无线组网技术中的安全问题*)

王昌达[1,2]　鞠时光[1]
(江苏大学计算机科学与通信工程学院　江苏镇江 212013)[1]
(卡尔顿大学计算机科学学院　加拿大渥太华 K1S 5B6)[2]

摘　要　无线组网技术当前主要有Sensor Network和Ad hoc Network两种。与传统的有线网络相比，无线网络同样使用类似于TCP/IP的分层协议进行通信。这样无线网络不仅继承了大部分有线网络的安全缺陷，而且由于使用无线信号传输数据，又使它具有了一些特有的安全问题。本文从信息安全学的角度，系统地综述了无线组网技术中的安全问题及对策，为这个领域的研究提供了清晰的问题结构。

关键词　信息安全，无线组网，Sensor Network，Ad hoc Network

Security in Wireless Network

WANG Chang-Da[1,2]　JU Shi-Guang[1]
(School of Computer Science and Communication Engineering, Jiangsu University, Zhengjiang 212013)[1]
(School of Computer Science, Carleton University, Ottawa, Canada, K1S 5B6)[2]

Abstract　Wireless network has two important members, i. e. Sensor Network & Ad hoc Network. Wireless network also uses multilayer protocol like TCP/IP to implement communications, which is similar with traditional wire network. From this point of view, wireless networks not only inherit most of disadvantages of wire network, but also introduce some new security flaws because use radio as media to communicate. This paper surveys the security problems of wireless network and their resolvent from the view of information security theory.

Keywords　Information security, Wireless network, Sensor network, Ad hoc network

1　引言

无线与有线组网技术相比，最大优点在于网络拓扑展开迅速、造价低廉。这种特性在战场、搜救和科学考察等野外环境下是不可或缺的。正因为如此，军方始终是无线组网技术的坚定支持者，一些影响深远的无线网络几乎全部诞生于军队之中，如美国陆军的Tactical Internet(TI, 1997)和美国海军的Extending Littoral Battle-Space Advanced Concept Technology Demonstration(ELB ACTD, 1999)等。随着IEEE802.11和Bluetooth产品的市场化，无线组网在民用方面同样显示出了巨大的潜力。Wireless World Research Forum(www.ist-wsi.org)公布的调查报告说，通过无线设备接入互联网的用户平均每两年增长20%～50%。

无线组网技术当前主要有Sensor Network和Ad hoc Network两种。它们的共同特点是：网络中没有专职路由器，每个节点(或部分节点)需要兼具路由功能。因为无线组网技术也使用类似于TCP/IP的分层通信协议，所以有线网络中的安全问题，如DoS、IP Spoofing等，在无线网络中几乎无一例外地被继承下来。又因为使用无线信号通信，这就使得无线网络的安全性能，如保密性、抗干扰性等，比有线网络更加脆弱。

本文组织结构如下：第2节提供无线组网技术的背景知识；第3节结合无线网络的特点讨论其安全目标；第4节对无线组网中的安全问题进行分类，讨论已有的解决方案；最后总结全文。

2　Sensor Network与Ad Hoc Network

无线组网技术中的关键问题有两个，即“网络拓扑”和“路由选择”。通过对这两种技术的分析，将有助于理解Sensor Network和Ad hoc Network中的安全问题。

2.1　网络拓扑结构

Sensor Network主要用于对某一区域的感应监控，如战场环境感知和野生动物追踪等。在Sensor Network中，每一个节点的地理位置可以是已知的，也可以是未知的。一般地，为了达到更好的通信和监测效果，在可能情况下，Sensor Network的节点一般会被布置成蜂窝状或网格状，这样每一个节点的地理位置都是清楚的。若在敌控区或自然条件恶劣的野外，往往会采用飞机空投节点的方式构建Sensor Network，在这种情况下，除非每个节点自身带有GPS一类的定位装置，否则精确地理位置不可知。

不同于Sensor Network中节点地理位置相对固定，Ad hoc Network中的部分或全部节点是可以移动的，因此Ad hoc Network也被称为Mobile Ad hoc Network(MANET)。

图1描述了一个Ad hoc Network拓扑结构变迁的简单过程。A,B,C,D,E是组成这个网络的5个节点，虚线圆环代表节点A的无线电信号覆盖范围，实线连接关系代表两个节点之间能直接通信。在图(a)中，节点D可以和A直接通信；在(b)中，由于D运动到了A信号覆盖范围之外，因此A和D

*)国家自然科学基金(No. 60373069)和江苏省自然科学基金(No. BK200204)资助项目。王昌达　博士，副教授，主要研究方向为信息安全技术；鞠时光　教授，博导，主要研究方向为信息安全、空间数据库技术。

间的通信需要借助 C 和 B 中继。Ad hoc Network 的拓扑结构是随节点的运动而不断变化的。

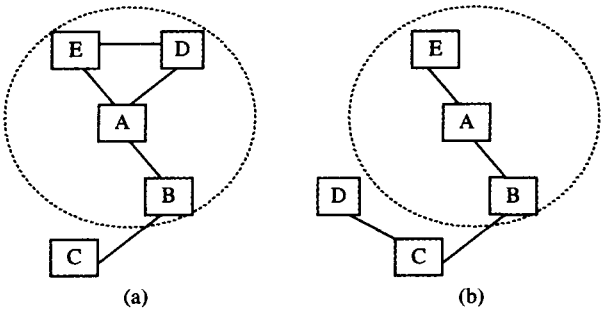

图 1　Ad hoc Network 拓扑结构的变迁

Ad hoc Network 在军事上可用于战场上士兵间的通信，也可以用于舰船、飞机和战车之间的通信。如美国海军的 Extending Littoral Battle-Space Advanced Concept Technology Demonstration(ELB ACTD,1999)，就是一个以舰队、飞机群和陆基指挥站为节点构造的 Ad hoc 网络，其结点规模在 20 个左右[1]。这个网络能有效克服地球的弯曲对无线通信的影响，从而使得指挥系统更加有效。这个系统的成功将最终取代以空中预警机为核心的军事指挥系统。因为预警机以大型运输机作为预警雷达的载体，不仅目标显著、自我保护能力差，而且一旦被击落，其效果相当于直接打击通信中枢。而使用 Ad hoc 通信方式，因为没有集中控制节点，任何单个节点或不超过一定比例的多个节点受到损坏，整个网络仍能正常运行。

Sensor Network 也有类似性质，而且早在越战期间就有过成功范例。通过在胡志明小道两侧空投大量的无线传感装置，美军建立了 Sensor Network，这样越军南下补给车队即使选择夜间关闭照明设备前进，这些传感器仍能通过捕捉汽车噪音发现目标，并将信号逐级接力传到指挥部，美军据此决定空袭的时间、地点和规模。

2.2　通信路由选择

有线网络中广泛存在着专职路由服务器，但在 Sensor Network 和 Ad hoc Network 中一般没有这样的装置。Sensor Network 和 Ad hoc Network 节点一般使用电池供电，受功率、波长和地理环境等因素的影响，无线信号不能传播到很远。为了保证网络中的节点彼此间能互相通信，网络中每个节点或部分节点就被要求具有路由功能。

如果网络中的每个节点都具有路由功能，这样的无线网络被称为 Flat Wireless Network，见图 2。如果网络中只有部分节点具有路由功能，这样的无线网络则被称为 Hierarchical Wireless Network[2]。在 Hierarchical Wireless Network 中，节点被划分成若干个 Cluster，每个 Cluster 有一个路由节点。在 Cluster 内部，节点间可以通过路由节点转发，也可以直接通信；不同 Cluster 间的节点通信，则需要经过路由节点转发，见图 3，每个矩形区域是一个 Cluster，黑色节点是路由节点。

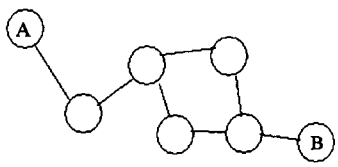

图 2　Flat Wireless Network

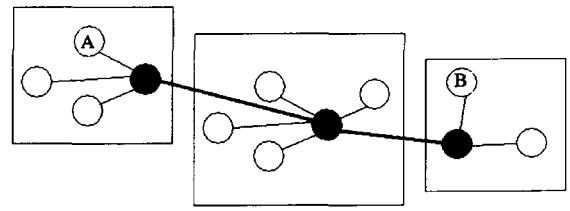

图 3　Hierarchical Wireless Network

Sensor Network 和 Ad hoc Network 的路由协议数量非常庞大，最保守的估计也在 100 种以上，而且新协议还在不断地被提出[3~5]。

按通信数据包的发送方式，这些路由协议可以简单地分为 4 类[1]，即 Unicast，Multicast，Broadcast 和 Geocast。Unicast 是指在发送节点的无线信号覆盖区域内，接收节点是唯一的；接收节点若不唯一，则是 Multicast 方式；Broadcast 是 Multicast 的一种特殊情况，即在发送节点的无线信号覆盖区域内，所有的节点都是接收节点；Geocast 是指发送节点只向特定地理位置的节点传输信号。

按路由表的建立方式，这些协议又可以分为 Proactive，Reactive 和 Mixed3 种。Proactive 方式是网络中的路由节点，通过预定的间隔时间，不断地查询网络连接情况并更新自己的路由表。Reactive 方式只在网络中的两个节点需要通信时，才根据需要查找并建立路由连接。Proactive 的优点是实时性好，缺点是会造成一些不必要的资源(如电池和无线带宽等)开销。Reactive 虽然能克服这些缺点，但实时性却比 Proactive 差。Mixed 方式是在网络中混合式使用 Proactive 和 Reactive 协议，所以 Mixed 方式其实是一种折衷方案。

Sensor Network 和 Ad hoc Network 的相同点在于：(1)两者均要求路由协议有良好的可扩展性(Scalability)，以便网络能在节点数量迅速增加或减少的情况下正常工作。(2)两者均要求良好的动态路由适应性。在 Sensor Network 中，单个节点因电池耗尽或被敌方损坏等原因而退出网络服务的情况时有发生，所以即便 Sensor Network 的节点本身不移动，它也不存在像有线网络那样相对稳定的路由表。

不能简单地把 Sensor Network 看成是节点不移动的 Ad hoc Network。在 Sensor Network 中，节点投放以后，就完全处于无人值守状态，某个节点一旦出现问题，就将完全退出网络。所以在 Sensor Network 中，首先要求节点的投放有一定密度，以提高系统的鲁棒性；其次要尽量延长节点的电池寿命，使其能为网络提供较长的服务时间。在 Ad hoc Network 中，节点的密度可以相对低一些，且节点的电池一般是可更换或可充电的，所以不同于 Sensor Network，Ad hoc Network 的电池只是重要而非决定性资源。

3　安全目标

无线组网技术中的安全目标主要有 5 个：可用性(Availability)、保密性(Confidentiality)、完整性(Integrity)、验证性(Authentication)和抗否认性(non-repudiation)[6]。这 5 方面的内容在字面上与有线网的安全目标一致，但内涵却有所不同。

3.1　可用性

可用性是要保证无线网络在任何情况下都能可靠运行，为合法用户提供服务。

无线保证可靠性比有线环境下困难得多。这主要表现在

以下几个方面:①有线网络中以打击可用性为主的一些攻击方法,如 DoS 等,在无线环境下同样有效。②敌方可以通过发射干扰信号的方式直接打击网络可用性。③在 Sensor Network 和 Ad hoc Network 中,可用性研究还有一项独特内容,即需尽量延长节点的电池寿命。

3.2 保密性

保密性是限制信息不泄露给任何未经授权的实体(Unauthorized Entity)。

由于无线信号的传播特性,敌方可以简单地选择侦听(Eavesdrop)获取信息,这比有线网络通过搭线窃听、获取信息要容易。在无线网络中不仅要保护通信内容的机密性,而且要保护通信路由的机密性[7]。这是因为通过对路由信息的分析,能揭示网络中节点的重要性,敌方可以据此进行选择性打击,以最小代价获得最大破坏效果。

3.3 完整性

完整性是保护信息在存储或传输的过程中不被非法篡改。

在有线网络中破坏信息的完整性,一般要取得网络的接入权限才可能实施。而在无线网络中,敌方可以使用同频发射装置,直接在无线信号中加注(Injection)攻击信息。此外,无线信号在传播过程中逐步衰减(Propagation Impairment),也能破坏信息的完整性。

与保密性的要求类似,无线网络不仅要保护通信内容的完整性,也要保护通信路由的完整性。

3.4 验证性

验证性是检验节点接入和操作权限的合法性。

通过检验节点合法性,可以剔除网络中的敌方节点,从而将攻击行为限制在网络之外。在有线网络中,验证性一般通过数字签名的手段实现。但这种方法在 Sensor Network 和 Ad hoc Network 中不太可行。尤其在 Sensor Network 中,数字签名的大运算量会迅速耗尽节点电池,从而威胁网络的可用性。尽管一些效率较高的签名算法不断被提出来,但在 Sensor Network 中计算量仍然显得过于庞大[7]。

目前加拿大 Carleton University 的 Entrust Lab,通过使用 Signal Analyser 分析节点无线信号的指纹(Signal Fingerprint)来实现无线网络中节点的验证性取得了较大进展[8]。与人类指纹类似,不同无线发射装置发出的信号也有自己的指纹特征,通过这种方法实现验证性能有效克服数字签名在无线网络中应用的缺点。

验证性的另一项内容是检验节点的操作是否具有相关权限。这能有效制止网络中叛变节点的危害行为,降低网络内部的风险性。

3.5 抗否认性

抗否认性是指网络内部的合法节点,不能否认它在历史上所执行过的操作。

抗否认性对于信息安全的作用在于审计,有效的验证方法一般就是有效的抗否认方法。在出现安全问题时,抗否认性使得通过日志文件审查能找出问题节点。但 Sensor Network 和 Ad hoc Network 都是分布式的,实现抗否认性的难点在于日志文件保存在那里,以及如何保护其不被篡改等。

4 安全问题

所谓安全问题,就是至少违背一项安全目标的问题。关于安全目标的讨论见第 3 节。

在 Sensor Network 和 Ad hoc Network 中,仅违背一项安全目标的安全问题比较罕见,所以按安全目标对安全问题进行分类研究不太可行。本文将根据安全问题的触发方式,即敌方采用何种破坏手段,来分类研究无线组网技术中的安全问题。

4.1 被动攻击

被动攻击(Passive Attack)是指通过无线信号侦听(Eavesdrop),获取敌方信息的攻击方法[7]。被侦获的信息可分为两类:"通信内容"和"通信路由"。

当前对抗被动攻击的主要手段是加密。仅对通信内容加密可以采用端到端(End to End)的加密方法;若同时还需对路由信息加密,则要采用点到点(Node to Node)的加密方法。

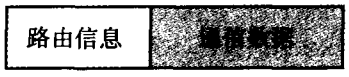

图 4 端到端加密

图 5 点到点加密

端到端(End to End)的加密方法是发送方仅加密通信内容(路由信息公开),接收方接收后用密钥解密出明文,见图 4,阴影部分表示加密数据。点到点(Node to Node)的加密方法是发送方首先加密通信数据,然后使用路由中第一个节点的公钥或是两者间的共享密钥加密路由信息,发送给路由中的第一个节点。路由中的第一个节点收到后,首先解密路由信息并找到路由中的下一个节点,然后用类似的方法再次加密路由信息发送。以此类推,直到信息到达接收方解密出明文为止,见图 5,不同阴影部分表示加密密钥不同。

由于电池容量的限制,在 Sensor Network 中一般不能使用计算量庞大的非对称密钥方法,即使在 Ad hoc Network 中使用非对称密钥,也要非常谨慎地考虑电池容量问题[1]。

点到点加密在每个节点都要进行加、解密运算,对整个无线网络的电能消耗比端到端加密要大。从表面上看,保护通信内容不被窃取的重要性似乎远大于保护通信路由不被窃取的重要性,所以点到点加密给系统带来的额外开销好像不太值得。但事实并非如此,在军用 Ad hoc Network 中路由保密的重要性,有时高于通信内容保密的重要性。这是因为敌方通过路由分析,往往能精确判定指挥节点的位置,从而有选择地进行"斩首"打击。一般地,如果以某一个时刻信息的流入或流出方向为网络中的所有节点构造一棵树,则根节点一般就是最高指挥节点。1996 年 4 月 21 日,前车臣总统杜达耶夫在使用卫星电话时被俄军导弹炸死。法新社事后报道说,俄军方当时有数架装载电子侦听设备的"伊尔 76"运输机在杜达耶夫出没的地区巡航,当其使用卫星电话时,这些设备通过捕捉无线信号确定电话使用者的地理位置,误差只有几米。这个例子充分说明了在无线通信中,对路由信息保护的重要性。

4.2 主动攻击

单纯的被动攻击只能获取信息,而不能造成敌方网络的瘫痪。主动攻击(Active Attack)是指通过使用积极手段,获取敌方敏感信息或使敌方网络陷入瘫痪的攻击方法[7]。

主动攻击可以分为两类："外部攻击"和"内部攻击"。外部攻击是指实施攻击的无线设备没有通过网络验证(Authentication)，即实施攻击的设备不被网络中的其它节点看作是网络的合法成员。与此相反，内部攻击是指攻击设备已经在网络中取得了合法身份。

很难评价到底是内部攻击危害大，还是外部攻击危害大，两者都能有效地破坏系统的安全性。但与外部攻击比，内部攻击具有隐蔽性(难以发现攻击节点)和潜伏性(只在特定的时刻发起攻击)等特点。

4.2.1 外部攻击

已知的外部攻击主要有 Radio Injection，Wormhole 和 Hello Attack 三种。

(1)Radio Injection。是指使用同频发射装置强行在敌方无线信号中注入虚假内容，以破坏信息的完整性或可用性为攻击目标。Radio Injection 注入的可以是虚假通信内容，也可以是虚假路由信息。

在无线网络中，使用笔记本电脑作为节点通信所消耗的能量大约是总能量消耗的 10%，而使用掌上型设备作为节点时，其比例则高达 50%[9]。若敌方在 Sensor Network 或 Ad hoc Network 中注入循环路由信息，在循环路由上的节点就会因为不断地转发信号而迅速耗尽电池并退出网络。这时敌方的攻击目标就不仅是完整性，也涵盖了可用性。实验数据表明，无线发射是接收信号时能量消耗的 3 倍[10]。

抵抗 Radio Injection 的主要手段是加密和签名。若敌方不知道密钥或签名信息，将无法注入有效的攻击信号。本文 4.1 节提到的"端到端"和"点到点"的加密方式，对抵抗 Radio Injection 同样有效。但加密尤其是使用非对称密钥加密，会极大地消耗节点有限的电能。所以，在仅需要保护信息完整性的前提下，有比加密更好的方法，即在通信内容中插入 MAC(Message Authentication Code)。MAC 是通信内容的指纹信息，若信息在通信过程中被篡改，将无法通过 MAC 验证。而任何不能通过 MAC 验证的信息都将被接收方丢弃。当前在 Sensor Network 和 Ad hoc Network 中，一般通过使用 Hash Chain 或 Hash Tree 来生成 MAC 信息[6]。MAC 可以看作是一种签名算法。

(2)Wormhole。此攻击是指敌方通过在无线网络中两个不能直接通信的节点间，建立一条能直接通信的高质量信道，使得这两个节点相信它们之间能够直接通信(Communication within one hop)的攻击方法[11]。

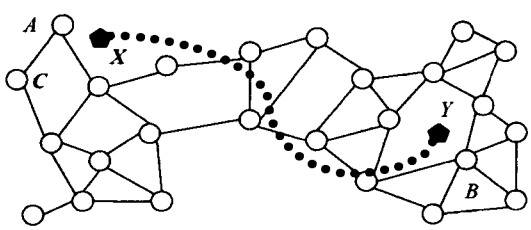

图 5 Wormhole 攻击

图 5 的虚线部分表示 Wormhole，它的存在使原本不能直接通信的节点 A，B 之间能够直接通信。由于 Wormhole 存在，A 与 B 间的路由变得简单，即 A、B 间的通信将不再依赖于网络中其它节点的转发(Multi hop)，并且 A、B 彼此相信对方处在自己无线信号的覆盖区域之内(One hop)[12]。Wormhole 存在也使 C 与 B 之间的通信路由得到简化，因为仅借助 A 的转发，C 就能实现与 B 通信，而在 Wormhole 不存在的时候，C、B 间的通信在两个 hop 之内是不可能完成的，所以 Wormhole 不仅控制了 A、B 间的通信，也控制了 A 附近节点与 B 附近节点之间的通信。

通过 Wormhole 敌方至少能发起 3 种不同方式的攻击，即 Eavesdropping，Sinkhole 和 Selective Forwarding。

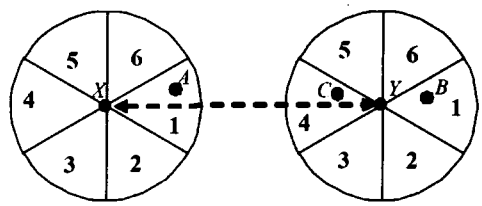

图 6 有 6 个方向的有向天线

Eavesdropping 是指 Wormhole 在转发信息的同时窃取信息的内容。一般通过加密的方法就能对抗这种攻击，参见本文 4.1 节中的方法。Sinkhole 是指在 Wormhole 建立之后的某一时刻，Wormhole 将流经它的信息全部吞噬，这样在新的通信路由建立之前，依赖 Wormhole 通信的节点间联系将被全部切断。有别于 Sinkhole 吞噬全部信息，Selective Forwarding 是有选择地吞噬流经 Wormhole 的信息，如吞噬网络中的重要信息而放过无关紧要的信息，或是有选择地切断特定节点间的联系，所以 Selective Forwarding 比 Sinkhole 难发现。

目前有两种对抗 Wormhole 攻击的手段：一种是 L. Hu 和 D. Evans[12]提出的使用有向发射/接收天线的方法。其核心思想是根据地磁方向，所有节点使用有向天线，这样发射节点如果使用向东的天线发射信号，那么接收节点只有使用向西的天线接收到数据才合法。如果接收方是在合法的天线方向上接收到信号，还需要再寻找可信的第三节点证实发送和接收方彼此在对方无线信号的覆盖区域内，见图 6。上述条件只要一个不满足，就断定信号是经 Wormhole 传送的。这种方法的问题是：①在网络的边缘区域，用于验证的可信第三节点不易找到；②由于地球磁场过于弱小，敌方通过对施加强磁场能彻底破坏网络的可用性。

另一种对抗 Wormhole 攻击的方法是 Y. Hu，A. Perrig 和 D. Johnson[13]提出的时间戳方法。其核心思想是在发射无线信号的同时包含信号的发送时间，接收节点根据信号达到时间和无线信号的传播速度，计算出该信号所传播的距离。如果距离超出了发射节点信号可能到达的距离，即认为该信号是通过 Wormhole 传播的并予以丢弃。这种方法的问题是：①在使用电池供电的 Sensor Network 和 Ad hoc Network 中，信号的发射距离一般只有数十米到数百米[1]，而无线信号是以光速传播的，所以信号传播所消耗的时间 Δt 是一个非常小的值。若以这种方法计算信号的传输距离，将要求整个网络有惊人准确的时间同步，误差至多不能大于 Δt，这在当前是很难以较低的代价实现的。②无线信号不是在真空中传播，障碍物阻挡、空气温度和湿度的变化都会带来信号传播速率的变化，而这样微小的变化就足以使该方法无法有效判别哪些信号是流经 Wormhole 的，而哪些又不是。

Wormhole 攻击的威胁在于它完全不需要在网络中取得合法身份，就能轻易地实现在有线网络中，只有具有合法身份的节点才能发起的攻击[14]。Wormhole 攻击方式的出现，使

得无线组网技术的安全性受到了空前挑战。

(3)Hello Attack。是指使用功率强大的同频无线发射装置,在敌方无线网络中向自己周围的节点广播 Hello 信号的攻击方法[10]。

在 Sensor Network 和 Ad hoc Network 中,节点通过广播自己的 Hello 信号建立网络路由表。收到 Hello 信号的节点并不转发 Hello 信号,而是按一定格式答复 Hello 信号。通过这种方法,网络中的节点就会知道哪些节点处于自己的无线信号覆盖区域内。如果敌方首先通过侦听获取网络中一个合法的 Hello 信号,然后使用功率强大的发射装置向网络中其它节点广播,收到该 Hello 信号的众多节点将按着协议约定回答该 Hello 信号,那么在整个网络中将会制造出一场响应该 Hello 信号的风暴(Flooding)。敌方通过反复地发起 Hello Attack,不仅能占用无线网络的带宽资源,而且能大量消耗节点的电能,从而破坏整个网络的可用性。

目前尚没有单独对付 Hello Attack 的有效方法。一般敌方用于攻击的发射装置,功率比网络中合法节点要强,所以网络中许多节点发送的 Hello 响应信号,因为功率小,根本不能到达敌方发起攻击的节点。但网络外部观察到的现象却是在某一时刻,网络中所有在敌方发射信号覆盖范围内的节点,都在向攻击节点发送 Hello 响应信号,所以 Hello Attack 也被看成是一种单向的 Wormhole[10]。因此能有效对抗 Wormhole 的方法一般都能有效对抗 Hello Attack,细节可参阅本文 Wormhole 的相关内容。

4.2.2 内部攻击

所谓内部攻击,是指敌方的攻击设备在无线网络中取得了合法身份[7]。与外部攻击相比,内部攻击较难被发现。

一般敌方有两种手段在无线网络中取得合法身份:一是俘获网络中的合法节点;二是欺骗网络的验证(Authentication)机制。至于如何防止合法节点被俘获,即节点的物理保护问题,不在本文研究范围之内。对欺骗网络验证机制的防范,首先可采用 Challenge-Response[14]作为 Authentication 方法,而非简单地使用 User_id 和 Password 判断用户身份;其次才是在网络中应用适当的入侵检测手段,因为现有的无线网络入侵检测机制都不太实用[15]。

入侵节点一旦在网络中取得合法身份,通信数据就可能流经该节点,这为敌方破坏信息的完整性和可用性提供了良机。本文前面提到的一些攻击手段如果在内部实施,其危害不仅比外部攻击时大,防范也更加困难。以 Hello Attack 为例,如果攻击节点在网络中有合法身份,那么发起 Hello Attack 的节点因为功率大、信号质量好,就能够迅速吸引其周边的节点通过它来通信。在 Hello Attack 节点吸引了周边的通信流量后,就能有选择地发起 Eavesdropping, Sinkhole 和 Selective Forwarding 等攻击(参见本文 4.2.1 节)。再以 Eavesdropping 为例,如果敌方节点在网络中具有合法身份,那么无论是点到点加密,还是端到端加密,都只能解决部分保密性问题。

Baruch Awerbuch 等[16]提出一种方法,能够发现网络中行为异常的节点。它能被用来对抗 Sinkhole 和 Selective Forwarding 攻击,但如果内部入侵节点仅采用 Eavesdropping,目前则没有任何有效的对抗方法。

下面讨论 Sybil Attack 和 Acknowledgement Attack 这两种只能在内部攻击时使用的方法。

(1)Sybil Attack。是指一个入侵节点,能在网络中的其它节点面前表现出不同身份的攻击方法[17]。

在 Sensor Network 和 Ad hoc Network 中,由于一个节点资源有限,同时也为了防止一个节点被敌方俘获而造成全部密敏感信息泄漏,一般采用分布式的存储策略[18],即将敏感数据分散地存储在不同的物理节点中。通过 Sybil Attack,一个入侵节点能获取超过一个合法身份所能获得的信息量,这破坏了系统的分布式存储策略。

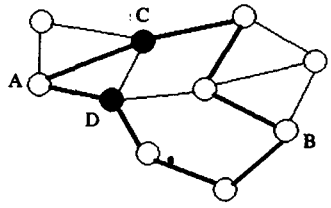

图 7 使用两条路由通信

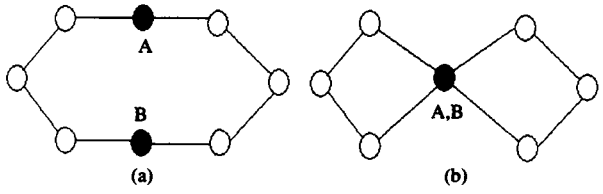

图 8 Sybil Attack 下的网络拓扑结构

Sybil Attack 还能破坏系统的多路由传输(Multipath Routing)[19]和网络拓扑结构的稳定性(Topology Maintenance)[20,21]。在无线网络中,考虑到路由变化迅速以及信号传输的可靠性等问题,两个节点间的通信有时会选择多路由传输,图 7 描述了节点 A、B 间的通信存在两条独立路由,如果一条路由工作的可靠性是 0.7,那么采用两条独立路由通信的可靠性就会提高到 $1-(1-0.7)^2=0.91$。在图 7 中,若节点 C、D 是同一个入侵节点通过 Sybil Attack 在网络中表现出的不同身份,那么 A、B 间的通信实际上已被敌方控制,其通信的可靠性并未因为使用多路由传输而提高。

有时为保证无线网络的通信效果,在某个特殊时段需要保持稳定的网络拓扑结构,而入侵节点通过发起 Sybil Attack 能有效地破坏这一策略。图 8 描述了一个入侵节点,通过 Sybil Attack 在网络中取得两个合法身份 A、B 对这一策略的破坏。图 8(a)描述了网络管理员看到的环状路由结构,图 8(b)则是实际的拓扑结构。

Chris Karlof 等[10]提出通过限制每个节点的邻接节点个数来把 Sybil Attack 的威胁将至最低。显然,这不是一个根本解决 Sybil Attack 攻击的方法。

(2)Acknowledgement Attack。是指,入侵节点在网络中冒充一些已经"死亡"合法节点的攻击方法[10]。

这些死亡节点的"复活",使网络相信原先一些不可用的路由现在已经恢复,原来一些不稳定的连接现在已经稳定。这样,入侵节点在吸引了一定的信息流量后,就能够有选择地发起 Eavesdropping, Sinkhole 和 Selective Forwarding 等攻击。

迄今为止,尚未见有专门对抗 Acknowledgement Attack 的方法。对抗 Acknowledgement Attack 可以采用通用对抗内部攻击的方法,即强身份验证,尽量限制敌方节点在无线网络中取得合法身份。

结束语 本文在无线组网技术特点的基础上,以两种典

型的无线网络 Sensor Network 和 Ad hoc Network 为例，系统地讨论了其中的安全问题。本文的讨论有两个基本假设：一是假设网络中的节点都是对等的，没有任何集中控制设备；二是假设网络中节点间的通信都是双向的，即如果 A 在 B 发射信号的覆盖范围内，那么 B 同样在 A 发射信号的覆盖范围内。如果不完全满足这两个条件，网络中还会有一些新的安全问题。

一些与有线网络完全相同的安全问题，如 Reply attack 和 IP spoofing 等，本文中未做讨论，有兴趣的读者完全可以参考有关的文献。另外，根据 Imrich Chlamtac 等[1]的划分，本文所讨论的安全问题仅限于 Transport & Network Layer 层，至于应用层和媒体层的安全问题，亦不在本文的研究范围之内。

一般来说，有线网络在应用层所具有的安全问题，无线网络的应用层一样有，如病毒和木马程序等。另外，在无线网络中，还必须考虑在应用层提供节点激励机制(Incentive)，以避免网络中的部分节点因不愿消耗有限电能，而不转发与自己无关信号的问题。在媒体层还需要考虑敌方通过物理损坏节点、采用大功率发射装置全向或定向对网络中的无线通信进行压制干扰等问题。上述这些安全问题，都是相对独立的研究方向，限于篇幅，有兴趣的读者可查阅相关文献。

无线组网技术是实现 Ubiquitous Computing 蓝图的基础，它不仅给通信带来了巨大的便利，也给网络安全技术提出了空前的挑战。

致谢 感谢加拿大 Carleton University 计算机学院的 Evangelos Kranakis 和 Michel Barbeau 教授，正是在这两位教授的指导下，笔者得以在 Entrust Lab 工作期间，从事了无线组网技术中安全问题的研究，两位教授已经连续 3 年作为 Ad Hoc 研究国际会议的组织者和发起者。感谢加拿大国家研究中心(NRC)的 C. Yong 教授，他在航空机载无线通信组网方面的见解让我受益匪浅。感谢与我同实验室的 J. Hall 博士，她无私的帮助使我能在第一时间引述她的研究成果。

参 考 文 献

1 Chlamtac I, Conti M, Liu J J N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 2003, 1: 13～64
2 Karlof C, Wagner D. Sensor Network Protocols and Applications. In: Proceedings of the First IEEE International Workshop on, 11 May 2003. 113～127
3 Beraldi R, Baldoni R. Unicast routing techniques for mobile ad hoc networks. In: Ilyas M, ed. Handbook of Ad Hoc Networks. CRC Press, New York, 2003
4 Belding-Royer E. Routing approaches in mobile adhoc networks. In: Basagni S, Conti M, Giordanos, et al. eds. Ad Hoc Networking. New York: IEEE Press Wiley, 2003
5 Belding-Royer E M, Toh C K. A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Communications Magazine, 1999. 46～55
6 Zhou Lidong, Haas Z J. Securing ad hoc networks. Network, IEEE, 1999, 13(6): 24～30
7 Karpijoki V. Security in Ad Hoc Networks. In: HUT TML 2000 Seminar Security, 2000. 1～16
8 Hall J, Barbeau M, Kranakis E. Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting. Communications, Internet and Information Technology (CIIT), St. Thomas, US Virgin Islands, November 2004
9 Kravets R, Krishnan P. Power management techniques for mobile communication. In: Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 98), Dallas, TX, October, 1998. 157～168
10 Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. In: Sensor Network Protocols and Applications. Proceedings of the First IEEE. 2003 IEEE International Workshop on, May 2003. 113～127
11 Hu Y, Perrig A, Johnson D. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. INFOCOM 2003, April 2003
12 Hu Lingxuan, Evans D. Using Directional Antennas to Prevent Wormhole Attacks. Network and Distributed System Security Symposium, San Diego, February 2004
13 Hu Y, Perrig A, Johnson D. Wormhole detection in wireless ad hoc networks: [Tech RepTr01-384]. Department of Computer Science, Rice University, June 2002
14 Bishop M. Computer Security: Art and Science. Addison Wesley, 2002
15 Dreef D, Ahari S, Wu Kui, et al. Utilizing the Uncertainty of Intrution Detection to Strengthen Security for Ad hoc Networks. In: Ad-Hoc, Mobile, and Wireless Networks, LNCS, 2004. 82～95
16 Awerbuch B, Holmer D, Nita-Rotaru C, et al. An On-demand Secure Routing Protocol Resilient to Byzantine Failures. In: Proceedings of the ACM Workshop on Wireless Security, 2002. 21～30
17 Douceur J R. The Sybil Attack. In: 1st International Workshop on Peer-to-Peer Systems(IPTPS '02), March 2002
18 Castro L. Practical Byzantine Fault Tolerance, Symposium on Operating Systems Design and Implementation. USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, 1999
19 Ishida K, Kakuda Y, Kikuno T. A routing protocol for finding two node-disjoint paths in computer networks. In: Internation Conference on Network Protocols, November 1992. 340～347
20 Xu Y, Heidemann J, Estrin D. Geography-informed Energy Conservation for Ad hoc Routing. In: Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2001
21 Chen B, Jamieson K, Balakrishnan H, et al. Span: An Energy-efficient Coordination Algorithm for Topology Maintenance in Ad hoc Wireless Networks. ACM Wireless Networks Journal, 2002, 8(5)

(上接第 83 页)

的视频流传输机制。近年来备受业界关注的蓝牙和 802.11b 技术各有自己独特的价值，均可用于建立无线 ad hoc 网络，用于近距离无线视频流传输。本文使用 NS2 模拟环境，设计了不同编码码率、不同路径长度环境下的模拟实验，对两种技术在视频流传输中的表现进行了对比和分析。模拟实验结果表明：低码率下具有较高带宽的 802.11b 技术更具优势，但随码率的上升，在码率超一定阈值范围后，抗干扰能力强的蓝牙技术性能表现更好。实验结果的分析表明：视频流传输路径中的信道容量、路径长度与码率 3 个因素之间相互作用，共同决定了解码视频的失真度。因此，必须综合考虑上述因素来设置路由机制，才能更有效地降低视频流的失真度，这也是我们未来的研究重点。

参 考 文 献

1 Bluetooth Specifications Version 1.1 [S]. http://www.bluetooth.org
2 The Working Group for Wireless LANs. IEEE standards 802.11b-1999 [S]. http://grouper.ieee.org/groups/802/11/
3 Frodigh M, Johansson P, Larsson P. Wireless ad hoc networking: the art of networking without a network [J]. Ericsson Review, 2000(4): 248～263
4 Wi-Fi(802.11b) and Bluetooth: An Examination of Coexistence Approaches (2001): [Online document], Mobilian Corporation, 2001. http://citeseer.nj.nec.com/461904.html
5 http://www.isi.edu/nsnam/ns/
6 http://www.ececs.uc.edu/~cdmc/ucbt/ucbt.html