基于多事件并发的无线传感网数据一致性信任评价

沈海波 张 宏 姜海涛 刘方斌
(南京理工大学计算机科学与技术学院 南京 210094)

摘 要 目前无线传感器网络的信任评价模型主要研究节点通信方面的信任,很少研究节点发送数据一致性方面的信任。数据一致性信任评价要求一段时间以内传感区域只发生一个事件,否则不但不能准确区分多个事件,还会把合法节点与恶意节点混淆,针对这一局限,提出一种适用于多事件并发的数据一致性信任评价方法。仿真结果表明,在传感区域多事件并发的时候,该方法能准确区分多个事件,也能发现并排除恶意节点,降低误判率。

关键词 无线传感器网络,多事件并发,数据一致性,信任评价
中图法分类号 TP391 **文献标识码** A

Data Consistency Trust Evaluation of Wireless Sensor Networks Based on Multi-event Concurrent

SHEN Hai-bo ZHANG Hong JIANG Hai-tao LIU Fang-bin
(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract Currently, trust evaluation models mainly research the trust of nodes communication and few of these models research the trust of data consistency. However, trust evaluation of data consistency requires that sensing area happens only one event in a period of time, otherwise events can not be distinguished from each other accurately and legitimate node may be mistaken as malicious nodes. To resolve this problem, we proposed a method of trust evaluation of data consistency which is suitable for multi-event is concurrent. Simulation results show that, when multi-event is concurrent in sensing area, networks can distinguish events from each other accurately. It also can discover and exclude malicious nodes and reduce the false positive rate.

Keywords Wireless sensor networks, Multi-event concurrency, Data consistency, Trust evaluation

1 引言

无线传感器网络(Wireless Sensor Networks, WSNs)是由许多分布式部署的传感器节点组成的无线网络,这些传感器只有有限的缓存、能量、计算能力以及交互能力[1],主要负责将监控和探测到的实时数据发送给基站。随着无线传感器网络在军事监视、环境监测、交通控制、医疗保健等领域的应用[2]日益复杂,人们对其安全性也提出了更高的要求。传统的基于密码体系的安全机制主要用于抵抗外部攻击,但无法有效解决由恶意节点产生的内部攻击[3]。信任评价机制根据WSNs以往的通信交互,聚合各种信息来对传感器节点进行信任认定,以区分合法节点和恶意节点,有效地解决了内部攻击[4]。

无线传感器网络的信任评价除了考虑与P2P网络和Ad-hoc网络中一样的通信因素外,还需要考虑数据、能量等因素,这是由传感器节点本身的功能和特性(采集数据、能量有限)所决定的[5]。目前大多数信任模型只考虑了通信因素。Junbeom Hur等人在文献[4]中提出了一种同时考虑通信、能量以及数据的信任评价模型(Trust Evaluation Model for Wireless Sensor Networks, TEM),该模型能够发现并排除恶意节点。但是这个模型在数据一致性评价方面要求一段时间以内传感区域中只发生一个事件,不适用于多事件并发的情况,否则不但不能准确区分多个事件,还可能会把合法节点当作恶意节点来处理。

针对上述问题,本文提出一种基于多事件并发的数据一致性信任评价方法(The Data Consistency Trust Evaluation Based on Multi-event Concurrent, DCTEMC)。该方法在计算信任值的时候对数据一致的邻居节点信任值增加,对数据不一致的邻居节点信任值保持不变,并通过比较信任评价的大小找出恶意节点。仿真结果表明,在传感区域多事件并发的时候,能准确区分多个事件,也能发现并排除恶意节点,并且针对恶意节点联合攻击的情况,能有很好的防御作用。

2 多事件并发时存在的问题

2.1 多事件并发

我们采用文献[4]中的假设,将传感区域划分为若干边长

到稿日期:2012-05-17 返修日期:2012-08-21 本文受国家自然科学基金(60903027),江苏省自然科学重大研究项目(BK2011023),江苏省自然科学基金(BK2011370),连云港工业攻关科技项目(CG1124)资助。

沈海波(1987—),男,博士生,主要研究方向为无线传感器网络安全,E-mail:hbshen29@163.com;张 宏(1956—),男,教授,博士生导师,主要研究方向为网络性能和信息安全;姜海涛(1985—),男,博士生,主要研究方向为无线网络路由协议;刘方斌(1985—),男,博士生,主要研究方向为无线网络安全。

为 $r/\sqrt{2}$ 的正方形网格，其中 r 为传感器节点的感知范围半径。在节点随机部署的情况下，也使每个网格有足够多的节点来感知该网格内发生的事件，以为该网格内的成员节点进行信任评估提供足够的信息。因为这样的网格划分已经非常细小了，所以假定在一定的时间间隔 Δt 内，同一网格只会发生一个事件。但是不同网格在同一时间间隔内允许同时发生多个事件，这就是多事件并发的情况。

2.2 存在的问题

本文以两个事件并发为例说明多事件并发时存在的问题。如图 1 所示，两个大的圆表示事件 X 和 Y 发生时能感知到事件的范围，在时间间隔 Δt 内，两个事件同时发生在两个相邻的网格 A 和 B 中。根据图中所示，最终反馈结果应该是网格 A 感知到事件 X，网格 B 感知到事件 Y，但 TEM 方法得出的结果是网格 A 和 B 反馈的都是介于事件 X 和 Y 之间的事件信息，不能准确区分两个事件。

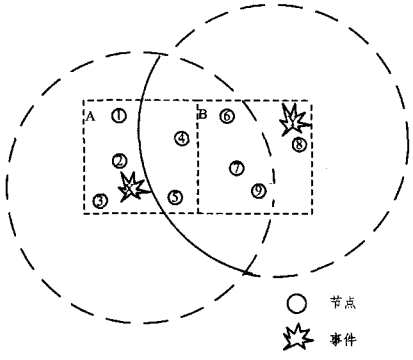

图 1 多事件并发演示图

另外 TEM 方法在区分合法节点和恶意节点上存在如下问题。假设感知到事件的传感器节点只把自己在 Δt 内先感知到的事件信息(包括感知到事件的时间和数据)广播给自己的邻居。考虑 A 中的成员节点 2，节点 2 只感知到了事件 X，其在时间间隔 Δt 结束前会对邻居节点(节点 1、3、4、5、6、7)广播的信息进行数据一致性计算，这些邻居节点感知到事件的情况有 4 种可能：1)只感知到事件 X，如节点 1、3；2)只感知到事件 Y，邻居节点中没有这样的节点；3)先感知到事件 X，后感知到事件 Y，如节点 4、5；4)先感知到事件 Y，后感知到事件 X，如节点 6、7。

因为我们假设传感器节点只会把在时间间隔内先感知到的事件信息广播给邻居，所以第 1)种情况和第 3)种情况的计算结果是一样的，数据一致性会很高，因为节点 2 对邻居节点 1、3、4、5 计算数据一致性时使用的是这些节点广播事件 X 的信息，提高了节点 2 对这些邻居节点的信任值；而相反，第 2)种情况和第 4)种情况的计算结果是一样的，数据一致性会很低，因为节点 2 对邻居节点 6、7 计算数据一致性时使用的是这些节点广播事件 Y 的信息，降低了节点 2 对这些邻居节点的信任值。在之后的若干时间间隔里经常发生类似多事件并发的情况，导致节点 6、7 的信任值持续累积下降，直至低于某个阈值 T_{min}[4] 而被认为是恶意节点，从而将节点 6、7 排除出网络。但是事实上这些节点是合法节点，并没有广播虚假信息。

3 数据一致性评价方法(DCTEMC)

考虑到无线传感器网络中的节点能量有限，本文的 DCTEMC 方法在计算信任值的时候把能量计算在内。本文方法主要分为 4 个步骤，先计算每个节点对自己的邻居的信任值；再由每个网格内的聚合节点计算出对该网格内所有成员节点的信任评价，这个过程需要聚合每个成员节点的所有邻居对自己的信任值；然后找出每个网格内感知到同一事件数量最多的节点；最后聚合节点根据信任评价聚合第 3 步找出的节点广播的事件信息并发送给基站。

3.1 数据一致性判定

网络中的每个节点并不需要计算对网络中所有其他节点的信任值，只要计算对自己邻居的信任值[6]。对于网格内的每个成员节点，该成员节点保存所有邻居节点的信任评价信息，如图 2 所示，其中 P_i 表示邻居节点所在的位置坐标；ID_i 表示邻居节点所在的网格序号；D_{0i} 表示邻居节点和该成员节点之间的距离；SD_i 表示邻居节点感知到事件的数据信息；CS_i 表示邻居节点与该成员节点感知到的事件有较高的数据一致性次数；C_i 表示邻居节点的数据一致性数值，由 CS_i 计算得出；F_i 表示当前时间间隔内邻居节点是否与该成员节点数据一致，用于统计该成员节点所在网格内感知到同一事件的节点数目；B_i 表示邻居节点剩余的能量；T_i 表示该成员节点对邻居节点的信任值。

P_i	ID_i	D_{0i}	SD_i	CS_i	C_i	F_i	B_i	T_i

图 2 信任评价信息图

多事件并发时，节点 j 会收到邻居节点 i 广播的事件信息 SD_i，假设节点 j 自己感知到的事件信息是 SD_j，如果 $|SD_j-SD_i|\leqslant\theta D_{j,i}$，则认为节点 i 感知到与节点 j 相同的事件，节点 j 对于节点 i 的 CS_i 就会增加，即 $CS_i=CS_i+1$。如果 $|SD_j-SD_i|>\theta D_{j,i}$，则认为节点 i 感知到与节点 j 不同的事件，暂且将节点 i 称为怀疑节点，节点 j 对于节点 i 的 C_i 保持不变。节点 j 对于邻居节点 i 的 C_i 由式(1)计算得出，可以看出，C_i 是随 CS_i 单调增加的，而因为 CS_i 要么不变要么增加，所以 C_i 是一直在增加的。

$$C_i=\frac{CS_i}{CS_i+2} \tag{1}$$

在这个过程中，F_i 会根据式(2)计算得出，只有当邻居节点与该成员节点在同一个网格内且感知到相同的事件 F_i 才会等于 1，否则为 0。当本次时间间隔结束后，F_i 重置为 0。

$$F_i=\begin{cases}0, & \text{if } ID_i\neq ID_0 \text{ or } |SD_j-SD_i|>\theta D_{j,i}\\ 1, & \text{if } ID_i=ID_0 \text{ and } |SD_j-SD_i|\leqslant\theta D_{j,i}\end{cases} \tag{2}$$

3.2 信任值计算

节点 j 对邻居节点广播的事件信息进行数据一致性判定后，由式(3)计算得出节点 j 对邻居节点的信任值 T_i，其中 w_1 和 w_2 分别代表数据一致性数值和剩余能量在信任评价中所占的比重，且 $w_1+w_2=1$。

$$T_i=w_1C_i+w_2B_i \tag{3}$$

当多事件并发时，由式(3)可知节点对邻居中感知到相同事件的节点的信任值是有明显提高的，提高部分主要是 C_i 的提高导致的，而节点对邻居中感知到不同事件的节点(即怀疑节点)的信任值是稍微降低的，这降低的部分是由 B_i 的降低造成的。但是这些怀疑节点广播的事件信息并非虚假信息，有一部分节点也感知到与这些怀疑节点相同的事件，这部分节点对这些怀疑节点的信任值是明显提高的。

3.3 信任评价聚合

在完成所有节点对自己邻居节点的信任值计算后，每个网格的聚合节点会对所有成员节点进行信任评价。当聚合节点对节点 i 进行信任评价时，只要收集节点 i 的所有邻居对 i 的信任值，就能由式(4)计算出该节点的信任评价 T_i'。式(4)中 k 为节点 i 的所有邻居节点数目，T_j' 为上一时间间隔结束时节点 i 的第 j 个邻居的信任评价。多事件并发时同一网格内的成员节点会感知到不同的事件，对于网格内每一个成员节点，先由式(5)计算出网格内与该成员节点感知到相同事件的成员节点数目 SN_i，很明显 SN_i 中有若干个最大值，分别对应感知到相同事件的节点，假设这些节点有 m 个，就可以根据式(6)进行数据聚合。式(6)中 T_i' 为节点的信任评价，为该节点广播的事件信息的可信程度提供了一个依据，m 为网格内感知到相同事件最多的成员节点数目。每次聚合完数据并发送给基站以后，每个网格会比较自己区域内成员节点的最新的信任评价，并选择信任评价最高的节点作为下一次聚合数据的聚合节点。

$$T_i'=\frac{\sum_{j=1}^{k}(T_j\times T_j')}{\sum_{j=1}^{k}T_j'} \tag{4}$$

$$SN_i=\sum_{j=1}^{k}F_j \tag{5}$$

$$SD=\frac{\sum_{i=1}^{m}(SD_i\times T_i')}{\sum_{i=1}^{m}T_i'} \tag{6}$$

多事件并发时，由 3.2 节分析可知不管是普通节点还是怀疑节点，都有邻居节点对其信任值的明显提高，所以最终由式(3)计算出的这些合法节点的信任评价都是有明显提高的。当恶意节点广播虚假信息时，数据一致性差，所有节点对恶意节点的信任值都会慢慢降低，降低部分只是由剩余能量降低造成的，这样恶意节点的信任评价就会慢慢降低，跟合法节点的信任评价明显提高有显著区别，一段时间之后，就能发现并排除恶意节点了。本文的方法也能解决恶意节点联合攻击的情况，恶意节点为了提高自己的信任评价，相互之间会提高对对方的信任值，这样由式(3)计算出的信任评价就会提高，但是式(2)中 B_i 最大为 1，C_i 最大只能接近 1，所以节点相互之间的信任值 T_i 最高也只能接近 1。如果恶意节点相互间的信任值大于等于 1 就暴露了，直接将其排除出网络；如果恶意节点相互间的信任值接近 1(即恶意节点之间每次相互提供的最大的信任值)，在网络中恶意节点数目较少的情况下，由式(3)计算出的信任评价即使提高也不会太大，一段时间之后信任评价提高比较少的就可以确定是恶意节点，并将其排出网络。

4 仿真实验与性能分析

4.1 实验环境

为了检验本文的数据一致性信任评价方法 DCTEMC 在多事件并发情况下的合理性和有效性，使用澳大利亚 NICTA 研究院开发的 Castalia 开源 WSN 模拟器进行仿真。实验仿真环境如下：100 个传感器节点随机布置在一块 150m * 150m 的传感区域，传感区域被划分为 9 个边长为 50m 的正方形网格。每个传感器节点有相同的感知半径为 70m，相同的初始能量 1 个单位，每广播一次事件信息能量减少 0.02 个单位，聚合节点发送聚合信息给基站每次也减少 0.02 个单位能量，当能量减少为 0 时节点死亡。本文重点考虑数据一致性的信任评价，所以将式(3)中剩余能量 B_i 的比重 w_2 设置为0.2，将数据一致性数值 C_i 的比重 w_1 设置为 0.8。实验监控传感区域内的温度变化事件，为了体现本文方法在多事件并发时的优越性，分别用文献[4]中的信任模型 TEM 和本文的方法 DCTEMC 进行对比实验，时间间隔设为 5s，每个时间间隔内在传感区域同时发生两个不同的温度变化事件。另外设置一些恶意节点，以证实本文方法在识别恶意节点方面的有效性。

4.2 实验结果和理论分析

图 3(a)和(b)表示网络中没有恶意节点的前提下，TEM 和 DCTEMC 两种方法在多事件并发时网络规模随时间变化的情况。(a)表示前 180s 的情况，(b)表示后 50s 的情况。由图可以看出，TEM 方法在多事件并发时，很快就有节点被排出网络的现象，原因是 TEM 方法会将部分合法节点当作恶意节点，而 DCTEMC 方法只有在传感区域内节点能量耗光时才会逐渐被排除出网络，有效延长了网络的寿命。图中 TEM 方法网络规模降低得较早，在不到 200s 的时间里网络规模已经减少了将近一半，而 DCTEMC 方法网络规模开始降低较晚，直到 200s 的时候才开始降低。由此可见 DCTEMC 方法能提高节点的生存时间，充分利用传感器节点的能量。

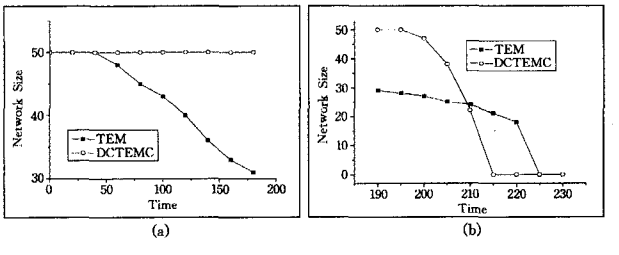

图 3 多事件并发网络规模变化

图 4 表示网络中有一个恶意节点时，该恶意节点所在网格感知到的事件情况，实验设计传感区域每个时间间隔同时发生一个温度为 100 的事件和一个温度为 80 的事件，恶意节点每次广播自己感知到的温度为 50。由图看出，本文的 DCTEMC 方法完全不受恶意节点影响，而 TEM 方法在前 25s 受恶意节点广播的虚假信息的影响比较大，因为这段时间还没排除恶意节点。即使在排除了恶意节点之后，在感知到事件信息的准确性上 TEM 方法还是没有 DCTEMC 方法高。DCTEMC 方法在每个时间间隔都能较准确地反馈本网格内多数节点感知到的同一事件信息，而 TEM 方法反馈的是本网格内所有节点感知到的事件信息的聚合。另外 TEM 方法对数据不一致性的节点的信任值是不断减少的，多事件并发时会导致网格内部分成员节点的信任评价持续降低，也会影响反馈给聚合节点信息的准确度，而 DCTEMC 方法对数据不一致性的节点的信任值是不变的，网格内成员节点的信任评价只会不断增加，不影响反馈信息的准确度。恶意节点一直发送虚假信息，它的信任评价每次都会降低，合法节点的信任评价是在不断地增加，一段时间之后恶意节点的信任

评价最低且与合法节点有明显的差距，则其就会被发现并排除出网络。

图5表示网络中某网格内恶意节点数目占60%时，该网格内传感器节点感知到的事件情况，实验设计传感区域每个时间间隔同时发生一个温度为100的事件和一个温度为80的事件，恶意节点每次都广播自己感知到的温度是50，以提高相互间的数据一致性，实现联合攻击。由图看出，在前30s内，DCTEMC方法没有排除恶意节点，反馈的信息是恶意节点广播的温度为50度的信息，一旦将恶意节点排除，每个时间间隔反馈的事件信息就比较准确了。而TEM方法在恶意节点联合攻击时，排除恶意节点的时间更慢，直到60s后才不受恶意节点的影响，因为恶意节点相互之间有较高的数据一致性，所以TEM方法中恶意节点的信任评价降低较慢，降低到低于阈值 T_{min} 的时间就比图4所用的时间久。由此看出，DCTEMC方法在解决多个恶意节点联合攻击的情况时能准确迅速分辨出合法节点和恶意节点，并将恶意节点排出网络。

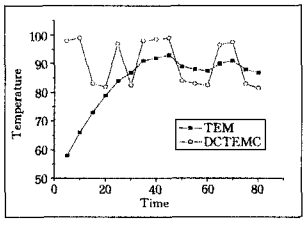

图4 单个恶意节点攻击时温度情况

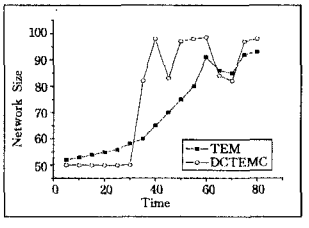

图5 多个恶意节点联合攻击时温度情况

结束语 本文提出了一种适用于多事件并发的无线传感网数据一致性信任评价方法，该方法在多事件并发时不会把合法节点当作恶意节点处理，且在有恶意节点攻击时能准确区别合法节点和恶意节点，并及时将恶意节点排除出网络，另外本方法还能抵御恶意节点的联合攻击。

参考文献

[1] Karhik S, Vanitha K, Radhamani D G. Trust management techniques in Wireless Sensor Networks: An evaluation[C]// International Conference on Communications and Signal Processing. 2011:328-330

[2] Lopez J, Roman R, Agudo I, et al. Trust management systems for wireless sensor networks: Best practices[J]. Computer Communications, 2010, 33:1086-1093

[3] 荆琦，唐礼勇，陈钟. 无线传感器网络中的信任管理[J]. 软件学报，2008，19(7)：1716-1730

[4] Hur J, Lee Y, Yoon H, et al. Trust evaluation model for wireless sensor networks[C]// The 7th International Conference on Advanced Communication Technology. 2005:491-496

[5] 刘方圆，严斌宇，张永齐，等. 无线传感器网络的信任模型研究[J]. 计算机测量与控制，2011，19(5)

[6] Yan Z, Zhang P, Virtanen T. Trust evaluation based security solution in Ad Hoc Networks[C]// NordSec 2003 Proceedings of the Seventh Nordic Workshop on Secure IT Systems. October 2003

(上接第135页)

产生出海量的视频数据时，你可想到这需要多大的监控管理平台，处理多少海量的数据吗？由于人手有限，大量的摄像视频无人监视，在规定期限无人查询就会被自动删除。理想情况是一旦有重要事件发生，系统就可以实时检测，警方可以快速响应，事后能快速查找到线索。如今，借助计算机强大的数据处理能力可以实现通过过滤掉视频画面中无用的或干扰信息，自动识别不同物体，分析抽取视频源中有用的关键信息，快速准确地定位事故现场，判断监控画面中的异常情况，并以最快和最佳的方式发出警报或触发其它动作，形成事前预警、事中处理、事后及时取证的全自动、全天候、实时监控的智能系统[13]。

结束语 基于“更强”的视角，超级计算机被本文视作计算机技术海洋中的“航母”，是国家综合国力的重要体现，是国家创新体系的重要组成部分。由于投资模式、运作方式、应用导向等因素不同，我国国家级超算中心与国际知名超算中心具有很大的差距。为了实现在核心应用方面创国际一流超算中心的建设目标，需要将核心应用关注到计算密集型、数据密集型的“高、精、尖”方面，以免造成“航母运载沙丁鱼”的尴尬。

参考文献

[1] Meuer H, Simon H, Strohmaier E, et al. TOP500 Supercomputer Site[OL]. http://www.top500.org

[2] 张云泉，孙家永. 2011年中国高性能计算机发展现状分析与展望[J]. 高性能计算机发展与应用，2012，38(1)：2-8

[3] 国家超级计算天津中心 [OL]. http:// www.nscc-tj.gov.cn, 2012

[4] 林新华. 应用和人才，非此即彼[J]. 中国教育网络，2010，6：21-22

[5] 赵毅，朱鹏，迟学斌，等. 浅析高性能计算应用的需求与发展[J]. 计算机研究与发展，2007，40(10)：1640-1646

[6] 国家超级计算深圳中心 [OL]. http:// www.nsccsz.gov.cn, 2012

[7] 莫则尧. 千万亿次并行计算研究与应用 [C]// 全国高性能计算学术年会. 2011

[8] Davis B. China's not-so-super computers [M]. The wall street journal, 2012-03-24

[9] Living Earth Simulator Project. FuturICT homepage[OL]. http://www.futurict.eu/sites/default/files/docs/files/002-24%20PLATFORM%20Living%20Earth%20Simulator_0.pdf, 2012

[10] 宋关福. 三维GIS的困境与出路[J]. 中国测绘，2010(1)

[11] Ynnerman A. Visualizing the medical data explosion[Z]. TED Speaking. 2012

[12] 上海科技发展研究中心. 上海“十二五”科技规划重点领域的国内外发展跟踪研究之四：国内外立体显示技术及产业发展态势分析[C]// 上海科技发展研究. 2011

[13] 计世资讯. 2010年中国智能视频监控市场报告[R]. 2010年中国国际信息通信展，2010