# 第 3 章　无线自组织网络攻防原理

本章首先介绍无线自组织网络的安全缺陷和两种经典的路由协议，然后介绍了针对路由协议攻击的一些方法，其中重点分析了两种攻击方式：泛洪攻击和黑洞攻击。详细讨论了其攻击原理，并设计了检测响应方法。最后，设计了一种适用于无线自组织网络的主动防护方法——移动防火墙，对其移动和防护原理进行了详细的分析讨论。

## 3.1　无线自组织网络的安全缺陷

有线网络自诞生之日起就不断受到安全专家的考验、黑客的侵袭和病毒的困扰，也正是在这样攻与防、矛与盾的斗争中，有线网络不断成熟，安全机制不断加强。时至今日，有线网络的安全技术已日臻完善。黑客想要攻破一个配置得当的有线网络是比较困难的，然而无线网络的出现使网络安全水平退到了 20 世纪 80 年代的水平。即使在网络安全技术比较先进的欧美国家，在一个无线网络应用比较普及的城市，一个经验丰富的黑客一定能找到大量存在严重安全漏洞的无线网络，并轻而易举地入侵。

无线自组织网络对恶意攻击显得比较脆弱。首先无线链路的应用使得无线自组织网络易受被动偷听与主动破坏的影响。无线自组织网络和有线网络不同，在有线环境中，攻击者必须获得进入网络的物理通道或穿过防火墙和网关的几条防御线，而对无线自组织网络的攻击可能来自各个方面，目标可能是任何一个节点，危害可能包括泄露机密信息、消息污染和伪装节点。这就意味着无线自组织网络没有明确的防御线，并且每一个节点都必须为遭遇直接或间接的攻击者做好准备。这使得无线自组织网络中的任何一个疏忽都可能导致整个无线自组织网络安全措施的沦陷。其次，移动单元如果没有充分的物理保护就容易被捕获、劫持和泄密。一旦某个单元被获取，则攻击者可以轻松接入整个网络并进行攻击。

传统网络中，主机之间的连接是固定的，网络采用层次化的体系结构，并具有稳定的拓扑。传统网络提供了多种服务以充分利用网络的现有资源，包括路由器服务、命名服务、目录服务等，并且在此基础上实现了相关的安全策略，如加密、认证、访问控制和权限管理、防火墙等。而在无线自组织网络中没有基站或中心节点，所有节点都是移动的，网络的拓扑结构动态变化[1]。并且节点间通过无线信道相连，没有专门的路由器，节点自身同时需要充当路由器，也没有命名服务、目录服务等网络功能。两者的区别导致了在传统网络中能够较好工作的安全机制不再适用于无线自组织网络，主要表现在以下几个方面[2]。

### 3.1.1　传输信道方面

无线自组织网络采用无线信号作为传输媒介，其信息在空中传输，无需像有线网络一样，要切割通信电缆并搭接才能偷听，任何人都可接收，所以容易被敌方窃听。无线信道又容易遭受敌方的干扰与注入假报文。

### 3.1.2　移动节点方面

因为节点是自主移动的，不像固定网络节点可以放在安全的房间内，特别是当无线自组织网络布置于战场时，其节点本身的安全性是十分脆弱的。节点移动时可能落入敌手而投降，节点内的密钥、报文等信息都会被破获，投降后的节点又可能以正常的面目重新加入网络，用来获取秘密和破坏网络的正常功能。因此，无线自组织网络不仅要防范外部的入侵，而且要对付内部投降节点的攻击。

### 3.1.3　动态的拓扑

无线自组织网络中节点的位置是不固定的，可随时移动，造成网络的拓扑不断变化。一条正确的路由可能由于目的节点移动到通信范围之外而不可达，也可能由于路由途经的中间节点移走而中断。因此，难于区别一条错误的路由是因为节点是移动造成的还是虚假路由信息形成的。由于节点的移动性，在某处被识别的恶意节点移动到新的地点，改变标识后，它可重新加入网络。另外由于拓扑是动态的，网络没有边界，防火墙也难以防御。

### 3.1.4　安全机制方面

在传统的公钥密码体制中，用户采用加密、数字签名、报文鉴别码等技术来实现信息的机密性、完整性、不可抵赖性等安全服务。然而它需要一个信任的认证中心来提供密钥管理服务。但在无线自组织网络中不允许存在单一的认证中心，否则不仅单个认证中心的崩溃将造成整个网络无法获得认证，而且更为严重的是，被攻破认证中心的私钥可能会泄露给攻击者，攻击者可以使用其私钥来签发错误的证书，假冒网络中任一个移动节点，或废除所有合法的证书，致使网络完全失去了安全性。若通过备份认证中心的方法虽然提高了抗毁性，但也增加了被攻击的目标，任一个认证中心被攻破，则整个网络就失去了安全性[3]。

### 3.1.5　路由协议方面

路由协议的实现也是一个安全的弱点，路由算法都假定网络中所有节点是相互合作的，共同去完成网络信息的传递。如果某些节点为节省本身的资源而停止转发数据，这就会影响整个网络性能。更可怕的是投降节点和参与到网络中的恶意节点专门广播假的路由信息，或故意散布大量的无用数据包，从而导致整个网络的崩溃。

为了更加具体详细地分析无线自组织网络中存在的各种攻击，下面先介绍一下无线自组织网络中两种经典的路由协议。

## 3.2　两种经典路由协议

### 3.2.1　DSR 路由协议

DSR(Dynamic Source Routing，RFC4728)[4]是由美国卡耐基梅隆大学 Monarch 工作组提出的一种使用源路由思想的 Ad Hoc 网络按需路由协议。DSR 协议主要应用于 200 个移动节点以内的 Ad Hoc 网络中。DSR 协议在各层上，都不需要发送周期性的广播如路由

信息、链路状态信息和邻居节点探测信息等，也不需要网络下层的协议提供上述的功能。

另外，DSR 协议选用的是源路由，源路由是一种由数据分组的发送节点决定整个传输过程中完整路径的路由机制。源节点在发送数据分组时将完整的路径显式的夹带在数据分组的头部，其中包含了源节点到目的节点的路径中的每一跳的 IP 地址。中间节点无须维护分组的路由信息，在接到数据分组后只需从数据分组头部提取出对应的下一跳的地址，修改 IP 头部的目的地址字段即可。

DSR 协议有两个主要的机制一起工作，以实现 Ad Hoc 网络中源路由的发现和维护。

(1) 路由发现(Route Discovery，RD)：只有当源节点试图向目的节点发送数据，并且尚不知道源节点和目的节点之间的路由时，启动路由发现机制。

(2) 路由维护(Route Maintenance，RM)：如果网络拓扑发生改变，例如，链路中断导致源节点和目的节点之间的路由无法再使用，此时便启动路由维护机制。

**1. 路由发现**

(1) 路由请求

节点有分组要求时，动态的广播 RREQ 路由请求分组应包括目的节点、请求分组发送节点地址、本分组 ID、路由记录、请求分组发送节点地址和本分组。用于唯一的标识 RREQ，以便于 RREQ 的接收处理。路由记录将累积地记下 RREQ 分组逐跳传播时所顺序经过的节点地址，从而完成路由发现的功能。

各节点对 RREQ 分组的处理如下：

- 如果在最近收到的“历史 RREQ 列表”中已存在，丢弃该 RREQ 分组，不作处理。
- 如果路由记录中包括本节点，丢弃该 RREQ 分组，不作进一步的处理。
- 如果本节点就是 RREQ 指定的目的节点，发送 RREP 路由应答分组。
- 其他情况，将本节点的地址添加到路由记录，重新广播更新后的 RREQ 分组。

(2) 路由应答

RREP 包含有目的节点接收到 RREQ 分组的路由记录。RREP 的目的是如何把这个路由记录告诉给源节点。先假设网络中所有的链路是双向的，那么目的节点到源节点的反向路由存在。RREP 分组沿反向路由传输到源节点。

前面在讨论无线 Mesh 网络特点时曾经提到，在无线网络中单向链路存在的可能性是很大的。那么当这种情况发生时，目的节点执行与源节点相同的反向路由发现过程，所不同的是目的节点 RREQ 分组捎带传送一个 RREP 分组，以寻求回到源节点的一条可行路由。

**2. 路由维护**

在按需路由协议中，没有周期性的网络测试过程，各节点需要执行路由维护进程，动态的监视活动路由的运行情况。

(1) 对于“逐跳 MAC 确认”的网络，链路的故障或变化由 MAC 层通告，节点将发送 RRER(路由错误报文)到源节点；源节点将删除该路由，重新进行路由发现。

(2) 对于“逐跳 MAC 不确认”的网络可利用无线传输的空间广播性，即当节点 $A$ 转发分组到下一跳 $B$ 时，$B$ 到 $B$ 的下一跳 $C$ 的分组转发也可被 $A$ 监听到。

例如图 3-1 中所示网络拓扑图，源节点 S 想与目的节点 $D$ 建立链接，则它向周围的邻居节点广播 RREQ 报文，报文中带有自己与目标节点的信息。对于邻居节点来说，首先会判

断之间有没有收到过该 RREQ 报文，如果有，则忽略这个报文；然后判断自己是不是 RREQ 报文中所描述的目标节点，如果是，则回复 RREP 报文给源节点 *S*，在此报文中包含了整条路由信息，即路径上所有节点的信息，并且使报文按照 RREP 报文上的信息传递给源节点 *S*；其余情况，则在此 RREQ 报文上加上自己的信息，并继续向周围邻居节点广播。如此下去，直至 *D* 收到 RREQ 报文为止。此时，*D* 就按照该 RREQ 报文上的路由信息，反向路由后发出 RREP 报文，并使该报文原路返回至源节点 *S*。至此，一条链路就建立完成了。

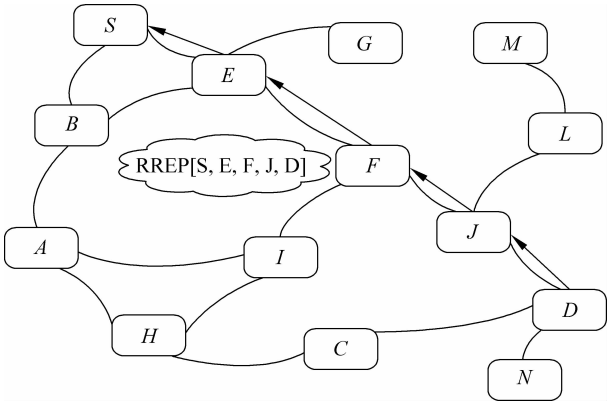


**图 3-1　路由发现**

### 3.2.2　AODV 路由协议

在 AODV 路由协议[5]中，当一个节点要向目的节点发送数据包时，会发起一个查找过程来定位目的节点。如果在特定的时间段内没有发现可用路径，则发起者节点认为目的节点不可到达。查找过程失败并且丢弃相应的数据包。另一方面，如果发起者节点收到其要求的路径消息，则更新路由表，产生一条通向目的节点的路径。

一旦产生一条路径，将会触发维护过程来监测该路径，如果一条路径不再被使用，则从路由表中删除该条路径。如果一条活动路由不可用，则上游节点立刻使用一个特定类型的控制包，来通知所有前驱节点中受到影响的节点。如果前面的节点还需要一条路径，那么受影响的节点会重新发起一个查找过程来寻找替代路径。

AODV 以分布式表驱动方式定义路由信息。这表示沿着特定路径的每个节点维护一个路由表项来到达目的节点，与仅源节点知道向目的节点转发的完整路径源路由的方法不同。AODV 允许每个节点维护一条通向目的节点并且是唯一的路径。一些其他路由协议允许多重路由查找。在这种情况下，如果有之前的路径失败，则选择使用另一条。

基于 AODV 的无线路由技术在 Mesh 无线网络有着极其广泛的应用，如今正在兴起的 Mesh 无线网络的多种解决方案所采用的路由协议都是由 AODV 协议改进而来，因此以下对 AODV 路由技术作详细的介绍。

**1. AODV 路由算法原理**

AODV 路由协议是一种按需的改进的距离向量路由协议，具有按需路由协议的特点即在 AODV 路由协议中，网络中的每个节点在需要进行通信时才发送路由分组，而不会周期性地交互路由信息以得到所有其他主机的路由；同时具有距离向量路由协议的一些特点，

即各节点路由表只维护本节点到其他节点的路由，而无须掌握全网拓扑结构。

AODV 路由协议中有三种类型的消息控制帧：路由请求(RREQ)、路由应答(RREP)和路由错误(RERR)消息。当源节点需要发送数据而又没有到目的节点的有效路由时，启动一个路由发现过程：向网络广播一个路由请求分组 RREQ，AODV 允许中间节点响应 RREQ，当收到请求的中间节点或目的节点有一条“足够新”的路由到达目的地时(“足够新”的意思是这条路由对应的目的序列号大于或等于 RREQ 中的目的序列号)，中间节点或目的节点以单播的方式向源节点返回一个 RREP 分组，RREP 沿着刚建立的逆向路径传输回源节点，源节点收到该 RREP 后则开始向对应目的节点发送数据。在数据传输过程中，当中间节点检测到一条正在传输数据的活动路由的下一跳链路断开或者节点收到去往某个目的地节点的数据报文，而节点没有到该目的地节点的有效路由时，中间节点向源节点单播或多播路由错误消息 RERR，源节点收到 RERR 后就知道存在路由错误，并根据 RERR 中指示的不可达目的地重新找路。在 RERR 中有一条链表，这条链表是由因为某条链路中断而导致无法到达的所有目的节点组成的。每一个接收到 RREQ 的节点都会保存到源节点的路由，当到目的节点的路由找到时就能用单播将 RREP 传回源节点。

**2. AODV 路由协议机制**

为了与目的节点进行单播通信，节点是如何产生 RREQ、RREP 和 RERR 消息的。这些消息数据是如何处理的。为了正确处理这些消息，某些状态信息是如何保存在所对应的目的地节点的路由表项中的。下面将对以上情况进行详细描述。

(1) 路由请求的生成与转发

基本上，如果在一个 MANET 中源节点 $A$ 在寻找目的节点 $B$，$A$ 需要向其邻居节点发送一个 RREQ 数据包，来让网络中其他每个节点知道它要寻找 $B$。目的节点序列号引用源节点 $A$ 已知的目的节点 $B$ 最近的路由序列号。如果没有找到的话则使用默认值 0。

每个收到广播 RREQ 的中间节点需要在一定范围内重新广播该消息，直到 RREQ 到达目的节点 $B$ 或者某个中间节点已知一条到达目的节点 $B$ 的新鲜路径。

两个 RREQ 的其他域是生存期 TTL 和广播 ID。

TTL 域允许一个查找发起者控制网络中 RREQ 传播的范围。例如，一个 TTL 域设置为 2 的 RREQ 数据包最多可从源节点传播两跳。当广播一个 RREQ 时，源节点设置 TTL 域来初始化跳数值并在做任何动作之前等待一个相应的时间段(RREP_WAIT _TIMEOUT)。如果碰巧在等待时间结束前收到一条路由消息，那么查找过程会成功结束。另一方面，如果在等待时间结束时没有收到任何回复，源节点重新广播一条同样的 RREQ 数据包，并且再次等待另一段时间，然而，RREQ 这次有一个更大的 TTL 值并且等待时间也会有所增加。TTL 值较大，新的 RREQ 就可以到达更多节点并且更有希望获得一条路径回复。

如果还是没有得到回复，源节点则继续增加 TTL 值重新广播 RREQ 消息，直到达到重传的最大次数，如果还没有找到，则取消该次查找。

此外，每个 RREQ 数据包都标记一个序列号，称为广播 ID。该标记可以使其他节点能够区分同一个节点发出的不同 RREQ，并且在每次广播后增 1。一对 <源 IP 地址，广播 ID> 唯一的标识一个 RREQ，拥有较大广播 ID 的 RREQ 更新鲜。作为一个中间节点，处理特定节点发送的 RREQ 时，记录相应的广播 ID 号。之后，中间节点仅处理同一个源节点发送的具有较大广播 ID 的 RREQ。其他广播 ID 值较小的 RREQ 则直接丢弃。

如果中间节点需要处理 RREQ，首先生成或者更新一条到达源节点 Source 的反转路

径。该路径最终用来将路由回复消息 RREP 传播到源节点 Source。一旦生成反转路径，中间节点检查自己是否储存了一条足够新鲜的到达目的节点 Destination 的路径，如果有，则生成路径回复数据包 RREP(见图 3-2)，并且沿着反转路径单播发送。此时，RREQ 不再需要再次广播。如果中间节点没有所需的路径，则在其生存期中增加一跳(TTL 值减 1)，判断 RREQ 是否过期(TTL=0)，若已过期则该 RREQ 不再被广播，若没有过期，则再重新广播，跳数域加 1，相应的序列号是源序列号，包含在 RREQ 中。

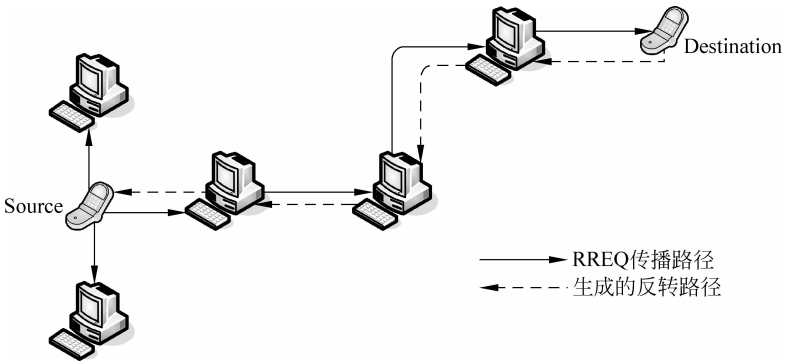


**图 3-2　RREQ 的传播及反转路径的生成示图**

(2) 路由回复的生成与转发

当一个节点拥有一条可用路径时(或者是目的节点或者是拥有足够新鲜路径的中间节点)，则向生成查找过程的源节点单播路由回复数据包 RREP。

RREP 包含源节点和目的节点的 IP 地址以及路由的序列号。也包含一个跳数域(和 RREQ 数据包中的一样)以及表示路由有效期的生存期 TTL 域。

路由回复消息 RREP 生成后，如图 3-3 所示，转发路径根据沿着生成的反转路径传播的路由回复消息建立。每个收到 RREP 的节点生成一条通向目的节点 Destination 的表项。目的节点序列号和跳数从 RREP 中得到，并且该路径的下一跳是最后一个转发 RREP 的节点。如果 RREP 还没有到达目的节点，则转发到反转路径的下一跳，当然，跳数域先增 1。

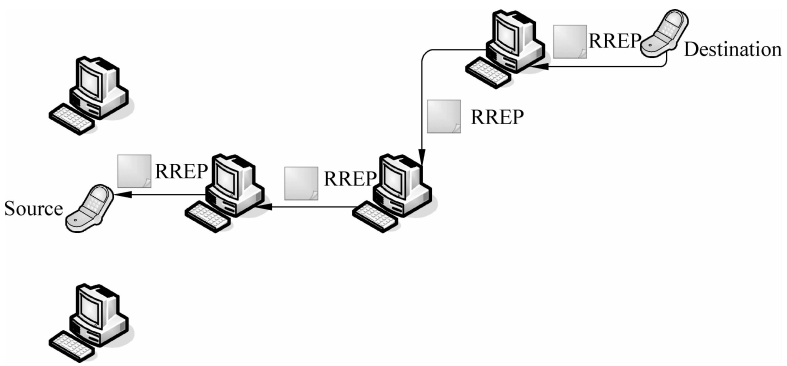


**图 3-3　RREP 的传播示图**

当 RREP 最终到达源节点，则不再需要转发。在源节点 Source 根据目标节点 Destination 生成一条转发路由表项后，自动销毁 RREP 数据包。查找阶段结束并且新的路由可以用来发送缓冲区里的数据了。

(3) Hello 消息的生成与处理

在 AODV 路由协议中,节点可以通过广播本地 Hello 消息来提供连接性信息。每 HELLO_INTERVAL 微秒内,节点检查在最近的 HELLO_INTERVAL 是否发出了一个广播报文(比如 RREQ),如果没有发送,它会广播一个 TTL 值为 1 的 RREP,称为 Hello 消息,Hello 消息的字段设置如下:

- 目的地 IP 地址:节点的 IP 地址。
- 目的地序列号:节点最新的序列号。
- 跳数:0。
- 生存期:ALLOWED_HELLO_LOSS×HELLO_INTERVAL。

任何时候节点收到来自邻居的 Hello 消息,节点应该确信它具有到这个邻居的有效路由,如果必要,建立一条这样的路由。如果路由已经存在,那么应该增加这条路由的生存期,需要的话应该至少为 ALLOWED_HELLO_LOSS×HELLO_INTERVAL。此外,还需确保包含 Hello 消息中的最新目的地序列号。

在 AODV 中,任何时候节点收到任何控制报文,也具有和收到显性的 Hello 消息一样的意义。因为它通过控制消息报文中的源 IP 地址,显示出到节点的有效连接性。

(4) 路由维护机制

在一条路径中检测到某段链路失效时,上游节点发出 RERR 数据包,将此消息通知该路径前面的节点。RERR 包含所有无法联系的目的节点的序列号。

在 RERR 通过转发路径传播时,每个受到影响的节点通过标记相应路径无效来更新路由表。对每个包含在 RERR 数据包中的目标节点,当前节点从 RERR 数据包中拷贝出相应的序列号,设置一个无限长的距离值并更新。而且,如果剩下的链表不为空,RERR 中其余当前不可到达的节点也要向前面的节点继续广播。当然,RERR 只在最少有一个节点不能到达时重传。而且,每个节点只在收到向同一目的节点转发数据的下一跳节点发送的 RERR 数据包时,使其针对某个目的节点的路由表项无效。如图 3-4 所示,即使中间节点 $C$ 收到 RERR,节点 $C$ 并不会取消通向 Destination 的路径,因为虽然节点 $C$ 收到从 $B$ 发来的 RERR,但是根据其路由表,它当前使用的到达 Destination 的路由下一跳并不是 $B$,所以 RERR 消息会被直接销毁。

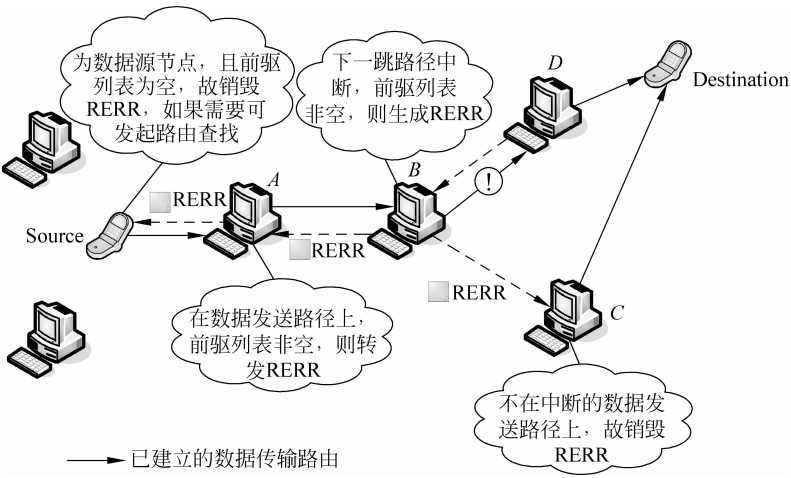


**图 3-4 路由维护机制示图**

## 3.3　无线自组织网络的路由攻击方法

关于针对无线自组织网络攻击的理论模型[6-8]，我们可以将无线自组织网中的攻击者分为两类：被动攻击者(passive attacker)和主动攻击者(active attacker)。被动攻击者仅仅对网络进行窃听；而主动攻击者在窃听的基础上向网络中注入虚假报文，后者比前者更具有攻击性。

无线自组织网络的安全问题中，最为突出的问题就是路由安全[9]。当前无线自组织网络所采用的各种路由协议侧重于路由效率的提升，而缺乏安全性的评估。设计者假定参与路由信息交换的所有节点都能诚实地转发和处理路由报文和数据，这导致无线自组织网络的路由安全容易遭受各种形式的攻击。常见的针对路由的攻击行为分为如下几种。

### 3.3.1　篡改

路由协议假定网络中节点都是相互合作的，转发报文的节点不会修改与其无关的路由信息，所以不检查路由信息的完整性。这使攻击者能够很容易地更改路由信息中任何字段，例如，AODV 路由中的序号和跳数，DSR 路由包中的路由节点序列等，从而产生错误的路由，如重定向、回路等，导致整个网络性能下降。攻击者能够篡改路由报文的根本原因在于节点无法对路由报文进行完整性检测。

### 3.3.2　冒充

因为路由协议并不认证报文的地址，所以攻击者可以声称为某个节点加入网络，甚至能够屏蔽某个合法节点，替他接收报文。其根本原因在于节点不能鉴别报文的来源。

### 3.3.3　伪造

攻击者可以伪造并广播假的路由信息。例如，广播某条存在的路由已中断，或编造一条并不存在路由。它可造成回路、分割网络、孤立节点等。其原因在于无法验证报文的内容。

### 3.3.4　拓扑结构与通信量分析

在路由查询和发送报文中都包含有明确的路由信息，如 DSR 报文头部就含有从源节点到目的节点的路由。攻击者能够通过偷听这些报文分析出节点相邻情况、所处位置等拓扑信息，可进一步通过流量分析，得出节点在网络中的功能和角色。借助这些信息，攻击者可准确地进攻网络控制节点或军事网络中的指挥员。

### 3.3.5　资源消耗攻击

无线自组织网络中的 DoS 攻击(拒绝服务攻击)是资源消耗型攻击的一种，DoS 攻击又可以分为针对个别节点的 DoS 攻击和针对全网络的 DoS 攻击。我们所常见的 RREQ 泛洪

攻击是一种针对全网络的 DoS 攻击，入侵节点大规模广播 RREQ 报文或者发送大量的恶意数据报文来消耗网络带宽和其他节点的系统资源，并最终导致有效通信不能正常进行。当一个节点发动泛洪攻击时，将选择很多不存在于已知网络中的节点，向“它们”发送 RREQ 报文，由于这些“目标节点”根本不存在，RREQ 报文将被不断转发直至 TTL 为 0。

### 3.3.6 虫洞攻击[10]

两个串通的攻击者，采用专用通路直接相联，越过正常的拓扑结构，直接转发路由查询报文，造成错误的路由拓扑信息。图 3-5 为虫洞攻击示意图，从 $S$ 节点到 $D$ 节点的正常路由应该为 $S—A—B—C—D$，但攻击者 $M_1$ 和 $M_2$ 通过 ABC 建立虚拟专用通道用来转发路由查询报文，这样形成了 $S—M_1M_2—D$ 的路由。因为后者路由跳数少，源节点选择了 $S—M_1M_2—D$ 作为发送路由。

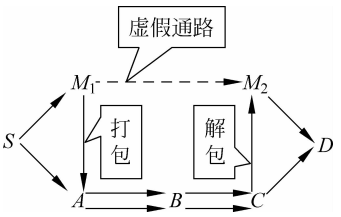


图 3-5 虫洞攻击示意图

### 3.3.7 黑洞攻击[11]

黑洞攻击是在路由查询中攻击者在没有至目标节点的路由情况下，抢先宣布有到目标节点的路由，使源节点建立通过该节点的路径，在随后的报文发送中，抛弃通过该节点的报文，形成抛弃报文的黑洞。

### 3.3.8 RUSHING 攻击[12]

在按需路由协议中，攻击者短时间内发送大量路由查询遍布整个网络，使得其他节点正常的路由查询无法提交处理而被抛弃。

下面详细介绍两种对网络影响较大的攻击方法：泛洪攻击和黑洞攻击。

## 3.4 泛洪攻击

泛洪攻击能针对无线自组织网络中的所有采用按需路由协议发动 DoS 攻击，例如，DSR、AODV、LAR[13] 等，甚至有些路由安全协议也不能幸免，如：SRP[14]、Ariadne[15]、ARAN[16]、SAODV[17]，因为它们只是提供节点相互认证，防止恶意节点修改路由协议报文其目的是防范外界的攻击，而对内部节点发动的 DoS 攻击丝毫不能防止，其安全认证的过程需要大量的计算，反而更增强 DoS 攻击的效果。

下面基于 AODV 来描述泛洪攻击方法，针对其他路由协议的攻击方法类似。

在 AODV 路由协议中，泛洪查找路由是非常消耗网络资源的，为了减少泛洪 RREQ 报文对网络的影响，AODV 协议采取了一些措施。首先设置了 RREQ 每秒最大发送数，每个节点在一秒内发送的 RREQ 报文数不能超过这个数值。其次，节点在发送的 RREQ 报文后，要设置一个最大查询往返时间，等候 RREP 的返回，如果超过最大查询往返时间没有收到节点回答才能准备重新的发送 RREQ 报文，但也不能立即发送，需要等待一段时间，该时间长短为 RREQ 查询往返时间的两倍。再次，RREQ 的泛洪查询范围必须依次递增，通过

RREQ 报文中的 TTL(Time-To-Live)进行控制，开始时设置范围小，查询不到时，再依次增加，直至收到 RREP 或达到最大限制。AODV 路由协议通过上述方法来控制泛洪 RREQ 查找的频率与范围，减少对网络资源的消耗。

但在泛洪攻击中，入侵者不顾这些规定，尽力消耗网络资源，攻击分为两步。第一步，入侵者选择路由查询的节点地址。如果它知道整个网络的地址范围，它将选择不在网络内 IP 地址作为路由查询的节点地址，因为没有节点能够回答它的 RREQ 报文，每个节点就要一直暂存的 RREQ 的信息和反向路由，直至超时才能删除这些信息，能够尽可能长时间占用资源。如果入侵者不知道整个网络的地址范围，它就随机选择一些 IP 地址进行路由查询。第二步，入侵者以选择好的 IP 地址为目标，大量、连续地发送 RREQ 报文。不管 AODV 设置的 RREQ 每秒最大发送数，尽力多发送 RREQ，同时直接将 TTL 设置为最大值，在全网内泛洪查找。如果发送 RREQ 的地址用完，就开始新一轮的发送，不顾 RREQ 的查询往返时间和退避时间。当入侵者采用上述方法发动 RREQ 泛洪攻击时，整个网络就会充满 RREQ 报文，导致通信带宽和节点两方面的资源枯竭。连续不断的 RREQ 在网络中泛洪发送，占用了大量无线通信带宽，导致网络拥塞，正常通信无法进行。对于节点来说，每收到一个 RREQ 报文，从上节 AODV 协议概述可知，它都要缓存 RREQ 报文的源节点地址、目的节点地址、上游节点地址和目的序列号并建立反向路由，该缓存要等待 RREP 或超时后才能释放。如果没有 RREP 到达，又不断接收新的 RREQ 报文，有限的缓存就会被消耗完毕。此时，如果其他节点要建立路由，再发送 RREQ 报文，这些节点就不能接收新的 RREQ 报文，导致正常的路由建立无法进行。图 3-6 显示一个泛洪攻击的流程。攻击节点 $H$ 向周围节点泛洪发送攻击报文，周围节点收到后继续泛洪传播，造成整个网络充满了攻击报文，网络性能严重下降，如图 3-7 所示。

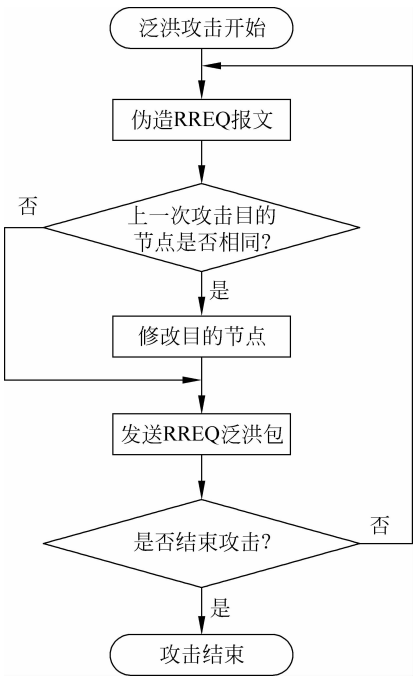


**图 3-6　泛洪攻击流程图**

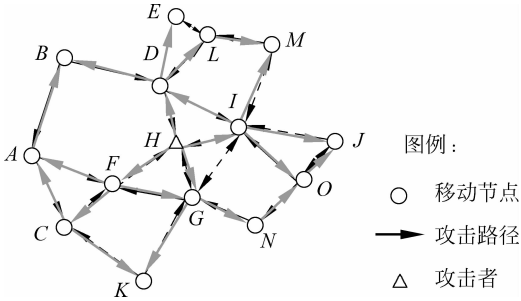


**图 3-7　泛洪攻击示意图**