基于信任的无线传感器网络安全路由研究

邓黎黎,刘才兴
(华南农业大学 信息学院,广东 广州 510642)

摘 要:通过分析无线传感器网络安全路由受到的攻击,以及对应的防御手段,提出了目前安全路由协议存在的主要问题。以信任研究为出发点,克服现有的安全路由协议的不足,从信任关系的角度设计无线传感器网络的安全路由协议,并且根据安全路由的安全目标,给出了基于信任的安全路由协议的设计的框架模型以及基于信任的安全路由的基本要求和设计原则。最后对无线传感器网络中基于信任的安全路由技术的研究进行了展望,提出了研究进一步发展的方向。

关键词:无线传感器网络;安全路由;信任模型;信任
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2010)06-0159-04

Research of Trust-Based Secure Routing Protocols for Wireless Sensor Networks

DENG Li-li, LIU Cai-xing
(College of Informatics, South China Agricultural University, Guangzhou 510642, China)

Abstract: The current situations of wireless sensor network security protocols, the existed problems were presented. Then the attacks which wireless sensor networks may suffer and the main defense means are summarized. The paper is concerned on the design of the routing protocol based on the trust to conquer the disadvantage of the existed protocols. After researching of the current trust-based routing protocols, give a detailed introduction to the model of the trust-based security routing protocols and the design principles. In the end, a panoramic view and detailed analysis of future trust-based security routing protocols for wireless sensor network is given.

Key words: wireless sensor network; security routing; trust model; trust

0 引 言

无线传感器网络(Wireless sensor network)是完全面向应用的以数据为中心的网络,在军事、监控和检测领域的应用越来越广泛,对 WSN 研究的关注和投入也愈来愈大,尤其是路由协议的研究与改进是目前的研究重点与热点。随着 WSN 中的关键性、敏感性数据传输任务以及在敌对的、无人值守环境中工作的应用场景日益增多,研究者设计路由协议时就要充分地考虑传感器节点的安全性、所选择路径的安全可信性。设计适合某些场景的可信安全路由算法决定着 WSN 具有更好地发展前景,有较大的实用价值。

1 WSN 安全路由的研究

在早期为 WSN 设计的路由协议主要以能量高效为目的,没有考虑节点的安全问题[1]。目前国内外不少研究者从节省能量、高效稳定等角度对无线传感器网络路由协议进行了较深入的研究与探索,也产生了不少对典型路由协议的改进成果[2],但是这些改进策略没有充分地考虑所形成路径的安全可信性,不能很好地适应 WSN 的某些安全应用场景。

1.1 WSN 安全路由的攻击和防御

WSN 的安全威胁主要来自攻击者的各种攻击行为,可以来自外部或内部[3]。现有的传感器网络路由协议容易受到的攻击如表 1 所示。

表 1 现有的 WSN 路由协议容易受到的攻击

路由协议	容易受到的攻击
TinyOs 信标	伪造路由信息,选择性转发,污水池,Sybil 攻击,虫洞攻击,Hello 泛洪攻击
定向扩散	伪造路由信息,选择性转发,污水池,Sybil 攻击,虫洞攻击,Hello 泛洪攻击
地理位置路由	Sybil 攻击,伪造路由信息,选择性转发
分簇路由协议	选择性转发,Hello 泛洪
能量节约拓扑维护协议	伪造路由信息,Sybil 攻击,Hello 泛洪攻击

在实际中,外部攻击者和内部攻击者常常同时存

收稿日期:2009-10-06;**修回日期**:2010-01-15
基金项目:国家高技术研究发展计划 863 计划项目(2006AA10Z246)
作者简介:邓黎黎(1985-),女,硕士研究生,研究方向为无线传感器网络安全路由;刘才兴,教授,研究方向为嵌入式与网络信息安全。

在,为了保障安全路由或将攻击限制在一定的范围内,研究人员已针对不同的攻击方法提出了不同的防御策略。针对表 1 中的各种路由协议受到的攻击,能够采取相应的对策,如表 2 所示。

表 2 WSN 攻击的解决办法

攻击	解决方法
外部攻击和链路层安全	链路层加密和认证
Sybil 攻击,Hello 泛洪攻击	身份认证 双向链路认证
虫洞攻击,污水池	比较难以防御,必须在设计路由协议的时候考虑
选择性转发	采用多路由技术
认证广播和泛洪	基于密码技术的广播认证

1.2 WSN 安全路由研究现状

针对路由安全问题,国内外的研究的文献近两年越来越多。SPINS[4]是较早的传感器网络安全框架,SPINS 分为 SNEP 和 μTESLA 两部分。TESLA 用于进行广播认证,SNEP 实现了数据机密性、数据认证、完整性和新鲜性保证等功能,描述了安全实施的协议过程,没有实际使用路由算法。有安全意识的路由 SAR[5]的思想是找出真实值和节点之间的关系,然后利用这些真实值生成安全的路由。INSENSE 入侵容忍路由协议[6],致力于为异构的、资源受限的传感器网络建立安全有效的基于树结构的路由,它的一个重要特点就是入侵容忍策略,即允许恶意节点(包括误操作节点)威胁它周围的少量节点,但威胁被限制在一定范围内,解决的办法是冗余机制。国内研究者也提出了多种安全路由方案[7~16],研究方法各有不同,一部分研究是基于已有的路由协议的改进[10~14],一部分是针对多种攻击设计新的安全协议[15,16],其中有不少关于考虑能量问题的安全路由协议,以及改进分簇路由协议,增加必要的安全机制的路由协议。

综上所述,当前在 WSN 路由安全领域的研究主要集中在两大方面:一是根据 WSN 资源受限的特点,针对已知的 WSN 及 Ad Hoc 路由协议建立攻击模型[3],以改进已知 WSN 路由协议的安全性或者改进已知 Ad Hoc 路由协议的性能,以适应 WSN;另一方面是设计新的适合于 WSN 的安全路由协议。结果导致一方面在复杂性、能量损耗和安全性等方面难以平衡,一般都侧重于强化某些性能,而以牺牲其他性能为代价;另一方面,一些安全路由协议是在现有路由协议基础上增加了安全机制,这使得在设计上增加了成本,使终端资源受限的 WSN 网络难以实现。这种基于抵御的安全模式无法满足网络连通性、动态性的需求,最重要的是,它本质上是一种附加、被动的防范方式,难以抵御那些具有隐蔽性、随机性、传播性的智能化攻击,未能解决网络安全脆弱性的本源问题[17]。于是,产生了信任管理以及信任模型的概念,并且将信任模型充分应用于 WSN 的簇头选举、安全路由等支撑技术中。

2 基于信任的 WSN 安全路由

信任管理在解决 WSN 中的内部攻击,识别恶意节点、自私节点及低竞争力节点,提高系统安全性、可靠性和公平性等方面有着显著优势。

已经有比较多的文献提出了无线传感器网络的安全路由的信任管理框架。TRANS(Trusting Routing for Location Aware Sensor networks)协议[18],为以数据为中心的传感器网络提供安全路由框架。该协议以基于地理位置的路由协议(如 GPSR)为基础,基于信任来选择安全路径和避开不安全的区域。目标节点使用具有松散时间同步特性的 μTESLA 协议来认证、查询消息,基于初始的认证,每个节点为其邻居节点设置初始的信任值,消息经过全部由可信节点组成的路径到达目的节点。

Crosby 等人[19]将信任引入到簇头选举中,并采取冗余策略和挑战应答(Challenge - Response)手段,用来降低泄密或者恶意节点被选择为簇头的概率,尽可能地保证选举出的簇头节点为可信节点,对于不可信的节点,挑战测试失败后加入黑名单列表,节点不再对其进行信任值更新。基于信誉的信任管理框 RFSN (Reputation - based Framework for Sensor Networks)[20]通过维护邻居节点的信誉来评估它们的信任程度。RFSN 以分布式方式运行在每个节点的中间层,在网络中不存在一个中心节点用来进行信誉的存储。作者在 RFSN 框架内,使用贝叶斯理论和 Beta 分布来进行信誉的表示、更新和整合,并设计了一个完整的系统。

Cheng 等人[21]提出一个基于信任模型安全路由机制 TRUSTEE。通过修改路由协议,使目的节点在接收到数据包时回复,参与路由的各节点以及源节点如果收到了回复包则认为邻居节点转发了数据包,增加其信任值,能够选择满足安全需求的最可信的路径。

张静等人在文献[22]中提出把网络的安全状态视为路由选择的度量之一,通过分析通信实体的安全机制和安全威胁来测量链路和节点的信任度,建立节点间的信任关系,并基于该信任模型定义和量化一种新的安全度量 SM(Security Metric),提出以 SM 为选路标准的安全路由算法 SMRA(Security Metric based Routing Algorithm),尽量避开不安全节点和链路,提高了网络传输率,可扩展应用于大规模网络的安全路由。但是为机密应用绕道选择更安全路径时,可能会相应增

加数据传输的路径跳数和延时等开销。

一种基于簇首节点的可信传感器网络路由协议 TRPBCH(Trusted routing protocol based cluster head for wireless sensor networks)[23]和基于信任的 LEACH 协议 TLEACH[24],采用网络分层思想,将安全检测工作分担到各层的簇首节点中,各层采用分布式的聚类算法,选举各层的簇首节点,对解决条件受到较大限制的 WSN 路由感染十分有效,它能有效地隔离问题节点,解决路由感染问题,提高了有效发包率,改善网络的安全性。降低了所有节点均要维护安全检测的系统代价,又消除了基站的安全瓶颈,使整个网络的能量均匀分布,延长了网络寿命。还有将节点可信度与群体智能优化算法结合[16],在路由中引入节点可信度,作为信息素的一个分配策略,类似 MPLS 的一个可信安全标签,建立可信安全路由,对目前尚无有效抵御办法的 Wormholes 攻击,效果显著。

文献[25]考虑节点与所选路径本身的可信度对信息传输安全性的影响,基于主观逻辑模型及节点可信度评价,提出了一种可信 LEACH 路由算法 TLEACH-BSL(Trusted LEACH routing algorithm based on subjective logic),该算法实现了分簇路由算法中节点及路径选择过程的可信度衡量,在稍微牺牲传输延迟的情况下,提高了数据包的成功到达率,保证了数据传输的安全性,适用于传输延迟要求不太严格、但数据传输安全性要求高的应用场景。

基于信任的安全路由算法利用信任模型及相关的信任管理技术解决 WSN 中节点间信任关系的建立、维护和管理问题,通过信誉机制规范分布式路由中节点行为,从而达到识别恶意节点,鉴别自私或低竞争力节点的效果。目前基于 WSN 安全路由的信任管理系统的研究着重于对"信任"进行量化评估,建立网络节点中的信任关系,并将网络中节点的所有相关信息量化,包括对被评估节点的行为观察、与被评估节点的交互记录以及其他节点的意见等,采用适当的计算模型得到对方的信任值,用信任值进行最合适的路由决策,提高网络的安全性、健壮性。

3　基于信任的 WSN 设计原则

文中在综述现有的基于信任的 WSN 的安全路由算法的基础上,给出了一个基于信任的 WSN 安全路由的结构框架,如图 1 所示。

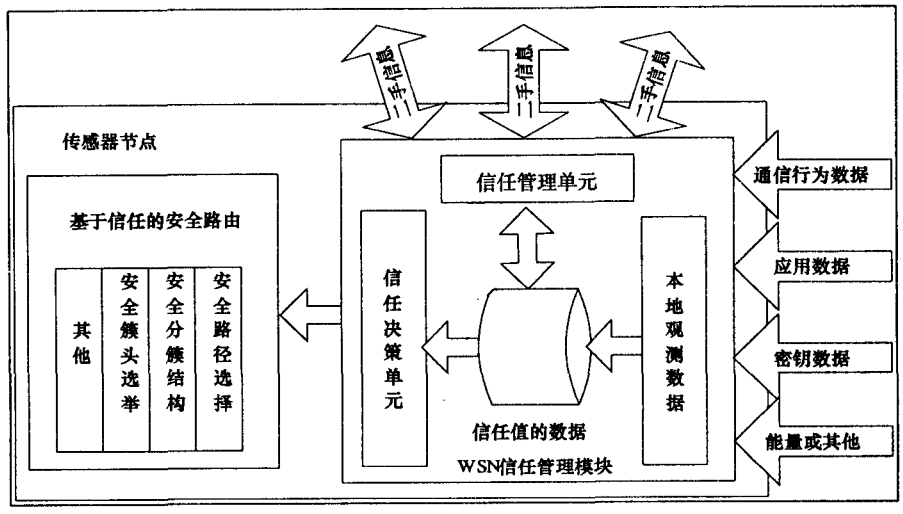

图 1　基于信任的 WSN 安全路由框架

由于无线传感器网络资源有限且与应用高度相关,针对 WSN 资源有限、节点通信和计算能力有限、传感器节点数量大且分布范围广、网络动态性强、以数据为中心等特点,认为基于信任的 WSN 安全路由算法设计应该满足以下原则和特点:

(1) 基于信任值计算的准确性。引入信任模型的实质是基于动态累积的客观事实执行信任评估,并根据评估结果执行基于信任的路由决策,以保证路由的安全性和有效性。包括对信任因素的提取、信任值的计算方式、信任阈值的设置以及信任值的更新等。

(2) 负载均衡。信任值根据节点的历史行为或者上下文环境共同决定,因此在通信过程中可能带来的存储、通信开销会大量消耗节点的资源,造成网络的负担。因此必须考虑在保证安全的基础上采用轻量级信任计算模型,保证网络资源不被迅速的消耗,平衡节点之间的负载,从而达到保证网络寿命的同时实现路由的安全。

(3) 容错性和可生存性。WSN 容易发生故障。无论是平面式路由、层次式路由,或者是以数据为中心的路由,要能够保证在网络发生故障时,要尽量利用节点易获得的网络信息计算路由能够很快的恢复。

(4) 安全性。无论网络环境怎样的恶劣,要求 WSN 管理体系结构能够确保节点之间的管理信息和数据进行安全的交换,考虑信任模型本身可能带来的风险因素,建立健壮的信任模型,不仅要能够抵御外部的攻击,还需要能够识别网络中存在的恶意节点。

4　结束语

由于传感器节点资源有限,而信任值的收集需要

很大传输能耗，所以在其他网络环境下常用的基于信任的信任管理系统迄今为止并没有在 WSN 中占据主导地位，很多系统也是对已有的系统进行简单的修改，有针对性地抵抗某些路由协议容易受到的几类攻击，。提高该类路由协议的安全性和可靠性。WSN 环境下的基于信任的安全路由有以下主要发展方向：

(1) 设计更适用于 WSN 的信任模型。从信任因素的获取、信任值的计算更新以及信任决策等方面根据 WSN 具体路由协议的需要重新设计轻量级的信任模型，也可以针对 Ad Hoc 网络或者移动自组织网络已有的模型做出改进，以适用于 WSN 的应用。将基于信任值的评价方式同其他的安全策略相结合，充分完善安全路由协议，考虑多种安全手段的有机统一，实现路由协议安全性的无缝接轨。

(2)传感器网络的许多应用场景要求多个基站协同工作，并且基站和节点可能都是移动的。而目前传感器网络的研究均是基于单基站，并且基站是静止的以及节点固定不动，这些研究不能够使用多基站和节点移动的应用场景。研究多个移动基站的传感器网络的路由和安全问题是非常必要的。

(3)基于能耗的考虑，充分利用现有 WSN 分簇路由协议的思想，从信任的角度对网络进行分簇，对网络实现分层信任管理，将整个网络的安全分配到每个簇，减少基站的安全负担，从而平衡整个网络负载，延长网络寿命。

因此，考虑安全约束、可信度评价对路由算法的影响，设计一些安全可信路由算法，能够更好地适合 WSN 的某些高机密或高敏感数据的传输场景，也更完善地丰富了整个 WSN 路由协议理论体系。

参考文献：

[1] 裴庆祺，沈玉龙，马建峰. 无线传感器网络安全技术综述[J]. 通信学报，2007，28(8)：113－122.

[2] 沈 波，张世永，钟亦平. 无线传感器网络分簇路由协议[J]. 软件学报，2006，17(7)：1588－1600.

[3] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures[J]. AdhocNetworks, 2003, 1(5): 293－315.

[4] Perrig A, Szewczyk R, Wen V, et al. SPINS: Security Protocols for Sensor Networks[J]. Wireless Networks, 2002, 8(5): 521－534.

[5] Avancha S, Underecoffer J, Joshi A, et al. Secure Sensor Networks for Perimeter Protection[J]. Computer Networks－the International Journal of Computer and Telecommunications Networking, 2003, 43(4): 421－435.

[6] Deng J, Han R, Mishra S. INSENS: Intrusion－Tolerant Routing in Wireless Sensor Networks[J]. Computer Communications, 2006, 29(2): 216－230.

[7] 覃伯平，周贤伟，杨 军，等. 基于无线传感器网络路由协议的安全机制研究[J]. 传感器技术学报，2006，19(4)：1276－1278.

[8] 周贤伟，覃伯平. 基于能量优化的无线传感器网络安全路由算法[J]. 电子学报，2007，35(1)：54－57.

[9] 程娅荔，何 波. 基于分簇的无线传感器网络安全组播路由协议[J]. 微计算机信息，2007，23(10)：75－77.

[10] 周东清，李 燕，苏庆福. 层次型结构无线传感器网络安全协议设计[J]. 计算机工程与设计，2007，28(10)：2329－2334.

[11] 王月姣，吴 越. 一种基于分簇的无线传感器网络安全路由协议[J]. 信息安全与通信保密，2008(1)：83－85.

[12] 孙雨耕，张聚伟，季 浩，等. 基于超图理论的无线传感器网络安全路由算法[J]. 天津大学学报，2008，41(2)：175－182.

[13] 杨 光，印桂生，杨 武. 无线传感器网络安全路由算法的研究与设计[J]. 计算机科学，2008，35(5)：55－59.

[14] 吴 迪，胡 钢，倪 刚，等. 无线传感器网络安全路由协议的研究[J]. 传感器技术学报，2008，21(7)：1011－1021.

[15] 庞辽军，焦李成，王育民. 无线传感器网络安全路由协议的设计与分析[J]. 传感器技术学报，2008，21(9)：1629－1634.

[16] 王 潮，贾翔宇，林 强. 基于可信度的无线传感器网络安全路由算法[J]. 通信学报，2008，29(11)：105－112.

[17] 林 闯，彭学海. 可信网络的研究[J]. 计算机学报，2005，28(5)：751－758.

[18] Tanachaiwiwat S, Dave P, Bhindwale R. Poster abstract secure locations: routing on trust and isolating compromised sensors in location－aware sensor networks[C]//Proceedings of the 1st international conference on embedded networked sensor systems. Los Angeles, USA: [s. n.], 2003: 324－325.

[19] Crosby G V, Pissinou N, Gadze J. A framework for trust－based cluster head election in wireless sensor networks[C]// The 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems. Columbia, MD: [s. n.], 2006: 13－22.

[20] Ganeriwal S, Srivastava M. Reputation－based framework for high integrity sensor networks[C]//In: Proc. of the 2nd ACM workshop on Security of Ad Hoc and Sensor Networks (SASN 2004). [s. l.]: [s. n.], 2004: 66－77.

[21] Cheng W F, Liao X K, Shen C X, et al. A trust－based routing framework in energy－constrained wireless sensor networks[C]//The 1st International Conference on Wireless Algorithms, Systems and Applications. Xi'an, China: [s. n.], 2006: 478－489.

[22] 张 静，胡捍英，童 珉，等. 一种基于信任模型的安全度量及安全路由算法设计[J]. 电子与信息学报，2008，30(1)：

(下转第 166 页)

Data = {"frame"}
SPECIFICATION ARPSpec
INVARIANT ARPTypeInvariant
= =

5 一个 ARP 欺骗实例

ARP 协议一个最大的弱点就是,一个主机可以接收任何主机发送过来的应答,这就使得允许第三方截获源主机的发送的 ARP 请求,然后将其自己的 MAC 地址发送过去。由于数据帧传送的时候是以 MAC 地址为标准传送,所以此时主机最后传送的数据帧就发送给第三方主机而不是目标机。在模型 ARP 中,加入攻击者行为如下:

ItuderRcv = ∧ begin = 1 ∧ KChan! Rcv
∧ K.val = "210.40.7.187" ∧ go' = 5 ∧ UNCHANGED<<begin,run,L,chan>>
ItuderSend(repy) = ∧ begin = 1 ∧ go = 5 ∧ LChan ! Send("44-45-53-54-00-99")
∧ UNCHANGED<<begin,run,K,go,chan>>

这两个行为的目的就是攻击者截获源主机的 ARP 请求,然后将自己的 MAC 地址 44-45-53-54-00-99 发送给源主机,然后源主机就会将数据帧发送攻击者。下面验证一个属性:

[]<>(KChan ! Send("210.40.7.187")) ∧[]<>TRcvD

这条属性是说如果源主机发送 ARP 请求,目的主机最后一定能收到源主机发送来的数据帧。具体用 TLA 描述如下:

- - - - - - - - - - MODULE MCARP - - - - - - - - - -
EXTENDS ARP
Property1 = []<>(KChan ! Send("210.40.7.187")) ∧[]<>TRcvD
THEOREM Spec => Property1
= =

协议开始运行时 K 通道中的初始值是 210.40.7.185,L 通道中的初始值是 44-45-53-54-00-00。状态 2 表示查找 ARP 缓存表,状态 3 表示经过查找后发现 IP 地址为 210.40.7.187 的目标机不在 ARP 缓存表内,因此转到状态 3 源主机通过通道发送 IP 地址到通道 K 中。此时 ARP 请求被攻击者截获因此转移到状态 4。状态 5 中,攻击者将自己的 MAC 地址应答通过通道 L 发送给源主机。最后使得源主机无法将数据帧发送给 IP 地址为 210.40.7.187 的目标机。这条路径如图 2 所示。

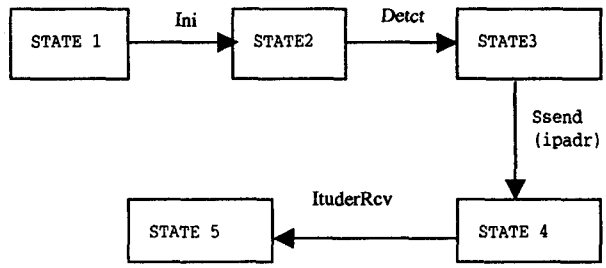

图 2 ARP 攻击路径

这条路径就是攻击者进行 ARP 攻击的路径。

6 结束语

ARP 攻击是一种非常专业化的网络攻击方式,它会给网络管理员增加很大的负担,破坏主机数据,窃取主机信息。文中用了一种新的方式用基于行为时序逻辑 TLA 的系统描述语言 TLA+对 ARP 协议进行了建模并且通过构造一个 ARP 欺骗实例并找出了一个攻击者路径。

参考文献:

[1] Internet Protocols CSC/ECE 573. The Address Resolution Protocol[R]. USA:N. C. State University,2005.
[2] 吴建平. 高等计算机网络——体系结构、协议机制、算法设计与路由器技术[M]. 北京:机械工业出版社,2003.
[3] Comer D E. 计算机网络与 Internet-网络应用[M]. 第 3 版. 北京: 清华大学出版社,2002.
[4] 吴 勇, 李 祥. ARP 攻击的分析与防范[J]. 计算机与信息技术,2008(8):7-9.
[5] Lamport L. The Temporal Logic of Actions[J]. ACM Transactions on Programming Languages and Systems, 1994, 16(3):872-923.
[6] Lamport L. Specifying Systems[M]. [s.l.]:Addison-Wesley Longman Publishing Co., Inc, 2002.
[7] Lamport L. Specifying Systems The TLA+ Language and Tools for Hardware and Software Engineers[M]. [s.l.]:Microsoft Research Addison_Wesley Publishing Version,2002.
[8] Stevens W R. TCP/IP 详解 卷 1:协议[M]. 范建华,译. 北京:机械工业出版社,2005.

(上接第 162 页)

10-15.
[23] 周 权,周小东. 基于簇首节点的可信传感器网络路由[J]. 传感器与微系统,2008,27(10):42-45.
[24] Song Fei, Zhao Baohua. Trust-based LEACH Protocol for Wireless Sensor Networks[C]//Proceedings of the 2nd International Conference on Future Generation Communications and Networking. Hainan, China:[s.n.],2008:200-205.
[25] 张留敏,李腊元,李春林. 一种基于主观逻辑的无线传感器网络可信路由算法[J]. 武汉理工大学学报:交通科学与工程版,2009,33(1):75-78.