

传感器网络中一种双重安全路由算法

张 锦^{1,3}, 沈亚敏², 董 婷², 朱望斌²

(1. 湖南大学 软件学院, 湖南 长沙 410082; 2. 湖南大学 计算机与通信学院, 湖南 长沙 410082;

3. 浙江大学 生物医学工程与仪器科学学院, 浙江 杭州 310027)

(paper_zhj@163.com)

摘 要: 传感器网络中节点有限的资源以及采用无线的方式转发数据使得在传感器网络内的安全性目标很难实现。基于已有的安全措施, 结合低功耗的多路径构造方法, 提出了一种具有双重安全性的路由算法。算法借助已有的安全加密措施及密钥分发策略, 提供一定的安全性, 并且在当上述措施无效时, 利用多路径的方式仍然能够再提供一定的安全保证。理论分析和模拟实验表明, 算法具有一定强度的抗攻击性和较好的安全性。

关键词: 传感器网络; 安全; 多路径; 加密

中图分类号: TP393.03 **文献标识码:** A

Double security-based routing algorithms for sensor networks

ZHANG Jin^{1,3}, SHEN Ya-min², DONG Ting², ZHU Wang-bin²

(1. College of Software, Hunan University, Changsha Hunan 410082, China;

2. College of Computer and Communication, Hunan University, Changsha Hunan 410082, China;

3. College of Biomedical Engineering and Instrumental Science, Zhejiang University, Hangzhou Zhejiang 310027, China)

Abstract: It is very difficult to get the security in sensor networks because of the limited resources of nodes and the wireless communication between nodes. A double security-based routing algorithms was proposed based on the existed security arrangement and low power consumption multipath. The existed security arrangement can provide security to some certain case and multipath can provide more security even when security arrangement failed. Theoretic analysis and simulation results show that the new algorithm has better performances.

Key words: sensor network; security; multipath; encryption

0 引言

Micro-Electro-Mechanical Systems (MEMS) 和无线通信技术的进展, 使得集数据采集、处理及通信功能于一体的无线集成网络传感器 (Wireless Integrated Network Sensors) 构成的可大规模配置的传感器网络 (Sensor Network) 成为可能, 并在环境与军事监控、地震与气候预测、地下、深水以及外层空间探索等许多方面显示出广泛的应用前景, 对传感器网络的研究正逐渐引起关注^[1,2]。

通常一种典型的传感器网络由成百上千或者更多的传感器节点构成, 与传统网络相比, 传感器网络具有以下特性: 1) 节点的能量、存储空间及计算能力等资源非常有限, 而且各种资源无法补充; 2) 节点分布极其稠密且数目很大, 每个节点均维护全局信息非常困难; 3) 与一般的 Ad Hoc 网络不同, 网络内的传感节点布置完毕后, 除了少数节点需要移动以外, 大部分节点都是静止的。

虽然传感器网络将被许多应用领域所使用, 但其安全性问题并没有被充分地考虑^[10]。文献[8,9]分别从不同的角度对传感器网络所面临的攻击类型进行了分析, 并对目前已有的路由算法的安全性进行了分析, 由于目前流行的路由算法

在设计时并没有考虑安全的问题, 使得其无法防御即使是最简单的攻击。而传感节点有限的资源使得传感器网络可以采用的防御手段非常有限。文献[3]以 Smart Dust 为原型给出了传感节点的物理指标, 节点具有 8 位的处理器, 512B 的 RAM 和 8KB 的内存用于指令执行, 其中 4500B 用于应用程序代码的运行, 这些资源远不能满足通常公钥加密体制的要求。在文献[6]中给出了硬件方面的发展使得节点有更充裕的资源, 如: 指令执行的存储空间可以扩展到 128KB, 用于存储数据的 RAM 可以扩展到 4KB, 而闪存可以扩展到 512KB, 但这些仍然无法满足需求。虽然, 硬件的成本会随着技术的进步而降低, 但是在可以预见的一段时间内, 节点的硬件资源无法满足诸如非对称加密体制的要求。因此, 对称加密体制成为目前传感器网络中数据加密的主要手段, 文献[4,5]中讨论了对传感器网络而言可用的块加密算法, 文献[6]中提出了不同类型的密钥所适用的加密情况。文献[7]中提出了概率密钥共享思想和相应的共享密钥发现协议, 其基本思想是构造一个密钥池, 从池中选取一定量的密钥给每个节点, 使得任意 2 个节点在概率 P 下有一个共享密钥。文献[4]中还提出了一种更新颖的 TESLA 协议用于广播安全, 其基本思想是构造密钥链和延时发送解密密钥的方法实现数据鉴别。

收稿日期: 2005-01-26; 修订日期: 2005-04-20

作者简介: 张锦 (1979-), 男, 河南信阳人, 助教, 博士研究生, 主要研究方向: 计算机通信网络、神经信息学; 沈亚敏 (1983-), 女, 湖南娄底人, 硕士研究生, 主要研究方向: 计算机网络安全; 董婷 (1979-), 女, 湖南长沙人, 硕士研究生, 主要研究方向: 无线传感器网络; 朱望斌 (1980-), 男, 湖南双峰人, 主要研究方向: 机器学习。

虽然研究人员提出了诸多的安全防护措施,但目前的路由算法很少考虑到安全的因素,而安全性的获得不是简单的在已有的路由算法上加入加密的措施即可的。因此,本文试图构造一种安全路由算法,算法借助已有的安全防护措施,实现数据保密、数据完整、数据鉴别,并且针对攻击模型,提出一种分布式多路径构造算法,在多条路径上同时转发一份数据,提高数据的冗余性,使得当采用的安全措施被攻破时,仍然可以以较高的概率保证至少一份数据的正确到达,进而警告 Sink 采取相应的措施。

1 攻击模型

针对传感器网络的攻击,大体可以分为独立攻击失效模型(图1)和关联攻击失效模型(图2)。其中独立攻击失效模型是指由于攻击而导致的单个节点失效,其攻击针对的是某个节点。在这种攻击模型中,某个节点的失效并不影响其邻节点的正常工作。如图1所示,黑色的点表示的是失效节点,这些失效节点并不影响周围节点的正常工作。而关联攻击失效模型是指由于攻击导致某个节点失效将同时导致失效节点周围一定范围内的节点全部失效。如图2所示,黑色的失效节点(如A和B)导致在一定范围内的节点(圆内的所有节点)都无法正常工作。

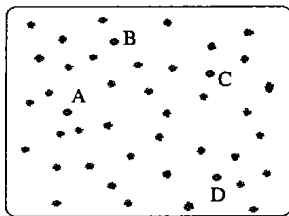


图1 随机独立攻击模型

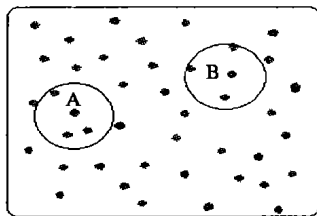


图2 关联攻击失效模型

2 安全路由算法

根据数据安全几个方面的要求,新算法结合相应的防护措施提供数据保密、鉴别、完整和更新,并使用多路径的方式提供高的数据冗余,进一步提高数据的安全性。算法实现可以分为如下几个阶段。

2.1 预配置阶段

在本阶段主要负责为节点配置必要的信息。每个节点将配置如下信息:

- (1) 一个临时的组密钥 $K_c^{[6]}$, 用于配置时的临时加密;
- (2) 根据文献[7]所述配置一定量的密钥, 密钥数量将根据应用的要求而调整;
- (3) 每个节点配置一个 master-key 用于使用单向函数等生产其他密钥。

2.2 散布稳定阶段

节点被散布到探测区域后,每个节点将发送通告报文,告知其拥有密钥的序号、位置和标识ID。通过设定报文TTL为1,可以使得节点信息只能被散布在1跳区域内。报文将用 K_c 加密。收到报文的任意节点先用 K_c 解密,然后,根据报文内容建立邻居表(Neighbors Table, NT),并且查找到其和任一直接邻居共享的密钥。根据文献[7]的结果可知,当密钥池为1000,每个节点从密钥池中抽取50个密钥就使得任2个节点有至少一对共享密钥的概率达到0.95,在本文中,每个节点被配置80个初始密钥,可以保证其有一对共享密钥的概率几乎达到1。

需要指出的是,即便 K_c 被破译,因为每个节点广播的是其所拥有密钥的序号,所以,攻击者并不能得到具体的密钥。因此,如果某节点怀疑报文的真实性,可以简单的丢弃报文,也可以使用二者共享的密钥发送询问报文以确认其信息的真实性。同时,为了保证报文的完整性,每个报文在被发送之前要使用相应的单向函数进行摘要,收方据此判断报文的完整性。

2.3 兴趣散布阶段

散布稳定阶段之后,每个节点均知道与其直接相邻的节点的正确信息。随后,目的节点D可采用合适的方式告知节点其所需要的信息。本文给出如下两种兴趣散布方法:

方法1: flooding 散布。这种方法实现简单,但能耗较大。在安全方面需要解决的就是广播安全问题,可以采用文献[4]提出的 μ TESLA 协议提供广播安全。其具体实现可描述如下: D 用其初始配置的 master-key, 并借助单向函数 F 计算一个长为 n 的单向密钥链, 其中 $K_i = F(K_{i+1}) (i = 1, 2, \dots, n)$; D 用 K_i 加密报文, 并广播出去; 等待一个较长的时延, 使得网络内每个节点都收到加密后的报文; D 广播发送 K_i ; 节点根据 K_i 解密报文得知相关信息。

需要说明的是,在协议中,节点需要一种松散的时间同步关系以保证节点可以判断当前收到的密钥 K_i 是针对那个时间段内收到的报文的,而这对于传感器网络是比较适合的,因为网络规模较大,使得报文的发送需要经过多跳进行,所以时间同步必然是松散的。此外,即便由于恶意的干扰导致某个 K_i 丢失造成节点无法解密全部报文的可能性很低,因为只要有一个 K_i 被正确收到,节点即可应用函数 F 而得到 K_0 到 K_{i-1} , 从而解密以前缓存的报文。

方法2: 基于曲线的散布。这种方法结合 TBF^[11] 和 Rumor Routing^[12] 来实现兴趣散布, 仅需一跳内的节点信息即可, 实现较为简单, 能耗较小。在安全方面需要解决的就是点到点的数据安全问题, 根据节点在“散布稳定阶段”所建立的 NT 可以非常容易的判断直接相邻节点间的共享密钥。其具体实现可以描述如下: 源节点 S 和目的节点 D 分别独立随机选取 $n (n > 4)$ 条直线作为报文的转发路径, 同时 S 发送报文 PS 声明其探测到的数据, 而 D 发送报文 PD 声明其位置和所需数据; PS 和 PD 沿着选择的直线被转发出去, 直到网络边缘节点为止, 转发报文的节点记录有关 S 和 D 的信息, 以及报文是从其哪个直接邻居转发而来的; 如果某个中间节点收到过 PS 和 PD, 发现某个 S 拥有某个 D 所需的数据, 节点将反向告知 S 有关 D 的信息(因节点收到过其直接邻居发送的 PS, 显然是有一条反向路径的)。文献[12]已经证明当 $n > 4$ 时, 分别发自 S 和 D 的直线几乎是肯定相交的(99.7%)。

在节点转发任何报文时, 节点将首先查找 NT 确定接收报文的节点, 以及和该节点共享的密钥, 然后将报文加密, 并用单向函数进行摘要, 求得 MAC (Message Authentication Code); 而接收到报文的节点如果没有和该节点共享密码将不能理解报文内容, 简单地丢弃报文即可, 而正确的节点将可以解密报文获取相关地信息, 并根据 MAC 来验证报文的完整性。需要指出的是: 节点只需使用 NT 表中的密钥即可, 而无须验证其预配置的每一个密钥, 其中多余的预配置密钥可以用于两节点间协商时作为选取的密钥之用。

2.4 多路径构造阶段

经过前两个阶段, 拥有 D 所需信息的 S 即可根据 S 和 D

的位置信息为数据转发构造转发路径。为了提高数据的安全性, S 不是只构造一条路径, 而是同时构造 N 条路径。路径构造之后的数据转发阶段可以在每条路径上都发送一份原始数据, 也可以根据文献[13]中的方法将原始数据分为 N 份, 每条路径上发送一份, 而 D 只需要收到 K 份即可完全恢复原始数据的内容, 以此降低能耗。构造的多路径一般可以分为: 路径之间无交点的多路径 (Disjoint Multipath, DM) 和路径之间有交点的多路径 (Braided Multipath, BM)。

N 条路径的构造方法是相同的, 具体构造过程可以参考文献[14], 这里只介绍其关键思想:

(1) S 确定报文转发的曲线类型。在本文中选取 B 样条曲线, 因为 B 样条曲线的次数和控制点数无关, 容易控制报文转发的路径, 而且计算量相对较小。尤其是曲线容易控制在安全方面有重要意义, 因为这可以使得 S 控制曲线绕过高威胁区域, 降低被攻击的危险。

(2) S 为每条曲线选择控制点。本文采用二次 B 样条曲线, 虽然需要三个控制点, 但是根据如下对 B 样条曲线的改进公式(1)可知: S 只需选择 1 个控制点, 然后根据 S 和 D 的位置信息计算出另外 2 个控制点的信息, 而且通过公式可以保证 S 和 D 分别成为曲线的起点和终点, 这也克服了 B 样条曲线相对与 Bezier 曲线的缺点。

$$\begin{cases} t=0 & P_{0,2}(0) = (V_0 + V_1)/2 \\ t=1 & P_{0,2}(1) = (V_0 + V_1)/2 \end{cases} \Rightarrow \begin{cases} V_0 = 2P_{0,2}(0) - V_1 \\ V_2 = 2P_{0,2}(1) - V_1 \end{cases} \quad (1)$$

(3) 然后 S 将三个控制点包含到路径建立报文中, 并根据相应的贪婪选取算法计算出下一跳节点。在安全路由中, 要求报文尽可能严格地按照选定的曲线转发, 因此应该从下一跳候选节点集合中选择沿曲线前进较少的节点作为下一跳, 并查 NT 表用与下一跳节点共享的密码加密报文, 摘要之后发送出去。同时, S 将构造简单的动态路由表标明源节点为 S, 目的节点为 D 的报文的下一跳 NH (Next-Hop)。

(4) 加密报文被每个直接邻居收到, 但是只有被选择的下一跳节点可以解密理解报文内容。下一跳节点重复如下过程: 解密→报文完整性验证 (根据摘要进行验证)→根据控制点和选取策略计算下一跳→构造路由表→加密→摘要→发送, 直到 D 为止。

这个过程在 N 条路径上同时进行, 需要指出的是: N 条路径的分布要合理, 要尽量等间隔的分布在整个探测区域内, 这样可以降低网络被攻击时路径同时失效的概率, 而且 S 应该为不同的路径选取完全不同的控制点, 这样可以构造完全不相交路径, 可以进一步降低某些节点被攻击而失效时可能造成的路径同时失效的概率。

2.5 数据转发阶段

路径建立之后, 报文转发即可根据路由表来进行, 报文发送之前要根据两点之间的共享密钥进行加密, 并用单向函数进行摘要, 当节点验证了报文的正确性后将重复上述过程进行转发直到 D 为止。通过 N 条路径, D 将收到的数据缓存起来直到 N 份数据全部到达, 然后 D 根据验证 N 份数据的内容, 如果 N 份数据内是完全相同的, 可以推测当前网络是安全的, 这时的数据是可信的; 但如果 D 发现某份数据和其他数据明显不同, D 将从该路径标识为可疑路径, 如果从该路径得到的数据连续和其他路径而来的数据不同, D 将完全忽略经过该路径转发而来的数据; 如果 D 发现有超过 $N/2$ 的路径

转发而来的数据均不相同, D 可以推测此时的网络已经面临很严重的安全威胁了, 而且极有可能有相当部分的节点已经被攻破, 这时 D 应该采取相应的措施进行保护, 比如: 重新散布节点而忽略全部的已有节点; 重新初始化路径等。

3 性能模拟

为了说明算法的安全性, 本文在理论上根据安全性的四个方面对算法进行了分析, 并针对第一部分提出的攻击类型验证了算法的抗攻击性。

3.1 理论分析

数据安全性一般包括如下四方面的内容: 数据保密性, 数据认证性, 数据完整性和数据更新性。

在算法中出现的每个报文均进行了加密, 或者通过组密钥, 或者通过共享密钥, 因此在该密钥的抗攻击能力内, 经过加密后的报文可以保证数据的保密性。而数据认证性 (鉴别) 可以在保证数据保密的同时获得。在算法中出现的每个报文均使用单向函数进行了摘要, 因此数据的完整性是可以保证的。而数据的更新性可以根据诸如 μ TESLA 协议提供的延时的方法获得, 也通过密钥池选取的多余密钥可以用于两个节点之间进行协商选取进而获得新的共享密钥用于加密数据, 从而获得一定的数据更新性。

同时, 本文算法的分布式特性, 也可以避免一些针对传感器网络而设计的攻击方法。例如, 由于算法中 D 接收了所有 N 条路径而来的报文之后才决定采用的报文内容, 这可以避免文献[8]中提出的误导攻击和文献[9]中提到的敌方采用的选择转发攻击。本文提出的算法并不维持多条连接, 从而也可以防止文献[8]中提到的敌方采用的洪泛攻击。

3.2 模拟实验

根据第一部分提出的针对传感器网络的攻击模型, 本文在如下环境下验证了算法采用多路径时的性能。模拟实验在一个给定的区域内 (100×100), 随机散布 N 个节点, 节点通信半径为 R , 分别改变 N 和 R , 验证在一定节点失效的情况下, 多条路径情况下, 仍然有效的路径数 (也即 D 可以收到至少一份正确数据的概率)。

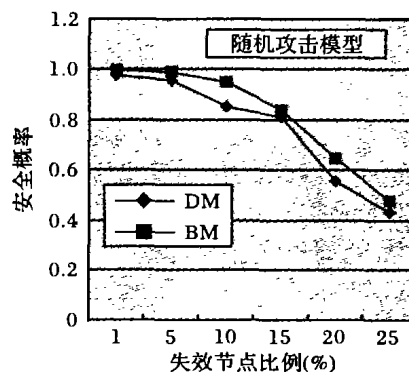


图3 随机攻击下的算法性能

图3、图4表示当 $N = 150, R = 20$, 同时构造 5 条路时, 算法针对独立攻击失效模型和关联攻击失效模型时至少存在一条安全路径的概率。其中, DM 和 BM 分别表示路径之间无交点的和有交点的的多路径。从图中可以得出如下结论: 1) 当建立的路径较多时, 多路径可以得到较好的性能, 而且 DM 和 BM 的性能差别不大; 2) 当失效的节点较多 ($> 15\%$) 或者失效半径较大 ($> 0.6R$) 时, 算法性能下降很快; 3) 在攻击强度大致相似的情况下, 算法抵抗关联攻击的能力更强些。

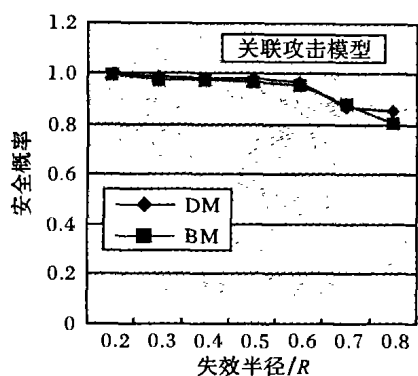
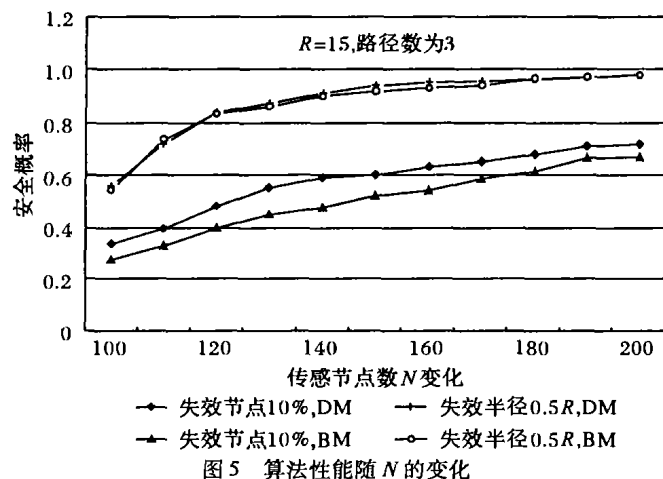
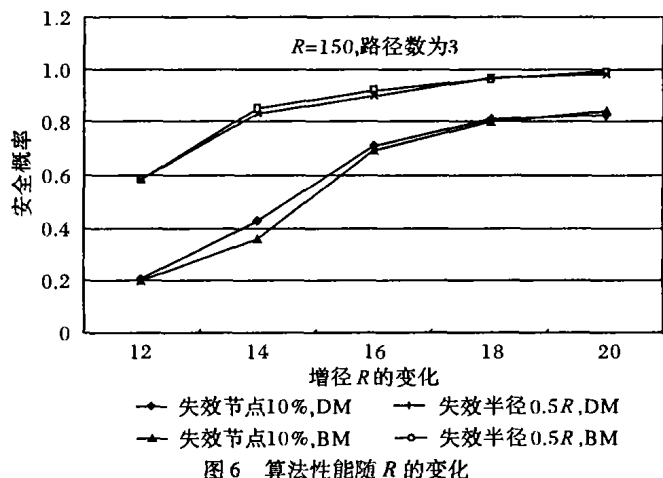


图4 关联攻击下的算法性能

图5表示当固定节点传输半径 R 和建立的路径数时,算法的性能;图6表示当固定节点总数和建立的路径数时算法的性能。从图中可以得出如下结论:1)在同等攻击强度下,节点数增加或者节点的传输半径增加,算法的性能都会得到提高,这主要是因为总节点数增加或者节点的传输半径都会使得节点的平均邻居数增加,从而使得可选的下一跳节点增加;2)算法对关联攻击的抵抗能力更强些,这主要是由于关联攻击导致的失效只是局限在一个局部范围之内的,而算法在构造多路径时已经有意识的使得路径尽可能地分布在整个区域中,从而增强其抗攻击能力;3)DM的性能要好与BM,这主要是由于DM中任一路径都是独立的,可以带来更大的数据冗余,不会出现在BM中一条路径上的节点失效导致另一条使用同一节点的路径也失效的情况,但是DM对资源的消耗要大一些;4)相比于总节点数,节点的传输半径对算法性能的影响更大些,这主要是因为,增大节点的传输半径导致的节点的平均邻居数增加更为明显。

图5 算法性能随 N 的变化图6 算法性能随 R 的变化

4 结语

针对某些传感器网络应用要求必须提供安全性的目标,本文结合已有的安全防御策略实现数据的保密、鉴别、完整和更新,并且利用多路径的方法提供数据冗余,使得即便是在一定数量的节点失效的情况下,仍然能够以较大的概率保证至少有一份正确数据到达目的节点,并提醒目的节点采取相应的措施。传感器网络由于节点资源的限制使得其安全性的获取非常困难,虽然提出了一些新的密钥配置、分发等策略,但并没有很完美地解决安全中的问题,这些也是我们下一步将要进行的研究工作。

参考文献:

- [1] AGRE J, CLARE L. An integrated architecture for cooperative sensing networks[J]. IEEE Computer, 2000, 33(5): 106-108.
- [2] AKYILDIZ IF, SU W, SANKARASUBRAMANIAM Y, et al. A Survey on Sensor Networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.
- [3] DOUMIT S, Agrawal DP. Self-Organized Criticality and Stochastic Learning-Based Intrusion Detection System for Wireless Sensor Networks[A]. MILCOM 2003[C]. Boston, Massachusetts, 2003.
- [4] PERRIG A, SZEWCZYK R, WEN V, et al. SPINS: Security Protocols for Sensor Networks[A]. Proceedings of Seventh Annual International Conference on Mobile Computing and Networks, MOBICOM 2001[C]. Rome, Italy: ACM, 2001.
- [5] AVANCHA S, UNDERCOFFER JL, JOSHI A, et al. Secure sensor networks for perimeter protection[J]. Computer Networks, 2003, 43(4): 421-435.
- [6] ZHU S, SETIA S, JAJODIA S. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks[A]. 10th ACM Conference on Computer and Communications Security (CCS'03)[C]. Washington DC, USA, 2003.
- [7] ESCHENAUER L, GLIGOR VD. A key-management scheme for distributed sensor networks[A]. Proceedings of the 9th ACM Conference On Computer and Communications Security[C]. 2002. 41-47.
- [8] WOOD AD, STANKOVIC JA. Denial of Service in Sensor Networks[J]. IEEE Computer, 2002, 35(10): 54-62.
- [9] KARLOF C, WAGNER D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures[A]. First IEEE International Workshop on Sensor Network Protocols and Applications[C]. 2003.
- [10] CHEE-YEE CHONG, KUMAR SP. Sensor Networks: Evolution, Opportunities, and Challenges[A]. Proceeding of the IEEE[C]. 2003, 91(8): 1247-1256.
- [11] NICULESCU D, NATH B. Trajectory based forwarding and its applications[R]. Technical Report DCS-TR-488, Department of Computer Science, Rutgers University, 2002.
- [12] BRAGINSKY D, ESTRIN D. Rumor routing algorithm for sensor networks[A]. Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications[C]. 2002.
- [13] DULMAN S, NIEBERG T, WU J, et al. Trade-Off between Traffic Overhead and Reliability in Multipath Routing for Wireless Sensor Networks[A]. Proceedings of the Wireless Communications and Networking Conference[C]. New Orleans, Louisiana, USA, 2003.
- [14] ZHANG J, LIN YP, XIA W, et al. TBF-Based Multipath Tolerant Routing for Sensor Networks[A]. Ninth International Conference on Communication Systems[C]. Singapore, 2004.