无线传感器网络安全路由研究

姚宣霞　郑雪峰
(北京科技大学计算机系　北京 100083)

摘　要　路由技术是无线传感器网络的关键技术，安全路由是保障其正常工作的基础。本文分析了无线传感器网络路由的安全状况，总结了路由攻击的各种方法，根据安全路由的目标，为一些复杂攻击提供了相应的防御措施，给出了安全路由协议的一些基本要求和设计原则。最后对无线传感器网络中安全路由技术的研究进行了总结和展望。

关键词　WSN，安全路由，认证

1　引言

无线传感器网络(Wireless Sensor Networks，WSN)是由分布在给定区域的大量传感器节点，通过无线通信技术自组织成的、面向任务的、以数据为中心的网络。作为一种新型信息获取系统，一方面，它具有传统网络不可比拟的优势，有着广阔的应用前景。另一方面，由于采用多跳路由机制，而且网络和节点资源都非常有限，使得其安全性很难保证，已成为阻碍其广泛应用的主要障碍。

在 WSN 中，节点具有双重身份，既要完成感应和处理任务，又要完成路由功能。路由技术是 WSN 的关键技术，路由协议往往与特定的应用相结合。常见的有基于查询的路由[1~3]、基于簇的路由[4]和基于位置的路由[5~6]，他们一般假定网络中的节点都是正常节点，会相互合作完成数据转发，在设计时并没有考虑到安全因素。事实上这种假设是不可靠的，基于这种假设的路由常遭受各种攻击。目前，虽然研究人员提出了许多安全防御措施，但路由安全并非是在已有的路由算法上简单地加入安全措施即可实现。因此，需要对 WSN 的安全路由技术进行研究。

2　WSN 路由面临的威胁

2.1　路由攻击者模型

对 WSN 路由安全的威胁可以从两个方面来考虑[7]。一方面，从攻击者的能力考虑，有节点级攻击者和笔记本级攻击者两种。节点级攻击者一般只能在其紧邻区域内进行无线链路的拥塞和偷听等破坏，而笔记本级攻击者则由于具有更加充足的电量和功能更强大的计算与通信设施，能够做更多的事情。例如，一个笔记本级的攻击者可使用其强大的收发装置对整个网络进行拥塞或偷听。若两个或多个笔记本级的攻击者联合起来可以在攻击者之间形成高带宽、低延迟的通信信道，对 WSN 发起各种复杂的攻击。

另一方面，从攻击者的来源考虑，可以分为外部攻击者和内部攻击者。外部攻击者一般通过制造和发送虚假路由信息、全部或部分地丢弃数据包以及使用有向天线等手段对路由协议进行攻击。内部攻击者常采用冒充或向其他节点发送恶意路由信息等方法进行攻击，由于内部攻击者属于网络的授权主体，受网络安全机制的保护，因此很难被检测到。

2.2　路由攻击的分类

对 WSN 进行路由攻击的方法很多，既可针对特定的路由协议也可针对其多跳路由机制，而且，不同类型的攻击者的攻击方式也往往不同，包括直接操纵用户数据的攻击和影响路由拓扑的攻击等。根据攻击目的和手段的不同，可将 WSN 的路由攻击分为以下几类[7]：

(1)虚假路由信息。这是针对路由协议最直接的攻击，对大部分路由协议都可以实施。通过对两个节点之间交换的路由信息进行欺骗、篡改或重放，攻击者可以创建路由环路、吸引或排斥网络流量、延长或缩短路由、产生虚假的错误信息、分割网络以及增加端到端的延迟等操作。例如在 GPSR[5]中，攻击者通过伪造位置通告可在数据流中创建路由环。

(2)选择转发。指攻击者有选择地或全部拒绝转发收到的数据包，当攻击者处于数据流的传输路径上时最有效。WSN 的很多路由协议都易遭受此类攻击。例如在 GEAR[6]中，由于需要根据剩余能量来分散路由职责，攻击者就可能总是宣称它有很多能量，这样它就能总是处于某条路径上，从而发起选择转发攻击。选择转发最简单的形式是攻击者拒绝转发收到的所有消息，形成路由黑洞，但这样攻击者可能会被当作失败节点排除在路由之外。

(3)污水井(Sinkhole)攻击。污水井攻击的目的是要诱惑几乎所有的来自某个特定区域的通信量都通过某个攻击者，从而创建一个以该攻击者为中心的像污水井似的洞。WSN 特殊的通信模式使它

特别易于遭受污水井攻击。其典型的工作方式是：根据所采用的路由算法，让一个攻击者对其周围节点很有吸引力。例如，攻击者通过欺骗或重放一条到达基站的高质量路由，吸引邻居节点将目的地为基站的分组交给它转发，并向各自的邻居节点通告这条高质量的路由，最终该区域的通信量几乎都要通过此攻击者，形成污水井。污水井攻击改变了数据包的传输方向，严重破坏了网络负载平衡，并为其他攻击提供了方便。

(4)女巫攻击[8]。攻击者拥有多个身份，能够极大地降低分布式存储、分散路由和多路路由等具有容错功能的路由方案的有效性。此外，女巫攻击还能对地理路由协议产生很大的威胁，因为这类路由通常要求节点与其邻居交换坐标信息，正常情况下，一个节点对其某个邻居节点来说只能有一个唯一的坐标，而使用女巫攻击，攻击者可同时有多个坐标信息。

(5)蛀洞(Wormhole)攻击。攻击者通过一条隧道(低延迟链路)在网络的一个地方汇集消息，在另一个地方重放这些消息来拉近两地节点之间的距离。最常见的做法是：让两个远距离的高级攻击者 A 和 B 串通起来，A 位于基站附近，B 在远处。B 通过声称自己与基站附近的节点可以建立低延迟链路来吸引当地节点将数据包发给自己，形成以 A 和自己为端点的蛀洞，此时 B 也是污水井节点。蛀洞常与选择转发和窃听联合使用。由于它使用一个私有的、对基本网络不可见的带外信道，因此很难被检测到。

(6)HELLO 洪泛攻击。WSN 的许多路由协议要求节点广播 HELLO 分组以向邻居节点声明自己的存在，一个收到 HELLO 分组的节点会认为它在发送者的正常通信范围内。这样一个笔记本级的攻击者就可以以足够大的能力向网络内的节点广播，让大量的节点误认为攻击者就是其邻居节点，从而尝试使用该路由，而那些离攻击者太远的节点发送的分组就会被湮没，使网络处于混乱状态。这就是 HELLO 泛洪攻击。

(7)确认欺骗。WSN 的一些路由算法依赖于隐含的或显式的链路层确认。由于采用广播介质，攻击者能够听到发向其邻居接点的信息，并可在邻居节点处于垂死状态时，冒充邻居接点发出假的链路层确认，使发送者将一条弱链路当成一条强链路或者将一个死掉的节点当成一个活动节点，这样沿着弱的或死掉的链路发送的分组就会丢失。

3 路由攻击的防御

3.1 路由安全目标

WSN 的主要用途是正确、实时地进行信息收集或跟踪。为了能够正常工作，在有恶意节点的情况下，路由协议应能确保从源到目的路径的正确发现，使任一合法的接收者能够验证收到的每条消息的完整性和消息发送者身份的真实性。这就是 WSN 的路由安全目标。

在只有外部攻击者存在的情况，实现上述安全目标并不困难。只要在链路层进行简单的加密和认证就能够阻止掉大多数针对 WSN 路由协议的攻击。例如，通过对数据进行加密，可以阻止攻击者加入拓扑，使多数选择转发和 HELLO 洪泛攻击失效。通过对链路层确认进行认证，确认欺骗也难于实施。但是，链路层的加密和认证机制并不是万能的，它不能抵御蛀洞和污水井攻击，而凡是由基站发起构造网络路由拓扑的协议都易遭受这两类攻击。

若存在内部攻击者，特别是存在功能强大的内部攻击者时，链路层的这些安全机制就完全失效了，有些安全目标甚至无法实现。因为内部攻击者是网络的授权主体，它能够通过欺骗、插入虚假路由信息、创建蛀洞或污水井、选择转发分组、使用女巫或 HELLO 洪泛等攻击方法对网络进行攻击。

3.2 路由攻击的防御

在实际中，外部攻击者和内部攻击者常常同时存在，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。

对于女巫攻击，一般使用对称密码体制对节点进行身份认证[7]。同时，为了避免攻击者与每个节点都建立共享密钥使认证失效，应当合理限制一个节点可以拥有的邻居节点个数。

对选择转发攻击，一般采取多路路由[9]或使用多条缠绕路径来抵御。

为了阻止广播或洪泛欺骗，常采用 μTESLA[10] 或类似的方法[11,12]进行非对称认证。

蛀洞和污水井攻击不对报文内容进行任何改动，因此只使用密码学的知识不能完全抵御这类攻击。最好的方法是设计使二者失去意义的路由协议。例如地理路由协议，它只根据本地的信息交互和信息请求构建拓扑，不从基站进行任何初始化，消息朝着基站的物理位置自然路由，因此，能够很好地对抗这些攻击。

不过，这些防御策略存在不同程度的局限性，而且对 WSN 的路由破坏常常是多种攻击联合作用的结果。因此只简单地使用这些防御策略并不能解决路由安全的所有问题，还有可能造成能量的过度损耗。另外，随着 WSN 各种相关技术的发展和应用的普及，新的攻击方法必将不断出现，为了实现安全路由的目标，必须根据应用和发展的需要，在设计路由协议时充分考虑各种安全因素，使协议本身具有抵御各种攻击的能力。

4 安全路由协议的设计

4.1 安全路由协议的基本要求

安全路由协议应该以 WSN 自身的特点为基础，与具体的应用相结合，满足下面几点基本要求：

(1)在路由发现过程中，能够识别和隔离非授权节点，排除它们对路由的影响。

(2)满足路由确定性，保证在存在路由的情况下能够发现路由信息。

(3)不暴露网络拓扑，在传输过程中，保证路由消息不能被非授权节点修改[7]。

(4)鲁棒性好，能够识别伪造的路由消息，并从恶意节点的破坏中自动恢复。

4.2 安全路由协议的设计原则

在设计安全路由协议时，应注意各种安全机制的局限性，始终将节约能量放在首位，以实现安全的最大化为目标。从下面几个方面进行考虑：

(1) 将尽量简单、易于实施作为路由协议的基本设计原则。

(2) 在目前条件下，认证机制最好基于对称密码体制，同时注意使用单向哈希链来提高系统的安全性。因为对称密码体制比公钥体制所需要的资源要少得多，这对于资源匮乏的 WSN 来说是至关重要的。虽然单单使用对称密码体制会严重影响数字签名等安全服务的实现，但是通过使用单向哈希链可以在一定程度上模拟这些服务，例如 μTESLA。

(3) 在使用冗余路径提高路由协议鲁棒性的同时，应注意冗余路径的局限性，因为路由切换往往在路由的端节点进行，若端节点没有检测到攻击，就不能切换路由。

(4) 对入侵采用限制或容忍的态度。在 WSN 中，一般无法得到入侵检测需要的正常参数值，因此很难实施入侵检测。而通过限制洪泛和使用合适的认证机制则可以尽可能地减小入侵者的破坏范围，因此，使用入侵容忍技术更加有效，如 INSENS[13]。

(5) 使用本地化的信任模型。节点能力的局限性和动态变化的拓扑使得 WSN 不宜采用集中式信任模型。同时，WSN 固有的广播特性和本地交互性又使传感器节点非常关心与它紧邻的节点的可信度，因此本地化信任模型更适合于 WSN 安全路由协议的设计。

(6) 注意设置合适的路由选择条件，使一些攻击失去意义。

(7) 尽可能降低路由开销[7]。路由开销主要体现在路由更新消息的传输上。由于节点的绝大部分能量都花费在传输上而不是本地处理上，因此，WSN 的任何网络安全协议都应将降低通信开销作为其重要目标。

结论 安全路由对于 WSN 的正常工作至关重要。结合具体的应用，构建高效的、具有很好鲁棒性的、能够抵御各种攻击的安全路由协议在目前和今后一段时间都是一个巨大的挑战。为了实现安全路由的目标，笔者认为应加强以下几个方面进行研究：

(1)加强密钥管理方案的研究，为安全路由提供基础保障。

(2)加强安全组播的研究，有效减少网络流量，延长网络的生命期。

(3)加强椭圆曲线密码算法在 WSN 中的应用研究。

(4)加强安全定位技术的研究，以定位技术实现路由认证。

(5)加强 WSN 安全体系结构的研究。

参 考 文 献

1 Intanagonwiwat C, Govindan R, Estrin D, Heidemann J. Directed diffusion for wireless sensor networking. IEEE/ACM Trans. on Networking, 2002,11(1):2～16

2 Braginsky D, Estrin D. Rumor Routing Algorthim for Sensor Networks. In: Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, Georgia, USA. ACM Press, 2002. 22～31

3 Chu M, Haussecker H, Zhao F. Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks. The Int'l Journal of High Performance Computing Applications, 2002,16(3):293～313

4 Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless sensor networks. IEEE Proceedings of the Hawaii International Conference on System Sciences. Washington: IEEE Communications Society, 2000. 175～187

5 Karp B, Kung H T. GPSR: Greedy perimeter stateless routing for wireless networks. In: Proc. of the 6th Annual Int'l Conf. on Mobile Computing and Networking. Boston, MA, ACM Press, 2000. 243～254

6 Yu Y, Estrin D, Govindan R. Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks. http://www2. parc. com/spl/members/zhao/stanford-cs428/readings/ Networking/Estrin _ geo-routing01. pdf. 2001

7 Karlof C, Wagner D. Secure routing in sensor networks: attacks and countermeasures. Ad Hoc Networks, 2003,1(1):293～315

8 Douceur J R. The Sybil Attack. http://www. cs. rice. edu/Conferences/IPTPS02/101. pdf, March 2002

9 Ganesan D, Govindan R, Shenker S, Estrin D. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. ACM SIGMOBILE Mobile Computing and Communications Review, 2001,5(4): 11～25

10 Perrig A, Szewczyk R, Wen V, culler D, Tygar J. SPINS: security protocols for sensor networks. Wireless Networks, 2002, 8(5): 521～534

11 Liu D G, Ning P. Multi-level μTESLA: Broadcast authentication for distributed sensor networks. ACM Transactions on Embedded Computing Systems (TECS), ACM Press, 2004,3(4): 800～836

12 Liu D, Ning P. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. http://www. isoc. org/isoc/conferences/ndss/03/proceedings/papers/17. pdf , 2003

13 Deng J , Han R , Mishra S. INSENS: intrusion-tolerant routing in wireless sensor networks [C]. In: Proceedings of the 2nd IEEE International Workshop on Information Processing in Sensor Networks. 2003. 349～364