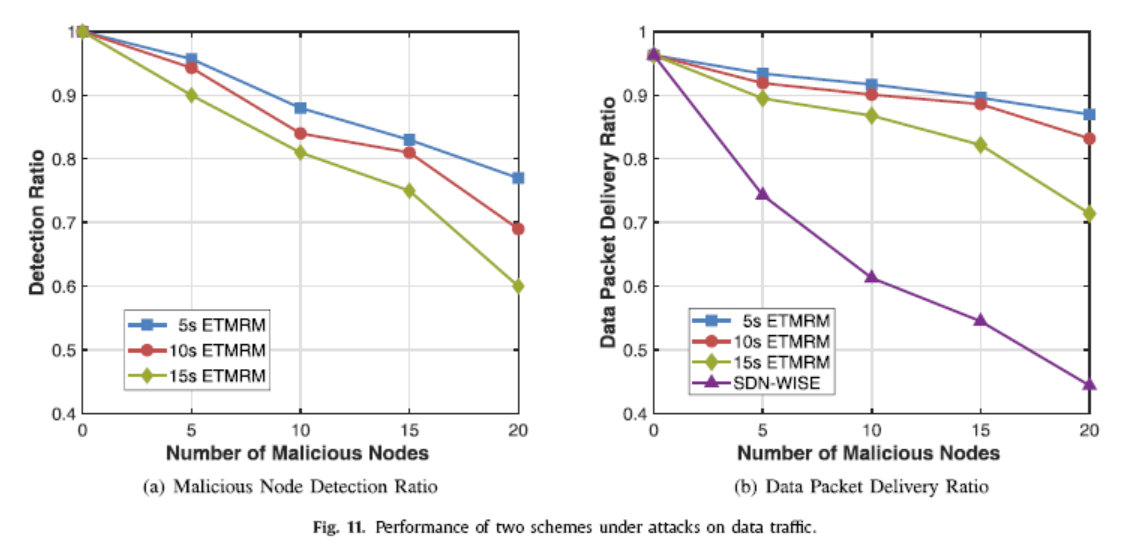
为了比较ETMRM和SDN-WISE对恶意攻击的抵抗能力，我们在不同的攻击类型和工作负载情况下进行了一系列实验。与攻击和信任机制相关的实验参数如表4所示。

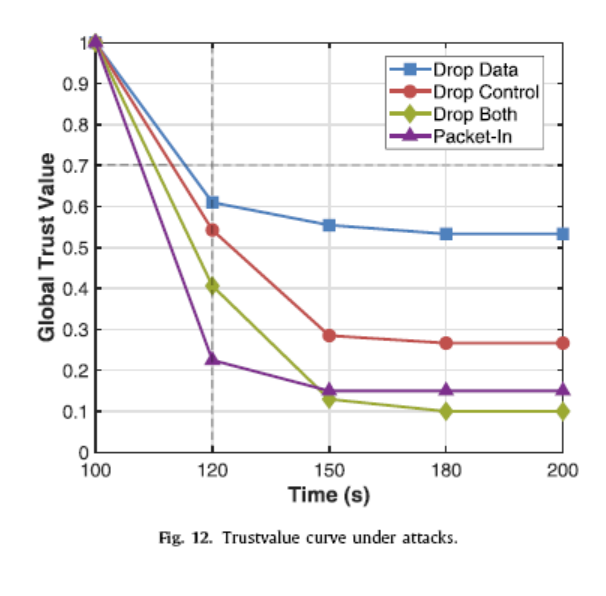
仿真时间设置为300 s，报告周期设置为30 s。我们分析了这两种方案在100秒和200秒之间的性能。将每个传感器节点的初始能量重置为5j，随机选择攻击节点。

6.5.1。对数据流量的选择性转发攻击

首先，我们测试了对数据流量的选择性转发攻击，攻击者将在其中丢弃接收到的数据包。这种攻击可以称为对数据流量[23]的灰洞攻击。如图11 (a)所示，随着恶意节点的增加，ETMRM的平均检测率逐渐降低。这是因为控制器将更难检测到大量报告受污染的攻击者。但是，当数据生成间隔变小时，检测率逐渐增大。这是因为数据生成间隔越小，两个节点之间的交互就越多。因此，节点将有更多的机会监视和评估其邻居节点是否是攻击者。当数据生成间隔为10 s时，图12显示了在没有提出信任隔离机制的情况下，每个报告时间的选择性转发攻击者的信任值曲线。我们看到全球Grey-hole攻击者的信任值数据流量将低于Tτ很快。总的来说，只要节点之间通信频繁，当恶意攻击者小于20%时，ETMRM的检测率可以高于77%。由于缺乏安全机制，SDN-WISE无法检测到恶意节点。

如图11 (b)所示，随着恶意节点的增加，SDN-WISE的平均包投递率急剧下降到44%。但是，当数据生成间隔为15s时，ETMRM保证了至少71.4%的包投递率，其中攻击节点20个。这是因为在前几轮报告期间，检测到的恶意节点将很快与网络隔离。利用最小AP广播机制，它们的邻居节点将接收drop规则，不再将数据包转发给它们。

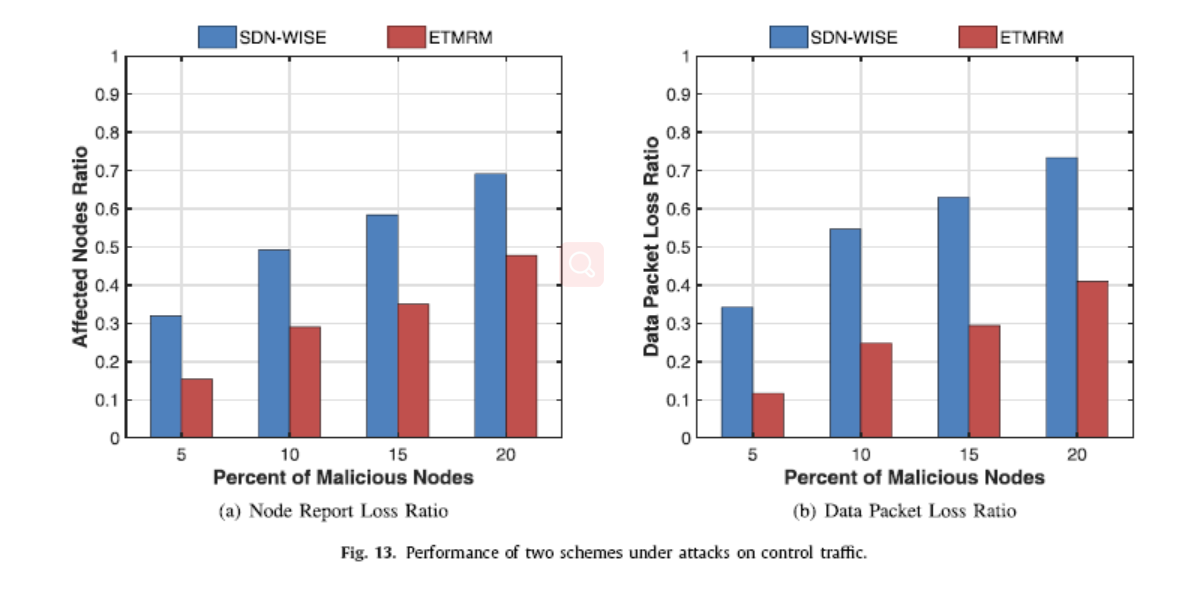




6.5.2。控制流量的选择性转发攻击

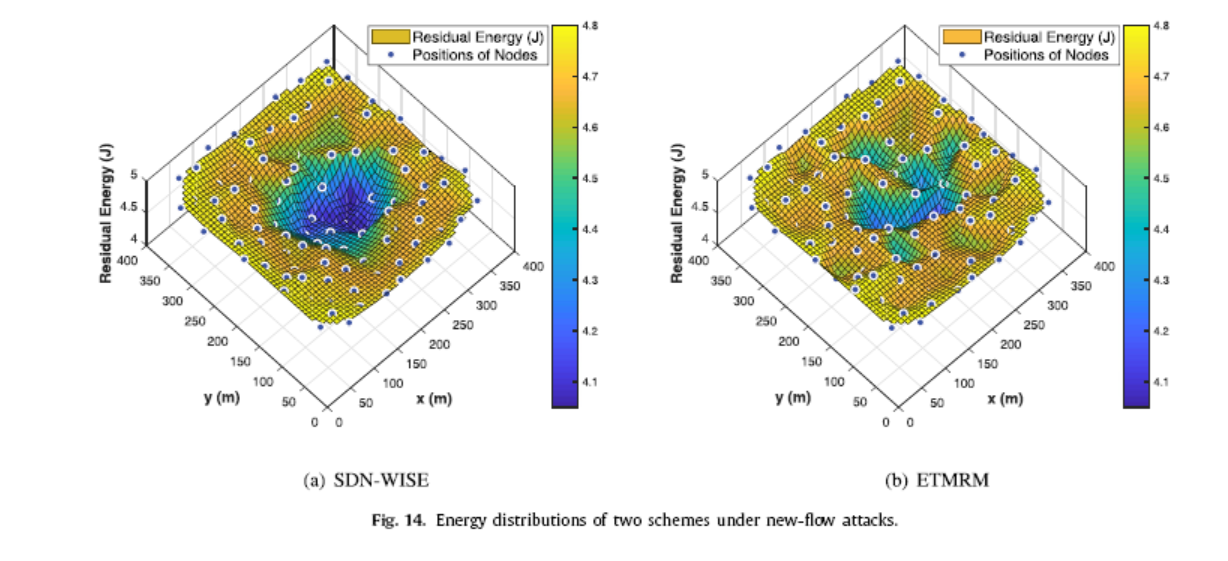
与SDN-WISE不同，ETMRM中的控制流量主要由APs转发。在一个有100个节点的传感器网络中，APs的数量在15到20之间。为了更好地进行比较，我们使用5%到20%之间的百分比来表示控制流量攻击者的数量。

删除控制包将影响网络的正常拓扑收集和规则设置操作。如图13 (a)所示，随着攻击者百分比的增加，故意丢弃报表包的节点的比率也在快速增长。在sdn中有20%的恶意节点，将近70%的报告包将丢失。这是因为在拓扑发现阶段，攻击者很容易通过谎称自己具有较高的剩余能量水平和与sink更近的距离来吸引控制流量。控制器无法获取底层节点状态，将影响路由决策。如图13 (b)所示，这种攻击也会导致数据包丢失率的增长。这是因为攻击者不仅删除报表包，还删除规则请求和响应包。在sdn网络中，当攻击者的百分比为20%时，数据包传输将中断73.4%。从图11 (b)可以看出，在SDWSNs中，对控制流量的攻击会比数据流量对网络造成更严重的破坏。在ETMRM中，如图13 (a)和(b)所示，当20%的APs被破坏时，47.7%的报告包和41.1%的数据包将受到影响。然而，这只发生在第一个报告期(100 s -120 s)，因为报告期t设置为30 s。虽然AP负责控制流量的转发，但一旦被本地信任模型判定为恶意节点，其成员和邻居APs将通过其他可选方式向控制器发送报告包。图12所示,其全球信任值的控制器将低于Tτ迅速在120年代报告时间点。此外，如果AP成为黑洞攻击者，同时丢弃数据和控制流量，那么到120秒时，其全局信任值将迅速下降到0.41。因此控制器可以利用全局视图和接收到的信任评估报告来检测错误行为AP，并将其替换为新的高信任AP。

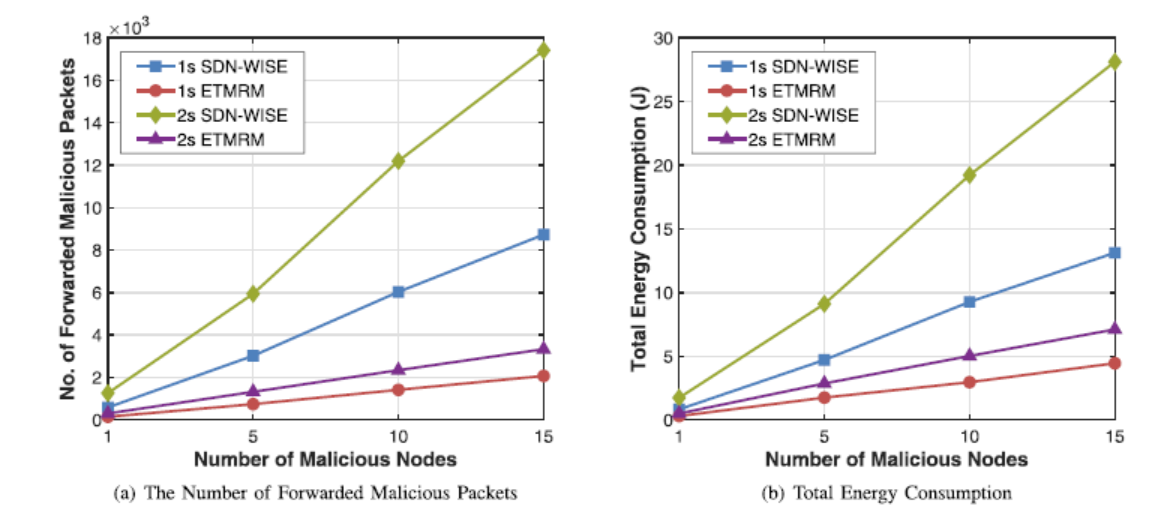


6.6。新的流攻击

我们首先测试一个位于{270 m, 230 m}位置的新流攻击者，攻击速率为2包/秒，攻击时间从100秒到200秒。正常的数据生成时间间隔设置为10年代和Fτ= 10。如图14 (a)所示，新流攻击者还在其周围形成一个能量洞，其邻居节点的剩余能量远低于平均水平。这是因为新流攻击者将向其邻居节点生成过多的新流，并导致频繁地向控制器发出包入请求。因此，与选择性转发攻击相比，这种攻击会对网络造成更严重的能量消耗破坏。但是，我们的方案可以在一定程度上缓解能量空洞现象，如图14 (b)所示。当控制器收到邻居节点的某些指控时，这个新流攻击者的全局信任值在120秒时急剧下降到0.23，如图12所示。然后它将立即与网络隔离。



此外，如图15 (a)和(b)所示，我们可以看到，随着sdn网络中新流攻击者和攻击率的增加，转发恶意包的数量和整个网络的总能量消耗迅速增加。但是，如上所述，攻击者将很快从ETMRM中的网络中隔离出来。因此转发的恶意数据包的数量要比sdn中的小得多。ETMRM的总浪费能量也小于SDN-WISE，如图15 (b)所示。



7.结论

SDWSNs同时面临着安全问题和能源效率问题。针对恶意转发行为选择转发攻击和新流攻击的特点，建立了一种高效的SDWSNs信任管理和路由机制。首先对传感器节点的流表进行扩展，实现了节点级的轻量级信任监控和评估方案。利用收集到的信息，提出了一种控制器级的集中式信任管理机制，用于检测和隔离恶意节点。然后设计了一种节能的报表消息聚合方案，以降低能耗，保证控制流量的传输。基于路由需求和全局安全状态，提出了一种考虑节点剩余能量和信任值的安全路由机制。实验结果表明，该体系结构能够有效地检测和响应恶意转发攻击。与SDN-WISE相关工作相比，该机制提高了数据包的传输率，降低和平衡了能量消耗，延长了网络寿命，降低了控制开销。