ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.7, July 2008, pp.1716−1730
DOI: 10.3724/SP.J.1001.2008.01716

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无线传感器网络中的信任管理*

荆 琦[1,2], 唐礼勇[1,2+], 陈 钟[1,2]

[1](北京大学 信息科学技术学院 软件研究所 网络信息安全研究室,北京 100871)

[2](北京大学 高可信软件技术教育部重点实验室,北京 100871)

Trust Management in Wireless Sensor Networks

JING Qi[1,2], TANG Li-Yong[1,2+], CHEN Zhong[1,2]

[1](Network and Information Security Laboratory, Institute of Software, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China)

[2](Key Laboratory of High Confidence Software Technoloies of the Ministry of Education, Peking University, Beijing 100871, China)

+ Corresponding author: E-mail: tly@infosec.pku.edu.cn

Jing Q, Tang LY, Chen Z. Trust management in wireless sensor networks. *Journal of Software*, 2008, 19(7):1716−1730. http://www.jos.org.cn/1000-9825/19/1716.htm

Abstract: Cryptography based security solutions are not enough for WSNs when there are attacks from interior, which are caused by compromised nodes. Trust management can deal with this problem efficiently, and enhance the security, reliability and impartiality of the system. This paper gives a detailed introduction to the characteristics, the taxonomy, and the design of the framework, the vulnerability analysis, the attack models and the countermeasures. Among which the design of the framework, including the trust factors, the computation models and the application of trust, is the core of a trust management system and is given a deep insight into. In the end, several typical trust management systems are introduced. A panoramic view and detailed analysis of current trust based systems in WSNs are given.

Key words: wireless sensor networks (WSNs); trust management; reputation; vulnerability; watchdog

摘 要: 作为对基于密码体系的安全手段的重要补充,信任管理在解决 WSNs(wireless sensor networks)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.综述了 WSNs 环境下信任管理的特点、分类方法、框架设计、脆弱性分析、攻击模型及对策,在此基础上介绍了 WSNs 下的典型信任管理系统.以信任计算模型为中心的 WSNs 环境下信任管理框架的设计是信任管理系统的核心,从信任要素、信任计算模型和信任值的应用这 3 个方面对其进行了深入讨论.最后,总结了 WSNs 环境下信任管理的研究现状,提出了值得参考的研究发展方向.

关键词: 无线传感器网络;信任管理;信誉;脆弱性;监控机制

中图法分类号: TP393 **文献标识码**: A

无线传感器网络(wireless sensor networks,简称 WSNs)近年来受到了学术界和产业界的一致关注.随着

* Supported by the National Natural Science Foundation of China under Grant No.60773163 (国家自然科学基金)
Received 2007-10-12; Accepted 2008-03-27

WSNs 应用的日益复杂,其安全需求也呈现多样性,传统的基于密码体系的安全机制主要用于抵抗外部攻击,无法有效解决由于节点被俘获而发生的内部攻击.而且由于传感器节点能力所限,WSNs 中往往采用基于对称密码算法的安全措施,当节点被俘获时很容易发生秘密信息泄露,如果无法及时识别被俘获节点,则整个网络将被控制.在实际应用中,WSNs 常常被部署在战场环境或者无法实施物理保护的环境中,节点被俘获的现象极易发生,这就需要有效机制及时识别被俘获节点,有针对性地采取相应措施以减小系统损失.信任管理被认为是对传统的基于密码体制安全措施的有效补充,在对等网络、网格以及普适计算环境等网络环境中已被广泛研究.

1 信任管理

1996 年,Blaze提出了信任管理的概念[1],用授权委托的方式解决"陌生人"授权问题.他提出的PolicyMaker和KeyNote将授权与公钥绑定,互相认识的个体根据相互间信任关系直接签署授权凭证,以授权委托的方式实现信任传递,两个陌生个体之间如果存在"信任链"就可以进行授权,也可以签署间接凭证.这种信任管理系统最终体现为一个分布式授权系统,许多其他分布式授权系统,包括SPKI(simple public key infrastructure)[2],RT(role-based trust-management framework)[3],dRBAC(distributed role-based access control)[4]等,也都采用了类似思想.授权个体收集被授权个体的所有相关信息(凭证),根据本地策略和授权请求通过策略推理引擎检查一致性,决定是否授权.虽然信任委托使得对客体的访问更加灵活,但是却削弱了客体所有者对客体的控制.文献[5]对信任系统的安全性进行了研究,即在系统中的策略发生变化时,会对访问控制产生多大影响.此外,策略的一致性检验、凭证的收集也是研究重点.在这里,授权凭证的签署可以看成授权个体与被授权个体之间信任关系的体现,授权个体赋予被授权个体与其信任等级相当的权限.但是这里的"信任等级"只是对授权客体模糊的主观认知(也可能基于某些客观因素,如其他个体颁发的凭证等),个体根据自己对被授权个体的"信任"作出授权决策,以策略的方式在授权凭证中描述.在这种信任管理系统中,信任通过凭证中的授权策略间接体现,信任不能被直接而精确地表达.

另一类主要的信任管理系统,对"信任"进行量化评估,个体将所有相关信息量化,包括对被评估个体的行为观察、与被评估个体的交互记录以及其他个体的意见等,利用适当的计算模型得到对方的信任值.用信任值可以灵活地调节网络安全措施的实施,包括密码算法强度、授权决策等,使之针对不同个体进行个性化管理.还可以将信任值用于路由层、应用层(如网上购物系统)等,用于提高网络的安全性、健壮性.这种信任管理系统中的信任往往体现为一个综合的信任值,不能很好地体现不同种类信任对系统的不同影响.个体间通过互相发送被评价个体的信任值来传递信任,信任管理策略主要包括抗攻击及决策应用等方面,一般较为简单,研究重点在于如何获得准确、适用的信任值.

个体间的信任是各信任管理系统中一致的基本因素,在此基础上,一些研究试图将上述两类信任管理相结合,充分发挥二者各自的优势.文献[6]力图用统一的四层模型集成各种现有信任管理系统,包括信息收集层、鉴别层、语意层及评价层,各层之间相对独立,可以利用现有信任管理系统的模块,比如将PolicyMaker用于语意层的策略推理.基于信任度的授权委托模型TBAD(trustworthiness-based authorization delegation model)[7],在授权委托过程中引入信任度,使授权委托不再是简单的二值决策,并且利用信任度门限值控制授权委托深度.

2 无线传感器网络中的信任管理

WSNs 具有节点资源有限、网络应用相对单一的特点.而且,一般情况下整个网络从属于一个机构.所以,WSNs 的授权策略较为简单,无须采取授权凭证方式的信任管理.而且,基于公开密钥算法的授权凭证的签署和授权凭证中公钥的使用也不适合于资源有限的 WSNs.所以,目前对 WSNs 的信任管理系统的研究主要集中于对节点进行信任值评估,借助信任值评估增强 WSNs 的安全性、健壮性等方面.

在WSNs设计伊始,针对当前因特网由于起步时设计上的安全缺陷引起的众多问题,研究者一致认为安全应该渗透到WSNs设计的各个方面.对于WSNs的信任管理,一直陆续有人关注.2003 年,Sapon等人基于信任管理识别问题位置以及问题区域[8],实现了基站与节点间基于地理信息的安全路由.2004 年,Ganeriwal-Srivastava提

出RFSN(reputation based framework for sensor networks)[9]是一个较为完整的基于信誉的WSNs中的信任管理系统.2005 年,Krasniewski等人的TIBFIT(trust index based fault tolerance for data faults in sensor networks)将信任用于安全的数据融合[10].2006 年,Garth等人将信任管理用于簇头(cluster head,简称CH)选举[11].2006 年以来,国内许多单位也开始针对无线传感器网络信任管理的研究,包括中国科学院软件研究所[12]、国防科学技术大学[13]、复旦大学[14]、东北大学[15]、武汉大学[16]等.

随着 WSNs 基础研究的逐渐成熟,相关应用的逐步拓展,对 WSNs 中信任管理的关注也逐年上升.由于传感器节点资源有限而导致的节点自私行为,以及由于节点被俘获而导致的恶意行为等,都会严重影响 WSNs 的正常运行.而节点被俘获后,其存储的秘密就会暴露,这对基于密码体系的安全措施构成了很大的威胁,所以,WSNs中安全架构的设计都要考虑如何在部分节点被俘获时仍能正常运转.用信任管理识别恶意节点、自私节点,识别错误数据,将信任管理应用于路由、数据融合、簇头选举等 WSNs 的各项基础支撑技术及应用支撑技术中,将信任管理与 WSNs 的安全架构相结合,可以全面提高 WSNs 的安全性和可用性.

2.1 无线传感器网络中信任管理的分类

2.1.1 无线传感器网络中信任管理的分类

层次式信任管理是指对信任值的评估、传递以及存储等管理具有层次特点,往往与网络拓扑及信任值的应用有着紧密联系.如基于基站与传感器节点自然的层次结构而形成的以基站为中心的信任管理;在有簇结构的WSNs中,会形成基站-簇头节点-普通节点的 3 层信任管理;在安全的数据汇聚应用中,信任管理往往基于汇聚树的层次结构.在层次式信任管理中,信任可以逐层传递,上级存储所有下级或者相邻下级的信任值[10].信任也可以逐级汇聚,形成不同层次的信任值[16,17].平面式信任管理是指在信任管理的过程中,网络中所有节点及基站地位是平等的,采取相同的计算模型和管理策略,没有明显的中心或层次[9].

2.1.2 全局信任管理和本地信任管理

全局信任管理是指节点在整个网络中具有唯一的信任值,一般在有簇结构的WSNs中常见[10,16].本地信任管理则是指被评估节点在不同评估节点处的信任值可能不一致,节点根据本地存储的信任值作出决策[8,13,18],或者根据本地信任值以及邻居节点发送的信誉综合决策[9,19].

2.1.3 基于信誉的信任管理和基于本地信息采集的信任管理

在进行信任评估时,由于信息不完全可能会造成评估值的偏差.为了获得更为准确的信任值,往往需要综合考虑其他节点的信任评估值以修正本地的评估结果,这就是基于信誉的信任管理的基本思想[9,12,17,19].但是在WSNs中,由于节点资源有限,为了减少通信及计算耗费,有的信任管理系统在信任值评估时,只简单考虑节点本身对被评估节点的观察结果以及交互行为评价等本地信息,节省了其他节点传输信誉值的能量耗费[8,11,13,18,20−22].

2.1.4 通用信任管理和应用相关信任管理

通用信任管理是指综合考虑信任定义的各方面要素定义的一套完整的信任管理框架,包括信息采集、传递、存储、计算、更新等信任管理各方面的设计.信任值的计算不具有针对性,是对节点可信性的一个综合评估,可以用于WSNs网络运行及应用的所有相关技术中[9,12,19].而应用相关信任管理具有很强的针对性,信任管理过程中的所有环节设计都与特定的应用密切相关,比如用于安全路由的信任管理往往需要识别自私节点、低竞争力节点[8,13,18],而用于安全数据融合的信任管理一般不需要处理自私节点,甚至在一些系统中,当恶意节点没有发送错误数据时(只进行丢包、更改目标地址等行为)也不会影响其信任值[8,20,21].

2.2 WSNs中信任管理框架

由于无线传感器节点资源有限,所以 WSNs 环境下的信任管理框架需要根据 WSNs 环境的特点进行传输、计算、存储等各方面的优化.WSNs 信任管理系统体系结构如图 1 所示.

2.2.1 信任要素

建立一个信任管理体系首先要明确信任的组成要素,即信任主要包括哪些方面的因素.这与信任的定义直

接相关,也是整个信任管理框架设计与实现的基本依据.不同的信任定义下信任的组成要素差别很大,如Grandison-Sloman[23]认为,信任是相信实体具有在一定上下文环境下进行可靠、安全行为的能力,这个定义就明确了:① 信任是上下文相关的;② 信任包括系统可靠性和安全性等方面的因素.而实际上由于对信任的定义不同,许多信任管理系统不考虑上下文信息,也有的不考虑系统可靠性方面的问题,还有的只研究自私节点问题,即将提高系统可靠性作为信任管理系统的主要目标.

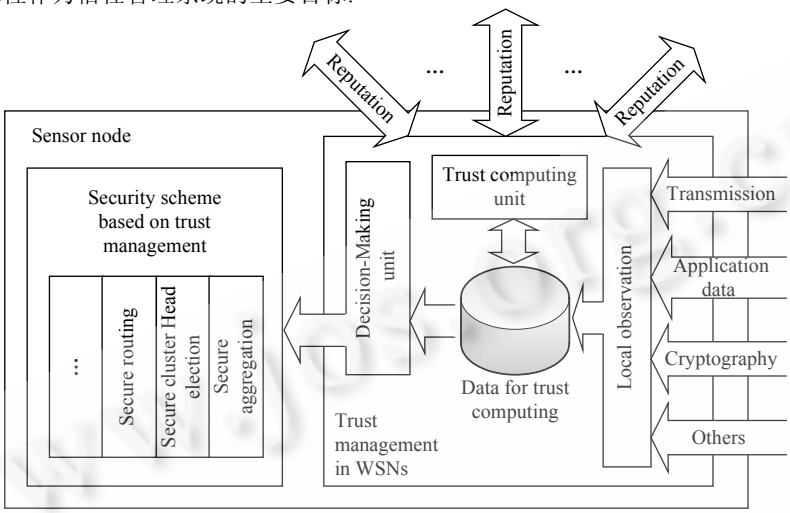

Fig.1 General architecture of trust management systems for WSNs
图 1 WSNs 信任管理系统体系结构

一般来说,WSNs 环境下信任主要来自对以下几方面因素全部或部分的综合评估:

(1) 通信方面的因素

在 WSNs 中,控制命令或应用数据的传输是节点可被观察到的主要行为.恶意节点可能会表现为丢弃、篡改数据包等行为,自私节点也可能会因为节省能量而丢弃需要转发的数据包.通过观察节点的通信行为识别恶意节点或者自私节点,是信任管理系统的常用机制.

常用的监控方法为将网卡设置为混杂模式[9,20,21,24],通过监听邻居节点的行为判断其是否正确转发了数据包.这需要在本地设置缓冲区,如果邻居节点及时转发了数据包,并且与缓冲区内的数据包一致,则认为节点可信,增加其信任值;否则,减小其信任值.但是,混杂模式下需要节点一直处于监听状态,这是十分耗能的做法,传感器节点需要定期地进入睡眠状态以节省能量.所以,许多信任管理系统不采用这种方式监控,或者在其他取代方法不可行时才采用.

另一种常用的方法是修改路由协议(常采用源路由方式)[8,13,19],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.

此外,还可以对一定时间间隔内邻居节点发送的数据包数量计数,如果超过了预设上限,可以怀疑其在进行DoS攻击;如果没有达到预设下限,可以怀疑其为自私节点[19].

通信方面的因素是大部分信任管理系统主要考虑的部分,但是,也有的信任管理系统不将其纳入考虑范围,如一些基于信任管理的安全数据融合[10,20],其信任值评估常常只考虑数据的一致性,而忽略节点的通信行为.

(2) 密码学方面的因素

在大部分应用中,信任管理机制是基于密码学安全机制的补充手段,用以提高网络的安全性.同时,密码机制也成为许多信任管理系统中信任评估的主要考虑因素之一.密码机制可以用于信任值的初始化——将拥有对密钥的邻居节点的信任值置为 1,否则为 0(信任值$\in$[0,1])[13].也可以用于信任值更新——若节点无法解密数据包为有意义的明文,则提高加密数据包节点的信任值,否则减低[11,19];若消息鉴别码(message authentication code,简称MAC)通过验证,则提高节点的信任值,否则,降低[19].在存在哈希链机制的系统中,如果当前哈希值不可推导,

则降低相应节点的信任值;如果当前哈希值可推导,但与上一哈希值相隔甚远,则可以认为传输过程中发生丢包,根据哈希链间隔适当降低相应节点信任值[19].

(3) 应用数据方面的因素

数据采集是WSNs的主要应用之一,传感器节点根据应用需要采集数据,通过sink传送至信息处理服务器.后者对所采集的数据进行分析、记录,有时会回复信息.在信息上传过程中,为了减少网络中的信息流量,减小传输能耗及存储需求,常常会采用数据汇聚(data aggregation,有时也称为数据融合——data fusion)手段.信任管理常常被用于提高系统对错误数据的容错能力,识别错误信息,提高上传数据的准确性.

数据可信性判断根据粒度可以分为是否有事件发生[10]以及被报告数据的内容是否一致[20,21,25,26].在判断数据一致性时,可以与数据融合技术相结合.

(4) 其他因素

除了上述几个主要因素之外,根据信任管理系统设计目标的不同,还有其他一些影响节点信任值的因素.文献[20,21]认为,信任值越高的节点,被选择执行任务的几率越高,电量耗费得越快,所以将电量作为信任值计算的考虑因素之一,以延长整个网络生命周期.文献[8,18]中将节点的可用性也作为信任值计算因素之一,在基于锚节点定位的WSNs中,可以利用锚节点定期探测节点的生存状态,也可以定期发送Hello消息以确定节点是否存活.但是,节点定期休眠也会影响其可用性.基于冗余增加判断的准确性是常用手段,所以许多系统要求网络部署有足够的密度[8,18,20,21].

2.2.2 信任计算

信任计算是信任管理系统的核心,包括信任值预定义、信任值初始化、信任值合成等步骤,其中信任值合成与更新是信任计算的核心.在对等网络及网格计算等网络环境下,概率模型、模糊集计算模型、博弈模型及有向图等模型都被尝试,适用于不同的应用.在WSNs环境下,由于计算、存储以及通信各方面的限制,不适于应用复杂的计算模型,信任管理系统一般采用比值计算等简单方法.

(1) 信任预定义

信任预定义主要确定信任的表示方式,如用模糊集表示、功能性元组表示还是单数值表示,大部分模型都是单数值表示.此外,还需要进一步确定信任值定义区间,信任表示为离散式的信任等级还是连续信任值区间,正负区间对称表示还是正区间,常用的信任值定义区间如[−1,1],[0,1],或者类似[−3, −2, −1,0,1,2,3]及[0,1,2,3]的等级表示.最后,还需要定义因素映射函数,即第 2.2.1 节中各类因素相对应的数据如何统一映射到相应区间内的数值表示,以参与信任值计算.

(2) 信任值初始化

信任值初始化与信任预定义直接相关,一般包括两种方式:全部节点统一初始化为相同信任值;或者通过一个初始化阶段进行节点信任值初始化.初始信任值分为悲观、乐观和中间值3种,相对应地,将所有节点初始化为信任值区间的最低值、最高值和中间值.悲观信任初始化可以防止恶意节点为了洗刷自身的低信任记录,伪装成新节点重新进入网络,但是不利于新节点正常加入网络.不过,由于WSNs一般结构相对静止,所以比较适合要求较严格的WSNs应用.从另外的角度来看,乐观初始化[10]也比较适合WSNs的特点—— 整个网络往往属于一个组织所有,具有天然的彼此完全信任的基础.有的信任管理系统通过一个初始化阶段进行信任值的初始化,一般是根据网络刚完成部署后可获得的数据进行,数据来源为第 2.2.1 节中的部分因素,如文献[8,18]根据鉴别机制和可用性进行信任值初始化,文献[13]将可以解密消息并用共享对密钥加密回复的节点信任值初始化为1.

(3) 信任值合成

在WSNs中,信任值的合并更多地是采用简单的比值与加法计算,尽量采用简单计算模型以节省能耗.总的来说,信任值的合成包括横向、纵向与分级3种.

(a) 横向合成

信任值的横向合成,主要包括节点本地获取的关于被评价节点各类信任因素数据(local information,简称LI)的合成(local sum,简称LS),来自其他节点的被评价节点信誉的合成(reputation sum,简称RS),以及LI与信誉的

合成(local-reputation sum,简称LRS)三方面.其中LI和信誉也被称为一手、二手信息.不同的信任管理系统横向合成的差异很大.由于信誉值的获得需要很大的传输能耗,所以有些系统只采取LS[8,13,18,20,21].但是,由于各类信任管理系统对于各类信任因素数据采集的方式不一样,很有可能发生信息不完整的情况,造成被评价节点的LS不能反映其实际信任值,所以还是有些系统采用LS与RS相结合的方式[9,17,19].可以分别LS,RS,然后进行LRS;也可以先LS再LRS;还可以用统一的公式直接LRS.

Table 1 Analysis of computational models for trust management in WSNs

表 1 WSNs 信任管理系统计算模型比较分析表

	Trust management system	Trust factors	Trust evaluation	Transverse integration	Vertical integration	Hierarchy integration	Communication payload	Computation cost	Storage
Simple weight model	[19], PLUS [27]	T, C,	LS-RS-LRS	–	–	–	A	L	H
	TRANS [8][18]	T, C, O	LS	–	–	–	MP	L	M
	SecCBSN [28]	T, O	RS-TU	V	–	–	A, MP	L	H
	GTMS[17]	I	(LS+TU)-RS-LRS	TR	R	GT	A	L	H
	RFSN[9]	T, C, D, O	(LS+TU)-(RS+TU) -LRS	TR, PR	R	–	A, MP	L	H
	[11]	T	LS	V	–	–	A	L	H
	[20], [21]	D, O	LS-RS	TR	–	GT	A	L	M
Exponential model	TIBFIT[10]	D	TU	–	P	–	–	L	L
	[7]	D	TU	–	P	–	–	L	L
Statistical model	BRSN[9]	T, C, D, O	LRS+TU	TR, PR	R	–	A, MP	L	H
	[29]	T, D	LS-RS-LRS	TR	R	–	MP	L	H
Game theory model	[24]	T, O	LS	–	–	–	–	L	M

I: Number of success/fail interactions, T: Transmission factors, C: Cryptography factors, D: Application data factors, O: Other factors; TR: Take (functions of) trust values of judges as the coefficients of reputations they sent, PR: Only “good” reputations considered, V: Vote; R: Higher proportion of RT, P: Higher proportion of PT; GT: Group trust value computing; A: Aggregation, MP: Packages specially for trust evaluation (acknowledge packages, beacon, *et al*.); H: High; M: Middle; L: Low

由于LS是基于节点本身采集的数据计算,所以被认为完全可信.但是对于其他节点发送的信誉值,则需要考虑其可信性.许多系统在RS时将其他节点于评价节点处的信任值作为其发送的信誉值的系数,节点在评价节点处的信任值越高,其发送的信誉值所占比重越大[9,19].此外,为了避免Bad-Mouthing攻击,许多系统只计算好的信誉值(只发送好的信誉值或者信誉值高于门限值时才参加计算)[9].但是,这样系统内就无法交流关于恶意节点或自私节点的信息,所以,有的系统接受可信任节点报告的坏信誉值,不过又会存在报复行为的可能性.如果最终采用LRS合成信任值,并将其作为信誉值传递,则会发生节点A对某节点进行信任评估时,其LS结果通过信誉值的传递回到A并参与RS及LRS的计算.为了避免这种循环现象的发生,文献[9]只将LS的结果作为信誉传递.

(b) 纵向合成

信任值的纵向合成是指信任在时间轴方向的计算,将近期信任值(recent trust,简称RT)与历史信任(past trust,简称PT)合并,也称为信任的更新(trust update,简称TU).信任值的横向合成与纵向合成交叉进行,根据具体的信任管理系统需求存在多种组合[16].如可以LS-TU,RS-TU,然后LRS[9];也可以LRS-TU.这里涉及到何时更新的问题,可以事件触发更新,也可以定期更新.用Beta分布表示信任值,基于贝叶斯公式进行信任值更新是信任管理系统常用的手段[9].

信任更新时根据 RT 和 PT 所占的比重可以分为两种更新方式:① PT 所占比重大,可以防止恶意节点在发现自己信任值过低时,短期内进行特定行为来弥补.② RT 所占比重大,也称为信任老化(aging),迫使节点一直处于正常状态,因为一旦发生恶意行为,就会被严厉惩罚.但是由于信任值随着时间流逝而降低,这对于通信不频繁地区的节点不公平.可以通过系统定期产生通信流量来弥补这一缺陷.

(c) 分级合成

在层次式信任管理系统中,有时存在信任的逐级合成,主要包括两类:① 在逐级上行过程中,所能获取信息的范围逐渐增加,对节点信任值逐级修正[21].② 每级结构有自己的信任值,如GTMS(group based trust management scheme)中节点和簇可以分别有自己的信任值[17],需要在节点、簇和网络分级进行相应的信任值的合成.

2.2.3 决策与应用

应用决策是体现信任管理系统价值的部分,与信任管理系统的目标紧密相连.虽然各类系统具体目标不同,但是信任管理系统的基本功能就是识别系统中的不可信节点,包括恶意节点、自私节点以及低竞争力节点.但是,这些节点本质上不同,要采用不同的策略.恶意节点一旦确定就要进入黑名单;自私节点要采取激励和惩罚措施,增加其参与的积极性;适当减少低竞争力节点的参与,提高公平性,延长整个网络的生命.信任值决策较多地采用门限值来判定特异节点.

对于具体应用,不同系统处理细节上也有很大差异.基于信任管理的安全路由用探测技术定位问题节点[8,18];将低信任、低竞争力节点从转发列表删除;广播黑名单或者修改路由协议绕过恶意节点.基于信任管理的安全信息融合将节点的信任值作为其采集数据的权重进行数据融合[20,21].在基于信任管理的簇头选举中,根据信任值选举出的候选节点还需要通过原簇头的Challenge-Response测试才可以正式当选[11].文献[13]根据文献[30]中的思想将不同安全性需求的数据划分等级,定义相应的信任等级,只有信任等级高于所传送数据对应的信任等级的节点才可以进入该类数据转发列表.在基于信誉的信任管理系统中,通过推荐协议实现信誉值的传送[9].文献[22]利用移动代理管理节点的信任.也有些信任管理系统只定义“单纯”的信任管理,不涉及具体的决策与应用细节[17].

3 针对 WSNs 中信任管理的脆弱性分析、攻击模型及对策

既然信任管理主要用于增强网络的安全性、可靠性,针对信任管理系统本身的脆弱性分析和攻击模型就显得尤为重要.WSNs中增加信任管理系统带来的系统安全性、可靠性方面的提高,如果不能抵消其带来的设计复杂性、能耗、脆弱性等方面的代价,则认为信任管理系统无须存在.Dolev-Yao是常用的网络攻击模型,是指在整个网络被控制的情况下,通信可能发生被窃听、丢弃、重放、修改、伪造等攻击行为.但是WSNs环境下针对系统的不同应用环境,攻击模型也有所不同.文献[31]认为,在WSNs环境中,除非攻击者预先获知网络部署地点,并部署好自己的监控设备,否则,在系统初始化阶段相对安全.也有研究者认为,Dolev-Yao模型没有涉及Sybil攻击、共谋等问题,所以不够全面[6].下面根据信任管理系统针对的目标节点的不同类别来进行系统的脆弱性分析,建立攻击模型.

3.1 恶意节点

恶意节点是指敌方部署的外来节点,或者被敌方俘获的网络中合法节点.恶意节点可能单个行动,也可能集体行动.多个恶意节点还有可能有计划地进行共谋,目前为止,对于共谋没有特别有效的对策.对于恶意节点,一般系统会采取较为严厉的措施,如文献[11]通过 challenge-response 机制确认某节点是恶意节点之后,将不再允许该节点或其他节点通过任何手段提升其信任值.信任管理系统针对的恶意节点行为主要分为以下 3 类:

(1) 直接恶意行为

直接的恶意行为包括丢弃数据包、更改数据内容、更改数据包地址、不按源路由规定而随意转发数据包、频繁发送伪造数据包等.黑洞攻击与灰洞攻击都是丢弃数据包的攻击行为,前者是指恶意节点将所有节点发送过来的数据包丢弃,后者与之不同的是选择性丢弃数据包.这些恶意行为可以用第 2.2.1 节(1)中所述方法发现.

(2) 间接恶意行为

间接的恶意行为是指通过降低正常节点信誉值(bad-mouthing),或者提高恶意节点信誉值,达到影响网络正常运行的目的,可以是单独节点的行为,也可以是共谋.对于 Bad-Mouthing 的对策见第 2.2.2 节中信任值的横向

合成.对于针对信誉的共谋一般可以采取提高信誉评价的代价的方法,为了达到提高/降低某节点信誉的目的,共谋节点必须付出很大代价.但是这种方法并不适合资源有限的 WSNs 节点,而且对于能力较强的入侵者(如PDA、膝上电脑等)也没有效果.

(3) 掩饰行为

在有信任管理的系统中,恶意节点为了延长自己作为正常节点留在网络中的时间,会有一些掩饰行为:

- 当发现自己信任值过低时更换标识作为新节点重新加入网络,对策见第 2.2.2 节.
- 当恶意节点发现自己信任值较低时,暂时停止恶意行为,在短期内努力提高自己的信任值.这种情况可以通过在纵向合成时加大历史信任的权重来防止,文献[9]中将 LS 与 RS 结果分开存储在 RDT 和 RT 两个表中,如果某节点在RDT中是合作节点,在RT中是不合作节点,则认为该节点属于近期努力提高自己信任值以弥补自己恶意历史行为的恶意节点.
- 恶意节点一段时间内累积好的历史记录,将自身信任值提高到一定程度后开始进行恶意行为.对策见第 2.2.2 节中纵向合成.

对于恶意节点的掩饰行为,有的系统采用不公开恶意节点信息的手段[9].恶意节点不知道自己在其他节点处的信任值,没有办法及时发现自己信任值已经降低到一定程度,进而无法及时采取补救行为.

3.2 非恶意节点

信任管理系统对于非恶意节点的识别主要是从提高系统的可靠性、公平性的角度来考虑.一些系统认为可靠性、公平性也体现了系统的可信赖程度,也是信任内涵的一部分.

- 自私节点

由于 WSNs 资源有限,为了节省自身能耗,自私节点将自身隔离在系统之外“不作为”,或者尽量减少自己的参与.比如不参与路由发现,以使自己不在任何节点的路由表中出现.可以通过监测节点的通信频率是否低于正常门限值来发现自私节点,或者采用激励制度使节点自发参与系统运行,获得较高信任值以便在自己需要时获得其他节点的合作.

- 低竞争力节点

在评估节点信任值时,将节点的能量、节点与目标节点的距离(安全路由系统中)等竞争力信息引入,在决策时体现公平,以延长网络生命.如文献[22]中引入节点可用性,文献[11,13]将电量引入节点可信度计算.但是这些因素的数据获取可能会引起系统误读:① 节点可能会因为系统设计或者临时技术故障而导致竞争力暂时降低,如节点在可用性探测时正在睡眠周期,节点由于缓冲区满而发生丢包行为等.对于这种情况可以提高历史信任值的比重,使得临时性的可疑行为可以被较容易地补救.② 正常节点可能会因为部署问题等客观原因,在某种信任值计算模型下信任值持续降低.如采用 aging 技术的信任计算,会导致不活跃区域的节点信任值不断降低,对策见第 2.2.2 节中信任值纵向合成.

表 2 对 WSNs 中信任管理系统相关的攻击模型进行了比较分析.由于某些攻击行为较为复杂,如 Sybil 攻击在协议栈多层都能发生;而且不同的攻击还可以相互结合,造成更严重的后果,如 Sybil 攻击和 DoS 攻击相结合增加隐蔽性,所以表 2 只概述了 WSNs 下信任管理系统主要针对的几种典型攻击、针对 WSNs 下信任管理系统的几种典型攻击以及每种攻击的典型对策.

4 典型 WSNs 下信任管理系统

随着传感器节点各方面能力的增强,WSNs 各项支撑技术的逐渐成熟,以及 WSNs 应用背景的迅速拓展,对 WSNs 的安全性与可靠性需求越来越强.由于信任管理在许多方面,尤其是在面对内部攻击时,具有显著优势,适合于 WSNs 这种节点极易被俘获的情况,所以针对 WSNs 的轻量级信任管理框架研究有逐渐增多的趋势.下面简要介绍几种 WSNs 下典型的信任管理系统,着重介绍其信任值计算模型.

4.1 无线传感器网络中基于信任的路由(trust routing for location-aware sensor networks,简称TRANS)

Tanachaiwiwat等人提出了TRANS[8,18],在基于地理信息路由的无线传感器网络中,查找并标识出可疑位置,实现基于信任的安全路由.

Table 2 Analysis of attack models concerned with trust management system for WSNs

表 2 WSNs 信任管理相关攻击模型比较分析

Attack models			R/O	Countermeasures based on trust management
Attack models aimed by trust management for WSNs	Dolev-Yao	Hello flooding and other analogous DoS attacks	R	Trust factor: Package number sent in a predefined time period Malicious nodes: The number exceeds a threshold
		Blackhole	R	Trust factors: Package number received vs. package number sent/corresponding ACK package number Malicious nodes: The latter is 0
		Greyhole	R, O	Trust factors: Package number received vs. package number sent / corresponding ACK package number Malicious nodes: The former<the latter
		Reroute, Fabricate	O	Trust factor: Contents of packages received vs. contents of packages sent Malicious nodes: Contents changed
	Sybil		R	Only communicating with trusted nodes
	Collude		O,R	According to concrete collude attacks
Attack models aiming at trust management for WSNs		Description	R/O	Countermeasures
	Bad-Mouthing	Send bad reputation to reduce the trust/reputation value of legal nodes	O	Reputation used in trust integration: Only "good" reputation; "bad" reputation from trusted nodes
	Sybil	Create a lot of node identities, counterfeit corresponding nodes to boost its own reputation or reduce others' reputations	O	Increase the cost of rating; binding keys to every legal node identity; find neighbor nodes in a faraway physical location
	Collude	The difference with Sybil attack: Collude nodes are real nodes	O	Increase the cost of rating
	New identities	Join in the network with a new node identity when have a low trust value	O	Increase the cost of creating new legal identities; give low initial trust values to new nodes
	Quality variations	Reduce QoS or do malicious action when nodes have high trust values which will not decrease under a threshold because of these behavior	R	Aging (see Section 3.2)

R: Random attacks; O: Objective attacks

(1) 目标:保证 sink 与节点间的安全路由.

(2) 条件:① 采用基于地理信息的路由;② 具有足够部署密度;③ sink 或基站采用μTESLA 进行安全广播.

(3) 相关定义(i是被评价节点标识):① C_i:密码学因子,如果node_i拥有共享密钥,则C_i=1,否则C_i=0;② $A_i=\sum_{j=1}^{n}\frac{QA_n}{n}$:可用性因子,利用锚节点信号或定期发送Hello消息探测节点是否可用,n为预设窗口大小,QA_j表示第j次探测时节点是否可用;③ $P_i=\sum_{j=1}^{m}\frac{QP_j}{m}$:转发率因子,$QP_j$表示第$j$次查询是否有回复;④ β:激励因子,为了减小初始化阶段数据包丢失的影响,以及减轻T_i的摆动而设计,可根据经验设置;⑤ T_i:节点信任值;⑥ 可信邻居节点:拥有共享密钥并且信任值在预设可信门限值上的邻居节点;⑦ 可信路由节点:离目标位置更近的可信邻居节点.

(4) 过程: $sink \xleftarrow[reply]{msg_1}$可信路由节点$\xleftarrow[reply]{msg_2}$可信路由节点$\xleftarrow[reply]{msg_3}\cdots\xleftarrow[reply]{msg_k}$目标节点.其中:

- msg_1=*encrypt*(*shared key*,(*request*,*sink's location*,*destination location*,*MAC*,*detour locations* (*optional*)))

- msg'_1=*decrypt*(*shared key*,msg_1),msg'_2=*add*(msg'_1,*trusted node's location*),msg_2=*encrypt*(*shared key*,msg'_2);msg_3至msg_k的生成过程与msg_2类似
- 目标节点:*decrypt*(*shared key*,msg_k);验证*MAC*;*reply*=*encrypt*(*shared key*,(*reply message*,*destination node's location*))
- Sink 接收到 reply,则将参与路由节点的 *QP* 增 1

(5) 信任计算: $T_i = C_i \cdot A_i \cdot \beta P_i$.

(6) 应用:① T_i用于选择可信路由节点;② 当某位置的T_i持续走低时,sink启动one-shot探测,定位可疑位置,将其加入黑名单广播给所有节点,或者将其嵌入数据包头以在路由时绕过.

4.2 基于信任的传感器网络中的容错系统

Krasniewski等人于 2005 年提出了TIBFIT [10],应用于有簇结构的无线传感器网络,簇头节点将所报告事件位置附近的节点分为发送报告与未发送报告两组,分别计算其信任值,认为高信任值一组中的节点可信.

(1) 目标:根据事件附近节点的报告及节点的信任值判断事件是否发生.

(2) 条件:① 采用LEACH[4,32]进行簇的生成及簇头选举;② 只考虑节点的 3 类错误行为(不考虑基于泛洪的DoS攻击):在规定时间内不报告自己监测范围内发生的事件;报告自己监测范围外发生的事件或者未发生事件;报告事件的位置错误.

(3) 相关定义:① NER(natural error rate):自然错误率,正常节点发生错误的几率;② TI(trust index):节点 i 的信任值,由簇头节点维护;③ SCH(shadow CH):影子簇头.

(4) 信任计算:

- 预设 *NER*=*fr*
- 节点i在*CH*存储一个对应变量v_i:

  when (*CH* 接到第 1 个报告)

  CH 启动计时器;

  when (计时结束)

  *CH*将事件地点附近节点(G)分为发送报告(G_A)和未发送报告(G_B)两组

  $TI_{G_A} = \sum_{\forall i \in G_A} TI_i$, $TI_{G_B} = \sum_{\forall j \in G_B} TI_j$

  if ($TI_{G_A} > TI_{G_B}$) then $((\forall i \in G_A) v_i = v_i + (1 - fr)$, $(\forall j \in G_B) v_j = v_j - fr)$ and vice versa

  $(\forall k \in G) TI_k = \mathrm{e}^{-\lambda v_k}$

(5) 应用:

- 判断是否有事件发生:设 $TI_{G_A} > TI_{G_B}$ (见信任计算部分),则认为 *GA* 中节点可信,即如果其报告有事件发生,则判断结果为有事件发生;反之亦然.
- 簇头选举:基于 LEACH 加入信任管理部分,如果新 *CH* 的 *TI* 低于预设门限值,则基站取消其簇头资格,重新发起 *CH* 选举.*CH* 任期满时将簇内所有节点*的 TI* 发送给基站,新 *CH* 产生后向基站请求其簇内所有节点的 *TI*.
- 簇头可靠性:采取增加两个 *SCH* 的方式加强 *CH* 可靠性:
  - 选取 *CH* 邻居节点中 *TI* 最高的两个节点作为 *SCH*
  - *SCH* 监听所有 *CH* 通信,并执行所有 *CH* 功能(除了向基站发送事件报告)
  - 如果发现 *CH* 有错误行为,则向基站发送自己的报告
  - 基站收到 *CH* 和两个 *SCH* 报告后,采取少数服从多数的原则.如果 *CH* 是"少数",则发起 *CH* 选举并降低 *CH* 的 *TI*

4.3 无线传感器网络中基于信任的安全数据融合

在无线传感器网络中,节点往往不只是简单地报告事件的发生,而是需要报告温度或湿度等具体数值.Hur等人[20,21]通过检查所采集数据的一致性来实现安全的数据融合.

(1) 目标:过滤掉欺骗性的或者不一致的数据,实现安全的数据融合.

(2) 条件:① 具有足够部署密度;② 不针对共谋问题;③ 采用基于锚节点的定位.

(3) 相关定义:① *GridID*:将WSNs划分为 $\frac{s}{\sqrt{2}}\times\frac{s}{\sqrt{2}}$ 大小的网格,并为每个格赋以唯一标识*GridID*,其中s为节点最远感知距离;② T_{ij}:节点i存储在节点j处的信任评估值;③ D_{ij}:节点i与j的距离;④ $S_i=\frac{ss_i-sf_i}{ss_i+sf_i}$:节点$i$事件报告的可信性,其中$ss_i$为成功次数,$sf_i$为失败次数;⑤ $C_i=\frac{cs_i-is_i}{cs_i+is_i}$:节点$i$采集数据的一致性,其中$cs_i$为一致次数,$is_i$为不一致次数;⑥ B_i:节点i的能量因子,反映了节点的剩余寿命;⑦ sr_i:节点i采集的数据;⑧ $sr_j^*=f(sr_i,r,D_{ij})$:节点i根据自己采集的数据sr_i、与节点j的距离D_{ij}以及事件发生位置与节点i的距离r计算得出的节点j采集数据的预期结果;⑨ T_i:汇聚节点计算的节点i的信任值;⑩ SR_{GridID}:网格*GridID*的数据汇聚结果.

(4) 信任计算(假设节点 i 与 j 是邻居节点):

每个节点都存有其所有邻居节点的信任计算相关数据

if (节点 i 与节点 j 在同一时间段内报告相同事件发生) then

节点j更新$ss_i=ss_i+1$;节点i更新$ss_j=ss_j+1$;

节点 i 检查数据一致性:

节点i在r的可能范围内计算得到sr_j^*的可能范围

if (sr_j在sr_j^*的可能范围内) then ($cs_j=cs_j+1$) else ($ic_j=ic_j+1$)

节点 j 以相同方法检查数据一致性

else {节点j更新$sf_i=sf_i+1$;节点i更新$sf_j=sf_j+1$;}

节点 j 计算 $S_i=\frac{ss_i-sf_i}{ss_i+sf_i}$, $C_i=\frac{cs_i-is_i}{cs_i+is_i}$;

节点 j 计算 $T_{ij}=\frac{W_1C_i+W_2S_i+W_3B_i}{\sum_{i=1}^{3}W_i}$,其中,$W_i\in[0,1]$且$\sum_{i=1}^{3}W_i\neq 0$

汇聚节点计算 $T_i=\frac{\sum_{j=1}^{k}(T_j+1)\times T_{ij}}{\sum_{j=1}^{k}(T_j+1)}$

(5) 应用:

- 选择汇聚节点:选择网格中T_i最高的节点作为汇聚节点
- 汇聚节点过滤不一致及恶意数据,计算网格数据汇聚结果SR_{GridID}发送给基站:

$$SR_{GridID}=\frac{\sum_{i=1}^{m}(T_i+1)\times sr_i}{\sum_{i=1}^{m}(T_i+1)}.$$

4.4 基于信任的无线传感器网络中的簇头选举策略(a framework for trust-based cluster head election in wirelesssensor networks)

簇头节点在具有簇结构的无线传感器网络中具有举足轻重的地位,Crosby等人[11]将信任引入了簇头选举中,并采取冗余策略和挑战应答手段,尽可能地保证选举出的簇头节点为可信节点.

(1) 目标:防止恶意节点被选举为簇头节点.

(2) 条件:节点设为混杂模式.

(3) 相关定义:① RF_i:节点i收到的要其转发的数据包数;② F_i:节点i已转发的数据包数;③ DM_i:被节点i修改内容的数据包数;④ AM_i:被节点i修改地址的数据包数;⑤ CRF_i:节点i收到的要其转发的控制包数;⑥ CF_i:节点i已转发的控制包数;⑦ CM_i:被节点i修改内容的控制包数;⑧ CAM_i:被节点i修改地址的控制包数;⑨ T_i:节点i的信任值;⑩ γ:预设的平均丢包率.

(4) 信任计算:

$$d_1=\frac{F_i}{RF_i},\ d_2=1-\frac{DM_i}{F_i},\ d_3=1-\frac{AM_i}{F_i},\ c_1=\frac{CF_i}{CRF_i},\ c_2=1-\frac{CM_i}{CF_i},\ c_3=1-\frac{CAM_i}{CF_i},$$

$$T_i=\omega_1d_1+\omega_2d_2+\omega_3d_3+\omega_4c_1+\omega_5c_2+\omega_6c_3+\gamma\ .$$

(5) 应用:簇头选举.

- 当自身能量低于一定的阈值时,*CH* 簇内广播选举新簇头消息
- 簇内节点选举自己邻居中信任值最高的一个,用与 *CH* 间的对密钥加密发给 *CH*
- *CH* 统计选票最多和次多的节点作为下任簇头和副簇头,将结果簇内广播
- 在新簇头节点上任之前,需通过与老簇头之间的挑战应答,如果失败
  - 则开始重新选举
  - 失败节点被列入黑名单,以后将不再对其信任值进行更新
- *CH* 定期广播征集不信任节点消息,簇内节点选择信任值最低的邻居发送给 *CH*,*CH* 对票数最多的节点进行挑战应答.

4.5 无线传感器网络中的通用信誉系统(reputation based framework for sensor networks,简称RFSN)

Ganeriwal-Srivastava于 2004 年提出了RFSN[9],其架构定义完整,是一个典型的基于信誉的信任管理系统.

(1) 目标:建立仅由可信节点组成的网络环境.

(2) 相关定义:① R_{ij}:节点i对j的信誉评价;② $(R_{ij})_D$:节点i通过对节点j的直接观察计算而得的直接信誉;③ D_{ij}:节点i对于节点j的最新监控结果;④ $(R_{ij})_{ID}$:节点i根据其他节点发送的关于节点j的信誉值计算而得到的间接信誉;⑤ T_{ij}:节点i对节点j的信任评估值;⑥ $E(\bullet)$:期望;⑦ (α_j,β_j):用来计算节点j信誉值的(成功,失败)信誉因子(从节点i的角度),初始值都为 0;⑧ ω_{age}:"老化"因子;⑨ (α_j^k,β_j^k):从节点k得到的关于节点j的(成功/失败)信誉因子.

(3) 信任计算:

- RFSN

$$R_{ij}=(R_{ij})_D+(R_{ij})_{ID},(R_{ij})_D=f(R_{ij},(R_{ij})_D),(R_{ij})_{ID}=(R_{ij})_{ID}+\sum_{n=1}^{n}\omega_{ik}\times R_{ki},\omega_{ik}=g(R_{ik})\ ,$$

$$(T_{ij})=E(R_{ij})\ .$$

- BRSN (Beta reputation system for sensor networks)

$$R_{ij}=\text{Beta}(\alpha_j+1,\beta_j+1)\ ,$$

$$T_{ij}=E(R_{ij})=\frac{\alpha_j+1}{\alpha_j+\beta_j+2}\ .$$

节点 i 与节点 j 最近合作成功/不成功次数分别为 r,s,则计算节点 j 的信誉值时需要进行参数更新:

$$\alpha_j^{\text{new}}=(\omega_{\text{age}}\times\alpha_j)+r,\ \beta_j^{\text{new}}=(\omega_{\text{age}}\times\beta_j)+s\ .$$

节点 i 从节点 k 处获得关于节点 j 的信誉因子后,节点 j 在节点 i 处的信誉值计算需要进行参数更新:

$$\alpha_j^{\text{new}}=\alpha_j+\frac{2\times\alpha_k\times\alpha_j^k}{(\beta_k+2)\times\left(\alpha_j^k+\beta_j^k+2\right)+2\times\alpha_k},\ \beta_j^{\text{new}}=\beta_j+\frac{2\times\alpha_k\times\beta_j^k}{(\beta_k+2)\times\left(\alpha_j^k+\beta_j^k+2\right)+2\times\alpha_k}\ .$$

(4) 决策与应用:只与信任值大于等于预设门限值的节点合作.

5 结 论

WSNs 下的信任管理与 WSNs 的结构特点、应用背景紧密相关.由于传感器节点资源有限,而信誉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誉的信任管理系统迄今为止并没有在 WSNs 中占据主导地位,很多系统只是对系统某方面功能进行简单修改,利用信任管理有针对性地提高该方面的安全性和可靠性,如路由、数据融合以及簇头选举等.由于 WSNs 中节点一般只存储其邻居节点的信誉值,而互为邻居的节点通过各种监控手段获得的一手资料往往差别不大,所以 WSNs 环境下横向信任合成只采用 LS 有其优势所在.此外,基于能耗考虑,也有很多系统不采用将节点设置为混杂模式的方法进行通信检测.在有簇结构的 WSNs 中,基站-簇头-普通节点的三级结构,对信任的存储、计算、共享等也提出了特殊的要求.总的来说,WSNs 下的信任管理要求轻量级的设计与实现.但是到目前为止,WSNs 下的信任管理系统大多停留在设计与仿真实验阶段,对于实际应用环境中各种信任管理系统的功效很少涉及,是否可以抵消系统中加入信任管理带来的各种耗费与风险还需要进一步检验.

由于无线传感器节点成本低廉,一般没有硬件防护措施.当节点被捕获后,其存储的秘密信息会很快泄漏.而基于密码学的安全手段在 WSNs 中主要是基于对称密码算法,所以需要及时识别被俘获节点并将其隔离.WSNs 中传感器节点易被俘获的特点使得信任管理在 WSNs 环境中的应用具有很强的实用性.无线传感器网络环境下的信任管理有以下主要发展方向:

(1) 将信任管理的思想与现有 WSNs 各项功能,尤其是各种安全措施紧密结合,如将信任管理与 WSNs 下的密钥管理、安全路由、安全的数据融合相结合,在邻居选择以及数据融合权值计算时加入节点的可信特性考虑,提高系统的安全性、可靠性.可以考虑对信任值进行功能性区分,而不是只采用一个综合的信任值,不同的信任值对应不同的采集信息和不同的应用,如对应于安全路由的信任值就可以考虑节点能量信息.

(2) 对现有信任管理系统进行改造.对现有的P2P、MANET等网络环境下的研究成果针对WSNs环境进行低能耗改造,是WSNs下研究的一个较为重要的方向.信任管理的研究在一些出现较早的网络环境下相对成熟,有些已大范围应用[32,33].但现有信任管理系统在能耗考虑及应用模式等方面都与WSNs中的信任管理有很大差异,需要进行有针对性的改造.如在电子商务中信任管理得到了很好的应用,但其信息主要来源于交易双方的主观评判,WSNs中信任管理信息来源则主要是邻居节点的检测数据;电子商务中个体信任值可作为交易时的参考,或者信誉计算的权值,来影响交易判断,在WSNs中信任的应用更为广泛,可以与系统性能、安全等方面紧密结合.

(3) 在 WSNs 实际应用环境中实施信任管理.WSNs 中的信任管理从实用层面可以分为两类,即综合性信任管理与功能性信任管理.综合性信任管理是指研究结果为较为抽象的信任管理框架,往往适用于很多应用.功能性信任管理是指基于信任的路由协议设计、基于信任的数据融合等.二者相比,后者有较多系统实现,前者往往集中在框架定义,缺乏较为全面的实现.但总的来说,无论哪种信任管理,由于 WSNs 应用范围的局限性,目前还没有像 P2P 下的信任管理系统那样有充实的数据证明其性能和优越性.

(4) 引入更加复杂、有效的信任管理模型.由于传感器节点能力的限制,目前 WSNs 中信任管理模型都较为简单,大多都是简单的概率计算模型,有些为了节省能耗只考虑本地收集的信息.随着软、硬件技术的发展,传感器节点自身能力不断提高;而且应用模式的拓展,新型传感器网络模式的出现,使得高能力传感器节点得以应用[34,35].在此前提下,可以考虑引入一些更加复杂、有效的信任计算模型.此外,随着像智能交通中的车载传感器网络等新型传感器网络形式的出现,一些新特点被引入,如节点具有较强移动性、节点邻居不再相对固定,需要新的信任管理模型以适应新型网络架构及应用的需求.

(5) 将风险评估与信任管理相结合.WSNs 与应用是紧密相关的,不同的应用对 WSNs 中信任管理的影响也不同.如在军用和民用环境下,节点被俘获的风险明显不同;在热带雨林和干燥平地环境下,节点遭到自然破坏的风险也有所不同.在决策时综合考虑风险和信任因素,可以增强信任管理的灵活性和可用性.如环境风险较高的情况下,可以考虑提高决策的信任值阈值,选择更可信的邻居节点,或者加大高信任值节点信息的权值.

References:

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. In: Dale, J, Dinolt, G, eds. Proc. of the 17th Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1996. 164−173.

[2] Ellison CM, Franz B, Rivest R, Thomas BM, Ylonen T. Simple public key infrastructure certificate theory. IETF RFC 2693, 1999.

[3] Li NG, Mitchell JC. RT: A role-based trust-management framework. In: Werner B, ed. Proc. of the 3rd DARPA Information Survivability Conf. and Exposition (DISCEX III). Washington: IEEE Computer Society Press, 2003. 201−212.

[4] Freudenthal E, Pesin T, Port L, Keenan E, Karamcheti V. dRBAC: Distributed role-based access control for dynamic coalition environments. Technical Report, TR2001-819, New York University, 2001.

[5] Li NH, Mitchell JC, Winsborough WH. Beyond proof-of-compliance: Security analysis in trust management. Journal of the ACM, 2005,52(3):474−514.

[6] Seng CY, Arbaugh WA. A secure trust establishment model. In: Werner B, ed. Proc. of the IEEE Int'l Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2006). Piscataway: IEEE Computer Society, 2006. 78−85.

[7] Ryutov T, Neuman C. Trust based approach for improving data reliability in industrial sensor networks. In: Etalle S, Marsh S, eds. Proc. of the IFIP Int'l Federation for Information, Vol.238. Boston: Springer-Verlag, 2007. 349−365.

[8] Tanachaiwiwat S, Dave P, Bhindwale R, Helmy A. Secure locations: routing on trust and isolating compromised sensors in location-aware sensor networks. In: Proc. of the SenSys 2003. New York: ACM Press, 2003. 324−325.

[9] Ganeriwal S, Srivastava M. Reputation-based framework for high integrity sensor networks. In: Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004). New York: ACM Press, 2004. 66−77.

[10] Krasniewski MD, Varadharajan P, Rabeler B, Bagchi S, Hu YC. TIBFIT: Trust index based fault tolerance for ability data faults in sensor. In: Werner B, ed. Proc. of the Int'l Conf. on Dependable Systems and Networks (DSN). Piscataway: IEEE Computer Society, 2005. 672−681.

[11] Crosby GV, Pissinou N, Gadze J. A framework for trust-based cluster head election in wireless sensor networks. In: Proc. of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS 2006). Piscataway: IEEE Computer Society, 2006. 13−22.

[12] Huang L, Li L, Tan Q. Behavior-Based trust in wireless sensor network. In: Shen HT, Li JB, Li ML, Ni J, Wang W, eds. Proc. of the APWeb Workshops 2006. LNCS 3842, Berlin, Heidelberg: Springer-Verlag, 2006. 214−223.

[13] Cheng WF, Liao XK, Shen CX, Li SS, Peng SL. A trust-based routing framework in energy-constrained wireless sensor networks. In: Cheng XZ, Li W, Znati T, eds. Proc. of the WASA 2006. LNCS 4138, Berlin, Heidelberg: Springer-Verlag, 2006. 478−489.

[14] Yu B, Chen HG, Yang M, Mao DL, Gao CS. A key management scheme for cross-layering designs in wireless sensor networks. In: Pan Y, Chen DX, Guo MY, Cao JN, Dongarra J, eds. Proc. of the ISPA 2005. LNCS 3758, Berlin, Heidelberg: Springer-Verlag, 2005. 757−768.

[15] Yin ZY, Zhao H, Lin K, Sun PG, Luo D, Zhang XY, Wang XY. A coverage-preserving node scheduling scheme based on trust selection model in wireless sensor networks. In: Proc. of the 1st Int'l Symp. on Pervasive Computing and Applications. Piscataway: IEEE Computer Society, 2006. 696−698.

[16] Xu MD, Du RY, Zhang HG. A new hierarchical trusted model for wireless sensor networks. In: Proc. of Computational Intelligence and Security (CIS). Piscataway: IEEE Computer Society, 2006. 1541−1544.

[17] Shaikh RA, Jameel H, Lee S, Rajput S, Song YJ. Trust management problem in distributed wireless sensor networks. In: Proc. of the RTCSA. Piscataway: IEEE Computer Society, 2006. 411−414.

[18] Tanachaiwiwat S, Dave P, Bhindwale R, Helmy A. Location-Centric isolation of misbehavior and trust routing in energy-constrained sensor networks. In: Hassanein H, Oliver RL, Richard III GG, Wilson LF, eds. Proc. of the IEEE Workshop on Energy-Efficient Wireless Communications and Networks (EWCN). Piscataway: IEEE Computer Society, 2004. 463−469.

[19] Yao ZY, Kim DY, Lee I. A security framework with trust management for sensor networks. In: Proc. of the 1st IEEE/CREATE-NET Workshop on Security and QoS in Communication Networks Athens. Piscataway: IEEE Computer Society, 2005. 190−198.

[20] Hur J, Lee Y, Hong SM, Yoon H. Trust management for resilient wireless sensor networks. In: Won DH, Kim SJ, eds. Proc. of the ICISC 2005. LNCS 3935, Berlin, Heidelberg: Springer-Verlag, 2006. 56−68.

[21] Hur J, Lee Y, Yoon H, Choi D, Jun S. Trust evaluation model for wireless sensor networks. In: Proc. of the ICACT 2005. Piscataway: IEEE Computer Society, 2005. 491−496.

[22] BoukercheA, Xu Li. ATRM: An agent-based trust and reputation management scheme for wireless sensor networks. In: Global Telecommunications Conf. (GLOBECOM). New York: IEEE, 2005. 1857−1861.

[23] Grandison T, Sloman M. A survey of trust in Internet application. IEEE Communications Surveys and Tutorials, 2000,3(4):2−16.

[24] Agah A, Das SK, Basu K. A game theory based approach for security in wireless sensor networks. In: Hassanein H, Oliver RL, Richard III GG, Wilson LF, eds. Proc. of the IEEE Int'l Conf. on Performance, Computing and Communications. Piscataway: IEEE Computer Society, 2004. 259−263.

[25] Zhang W, Das SK, Liu YH. A trust based framework for secure data aggregation in wireless sensor networks. In: Proc. of the IEEE SECON 2006. Piscataway: IEEE Computer Society, 2006. 60−69.

[26] Roosta T, Meingast M, Sastry S. Distributed reputation system for tracking applications in sensor networks. In: Proc. of the 3rd Annual Int'l Conf. on Mobile and Ubiquitous Systems: Networking & Services. IEEE, 2006. 1−8.

[27] Yao ZY, Kim D, Doh Y. PLUS: Parameterized and localized trust management scheme for sensor networks security. In: Proc. of the IEEE Int'l Conf. on Mobile Adhoc and Sensor Systems (MASS). Piscataway: IEEE Computer Society, 2006. 437−446.

[28] Hsieh MY, Huang YM, Chao HC. Adaptive security design with malicious node detection in cluster-based sensor networks. Computer Communications, 2007,30(11):2385−2400.

[29] Probst MJ, Kasera SK. Statistical trust establishment in wireless sensor networks. In: Proc. of the Int'l Conf. on Parallel and Distributed Systems. IEEE Computer Society, 2007. 1−8.

[30] Slijepcevic S, Tsiatsis V, Zimbeck S, Potkonjak M, Srivastava MB. On communication security in wireless ad-hoc sensor networks. In: Proc. of the 11th IEEE Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE 2002). Washington: IEEE Computer Society, 2002. 139−144.

[31] Anderson R, Chan H, Perrig A. Key infection: Smart trust for smart dust. In: Proc. of the 12th IEEE Int'l Conf. on Network Protocols (ICNP 2004). Los Alamitos: IEEE Computer Society, 2004. 206−215

[32] Page L, Brin S, Motwani R, Winograd T. The pagerank citation ranking: Bringing order to the Web. In: Stanford Digital Library Technologies Project. 1998. http://dbpubs.stanford.edu/pub/1999-66

[33] Kamvar SD, Schlosser MT, Garcia-Molina H. The eigentrust algorithm for reputation management in P2P networks. In: Proc. of the 12th Int'l World Wide Web Conf. New York: ACM Press, 2003. 640−651.

[34] http://cartel.csail.mit.edu/

[35] http://research.cens.ucla.edu/areas/2007/Urban_Sensing

荆琦(1974－),女,黑龙江大庆人,博士生,主要研究领域为网络与信息安全,信任管理,分布式访问控制,无线自组织网络安全.

唐礼勇(1972－),男,博士,副研究员,主要研究领域为网络与信息安全,系统软件.

陈钟(1964－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网络与信息安全,面向领域的软件工程.