基于 OPNET 的分布式协议攻击的性能研究

张俊清，董阳泽，张刚强，刘俊凯
(水声对抗技术重点实验室，上海 201108)

摘要：目前，对水声网络协议干扰和攻击的研究大多采用单个节点的攻击方法。在此基础上，为提升攻击性能，研究了分布式协议攻击方法。通过 OPNET 仿真软件构建水声网络模型，采用不同的协议攻击方法对目标水声网络进行攻击仿真研究，包括单节点工作方式和多节点的分布式协议攻击。比较了不同的工作方式达到的干扰效果以及不同协议攻击方法的分布式攻击工作方式的干扰效果。结果表明，采用分布式协议攻击工作方式，在其他条件相同的情况下，目标网络吞吐量比单节点攻击工作方式多下降了 5%以上，对水声网络的干扰效果更佳。

关键词：水声网络；网络协议攻击；分布式协议攻击
中图分类号：TB567 **文献标识码**：A **文章编号**：1000-3630(2019)-01-0039-07
DOI 编码：10.16300/j.cnki.1000-3630.2019.01.006

Performance of OPNET based distributed protocol attack

ZHANG Jun-qing, DONG Yang-ze, ZHANG Gang-qiang, LIU Jun-kai
(*National Key Laboratory of Science and Technology on Underwater Acoustic Antagonizing*, *Shanghai*, 201108, *China*)

Abstract: At present, the research on the interference and attack of underwater acoustic network protocols is mostly based on the attack method of single node. Distributed protocol attack methods are studied in this paper. The underwater acoustic network model is constructed by OPNET simulation software, and different protocol attack methods are used against the target underwater acoustic network. The interference effects of single-node mode and multi-node distributed protocol attack mode are studied via simulation, The interference effects of different working modes and the interference effects of distributed attack of different protocols attack methods are compared. The simulation shows that under the same conditions, The distributed protocol attack mode can reduce target network throughput by about 5%, and the interference effect on underwater acoustic network is better.

Key words: underwater acoustic network; attack against network protocol; distributed protocol attack

0 引 言

随着水声网络的发展和广泛运用，在海洋军事和民用领域发挥着越来越重要的作用。将水声网

引入水声对抗领域，是“网络中心战”在水下战场空间的必然趋势。因此，水声网络对抗作为水声对抗中的重要内容，是引发敌我双方围绕水声网络展开一系列的攻防行动[1]。

目前，对水声网络攻击的研究中，大多都是通过单一干扰节点来破坏网络软件和硬件，达到降低网络性能，或者获取敌方网络的数据信息的效能。对单个干扰节点进行干扰，由于干扰范围有限，能量相对集中，通常使用大功率进行干扰，干扰节点被发现的可能性较大。如果充分利用协议有关信息，采用分布式协议攻击的工作方式，干扰节点之间相互配合，通过多跳干扰或者干扰节点之间协同，可以提高水声网络的干扰效果。由于消耗能量较低，因此被发现的概率也较低。

在过去的 20 年间，已有针对水声网络协议攻击方法的研究。文献[2]、[3]从理论上介绍了水声网络各层面临的各种威胁以及各种攻击方法的原理，但没有给出具体的仿真结果；文献[4]研究了基于位置的路由协议基于深度路由(Depth Based Routing, DBR)和基于矢量转发协议(Vector-Based Forwarding Protocol, VBF)路由协议的攻击可行性；文献[5]研究了水声网络拒绝服务攻击，针对水声网络路由层协议攻击进行了仿真研究；文献[6]、[7]对水声通信网媒质接入控制(Medium Access Control, MAC)层协议攻击进行了可行性分析和性能仿真分析，主要针对单节点工作方式。

利用 OPNET 软件，本文首先建立目标水声网络模型，研究采用分布式协议攻击对水声网络进行攻击的方式方法；然后通过仿真，分析不同的工作方式的干扰效果；最后就不同协议攻击方法的分布式工作方式的干扰效果进行了比较和讨论。

收稿日期：2017-12-10; **修回日期**：2018-01-18
作者简介：张俊清(1991－)，男，湖北襄阳人，硕士研究生，研究方向为通信与超声技术。
通讯作者：张俊清，E-mail: zhangjunqing726@163.com

1 水声网络协议攻击

这里首先介绍几种常见的水声网络协议攻击的方法。

(1) 蠕虫洞攻击是通过攻击节点在源节点和目的节点之间建立一条虚假路径，当源节点发送数据时，通过虚假路由，攻击节点接收的到数据包可以选择是否发送给攻击者。蠕虫洞攻击原理如图 1 所示。

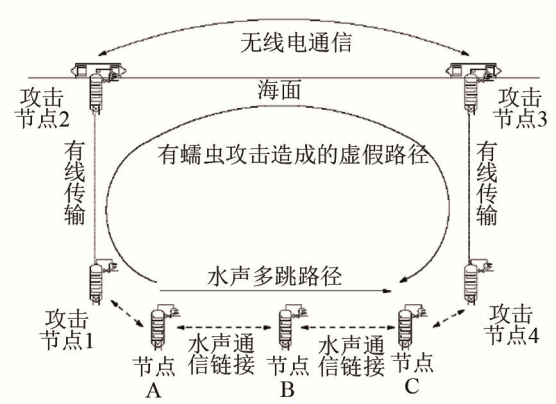

图 1 水声网络的虫洞攻击示意图
Fig.1 Schematic diagram of the wormhole attack in underwater acoustic network

图 1 中，节点 A 向 C 发送信息时，A 发送路由请求包，建立路径 A-B-C，向节点 C 传输数据信息。蠕虫洞攻击时，节点 A 发送路由请求包时，被攻击节点 1 收到，然后将其发送给攻击节点 4，攻击节点 4 重发节点 A 的路由请求包，节点 C 接收 A 的路由请求包，通过此路径，A 将会收到 C 的路由回复信息，A 会建立路径 A-C，A 就会通过此路径发送数据信息给 C，攻击节点在接收到数据信息后可自行确定是否发送给攻击者。

(2) 黑洞攻击是攻击者发送伪装的路由信息，声明自己有到网关节点最近的路由节点。这样网络中其他节点就会把攻击节点误认为最优的路由节点，从而会优先选择攻击节点作为路由节点，攻击节点像黑洞一样吸引数据包流向自己。黑洞攻击原理如图 2 所示。

图 2 中，攻击节点发送伪造的路由信息给周围的普通节点，告诉周围的普通节点自己是离网关节点最近的，攻击节点周围的普通节点将会建立一条经过攻击节点的路径，当它们发送数据时，都会经过攻击节点。

(3) 请求发送/清除发送(Request to Send/Clear to Send, RTS/CTS)握手协议攻击是攻击者占用信道不断发送伪造的 RTS 帧，使周围正常节点很难使用信道进行正常通信。RTS/CTS 握手协议的攻击原理如图 3 所示。

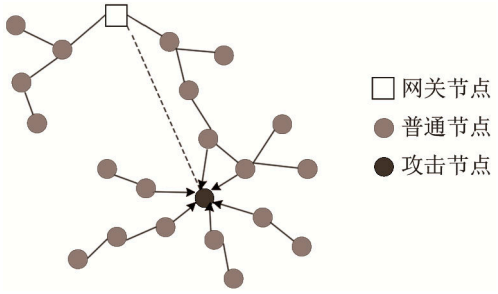

图 2 水声网络的黑洞攻击示意图
Fig.2 Schematic diagram of the blackhole attack in underwater acoustic network

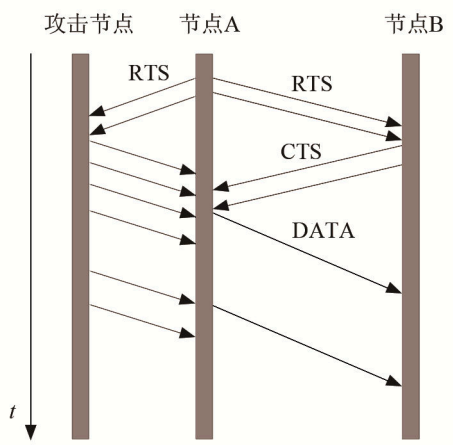

图 3 水声网络 MAC 层握手协议攻击原理图
Fig.3 The principle of MAC protocol attack in underwater acoustic network

图 3 中，当节点 A 要给节点 B 发送数据时，攻击节点不断发送伪造的 RTS，节点 A 收到攻击节点的 RTS 时，将会执行随机退避，等待信道空闲时方可发送数据。若攻击节点一直占有信道，节点 A 将会一直不能传输数据。

(4) RTS 占用目的节点攻击的原理是当源节点给目的节点发送 RTS 时，攻击节点抢在正常节点握手之前和目的节点进行通信，从而使正常节点不能正常通信。RTS 占用目的节点攻击原理如图 4 所示。

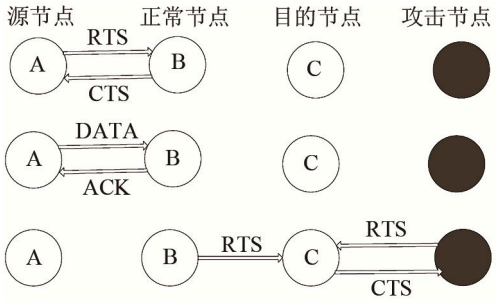

图 4 RTS 占用目的节点方法的干扰示意图
Fig.4 The interference diagram of the RTS method occupying destination node

图 4 中，源节点 A 向目的节点 C 发送数据，A 先发送给中继节点 B，B 再发送给目的节点 C。攻击节点在 B 发送给目的节点 C 之前，一直给 C 发送 RTS 控制帧进行通信，使 B 不能和 C 进行通信。

(5) 分布式攻击根据多个攻击节点是否协同工作分为两种情况：

① 多个攻击节点独自工作

这种情况下，每个攻击节点独立工作。若干个攻击节点均匀散布在网络节点的活动区域内，每个攻击节点负责一个区域，多个节点实施干扰，实现对网络内主要节点的干扰破坏。

② 多个攻击节点协同干扰

在一个网络内布设多个攻击节点，这些节点之间利用单独的隐蔽信道交换必要的信息，实现多个攻击节点协同攻击。

2　目标水声网络建模

本文采用 OPNET Modeler[8]建立目标水声网络仿真模型。针对水声信道的特点，在 OPNET 中对水声网络物理层、数据链路层(主要是其中的 MAC 层)和路由层进行相应的建模。水声网络体系结构如图 5 所示。

图 5　水声网络体系结构

Fig.5　Underwater acoustic network architecture

通过设置 OPNET 的管道模型，实现水声信道的物理层建模，MAC 层采用载波侦听多址接入/冲突避免(Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA)[9]的握手机制，路由层采用基于距离矢量的按需路由协议(Ad-hoc On-De- mand Distance Vector, AODV)[10]建模。

2.1　网络模型

图 6 为本文建立的目标水声网络 OPNET 模型。图 6 中包含 9 个网络节点，随机分布在 4 km× 4 km 的范围内。

2.2　节点建模

网络节点模型如图 7 所示。图 7 中，源端模块随机产生数据包，终端模块接收处理数据包，其中的水听器无指向性；网络层主要负责路由生成和数据转发，采用 AODV 协议，包括路由发现和路由维护两个部分：当一个节点需要向另一个节点发送数据，而当路由表中没有那个节点的路由时，它会试图发现一个新的路由。路由发现使用路由请求消息(RREQ)完成，RREQ 消息在网络中广播，直到包含有目的节点的新鲜路由节点或者目的节点自己对路由请求消息做出回应，并发送路由应答消息(RREP)。该 RREP 消息回传给源节点，并在消息回传的过程中，建立源节点和目的节点端到端的路径。路由发现负责寻找到达目的节点的路径；路由维护负责对已经建立的路由有效性进行检测，并且在发现路由由于节点移动等原因失效时重建路由。

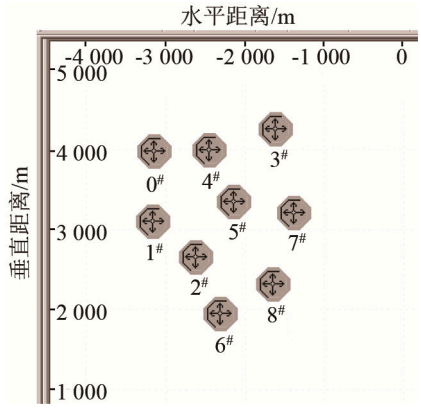

图 6　目标水声网络拓扑结构

Fig.6　Target underwater acoustic network topology

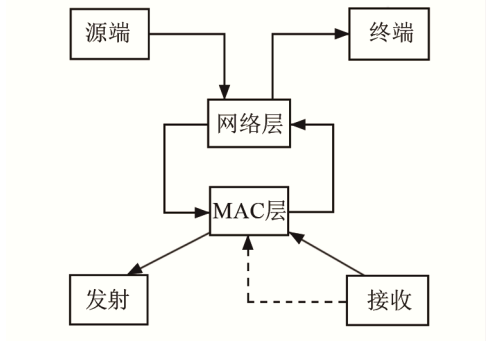

图 7　节点模型

Fig.7　Node model

进程模型如图 8 所示。MAC 层采用 CSMA/CA 协议，其进程转移如图 9 所示。

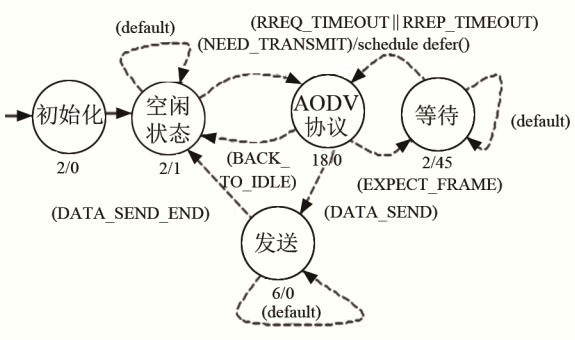

图 8　网络状态转移图

Fig.8　Network state transition diagram

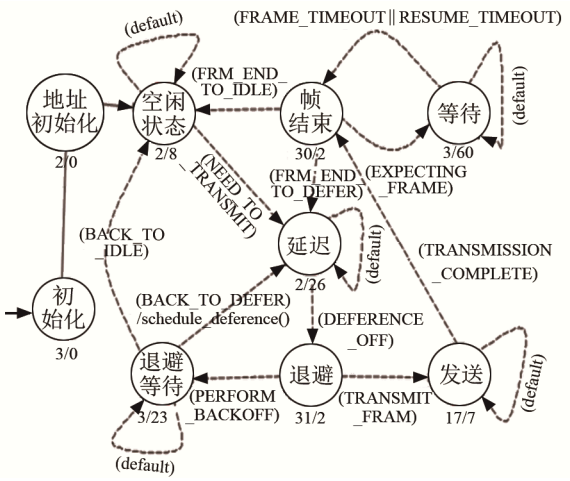

图 9 MAC 进程模型

Fig.9 MAC process model

3 仿真及结果分析

3.1 仿真参数设置

OPNET 包括 14 个管道阶段[11]，模拟数据帧在信道中传输，这些管道模型主要针对空中无线信道。水声网络仿真中，水声信道需要重新定义管道参数。本文采用文献[12]的方法，在传播时延、接收功率、背景噪声三个管道阶段分别建立了水声信道声速、传播损失和海洋环境背景噪声模型，参数设置如表 1 所示。

表 1 水声网络仿真参数设置

Table 1 Simulation parameters for underwater acoustic network

管道参数	参数设置
调制方式	BPSK
信道带宽/ kHz	10
数据传输速率/(bit·s^{-1})	1 024
水声信号传播速率/(m·s^{-1})	1 500
传输最大距离/m	1 000
海水吸收系数(α)	$\frac{0.11f^2}{1+f^2}+\frac{44f^2}{4100+f^2}+3.02\times10^{-4}f^2$
传播损耗(TL)	$15\lg(R)+\alpha R-45$
数据包长度/bit	512
数据包时间间隔	uniform(30,90)
竞争窗的最小值	5
竞争窗的最大值	20
分布式帧间间隙(DIFS)	1.08 s
短帧帧间间隔(SIFS)	0.01 s
时隙(Slot)	1.08 s
最大缓冲区大小/bit	256 000
最大重传数	5
ACK 帧大小/bit	80
RTS 帧大小/bit	80
CTS 帧大小/bit	80
DATA 帧头大小/bit	80
错误率	0.000 01
RREQ 大小/bit	80
RREP 大小/bit	80
目的节点地址	(a)
MAC 地址	(b)

注：f 为声波频率(单位：kHz)，R 为收发端距离(单位：km)。

3.2 仿真及分析

3.2.1 目标网络性能

本文选取成功接收包数目、网络吞吐量和端到端平均时延等参数反映网络性能。

成功接收包数目是指源节点发送数据给目的节点，目的节点成功接收的包。

平均吞吐量(Throughput)是指单位时间内被成功接收的数据包数量(单位：bps)：

$$T_{TH}=(N\times p_{\text{size}})/T_{\text{s}} \tag{1}$$

其中：N 表示成功接收包数量，p_{size} 表示数据包大小，T_{s} 表示仿真时间。

端到端平均时延为发送节点产生数据包，到目的节点成功接收到数据包所需要的平均时间。

图 10 为目标网络(无攻击)成功接收数据包数量随时间的变化。图 10 中，每个节点都是随机产生数据包，数据包的目的地址也是随机产生的。当两个或者以上数据包同时到达同一个中继节点或者目的节点时，数据包将会发送碰撞，中继节点或者目的节点接收不到数据包，数据包将会重传 5 次；重传次数超过 5，数据包将会被丢弃。由于数据包的碰撞，使得丢包率为 7.29%(仿真时间内发送了 2 400 个数据包，到达目的节点的数据包为 2 225 个)。

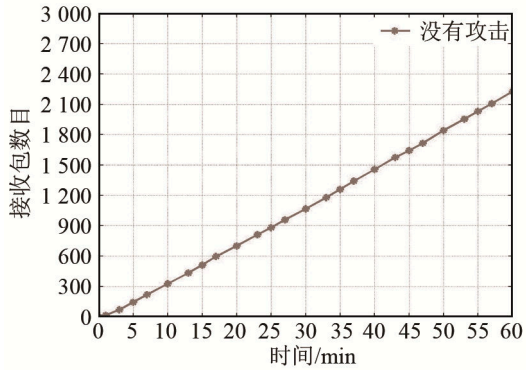

图 10 无攻击节点成功接收数据包数随仿真时间的变化

Fig.10 Variation of the number of successful packets received by no-attack nodes with simulation time

图 11 为网络吞吐量随时间的变化。由图 11 可见，达到稳定状态时，网络吞吐量约为 31.563 bps。

图 12 为网络端到端平均时延随时间的变化。图 12 中，由于节点之间相距有一定距离，传播需要一定时间，并且节点接收数据包还有处理时延存

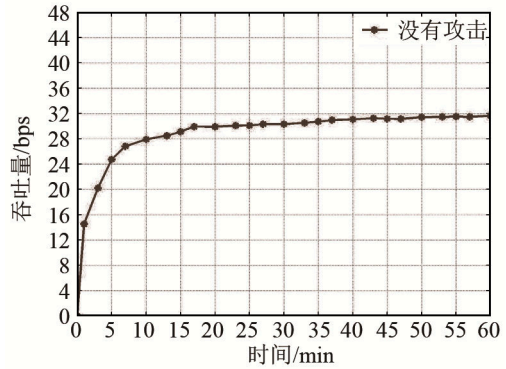

图 11　无攻击节点网络吞吐量随仿真时间变化
Fig.11　Variation of the throughput of the no-attack node network with simulation time

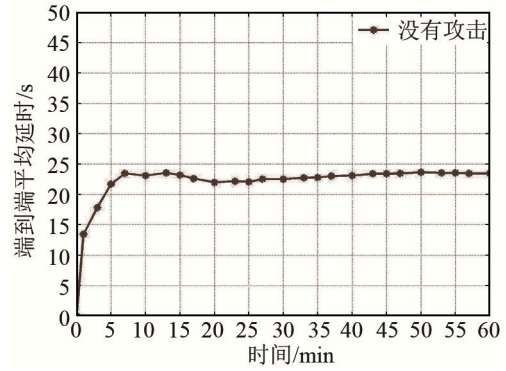

图 12　无攻击节点网络端对端时延随仿真时间的变化
Fig.12　Variation of the end-to-end delay of the no-attack node network with simulation time

在，稳定状态下，网络的端对端平均时延约为 24 s。

3.2.2　蠕虫洞攻击仿真

图 13 是针对网络层路由协议的蠕虫洞攻击，采用单节点工作方式和分布式攻击方式，网络的吞吐量随时间的变化情况的比较。

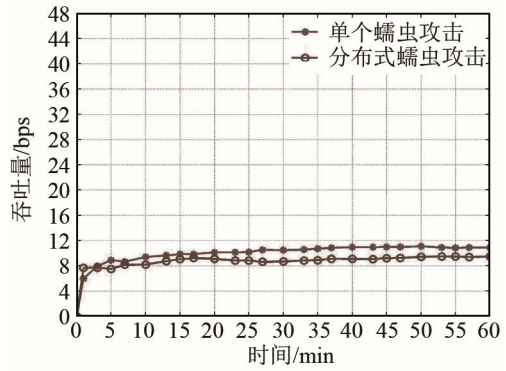

图 13　蠕虫洞攻击吞吐量随仿真时间的变化曲线
Fig.13　Variation of the network throughput under wormhole attack with simulation time

由图 13 可见，单节点工作方式和分布式工作方式，使网络吞吐量分别下降了 65.5%和 70.5%，分布式协议攻击对网络的干扰效果优于单节点协议攻击。

图 14 是针对网络层路由协议的蠕虫洞攻击，采用单节点工作方式和分布式攻击方式，统计网络端对端平均时延变化情况的比较。

从图 14 可知，单节点工作方式使网络端对端时延更大，这是由于单节点工作方式中，每一对蠕虫对在检测到网络有信息时，都会转发网络中路由请求包，这使网络链路更加堵塞。而分布式攻击工作方式，蠕虫节点对之间可以相互通信，避免攻击节点之间重复发网络路由请求包，网络延时减小。

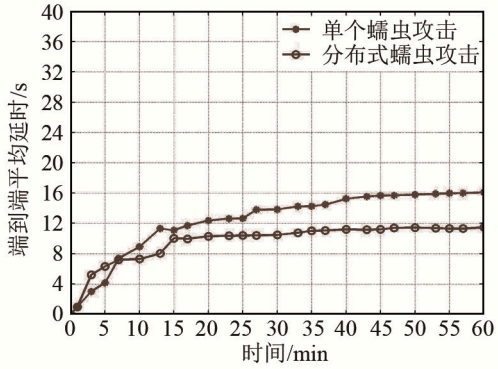

图 14　蠕虫洞攻击端对端到平均延时随仿真时间的变化曲线
Fig.14　Variation of the end-to-end delay of the network under wormhole attack with simulation time

3.2.3　黑洞攻击仿真

图 15 是针对网络层路由协议的黑洞攻击，在不同工作方式下的吞吐量随时间的变化情况。

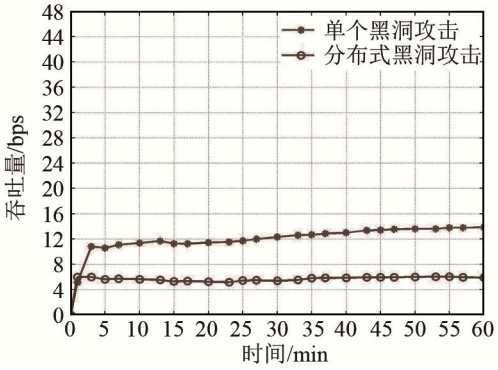

图 15　黑洞攻击吞吐量随仿真时间的变化曲线
Fig.15　Variation of the network throughput under blackhole attack with simulation time

从图 15 可知，分布式攻击方式使网络吞吐量下降了 81.37%，单节点工作方式使网络吞吐量下降了 56.2%，分布式协议攻击干扰效果更优。

图 16 是针对网络层路由协议的黑洞攻击，在不同工作方式下的网络端对端平均时延情况。

由图 16 可知，单个黑洞攻击和分布式黑洞攻击对网络端对端平均延时的效果相同。

总的来说，分布式黑洞攻击的攻击效果优于单节点工作方式的攻击效果。

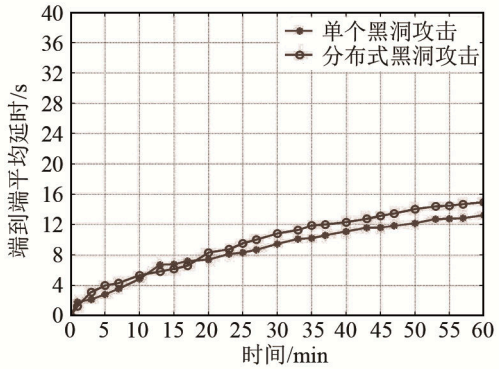

图 16 黑洞攻击端对端到平均延时随仿真时间的变化曲线
Fig.16 Variation of the end-end delay of the network under blackhole attack with simulation time

3.2.4 RTS/CTS 握手协议攻击

图 17 是针对 MAC 协议的 RTS/CTS 握手协议攻击，采用单节点工作方式和分布式工作方式仿真，网络吞吐量随时间的变化情况。

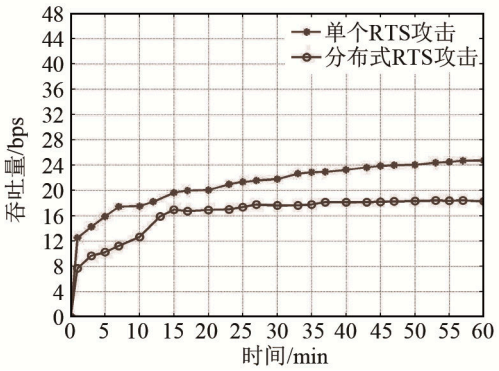

图 17 RTS/CTS 攻击吞吐量随仿真时间的变化曲线
Fig.17 Variation of the network throughput under RTS/CTS attack with simulation time

从图 17 可知，分布式 RTS/CTS 握手协议攻击网络吞吐量约为 18.354 bps，下降了 41.99%；单节点攻击方式使网络吞吐量下降到 24.702 bps，下降了 23.09%。分布式 RTS/CTS 握手协议攻击网络吞吐量更低。

图 18 是针对 MAC 协议的 RTS/CTS 握手协议攻击，采用单节点工作方式和分布式工作方式仿真，网络端到端平均时延随时间的变化情况。

由图 18 可见，分布式 RTS/CTS 握手协议攻击网络端到端平均时延达到 361 s，单节点攻击方式使网络端到端时延达到 165 s，分布式网络攻击方式网络端到端延时更大，攻击效果更好。

3.2.5 RTS 占用目的节点攻击

图 19 是 RTS 占用目的节点攻击，在不同工作方式下，网络吞吐量随时间的变化情况。

由图 19 可知，分布式 RTS 占用目的节点攻击网络吞吐量约为 20.537 bps，下降了 35.01%；单节点攻击方式使网络吞吐量下降到 28.018 bps，下降了 11.39%。分布式 RTS 占用目的节点攻击的网络吞吐量更低，攻击效果更好。

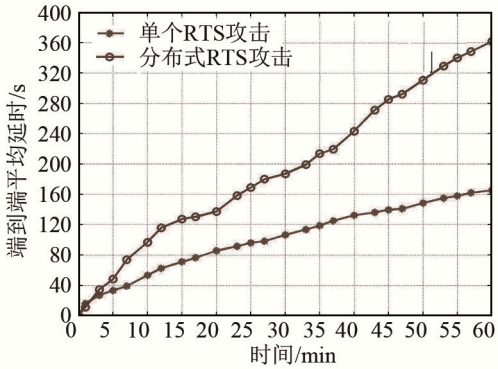

图 18 RTS/CTS 攻击端对端到平均延时随仿真时间的变化曲线
Fig.18 Variation of the end-end delay of the network under RTS/CTS attack with simulation time

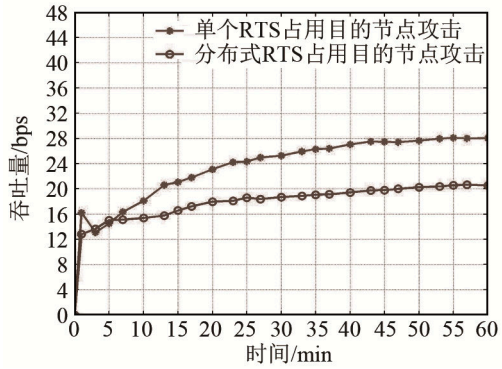

图 19 RTS 占用目的节点攻击吞吐量随仿真时间变化曲线
Fig.19 Variation of the network throughput under the attack of RTS occupying destination node with simulation time

图 20 是 RTS 占用目的节点攻击，在不同工作方式下，端对端平均时延随时间变化情况的对比。

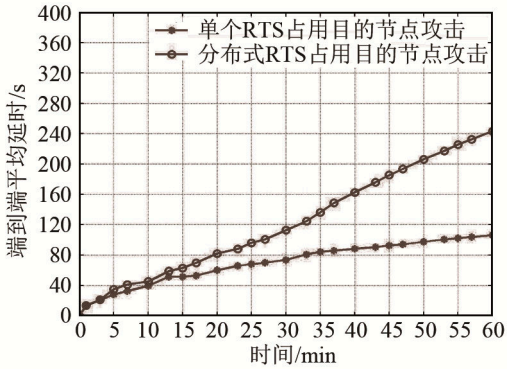

图 20 RTS 占用目的节点攻击端对端到平均延时随仿真时间变化曲线
Fig.20 Variation of the end-end delay of the network under the attack of RTS occupying destination node with simulation time

由图 20 可知，分布式 RTS 占用目的节点攻击网络端到端平均时延达到约 243 s；单节点攻击方式使网络端到端时延达到 106 s。分布式 RTS 占用目

的节点攻击网络端到端延时更大，攻击效果更好。

3.3 仿真比较

表 2、3 分别给出了单节点攻击与分布式攻击效果的仿真比较。

表 2　单节点协议攻击方法干扰效果
Table 2　The interference effect of single node attack

单节点协议攻击方法	网络吞吐量下降率/%	端对端平均时延/s
蠕虫洞攻击	65.50	16.0
黑洞攻击	56.20	13.2
RTS/CTS 握手协议攻击	23.09	165.0
RTS 占用目的节点攻击	11.39	106.0

表 3　分布式协议攻击方法干扰效果
Table 3　The interference effect of distributed protocol attack

分布式协议攻击方法	网络吞吐量下降率/%	端对端平均时延/s
蠕虫洞攻击	70.50	12.0
黑洞攻击	81.37	14.9
RTS/CTS 握手协议攻击	41.99	361.0
RTS 占用目的节点攻击	35.01	243.0

需要说明的是，分布式蠕虫攻击端到端时延减小，但对于网络攻击效果来说，首先看整个网络的信息量损失率即网络吞吐量的下降率，如果网络信息损失率很高，那么网络延时变小对网络攻击效果几乎没有影响；如果干扰前后网络信息几乎没有损失，网络延时越大越好。总的来说，分布式协议攻击对网络干扰效果优于单节点协议攻击。

4　结 论

通过 OPNET 仿真了网络层蠕虫洞攻击和黑洞攻击，以及 MAC 层的 RTS/CTS 握手协议攻击和 RTS 占用目的节点攻击，分析比较了单节点攻击方式和分布式攻击方式。

研究表明，分布式协议攻击方法可以提高网络的干扰性能，使网络吞吐量大大降低，部分方法可以提高端对端时延。在相同条件下，对于网络层协议攻击，分布式黑洞攻击对网络的干扰效果优于分布式蠕虫攻击；在相同条件下，对于 MAC 层协议攻击，分布式 RTS/CTS 握手协议攻击对网络的干扰效果比分布式 RTS 占用目的节点攻击效果更好。

水声网络协议攻击作为水声对抗的一个新的组成部分，在未来国家海洋安全方面有重要意义。通过对水声网络分布式协议攻击的仿真研究，为实际水声网络对抗提供了一些理论参考，表明了该攻击方法有较好的对网络的干扰效果。由于目前国内对水声网络协议对抗的研究仍主要处在实验室研究阶段，还缺乏试验验证。希望本文研究对该领域的发展起到一定的参考作用。

参　考　文　献

[1] DONG Y Z, LIU P X Underwater networked acoustic warfare-concepts and key technologies[C]//Proceedings of 9th Western Pacific Acoustic Conference, Korea, 2006: 22-28.

[2] DOMINGO M C. Securing underwater wireless communication network[J]. IEEE Wireless Communication IEEE, 2012, **18**(1): 22-28.

[3] CONG Y P, YANG G, WEI Z Q, et al. Secuity in underwater sensor network[J]. IEEE Communication system security, 2010, **1**(1): 162-168.

[4] ZUBA M, FAGAN M, CUI J H, et al. A vulnerability study of geographic routing in underwater acoustic networks[C]//IEEE Conference on Communications and Network Security (CNS) 2013: 109-117.

[5] DONG Y Z, DONG H F, ZHANG G Q. Study on denial of service against underwater acoustic networks[J]. Journal of Communications, 2014, **2**(4): 135-143.

[6] KONG J J, JI Z R, WANG W C, et al. Low-cost attacks against packet delivery, localization and time synchronization services in underwater sensor networks[J]. ACM Workshop on Wireless Security, 2005, **23**(3): 87-96.

[7] 张刚强，张俊清，刘俊凯. 水声网络 MAC 层协议攻击仿真[C]//中国声学学会水声学分会全国水声学术会议, 2016.
ZHANG Gangqiang, ZHANG Junqing, LIU Junkai. Simulation study on underwater acoustic network MAC layer protocol attacking[C]//Proceedings of Conference on Underwater Acoustics of CAS, 2016.

[8] 陈敏. OPNET 网络仿真[M]. 北京: 清华大学出版社, 2004.
CHEN Min. OPNET Network Simulation[M]. Beijing: Tsinghua University Press, 2004.

[9] 赵瑞琴，申晓红，姜喆. 水声信息网络基础[M]. 西安: 西北工业大学出版社, 2017.
ZHAO Ruiqin, SHEN Xiaohong, JIANG Zhe. Underwater Information Network Foundation[M]. Xi'an: Northwestern Polytechnical University Press, 2017.

[10] 吴松伟. 水声自组网节能路由协议研究[D]. 哈尔滨: 哈尔滨工程大学, 2010.
WU Songwei. Research on energy saving in routing protocol of autonomous underwater acoustic network[D]. Harbin: Harbin Engineering University, 2010.

[11] 张铭，窦赫雷，常春藤. OPNET Modeler 与网络仿真[M]. 北京: 人民邮电出版社, 2007.
ZHANG Ming, DOU Helei, CHANG Chunteng. OPNET Modeler and network simulation[M]. Beijing: The People's Posts and Telecom Press, 2007.

[12] XU X N，CHENG E，LIN W．Research on MAC protocol for underwater acoustic network based on OPNET[C]//Proceedings of Computer and Modernization Conference, 2013: 181- 184.