Proceedings of the 2017 IEEE
International Conference on Information and Automation (ICIA)
Macau SAR, China, July 2017

Simulation and Performance Analysis of Distributed Attack against MAC Layer of Underwater Acoustic Network Based on OPNET

Junqing ZHANG, Yangze DONG
National Key Laboratory of science and Technology on
Underwater Acoustic Antagonizing
Shanghai201108, China
zhangjunqing726@163.com

***Abstract* - The principle of attacking methods against the MAC layer of underwater acoustic network is first introduced briefly. Underwater acoustic channel characteristics are modeled corresponding Propagation Delay, Received Power and Background Noise by using OPNET pipeline stage. MAC Layer and Network Layer modules of network node are implemented. The results of a single node attack and two nodes distributed collaborative attack such as throughput and packet dropping ratio were collected via statistical analysis. The simulation results show that packet dropping ratio with the distributed Cooperative attacks of two nodes is higher and throughout is lower during simulation time. This may be a basis for further research on multi-node distributed collaborative attacks.**

Index Terms - underwater acoustic network; Distributed attacks on protocols; OPNET simulation.

I. INTRODUCTION

With the network-center warfare[1] proposed, the network was introduced in the underwater acoustic countermeasure, causing the adversary to attack and damage the software, hardware based on underwater acoustic network and underwater network communication. Therefore, the adversary and the two sides will launch a series of offensive and defensive operations around the underwater acoustic network. The underwater acoustic attack consists of underwater acoustic communication interference and network protocol attacks. MAC (Medium Access Control) is an essential component of the underwater acoustic network which determines the sharing efficiency of the wireless channel of the restricted channel. According to the literature[2], we can know that underwater acoustic network poses unique challenges due to the harsh underwater environment, such as limited bandwidth, high-noise, high and variable propagation delays, have high bit error rates and temporary losses of connectivity caused by multipath and fading phenomena. In order to reduce the data conflict and conceal the exposed terminal problem, the multi-node wireless underwater acoustic network uses the RTS/CTS (Request to Send/Clear to Send) mechanism.

In this paper, we study the attack of the MAC layer on the underwater acoustic network. The attacker selectively relocates or fakes the control information by detecting the channel signal. The results of a single node attack and two nodes distributed collaborative attack such as throughput and packet dropping ratio are collected by statistical analysis. The simulation results show that packet dropping ratio with the distributed Cooperative attacks of two nodes is higher and throughout is lower during simulation time.

The rest of this paper is organized as follows. In section II, we review related literature and some previous work. In section III, we describe the MAC Layer protocol attack principle. In section IV, we present the network model and related knowledgeable. In section V, we present the simulation results and simulation analyses. In section VI, we conclude by summarizing our contributions and identifying directions for future research.

II. RELATED WORK

A number of techniques for Denial of attack for terrestrial sensor networks have been addressed in several

978-1-5386-3154-6/17/$31.00 ©2017 IEEE

papers. However, to the best of the authors' knowledge, this work is the first to study the distributed Attack against MAC Layer of Underwater Acoustic Network. Many previous solutions and theoretical may not be feasible for the underwater environment.

In particular, in[3], the possible MAC blocking attacks are presented in wireless LAN and prove the feasibility of the attack method by throughput suddenly dropping. But there is no further study of multi-node attack effect and it is not directed against the underwater acoustic network. In[4],[5], a preliminary spoofing based attack model for underwater geographic routing protocols is proposed, using Depth-Based Routing(DBR) as a case study. Detailed simulation analysis on attack the performance using various network topologies and studied the performance of different spoofed depths is provided. Our work is aimed to distributed cooperative attacks of two nodes, using AODV (Ad hoc On-demand Distance Vector Routing) as a network layer case study. Thus, in the paper, we will focus on the distributed cooperative attacks of two nodes against MAC Layer of Underwater Acoustic Network.

III. MAC LAYER PROTOCOL ATTACK PRINCIPLE

A. *MAC layer working principle*

If the upper layer sends data, LLC Layer (Logical Link Control) will receive data in accordance with the rules, and perform media access to make sure the network whether can send data. When the network node sends data, MAC Layer will add some control information to this data and send to the physical layer in the specified frame format.

When destination node receives data, MAC layer will complete the following tasks:

1) Receiving data frames from physical layer.

2) Checking the control information of the received data frames to determine whether an error has occurred.

3) Sending data frames to LLC.

B. *RTS/CTS working principle*

When the sender wants to send data, the sender can subscribe to the channel by exchanging the control information. Firstly, the sender node checks the channel whether is idle. If the channel is busy, the node will implement the back-off algorithm until the channel is idle. If the channel is idle, the sender will send RTS frame including sender node address, receiver node address, and channel occupancy time and so on. Other nodes will be delayed for some time when they have received RTS frame (Time is included by RTS frame). When receiver receives the RTS frame and will respond CTS frame. If the sender node receives CTS, it will start sending data packets.

C. *RTS/CTS attack principle*

RTS attack: Attacker occupies channel and sends RTS frame continuously. The normal node will be loaded in accordance with RTS inside the time period to maintain a period of silence until the end of this data transmission. When attacking, the attack node to send RTS frames, surrounding normal nodes will be difficult to communicate using channels.

CTS attack: Attacker sends faked or spoofed CTS frame, and normal nodes that receive the CTS frame will consider the channel to communicate and stop the communication for a specified period of time. In order to avoid being detected, an attacker can send a CTS frame group in a period of time, so that an attacker can be hidden in the next attack period, as long as the attacker controls the sending time of CTS, the normal node will never be able to use the channel.

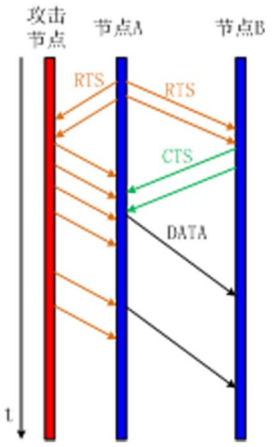

Figure.1 underwater acoustic network MAC layer handshake protocol attack principle

In the paper, we research that the attack node random forwarding some times when it receives the normal node RTS or CTS frame. The purpose is to destroy the normal handshake protocol between nodes, so that the nodes cannot establish a normal communication or communicate difficulties, as is shown in figure 1.

IV. SIMULATIONS