

一种基于节点多角度信任的无线传感器网络

董慧慧 郭亚军

(华中师范大学计算机科学系 武汉 430079)

摘要 基于通信的信任模型不能完全解决无线传感器网络面临的安全威胁和节点能量不足的问题。提出一种基于节点通信、数据和能量相结合的信任模型,将传感数据和节点能量加入节点信任评估因素中,通过不同的信任计算方法得出各自的信任值,建立一个节点更加可信的无线传感器网络。模拟实验结果表明,基于通信一种因素的信任模型不足以决定一个节点的可信性,基于多角度的信任模型能够更简单、准确地判断一个节点的可信性。

关键词 无线传感器网络,通信信任,数据信任,能量信任

Wireless Sensor Networks Based on Multi-angle Trust of Node

DONG Hui-hui GUO Ya-jun

(Department of Computer Science, Huazhong Normal University, Wuhan 430079, China)

Abstract The trust model based on communication can not completely solve the problems of security threats and lack of energy in wireless sensor networks. A trust model based on communication, data and energy was proposed in this paper, which added the sensing data and the node's energy in the factors of trust assessment, and used different methods to calculate the separate trust values. By this way, a wireless sensor network of node more reliable could be established. Simulation results show that, one model only based on communication trust is not enough to decide on the trustworthiness of a node, and the model based on multi-angle trust can judge the credibility of a node more simply and accurately.

Keywords Wireless sensor networks, Communication trust, Data trust, Energy trust

无线传感器网络(Wireless Sensor Networks, 简称 WSNs)由大量具有无线通信、有限数据处理和监测能力的传感器节点组成。这些传感器节点体积小,电池供电,一般被部署在无人照看或敌方区域,可用来监测环境、安防森林、跟踪目标、收集敌方信息等。随着 WSNs 日益广泛的应用,其自身能量有限、无法保证安全的部署区域以及网络拓扑结构动态变化太快等特点导致它的安全隐患越来越大。传统的基于密码学的安全机制可以抵御外部攻击,但是无法有效抵御节点容易被俘获的内部攻击,这就需要有效的机制来及时识别被俘获节点,采取相应补救措施以减少系统损失。

1 WSNs 中的信任管理

信任管理现在已经成为基于密码学安全措施的有效补充手段,在传统的 P2P 网络、普适计算以及网格等网络环境下都得到广泛的研究和应用。尽管研究者已经开始研究无线传感器网络中的信任问题,但是他们仍然沿用的是传统网络中利用授权凭证进行信任管理的方式,这对于节点资源有限、网络应用相对单一的 WSNs 来说是不适合的。所以,目前 WSNs 的信任管理系统的研究主要是通过对节点进行信任值评估来增强 WSNs 的安全性。

不可信节点是 WSNs 的一个重要安全隐患。信任管理

系统针对不同的目标节点将不可信节点分为恶意节点、自私节点、低竞争力节点^[2-4]等3类。

恶意节点是指具有直接恶意行为和间接恶意行为的节点。直接的恶意行为包括丢弃要转发的正常数据包、更改数据内容、更改数据包地址、随意转发数据包、发送假数据包等。间接的恶意行为是指故意降低正常邻居节点的信誉值,或者提高恶意节点的信誉值、更换新标识重新加入网络等,以扰乱网络正常的信任管理。

自私节点指的是网络中为了节省自身电池能量而不参与服务的节点。比如不参与路由发现,使自己在任何节点的路由表中都不出现。

低竞争力节点指节点的能量很低,不足以提供服务,过度地使用则会造成网络的生命周期缩短。

以上3种类型的不可信节点的行为在 WSNs 中会直接影响节点间的信任关系。第3节中进行的信任计算工作将会根据信任值的大小发现这些不可信节点,及时采取相应措施以保证整个网络的安全。

目前对于 WSNs 中节点信任值的评估主要是基于节点通信信任(成功或失败)的角度。现在通用的一个建立可信节点的 WSNs 信誉系统是由 Ganeriwal-Srivastava 提出的 RF-SN^[1]模型,其架构定义完整,利用 Beta 概率函数来计算信任

到稿日期:2008-10-28 返修日期:2009-01-07 本文受国家自然科学基金(项目编号:60773008),国家 863 项目(项目编号:2007AA01Z138),湖北省教育厅科技项目(项目编号:B20084002),中国博士后基金(项目编号:20070410953)资助。

董慧慧(1983-),女,硕士生,主要研究方向为信息安全,E-mail: dhh003@163.com;郭亚军(1965-),男,博士,教授,主要研究方向为计算机安全与保密、普适计算等。

值。但是在计算过程中,它只考虑了通信方面的因素。另外,有研究者针对数据因素单独提出基于信任的传感器网络中的容错系统或安全数据融合方法。在这些研究中,他们只是单独考虑数据信任而没有考虑通信信任和能量信任。事实上,单独从通信或者数据一个角度来决定 WSNs 的节点信任是不够的。因为相对于其他类型的网络,WSNs 的节点不但具有路由选择的通信能力,还有独特的监测能力,可以发送和接收传感数据,而且节点的能量对于整个网络的生命周期有至关重要的作用。因此,对于无线传感器网络的信任管理,通信、数据和能量三者的信任都是不可缺少的。只是需要新的技术来检查实际传感数据和平衡节点能量,需要新的信任值计算方法,使三种因素结合的信任值计算更加简单有效,减少计算复杂度和时间复杂度,为 WSNs 制定一个合理的联合信任。

2 WSNs 中的信任模型

信任关系的建立一般取决于实体间直接和间接交互行为的评价。直接信任指的是本地观测信任值,即第一手资料;间接信任指的是邻居节点发送的信誉值,即第二手资料。在 WSNs 节点通信信任值计算的模型中,使用了直接信任和间接信任相结合的方法。

当然,除了考虑与 Ad hoc 和 P2P 网络信誉系统中一样的通信信任因素外,WSNs 还要考虑传感数据的可信性和节点剩余能量的可用性。因为单独从通信角度来看不足以决定 WSNs 中的节点是否可信,这点可以通过第 4 节的实验比较进行证明。

在数据信任方面,根据事件发生周围的节点是否发送报告和节点本身的信任值可以判断事件发生的真实性,从而更新一个节点的容错信任值。事件发生后,通过检查传感器节点采集的具体数据(比如报告温度、湿度和大气压值等)是否一致,可以计算一个节点的融合信任值。本文在数据信任值计算过程中采用上述数据容错和数据融合相结合的方法。

节点能量信任的信任值计算则直接采用简单的阈值比较法。

下面先定义一个无线传感器网络的场景,区分前面提到的通信信任、数据信任和节点能量信任。假设节点(1,2,3)和一个数据融合中心 DFC(Data Fusion Center)组成一个 WSNs 的场景,如图 1 所示。在此场景下,节点的部署是为了监测事件和向 DFC 汇报传感数据。无论节点中是否存在敌方节点,节点间都可以通信,即发送和接收信息(比如路由选择),但是也许出于某种原因,节点可以不汇报自己的传感数据。相反,节点也可以汇报自己的传感数据却不发送来自其它节点的信息(路由选择)。此外,节点可以根据剩余能量决定是否接收或发送信息。

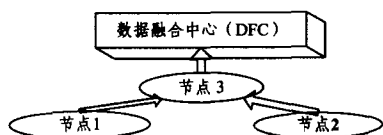


图 1 无线传感器网络模型

例如,如果图 1 中的节点 3 向 DFC 转发所有来自节点 1 和节点 2 的信息,这意味着它在通信方面是非常值得信任的。但是如果节点 3 是敌方节点,在有一个同伙入侵者正在该场

景活动时,它不会向网络中的其他节点汇报自己真实的传感数据,这种情况下通信方面虽然非常值得信任,但数据方面却不值得信任。相反,如果网络中所有节点同时发送它们的传感数据(比如温度、压强等)给节点 3,由于通信代价非常大,节点 3 没有接收节点 1 和节点 2 的路由选择信息,这样节点 3 在数据方面是非常值得信任的,但是在通信方面来看却是不值得信任的。除了上述两种情况外,如果节点 3 在接收了所有节点发送的传感数据和路由选择信息之后,没有足够的剩余能量向 DFC 汇报,则节点 3 虽然在通信方面和数据方面都值得信任,但是其自身的剩余能量是不能信任的。因此,需要一个能够发现这种情况的机制,以把这种情况及时报告给其他节点和 DFC。

基于上述分析,扩展以前单独基于通信信任的信任模型,结合数据信任和节点能量信任建立一个新的信任模型,如图 2 所示。

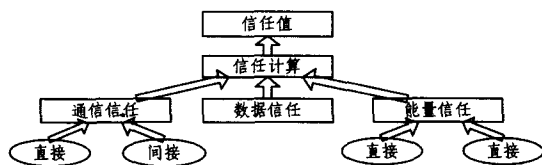


图 2 WSNs 中一种节点信任计算模型

3 WSNs 中的信任计算

3.1 通信信任计算

在本文中,通信信任是指在 WSNs 中两个可以互相发送和接收信息的节点之间的信任值的计算。关于 WSNs 的信任计算,研究者已经在不同的应用领域提出几种不同的信任计算方式。Ganeriwai 和 Srivastava 为 WSNs 建立的 Beta 信任模型是利用 Josang 和 Jsmail^[5]的工作获得电子商务环境中交易节点的信誉率。Srinivasan, Teitebaum 和 Wu^[6]也提到在 WSNs 中利用 Beta 信誉系统的可能性。本文结合以上研究方法,利用简化的 Beta 信任模型进行通信信任的计算。

对于 $Beta(\alpha, \beta)$ 分布的概率密度分布函数的数学形式是

$$f(x|\alpha, \beta) = \frac{1}{B(\alpha, \beta)} x^{\alpha-1} (1-x)^{\beta-1} \quad (1)$$

其中, $0 \leq x \leq 1, \alpha > 0, \beta > 0$ 。

这个概率分布函数可以应用于节点信誉的建模。因为在节点信誉系统中,假设节点成功交易的次数为 s ,失败交易的次数为 f ,使用 Beta 概率模型很容易完成新的交易结果评估,即只要使 $s+1, f+1$ 作为新的参数,就可以完成对被评估节点的直接信任的更新计算。

对 WSNs 中的任意节点 i 由邻居节点 j 得到一个信誉 $R_{i,j}$, $R_{i,j}$ 通过简化的 Beta 信任模型和 $s_{i,j}$ 及 $f_{i,j}$ 两个参数得到,即

$$R_{i,j} = Beta(s_{i,j} + 1, f_{i,j} + 1) \quad (2)$$

其中, $s_{i,j}$ 是节点 i 和 j 成功交易的次数, $f_{i,j}$ 是失败交易次数。

信任定义为信誉的期望值,则可以由式(1)和式(2)计算出节点 i 的直接信任值 $T_{i,j}^d$,即

$$T_{i,j}^d = E(R_{i,j}) = \frac{s_{i,j} + 1}{s_{i,j} + f_{i,j} + 2} \quad (3)$$

节点 i 的间接信任值是通过节点 j 的邻居节点 k 间接得出的。节点 j 收到节点 k 对节点 i 的信誉评估值 $R_{i,k}$, 参数分别为 $s_{i,k}$ 和 $f_{i,k}$ 。根据这个新的信誉值和式(3)得出的节点 j

对节点 i 的直接信任值 $T_{i,j}^d$, 节点 j 可以得出被评估节点 i 的综合信任值 $T_{i,j}$, 即

$$T_{i,j} = E(R_{i,j}) = \frac{s_{i,j} + 1}{s_{i,j} + f_{i,j} + 2} \quad (4)$$

其中, $R_{i,j} = \text{Beta}(s_{i,j}, f_{i,j})$, 参数 $s_{i,j} = s_{i,j} + \frac{s_{i,k}}{2}$, $f_{i,j} = f_{i,j} + \frac{f_{i,k}}{2}$ 。

3.2 数据信任计算

在 WSNs 中, 由于它独特的传感器节点具有监测传感数据能力, 数据的可信性也是影响节点可信性的重要因素。在本文中, 数据信任指的是针对系统的数据容错能力和数据内容的一致性进行信任值的评估。通过数据信任值的计算, 可以及时发现自私节点, 以采取相应的安全措施。Josang 的信任模型^[7,8]曾在 WSNs 中用来处理数据流不确定因素的问题。Krasniewski 等人提出基于信任的容错系统 TIBFIT^[9], 计算具有簇结构的 WSNs 中的节点信任值。Hur 等人^[10,11]提出基于信任的安全数据融合算法, 通过检查数据的一致性来计算数据融合的信任值。本文结合 Krasniewski 和 Hur 等人的研究方法, 提出一个简化的数据信任计算方法。

定义 1(Region) 将 WSNs 划分为 $\frac{\sqrt{n}}{d} \times \frac{\sqrt{n}}{d}$ 大小的域, 每个域有自己的标识 RegionId, 其中 d 是每个域中节点感知的最远距离。

定义 2(T_i) 节点 i 的容错信任值, 只能取值 0 或 1; N_i : 每个域中发送报告的节点个数; N_f : 未发送报告的节点个数; w_1 : 容错信任在数据信任中的权值。

定义 3($T_i^u = \frac{us_i - uf_i}{us_i + uf_i}$) 节点 i 发送报告的可信性, 其中 us_i 是发送成功的次数, uf_i 是发送失败的次数; w_2 : 报告可信性在数据信任中的权值。

定义 4($T_i^v = \frac{vs_i - vf_i}{vs_i + vf_i}$) 节点 i 采集数据的一致性, vs_i 为一致性次数, vf_i 为不一致性次数; w_3 : 数据一致性在数据信任中的权值。

WSNs 中节点 i 数据综合信任值记作 T_i^d , 计算过程如下:

(1) $m = N_i - N_f$ 。若 $m > 0$, 则 $T_i^d = 1$, 否则 $T_i^d = 0$;

(2) $T_i^d = w_1 T_i + w_2 T_i^u + w_3 T_i^v$ 。

3.3 能量信任计算

在 WSNs 系统中, 网络的生命周期和节点能量有密切的关系。由于它特有的传感器节点, 节点能耗主要用在数据采集、路由以及数据融合方面。如果过度消耗个别节点的能量, 生存周期就会剧减。因此, 通过对节点能量的信任计算, 可以随时了解节点的现有能量, 避免低竞争力节点的过度使用。在本文中, 节点能量信任指的是节点现有的能量是否低于一个既定的阈值, 能否完成新的通信和数据处理任务。

定义 5(T_i^e) $T_i^e \in [0, 1]$, 节点 i 的能量信任值。

定义 6(θ) $\theta > 0$, 节点能量阈值; 若节点能量低于阈值, 则 T_i^e 为 0。

定义 7(E_i) 节点 i 的现存能量; $e_{w,i}$ 为节点 i 发送和接收数据包所需要的能量; $e_{d,i}$ 为节点 i 数据采集或处理所需的能量。

WSNs 中节点 i 能量的信任计算过程如下:

$$(1) T_i^e = \frac{E_i}{e_{w,i} + e_{d,i}}.$$

(2) 若 $T_i^e \geq \theta$, 则节点 i 的能量信任值 $T_i^e = \frac{1}{T_i^e}$, 否则 $T_i^e = 0$ 。

4 实验与分析

在模拟实验中比较了在两种不同状况下节点 i 和 j 之间的信任关系, 即所有节点完全可信和节点 i 或 j 是不可信节点这两种情况。

由于基于通信、数据和能量的信任计算中, 3 个方面在不同需求的情况下侧重点会有所不同, 因此应视情况来确定各自在联合信任中的权重。在此次实验中对通信、数据、能量信任采用的权重分别是 50%, 30% 和 20%。而在仅仅基于通信信任角度的简化 RFSN 模型中, 通信信任的权重是 100% 的, 即不考虑数据和能量信任。

第一种所有节点完全可信情况下的比较结果如图 3 所示。随着交易次数的增加, 在没有不信任节点(恶意、自私、低竞争力节点)出现的理想状态下, 基于通信信任角度的 RFSN 模型与基于多角度信任的模型(通信、数据、能量)两种信任管理方式下的节点信任关系相似, 节点 i 和 j 之间的信任关系趋近于 1。

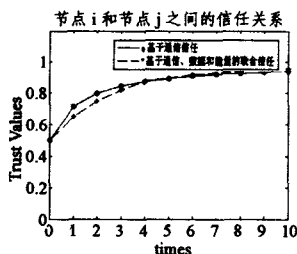


图3 节点完全可信

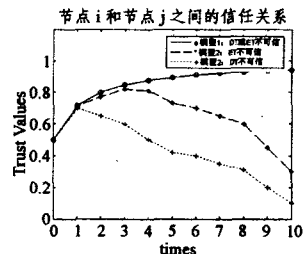


图4 节点 i 不可信

如果某些节点只在通信方面可信, 而在数据或能量方面不可信时, 两种信任模型下的节点信任关系就完全不一样。图 4 表明了节点 i 成为不可信节点后两种信任模型下节点 i 和节点 j 之间的信任关系。模型 1 和模型 2 分别是基于通信信任的 RFSN 模型和基于多角度信任的模型。CT 代表节点通信信任, DT 代表节点数据信任, ET 代表节点能量信任。

图 4 表明了基于通信信任角度的 RFSN 模型并不能发现数据和能量方面的不可信行为, 而基于多角度信任的模型随着交易次数的增加, 可以迅速地识别不可信节点, 提高了 WSNs 的安全性。

结束语 通过建立通信、数据和能量相结合的信任模型, 可以更加容易识别 WSNs 中的不可信节点; 通过简便的信任值计算方法, 可以节约节点计算耗能, 降低计算复杂度和时间复杂度, 从而建立一个节点更加可信的无线传感器网络。

随着对 WSNs 的信任管理研究, 将通信信任、数据信任和能量信任有效地结合起来解决 WSNs 的信任问题, 是下一步将要进行的工作。

参考文献

- [1] Ganesiwal S, Srivastava M. Reputation-based framework for high integrity sensor networks[C]// Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks. Washington DC, October 2004: 66-77

(下转第 82 页)

仿真结果表明,采用时延作为重新计算路由的尺度时,采用切换优化策略下的时延大于无切换优化策略下的时延。这是因为,切换优化以减少切换次数为目标,而无切换优化的情形下,切换时,总是以最大仰角的星地链路的卫星为接入卫星,因此,无切换优化的情形下的总平均时延为 0.06193s,优于有切换优化的情形下的时延 0.06218s。

采用时延作为重新计算路由的尺度时,链路切换次数和时延性能如表 2 所列。

表 2 时延最小切换策略下的性能

	切换次数		平均时延 (s)	时延抖动/ 方差
	星地链路	星间链路		
切换优化情形	327	2576	0.06218	0.01152
无切换优化情形	429	3155	0.06193	0.01102

采用时延作为重新计算路由的尺度时,有切换优化和无切换优化的时延性能均优于跳数最少切换策略下,这两种情形的性能。这是因为在无切换优化策略下,切换时,以仰角最大的卫星为接入卫星,客观上是选择离终端最近的卫星。同时,又以时延为重新计算路由时的代价尺度,在此情形下可以达到时延最小的目标。另一方面,星地链路、星间链路的切换次数与跳数最小时的切换次数相当。而且,以时延为重路由尺度时,采用切换优化时的切换次数也小于无切换优化策略的情形。

仿真实验还表明,该算法具有较好的可定制特性,通过配置切换优化参数、算法策略选择参数,能够方便地实现不同策略的配置,以便对跳数最少策略、传播时延最小策略以及单分组传输时延最小策略(即大带宽链路优先选择)、“下一颗”卫星切换优化策略等进行灵活配置和仿真分析比较。

结束语 本文对低轨移动通信卫星星座进行了深入分析,研究了移动卫星通信网络中的切换问题,提出了低轨移动卫星切换方案,包括星地链路切换算法和重新计算路由算法。仿真实验表明,时延最小策略下的无切换优化策略具有最优的时延性能。而从减少切换次数的角度考虑,可采用切换优

化策略。仿真实验还表明,本文提出的链路切换算法具有良好的可定制性和灵活性。

参考文献

[1] Deler A, Pierucci L. Next-generation mobile satellite networks[J]. IEEE Communications Magazine, 2002, 40(9): 150-159

[2] Zahariadis T, Vaxevanakis K G, Tsantilas C P, et al. Global roaming in next-generation networks[J]. IEEE Communications Magazine, 2002(2): 145-151

[3] Gkizeli M, Tafazolli R, Evans B. Performance analysis of handover mechanisms for non-geo satellite diversity based Systems[C]//IEEE GLOBECOM'01. 2001: 2744-2748

[4] Bottcher A, Werner B. Strategies for handover control in low earth orbit satellite systems[C]// Vehicular Technology Conference, 1994 IEEE 44th. 1994: 1616-1620

[5] Cho S, Akyildiz I F, Bender M D, et al. A new spotbeam handover management technique for LEO satellite networks[C]//IEEE GLOBECOM '00. 2000: 1156-1160

[6] Cho S. Adaptive dynamic channel allocation scheme for spot-beam handover in LEO satellite networks[C]//IEEE VTS-Fall VTC 2000. 52nd. 2000: 1925-1929

[7] Nguyen H N, Lepaja S. Handover management in low earth orbit satellite IP networks[C]//IEEE GLOBECOM '01. 2001: 2730-2734

[8] Walker J G. Satellite constellations[J]. J British Interplanetary Soc, 1984, 37: 559-571

[9] Rider L. Optimized polar constellation for redundant earth coverage[J]. Journal of the Astronautical Sciences, 1985, 33(2): 147-161

[10] 刘刚, 苟定勇, 吴诗其. 低轨卫星星座网的切换研究[J]. 通信学报, 2004, 25(4): 151-159

[11] McCanne S, Floyd S. The LBNL network simulator, ns-2[OL]. <http://www.isi.edu/nsnam/ns>. 1997-10-01/ 2007-05-18

(上接第 45 页)

[2] Tanachaiwiwat S, Dave P, Bhindwale R, et al. Secure locations: routing on trust and isolating compromised sensors in location-aware sensor networks[C]// Proceedings of the SenSys 2003. New York: ACM Press, 2003: 24-32

[3] Cheng W F, Liao X K, Shen C X, et al. A trust-based routing framework in energy-constrained wireless sensor networks[C]//Cheng X Z, Li W, Znati T. eds. Proc. of the WASA 2006. LNCS 4138. Berlin, Heidelberg: Springer-Verlag, 2006: 478-489

[4] Tanachaiwiwat S, Dave P, Bhindwale R, et al. Location-Centric isolation of misbehavior and trust routing in energy-constrained sensor networks[C]//Hassanein H, Olive R L, Richard III G G, et al., eds. Proc. of the IEEE Workshop on Energy-Efficient Wireless Communications and Networks (EWCN). Piscataway: IEEE Computer Society, 2004: 463-469

[5] Srinivasan A, Teitelbaum J, Wu J. Distributed Reputation-based Beacon Trust System[C]// Proceedings of 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. 2006: 277-283

[6] Josang A, Ismail R, Boyd C. A Survey of Trust and Reputation Systems for Online Service Provision[J]. Decision Support Systems, March 2007: 618-644

[7] Wagner D. Resilient Aggregation in Sensor Networks[C]//Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks. Washington DC, 2004: 78-87

[8] Krasniewski MD, Varadharajan P, Rabeler B, et al. Trust index based fault tolerance for ability data faults in sensor[C]//Werner B, ed. Proc. of the Int'l Conf. on Dependable Systems and Networks (DSN). Piscataway: IEEE Computer Society, 2005: 672-681

[9] Hur J, Lee Y, Hong S M, et al. Trust management for resilient wireless sensor networks[C]//Won D H, Kim S J, eds. Proc. of the ICISC 2005. LNCS 3935. Berlin, Heidelberg: Springer-Verlag, 2006: 56-68

[11] Hur J, Lee Y, Yoon H, et al. Trust evaluation model for wireless sensor networks[C]//Proc. of the ICACT 2005. Piscataway: IEEE Computer Society, 2005: 491-496