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，然后介绍针对路由协议攻击的一些方法，其中重点分析两种攻击方式：泛洪攻击和黑洞攻击。详细讨论其攻击原理，并设计检测响应方法。最后，设计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回到 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，攻击者就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，无须像有线网络一样，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移动造成的还是虚拟路由信息形成的。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，致使网络失去了安全性。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)[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地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标节点发送数据,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,则丢弃该RREQ分组,不作处理。
- 如果路由记录中包括本节点,则丢弃该RREQ分组,不做进一步的处理。
- 如果本节点就是RREQ指定的目的节点,则发送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,那么目标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,目标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,动态地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 报文中加上自己的信息，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。

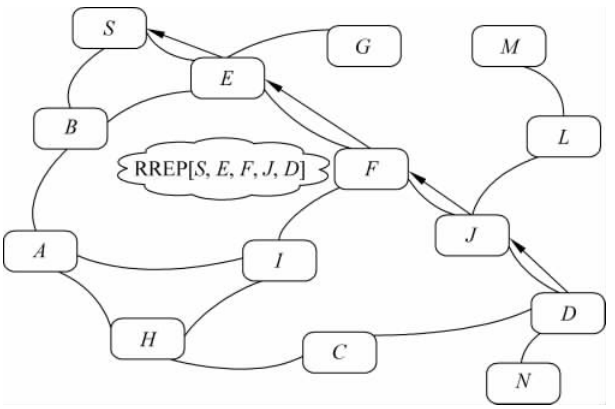

图 3-1　路由发现

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标节点。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标节点不可到达。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，产生一条通向目标节点的路径。

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标节点，与仅源节点知道向目标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标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，下面对 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,则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,则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，则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。

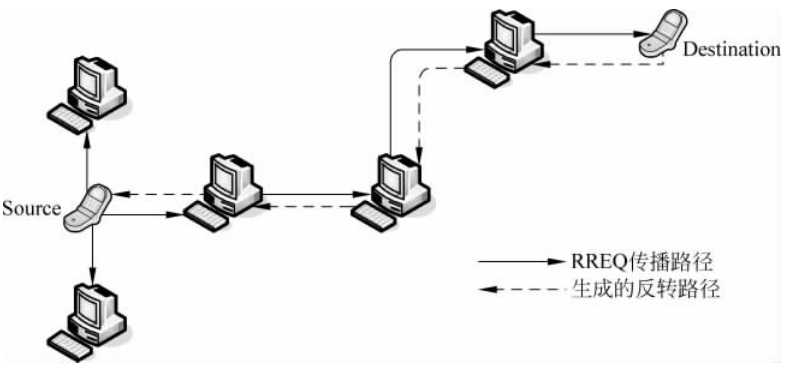

图 3-2　RREQ 的传播及反转路径的生成示图

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(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。

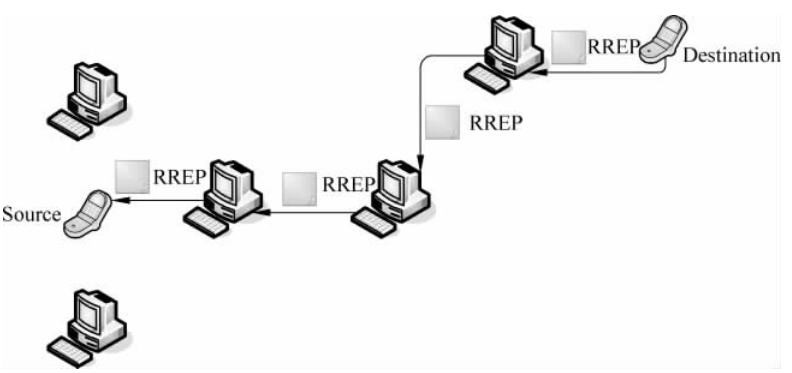

图 3-3　RREP 的传播示图

当 RREP 最终到达源节点时，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(例如 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,则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,还须确保包含 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 数据包中复制出相应的序列号,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 也并不会取消通向 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。

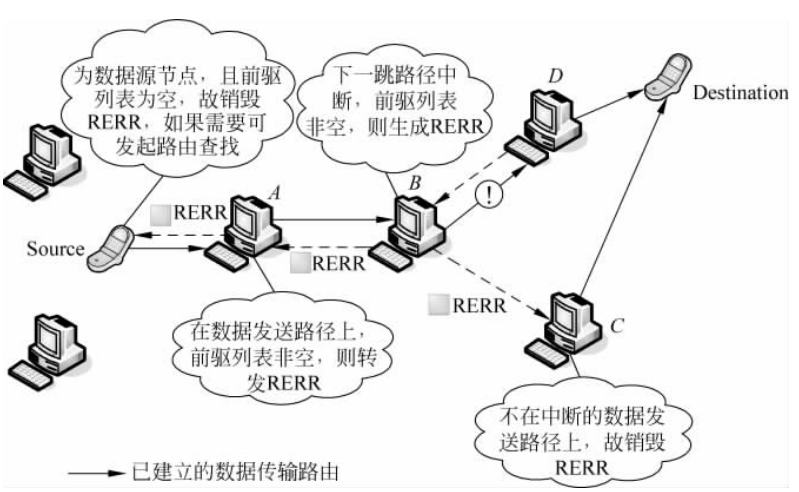

图 3-4 路由维护机制示图

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]，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，因此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的任何字段，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，替它接收报文。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。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

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[10]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A—B—C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_1—M_2—D的路由。因为后者路由跳数少,源节点选择了S—M_1—M_2—D作为发送路由。

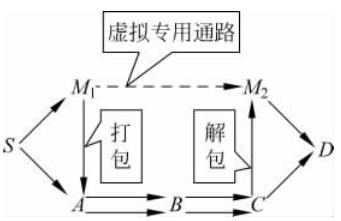

图3-5 虫洞攻击示意图

3.3.7 黑洞攻击

黑洞攻击[11]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

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[12]。

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1s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还没有收到节点回答才能准备重新发送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的 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 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，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。

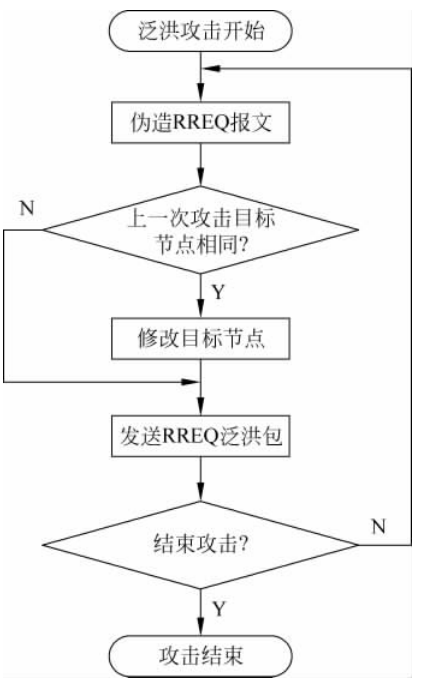

图 3-6　泛洪攻击流程图

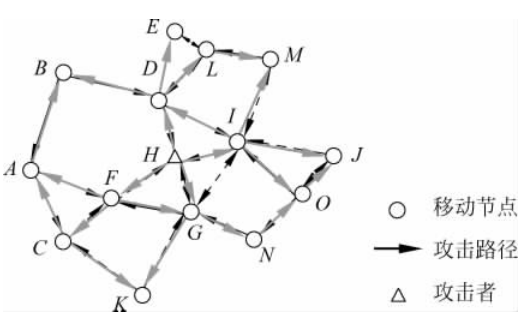

图 3-7　泛洪攻击示意图

3.5 泛洪攻击检测及响应

下面提出的两种检测泛洪节点的方法,都运用了门限的概念。

(1) 自动丢包机制。节点每隔一定时间统计所收到的 RREQ 数量,如果从某个节点发出的 RREQ 包的平均频率高于我们事先设定的一个门限值,则自动丢掉该包。缺点是自动丢包处理会降低网络的吞吐量,另外该方案不能识别这些被判为不正常的 RREQ 控制报文是发自泛洪节点,还是替泛洪节点转发 RREQ 包的受害节点,因此可能会将正常节点发出的 RREQ 包也丢弃。

(2) 监听检测机制。它将节点监听和节点信誉机制结合起来,这种检测机制是比较有效的。比较简单的一种机制是:邻节点监听机制规定网络中的每个节点均计算经过其 RREQ 的频率,如果来自同一个节点的 RREQ 频率超过了某个门限值,则邻节点将会视这个 RREQ 包的源节点为恶意节点,并把它加入黑名单。

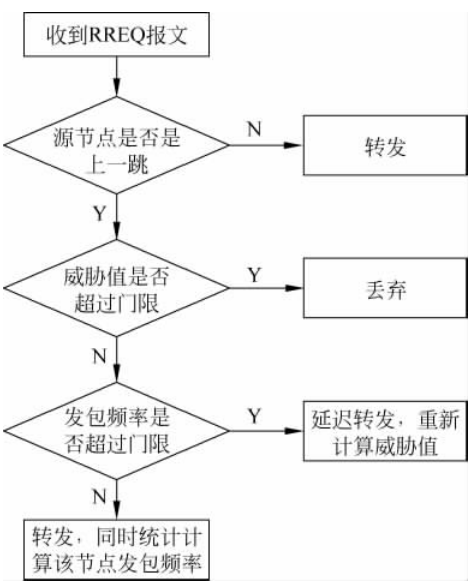

图 3-8 泛洪节点检测响应流程图

我们对这种监听检测机制进行改进,首先引入"绝对威胁值"这个概念,当一个节点的威胁值超过了我们设定的门限时,我们认为这个节点是攻击节点,则丢弃它发出的 RREQ 包。

具体流程如图 3-8 所示。当节点收到一个 RREQ 报文,首先判断上一跳是否为源节点,如果不是,则继续转发;如果是,则首先判断该节点的威胁值是否高于门限,是则丢弃该 RREQ 包,不是则继续判断 RREQ 发包频率是否超过门限,没超过则继续转发,超过则重新计算威胁值,延迟转发 RREQ 包。

绝对威胁值的计算方式

$$S = 1 - \frac{1}{2^n}$$

n 为节点发送 RREQ 包频率超过门限的次数。从这个公式可以看出,当 $n=0$ 时,标准威胁值 $S=0$,即每一个节点的初始标准威胁值都是 0,当 n 增大时,S 也是指数增长趋近于 1 的。这样,可以设置一个门限值 S_0,当 $S \geqslant S_0$ 时,我们就认为这个节点是泛洪节点而丢弃所有来自它的 RREQ 包。

3.6 黑 洞 攻 击

黑洞攻击是一种拒绝服务攻击。攻击者声称自己是信宿节点或者有一条最新的到信宿节点的路由来吸引分组,但并不将分组转发出去,就好像宇宙空间中的黑洞一样。在 DSR

路由协议下，我们所采用的黑洞攻击方式有两种：被动黑洞和主动黑洞。

3.6.1　被动黑洞攻击

被动黑洞攻击就是一个网络中存在的黑洞，当所有数据包进入了黑洞就不会再出来，即黑洞节点会丢弃所有经过它的数据包。如图 3-9 所示，假设源节点 S 到目的节点 D 的路由是 $S\rightarrow1\rightarrow M\rightarrow4\rightarrow D$。当恶意节点 M 开始进行被动黑洞攻击时，所有通过节点 M 的数据包都将被丢弃，节点 S 与节点 D 的通信也将终止。但是因为被动黑洞节点依然转发路由包，也就是 RREQ 包和 RREP 包。所以当 S 重新寻找节点 D 的时候，节点 M 又会出现在新的路由链路上，也就是新的路由链路又将失去作用。黑洞节点通过这种方式来干扰正常的节点间通信，扰乱整个网络的正常工作。

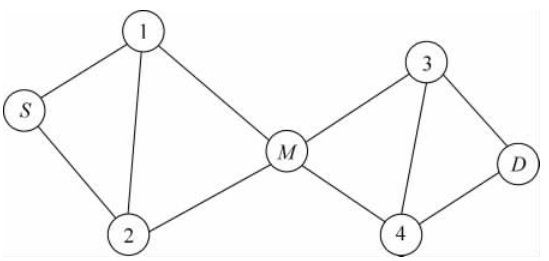

图 3-9　被动黑洞攻击

一般意义上的黑洞节点称为被动型黑洞，这种攻击者转发经过自己的路由报文，但丢弃所有的数据报文。由于没有向网络注入虚假报文，仅仅对网络拓扑进行攻击，因此，这种黑洞攻击是一种被动的路由扰乱型攻击。

被动黑洞攻击流程如图 3-10 所示。

3.6.2　主动黑洞攻击

被动黑洞攻击有种愿者上钩的味道，对网络的危害性并不是很大，尤其是对如图 3-11 所示的拓扑情况。在图 3-11 中，源节点 S 到目的节点 D 之间存在两条路由：$S\rightarrow1\rightarrow D$ 和 $S\rightarrow M\rightarrow D$。首先在路由选择上，如果恰好选择了 $S\rightarrow1\rightarrow D$ 这条路由，那么黑洞节点 M 的攻击就没有了效果。其次，就算源节点 S 选择了 $S\rightarrow M\rightarrow D$ 这条路由，那么在发送失败后，S 会再次进行路由选择，此时又有可能让 S 节点选择 $S\rightarrow1\rightarrow D$ 这条路由。另外，如果源节点 S 向目的节点 D_2 发送数据包，那么 M 根本就不在这条路由上，也就无法进行攻击了。

正是因为被动黑洞攻击有其局限性，所以出现了主动黑洞攻击这种更具破坏性的攻击方式。主动黑洞攻击，就是恶意节点在收到 RREQ（路由请求包）时，在回复的 RREP（路由应答包）中向对方声

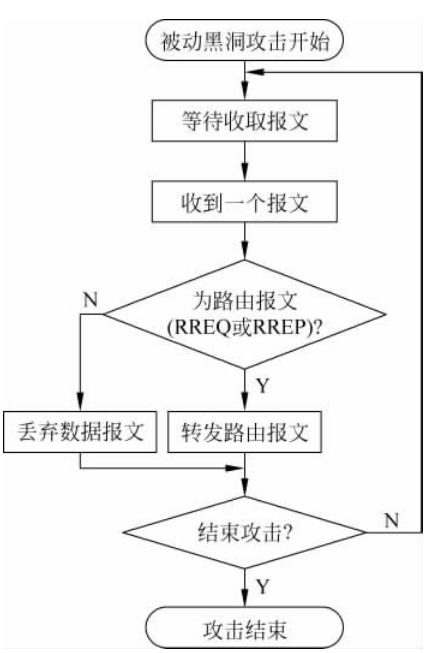

图 3-10　被动黑洞攻击流程图

称,我的下一跳就是目的节点,以此来吸引更多的数据包发向自己,在扰乱正常通信的同时也扰乱了整个网络的路由信息的获取,严重影响网络负载。

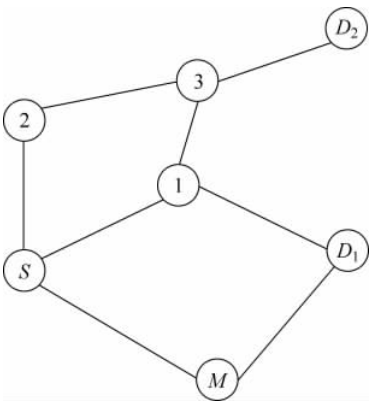

图 3-11 被动黑洞攻击缺陷

当恶意节点是主动黑洞攻击节点时,在图 3-11 中的 S 节点要向 D_2 发送数据,先会广播 RREQ 包,查询到 D_2 节点的路由信息。这时,恶意节点 M 收到了这个 RREQ,马上回复一个 RREP,声称自己的下一跳就是 D_2 节点。必然的,S 节点不会再考虑 $S\rightarrow 1$ 或是 $S\rightarrow 2$ 这两条路由,而把数据包发向恶意节点 M。恶意节点 M 就达到了吸引流量的目的。

对于主动黑洞攻击,攻击者收到来自其他节点的 RREQ 报文后,直接回复 RREP,谎称目标节点就是自己的下一跳,经过自己到目标节点的路由是最近的。源节点很可能在收到正确的 RREP 报文之前先得到来自主动黑洞的伪 RREP(源节点是按照最先收到的 RREP 报文记录的路由发送数据报文),此时,数据报文必然被发送到黑洞节点。由于主动黑洞篡改了路由,更多的数据包会交由攻击者来转发,从而达到了对网络更好的攻击效果。

主动黑洞攻击流程图如图 3-12 所示。

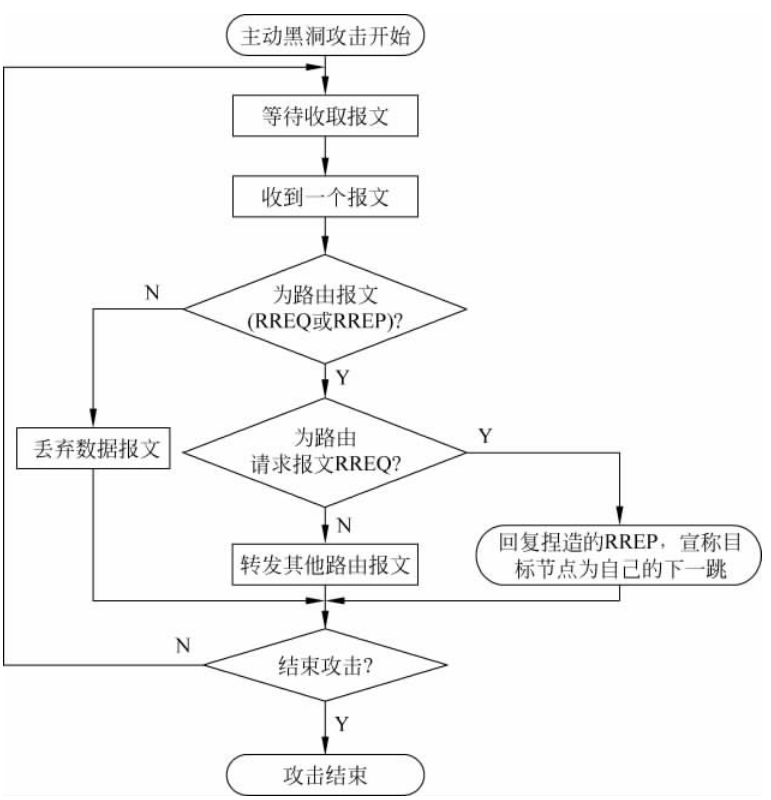

图 3-12 主动黑洞攻击流程图

3.7　黑洞攻击检测及响应

在无线网络中报文都是广播出去的，也就是邻居节点可以相互听到对方所发出的任何包。所以当一个节点转发数据报时，邻居检测系统会确认路由的下一跳节点是否转发了该报文，可以以此判断邻居节点是否有恶意行为。

假设有 A、B、C、D、E 五个节点，如图 3-13 所示。A 经过 B、C、D 发送数据给 E，节点 B 并不能直接和 D 通信，但是 B 可以监听 C 发出的报文。这样，A 缓存下刚发送的数据报，在听到 C 转发的数据报后，与缓存的数据包进行对比，如果一致，表明此数据报已经发出；如果不一致，说明 C 节点有恶意篡改行为。如果数据报在缓存中保留超过一定时间，则认为 C 没有正常工作。在后两种情况下，B 对于 C 的行为会给予一次计数，如果这个次数高于设定的一个阈值，则 B 确定 C 节点是恶意节点，并把这个信息在链路中广播。继续采用前述的方法和计算公式，用 C 被举报的次数 n 来确定 C 的威胁值 S，当威胁值大于一个设定的阈值 S_0 时，就可以认定 C 是黑洞节点，将其排除出网络环境。

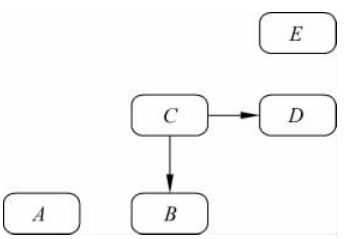

图 3-13　*B* 监听到 *C* 发给 *D* 的数据报文

3.8　基于移动防火墙的无线自组织网络主动防护机制

3.8.1　主动防护算法概述

随着无线自组织网络的广泛应用，无线自组织网络的安全保障变得日益重要。现有防范网络入侵的方法可分为三类：入侵阻止、入侵检测和入侵响应。入侵阻止是利用认证、加密和防火墙技术来保护系统不被入侵者攻击和破坏。但是，这类防护方法应用在无线自组织网络环境之中会受到条件的限制，例如网络拓扑动态变化，没有可以控制的网络边界，使得防火墙无法应用。节点在移动时也可能被敌方俘获而投降，投降节点拥有合法的密钥，加密和认证也失去了作用。因此，尽管入侵阻止方法在传统网络中发挥了重要的作用，但在无线自组织网络中却难以发挥作用。入侵检测通过分析节点的行为来确定入侵者，按照检测技术，可以分为基于特征的和基于异常的入侵检测。迄今为止，无线自组织网络安全的研究主要集中于入侵阻止和入侵检测。如何在无线自组织网络环境下实现入侵响应还未见相关参考文献。无线自组织网络由于其资源有限相当脆弱，如果不对入侵者产生及时的响应，阻止其攻击行为，就可能会造成整个网络崩溃。相关研究参考文献表明，当攻击者发动泛洪攻击时，在 7min 内整个网络的报文传输率由 97%下降到 9.4%，网络流量几乎全部被阻塞，网络无法正常运行。同时，由于其自组织、缺乏集中控制的特点，特别是在多个管理域的环境中，会使得人工的响应措施难以实施。

由此可见,尽管入侵阻止和入侵检测技术在防止入侵方面发挥了巨大的作用,但是它们都是被动的防御措施,它们所能取得的效果就是防止正常节点成为入侵行为的牺牲者。它们不能有效地消除入侵根源——入侵者。入侵者能够继续存在并危害网络系统。为了能够从根本上消除入侵行为,课题组提出了基于移动防火墙的无线自组织网络主动防护模型。

一种通常的做法是检测出入侵者后,把它记入一个黑名单,然后通过全网广播此黑名单,从而使那些未知的节点能提前获知入侵者,进行防御,避免了重新识别的开销和安全危害。从安全性的角度而言,全网广播黑名单的方式无疑能够将入侵者信息传递到网络中的全部节点,从而有效隔离入侵者,使其无法对网络造成过大的伤害。但是,全网广播带来的开销是巨大的,它不仅对资源造成巨大浪费,同时也会对网络的正常运作带来不利的影响。特别是随着无线自组织网络规模的不断增大,全网广播开销将增大到不可接受的程度,因此全网广播黑名单只能适应于小规模的无线自组织网络。

入侵者受到攻击能量、信号的感知、布局以及障碍的限制,通常活动区间有限。我们认为入侵者的移动并不都是广域范围的。因此,采用全网广播方式通常也带来较大的浪费,很多节点并不需要了解入侵者信息。另外,既然入侵者是移动的,那么也没有必要一次性占用大量资源进行全网广播,而是要跟随其移动进行有限范围的通知,以实现跟随攻击阻断。我们提出的移动防火墙响应模型,可以解决全网广播所存在的问题。方法是将广播黑名单仅仅局限于入侵者的周围区域,并且随着入侵者的移动,逐渐地转告其周围节点,使它们能在入侵者到来之前,获知入侵者的信息,并在入侵者接近时进行阻击,从而在其周围形成一堵移动防火墙。这样,由于入侵者通常并不会遍历整个网络,移动防火墙的报文发送只涉及入侵者所经过的区域,从而能够在不影响整个网络安全性的前提下大大地减少开销。以下详细论述主动防护模型,分为簇的形成机制、信号强度检测、入侵响应策略、移动防火墙设计等部分内容。

3.8.2 簇形成机制

为了更好地节约报文的开销,首先提出了建簇的概念。

簇的形成主要是通过一种选举算法来进行的。选举算法由两部分组成:选举阶段和维持阶段。整个网络对于选举阶段的时间和一个决策节点的维持阶段的时间都有明确的规定。在规定的选举时刻点,每个节点根据自己的能力(网络吞吐量等性能)来竞争决策节点,每个节点都能以一定的概率(能力越强,概率越大)发送告示报文来声称自己是决策节点,任何收到此告示报文节点就成为该决策节点所管辖的簇的成员节点,不能再发告示报文。告示报文只能在一跳范围内传播,不能被转发。因为通信是双向的,某个节点能收到告示报文,那么它所发出的报文也能被决策节点收到,所以决策节点能够监视告示报文传播范围内的节点行为。当收到多个告示报文后,节点会选择其中ID较小的一个,并回复应答报文。经过一定的应答时间后,决策节点发出通告报文以告诉成员节点本簇的所有成员。当区域内选举出一个决策节点后,就进入了维持阶段,在维持阶段,决策节点不需要广播告示报文,决策节点有义务保持静止,而普通节点可以离开(但是针对无线自组织网络移动性不大的特点,这些移动可以忽略),决策节点根据信号强度,当发现有节点离开时,决策节点自行地从它的成员名单中去除该节点,而有新节点进入后,发送一个告示广播告诉它。决策节点在到了维持时间后,就自动卸任。整个网络开始重新启动一个新的选举过程,为了保证公平和随机性,

上一届的决策节点将不能参加下一届决策节点的选举，除非整个区域只有它一个节点存在。

决策节点的选举是公平而又合适的。所谓公平性，即每个节点都能够有公平的机会选为决策节点，同时每个节点有相同的服务时间，并且不能连任。周期性地更换决策节点，保证了检测的安全性。如果有某个节点是入侵者，又被选举为决策节点，那么在其作为决策节点的期间可以攻击网络而不被发现。但它的任期结束后，又会选出新的决策节点，此时就会发现入侵者。所谓合适性，即被选为决策节点的概率和节点的能力有关，因此不会选择那些网络负载已经很大的节点作为决策节点，这样做不会导致决策节点成为网络的瓶颈。

虽然，就短期而言，簇的建立会带来一定的额外开销，但是在簇形成以后，整个网络入侵响应的报文开销被局限于簇的内部，大大降低了因通知整个网络而带来的不必要的报文浪费。因此，簇的形成必定会从长久上给整个网络带来开销上的节省。

3.8.3　信号强度检测

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，任何人都可接收，所以容易被敌方窃听。但是，也正是由于这个原因，入侵者也因此暴露了自己的身份。例如 AODV 等协议，要求每个节点必须定期地发送 Hello 报以确认邻居节点的情况，这样，在入侵者移动的同时，它周围的节点必定会感知到它的信号强度，入侵者在它移动的同时也因此留下了自己的行踪。那么，只要响应策略得当，在入侵者被检测出以后，能够及时地告知其周围的节点，并且这些节点主动对其进行信号的检测，当发现入侵者信号强度增强时，再进行阻击和响应，进而将入侵者牢牢地困于移动防火墙之中。

同时，由于保持阻击必定会带来额外的能量消耗，当节点检测到入侵者的信号强度减弱并持续一定时间以后，可以认为入侵者暂时对自己是构不成威胁的，因此对其解除阻击，以节约能量开销。

3.8.4　入侵响应策略

在基于簇的概念以后，也就产生两类节点：决策节点与普通节点。决策节点由于具有更高的能力，担负起了信息的收集、判断以及发布统一的阻击命令等任务。并且，由于我们的选举算法每个簇的决策节点与它簇中其他的节点相距仅仅一跳，因此，决策节点与普通节点的通信在开销上达到了最小化。普通节点拥有最基本的入侵阻止以及入侵检测能力，并且在阻击入侵者的同时，普通节点还会对入侵者采取响应操作，它会自主地通过发布一跳预警广播来告知自己的决策节点。

在这里，基于簇的概念，我们定义三种名单：黑名单、灰名单与预警名单。每个节点都拥有一张黑名单和灰名单，而决策节点还要拥有一张预警名单。我们规定簇中的所有节点必须有严格的统一性，而决策权仅仅来自于决策节点。只有决策节点才能发布黑名单广播通知簇中其他节点入侵者的存在。下面来详细介绍这三张表的作用和来源。

灰名单是通过节点自身的检测，或者收到来自其他节点（非决策节点）的入侵警报后添加的，对于灰名单中的记录，节点需要对其进行定期地信号检测，并在信号强度大于阈值后进行阻击，但是，由于灰名单并非来源于本簇的决策节点，普通节点需要在感测到入侵者后进行预警广播，通知决策节点，由其来判断是否需要整个簇一起阻击该入侵者。

因此决策节点需要负责一张预警名单，用于记录本簇中的其他节点发出的预警信号，这

张表包含两个属性：一个是入侵者ID(可以是入侵者的IP地址)，另一个是来自不同节点的预警次数。决策节点每收到一个来自本簇普通节点的预警警报后，将在对应的记录中加一，但对于同一个节点发来的针对同一个入侵者的预警警告不进行累加，当记录到底到达预警信号的数量阈值后(这个数量取决于整个簇的大小)，说明入侵者已经完全进入本簇，决策节点进行黑名单广播通知整个簇。预警名单通常会进行定期的清空，以防止累计效应而带来的误报。

在普通节点收到来自本簇的决策节点发出的黑名单广播后，普通节点自己将其添加到自己的黑名单中。并且会检查其灰名单中是否有这个入侵者记录，如果有，则将其从灰名单中删除，如果没有，则需要发出一跳的入侵警告广播以告诉自己的非本簇邻居节点。这样也就保证了在入侵者移动的时候，所有的普通节点都能在其可以对自己进行攻击之前被通知到该入侵者的存在，提前形成一道“防火墙”，对入侵者进行阻击。在以后的时间里，对于黑名单中的记录，节点需要定期地进行信号检测，并在信号强度大于一个阈值后进行阻击。然而，节点不须再考虑发送任何消息以通知其他节点，因为对于移动性不大的无线Mesh网络而言，此时已经可以确保非本簇的邻居节点已经被告知入侵者的存在。

3.8.5 移动防火墙设计

在固定网络中，防火墙安装于整个网络的入口处，负责过滤不安全的报文，以保护内部主机免受外部的攻击。无线自组网络由于节点可随意移动，没有明确的网络边界，所以无法使用防火墙。为此，建立了簇的概念，以此来形成网络中的局部边界。无线自组网络中节点之间的通信必须借助邻居节点的转发，如果邻居节点拒绝转发报文某个节点，则该节点就都被隔绝于网络。移动防火墙是利用上述思想进行设计的。

首先，每个节点都能够自我拥有入侵检测以及入侵阻击能力，当检测出入侵者后，节点会自我对其进行阻击，同时需要发送预警信号通知其决策节点。由于无线网络的信号是在空中传播的，节点的邻居节点都能收到它发出的预警信号，在接收到预警信号后，这些邻居节点都会将这个入侵者记录于自己的灰名单中，并开始对其进行信号检测。而决策节点在收到预警信号后，通过其数量与阈值的比较，判断是否需要全簇广播黑名单。

当入侵者移动后，检测到它信号强度超出阈值的节点必然增多，因此也就有了更多的预警信号，如果某个决策节点在收到更多的来自本簇的普通节点的预警信号后，就会判定该入侵者已经进入本簇，因而发出黑名单广播。收到这个广播后，整个簇对其进行阻击，将入侵者包围其中，并且每个普通节点发出一跳广播通知其临簇节点。当入侵者试图突破防火墙时，临簇的节点在感知到信号强度后，又会通知它们的决策节点，新的一个包围圈又形成了。这样，入侵者始终被一层移动防火墙所包围着。

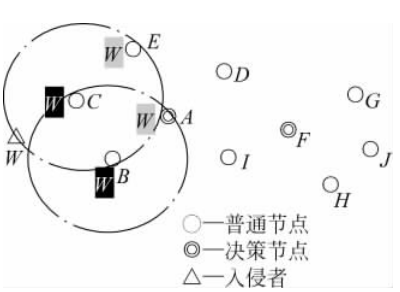

图3-14 *B*、*C*节点受到*W*攻击

为进一步论述如何实现防火墙的移动性，下面举一个移动防火墙的例子来说明(见图3-14)。场景中包含两个簇，分别是簇1：*A B C D E*和簇2：*F G H I J*，*A*和*F*分别为决策节点。

从图3-14中可以看到，攻击节点*W*发动了攻击，*C*和*B*节点受到它的攻击后，识别出它是入侵者，从而

将其加入各自的黑名单，通过一跳黑名单广播告诉自己的邻节点 E 和 A：W 是入侵者，收到广播后，E 和 A 同时将 W 加入各自的灰名单。

当入侵者 W 靠近决策节点 A 后，A 断定入侵者已经进入了本簇，因此将 W 从灰名单中转入黑名单，并发送一跳黑名单广播给簇的其他节点。之后，W 又靠近了 E，但由于 E 已经收到了簇头的黑名单广播，并且没有非本簇的邻居节点，所以仅仅接收黑名单。由于簇内的 C、B 节点已经于发送预警信号的同时，发送过一跳的灰名单广播，因此仅仅将入侵者 W 插入自己的黑名单中。而 D、E 节点则在将入侵者插入自己的黑名单后，发送一跳的灰名单广播告诉周围的其他簇邻居，如图 3-15 所示。

从图 3-16 中可以看到，整个簇内的所有节点因此都将 W 加入了各自的黑名单，同时相邻簇边界上的 I 和 H 在分别收到来自异簇的 A 和 D 广播，将 W 加入各自的灰名单中。这时入侵者 W 已经到达簇 1 的内部，但是在它发起攻击之前，显然在其周围的节点已经都将其列入了各自的黑名单中，并且在更外一层的节点都已经将其列入了各自的灰名单中，从而使 W 被一道“防火墙”所隔离。

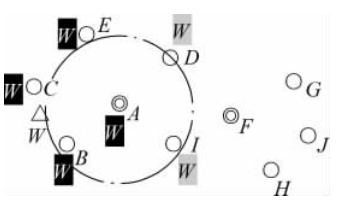

图 3-15　决策节点 A 广播黑名单

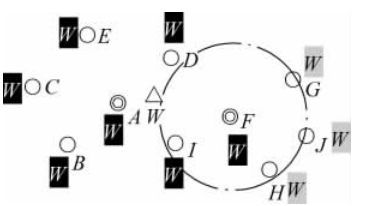

图 3-16　A 广播黑名单后

从图 3-17 中可以看到，入侵者 W 由于攻击未果，试图往网络中的其他方向寻求入侵，它向簇 2 方向移动，当它相对于节点 H 和 I 的信号强度大于阈值时，节点 H 和 I 分别向决策节点 F 发出预警信号并发出一跳灰名单广播给邻节点。决策节点 F 在收到了簇内两个节点的预警信号后，判定入侵者 W 已经进入本簇，因此广播黑名单。此时，如果 W 向 I 和 H 发动攻击，由于它们的灰名单中都记录有 M 节点，因此会进行阻击，使得 M 的攻击不会对网络造成影响。

从图 3-18 中可以看到，整个簇 2 的所有节点因此都将 W 列入了自己的黑名单中。当入侵者 W 进入到簇 2 的内部时，它又已经被包围在一堵新的“防火墙”中了。也正是由于防火墙的形成伴随着入侵者的移动，我们称其为移动防火墙。当入侵者在簇 2 内停留一段时间后，由于簇 1 内的节点相对于它的信号强度已经小于阈值，并且持续了一定时间，因此簇 1 内的节点将自动解除阻击，节约能量。

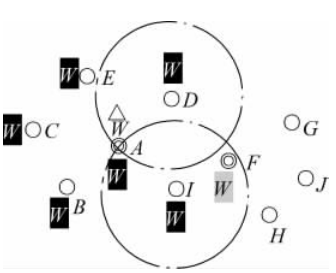

图 3-17　W 接近节点 I、H

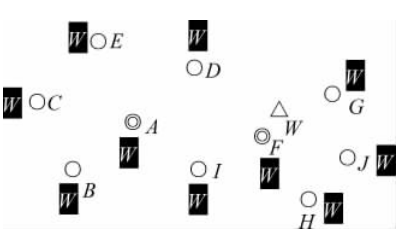

图 3-18　F 广播黑名单后

下面再给出对于整个网络中移动防火墙的机制示意图(见图 3-19～图 3-21)。

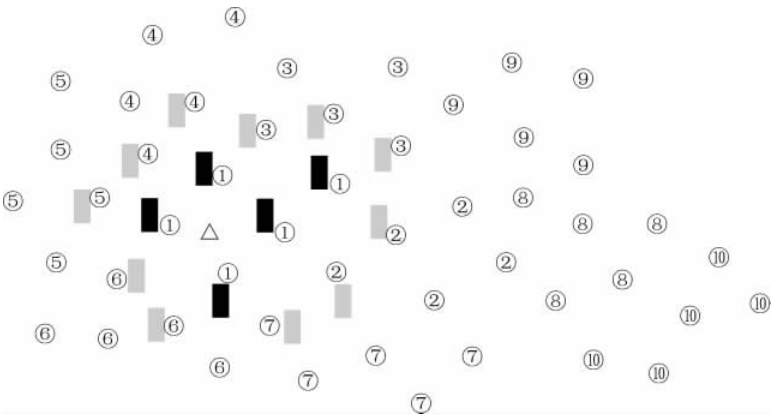

图 3-19 攻击节点在簇 1 内

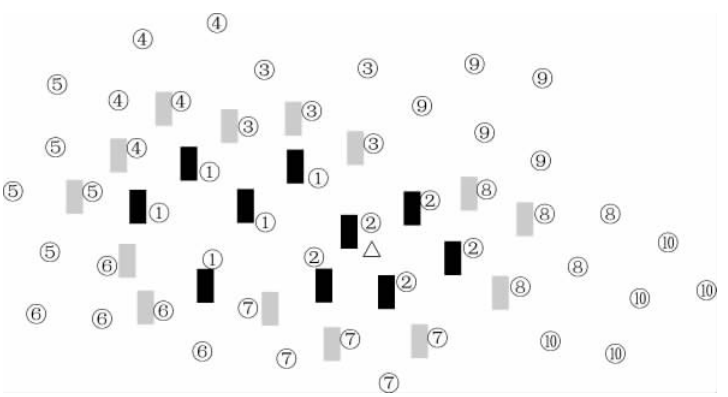

图 3-20 攻击节点进入簇 2

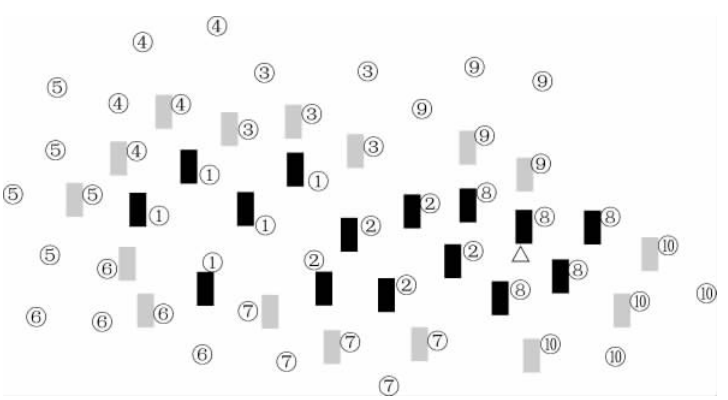

图 3-21 攻击节点进入簇 8

移动防火墙是随着入侵者的移动而遍及网络的,大大减少了由于入侵者未到达某一区域而泛洪已经将黑名单发送给那个区域的节点,从而造成的不必要的开销浪费。

在任何时候,入侵者周围的所有节点都在各自的黑名单中记录有该入侵者,并且在它们更外一层的所有节点都在各自的灰名单中记录有该入侵者。

通过信号强度的大小来判断是否要阻击入侵者，使得入侵者在被发现后，在任何时候都无法成功地攻击网络。

参 考 文 献

[1] Yih-Chun, Hu Perrig A. A Survey of Secure Wireless Ad Hoc Routing[J]. IEEE Security & Privacy Magazine, 2004, 2(3): 28-39.

[2] Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capku. The Quest for Security in Mobile Ad Hoc Networks[C]//Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking & Computing 2001. Long Beach, CA, USA, 2001.

[3] Zhou L, Haas Z J. Securing Ad Hoc Networks[J]. Ad Hoc Networks, 1999, 13(6): 24-30.

[4] David B Johnson, David A Maltz, Yih-Chun Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks(DSR)[EB/OL]. [2017-01-01]. http://www.cs.cmu.edu/~dmaltz/dsr.html.

[5] Perkins C, Belding-Royer E, Das S. Ad Hoc On-Demand Distance Vector(AODV)Routing[EB/OL]. [2017-01-01]. http://www.nexoncn.com/read/885ad08385f111f1378a3403.html.

[6] Hu Y, Perrig A, Johnson D B, et al. Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks[C]//Proceedings of the 8th Annual International Conference on Mobile Computing and Networking. Atlanta, Georgia, USA, 2002.

[7] Hu Y, Perrig A, Johnson D B, et al. Wormhole Attacks in Wireless Networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 370-380.

[8] Mölsä, J V. Increasing the DoS Attack Resiliency in Military Ad Hoc Networks[C]//Military Communications Conference. Atlantic City, 2005.

[9] Yi Ping, Jiang Yi Chuan, Zhang Shiyong, et al. A Survey of Security for Mobile Ad Hoc Networks [J]. ACTA Electronica Sinica, 2005, 33(5): 893-899.

[10] Mirkovic J, Reiher P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(2): 39-53.

[11] Vikram Gupta. Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks[C]// Proceedings of MILCOM. Anaheim, 2002: 1118-1123.

[12] Aad I, Hubaux J P, Knightly E. Denial of Service Resilience in Ad Hoc Networks[C]//Proceedings of the 10th Annual International Conference on Mobile Computing and Networking(MobiCom2004). Philadelphia, USA, 2004.

[13] Young-Bae Ko, Nitin Vaidya. Location-Aided Routing(LAR) in Mobile Ad Hoc Networks[C]// Proceedings of the Fourth International Conference on Mobile Computing and Networking (MobiCom'98). Dallas, Texas, USA, 1998.

[14] Papadimitratos P, Haas Z. Secure Routing for Mobile Ad Hoc Networks[C]//Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference. San Antonio, TX, 2002.

[15] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, et al. A Secure Routing Protocol for Ad Hoc Networks[C]//Proc of 2002 IEEE International Conference on Network Protocols(ICNP). Paris, France, 2002: 78-89.

[16] Manel Guerrero Zapata. Secure Ad Hoc On-Demand Distance Vector Routing[J]. ACM Mobile Computing and Communications Review(MC2R). 2002, 6(3): 106-107.