Study on Denial of Service against Underwater Acoustic Networks

Yangze Dong[1, 2], Hefeng Dong[1], and Gangqiang Zhang[2]
[1] Norwegian University of Science and Technology, Trondheim 7491, Norway
[2] Shanghai Marine Electronic Equipment Research Institute, Shanghai 201108, China
Email: {yangze.dong, hefeng.dong }@iet.ntnu.no; evuj@163.com

***Abstract*—**In ocean exploration and other maritime engineering, UAN (Underwater Acoustic Networks) is bound to play more important roles. Thinking of the serious environment UAN operates, safety and security must be guaranteed first. Among the possible attacks against UAN, DoS (Denial of Service) is a class of commonly-used methods. The basic procedures of different DoS attacks are analyzed and some of the DoS attacks against UAN are simulated to investigate their effects to lower the performances of UAN. Flooding, wormholes and selective forwarding attacks against UAN are studied via simulation. At last, some recommendations are given to improve the security performance of UAN based upon the results of simulations.

***Index Terms*—**underwater acoustic networks, security of UAN, DoS attacks, flooding, wormholes, selective forwarding

I. Introduction

With the development of underwater acoustic communications and network technologies (in other fields such as cable, territorial, radio, satellite networking), the past three decades have witnessed the rapid progresses of underwater acoustic networks (UAN) to meet the demands of ocean data collection and surveillance [1].

There have been many experimental and practical UANs nowadays. AOSN (Autonomous Ocean Sampling Network) is one of the earliest implement of UAN, which was developed in the US [2], [3]. From ALAN (Acoustic Local Area Networks), there have been quite a few UANs developed, such as DADS (Deployable Autonomous Distributed System), Seaweb for FRONT (Front-Resolving Observational Network with Telemetry), NeMON (New Millennium Observatory Network). In Europe, similar systems are also under investigations, e.g., Roblink (Long Range Shallow Water Robust Acoustic Communication Links) [4], LOTUS (LOng range Telemetry in Ultra-Shallow channels), SWAN (Shallow Water Acoustic Networks) [5], and ACME (Acoustic Communication Network for the Monitoring of the Underwater Environment) [6], [7], etc.

Manuscript received September 9, 2013; revised February 1, 2014.
This work was partly supported by the China Scholarship Council and partly sponsored within the project CAMOS by the Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology.
Corresponding author email: yangze.dong@iet.ntnu.no.
doi: 10.12720 /jcm.9.2.135-143

In most of the applications, UANs would not be used solely. There is a trend to join UAN into an integrated huge network, including territorial, radio and satellite networks. A cross-disciplinary project, the lighthouse project CAMOS (Coastal and Arctic Maritime Operations and Surveillance) Sensor Networks, has been developing here at NTNU. The primary objective is to develop a robust integrated communication framework that integrates underwater, terrestrial radio and satellite communications in a resilient infrastructure. In this way, a multitude of applications can be supported, specifically, within sensor networking in the Arctic region.

Lessons learnt from the Internet and other kinds of networks tell that there should not be an idealistic expectation of thinking that the networks would operate properly forever without any measures on security. In fact, the security threats' existence is a serious problem to be taken into account.

Among the possible threats, DoS is commonly used to degrade the performances of UAN. It is indispensable to find effective and efficiency countermeasures from recently researches on this area. Andrea Caiti put forward a kind of cooperative algorithm to continue group mission of vehicles after suffering DoS attacks. However, it was just an aftermath-dealing method, not contrasting against DoS [8]. Md. Ahasan Habib summarized some of the DoS attacks against UANs, and pointed out that most of the networking schemes did not take security into account [9]. Jiejun Kong presented a two-tier localization approach to identify wormholes of various lengths, as a basis of countermeasure against wormholes attacks to UANs [10].

To deal with the threats of security, especially to DoS attacks, the attack styles and methods should be known well firstly. In this paper, some results of our study on DoS attacks against UAN are presented, including the threats analysis and some simulations. The results could be used as basis of further work on counterworking against DoS attacks.

The rest of the paper is arranged as follows. Section II gives the demands of UAN after presenting the general security goals of networks, together with the characteristics of UAN, especially on security risks. In Section III, some of the attack methods against UAN are analyzed, focuses are on DoS attacks in routing layer; Section IV performs simulations of some DoS attacks

using OPNET to show the destructive effects on UAN. A brief summary of the simulation and recommendations to secure UAN are proposed in Section V. Finally, conclusions are drawn in Section VI.

II. Security Demands of UAN

A. General Security Goals of Networks

Efficient information exchange among nodes is the main task of a network. To achieve such objective, there are several general goals of a network corresponding to the considerations of security [11].

- **Availability:** This means that the network assets are available to authorized parties and should ensure the survivability of network services at any circumstances.
- **Data Confidentiality:** The network should confirm that communication information between nodes do not leak to other nodes.
- **Data Authentication:** To allow the receiver to verify that the data were really sent by the claimed sender.
- **Data Freshness:** This implies that the datasets are recent, and it ensures that no adversary replayed old messages.
- **Data Integrity:** To ensure the receiver that the received data are not altered in transit by an adversary.

B. Characteristics of UAN [12]

Compared with other kinds of networks, UAN has some unique characteristics because of the different operation environment.

TABLE I. Main Differences Between UAN, WSN and ASN

Items	UAN	WSN	ASN
Cost	Expensive	Cheap	Moderate
Energy	Consumable	Saving	May be from electric supply
Scale	Huge	Small	Moderate
Deployment Density	Sparse	Dense	Moderate
Node Mobility	Static and mobile	Generally static	Static and mobile
Node Robustness	Poor	Poor	Robust
Memory	Rather large	Very limited	Limited
Calculation Ability	Rather strong	Very limited	Limited
Applications	Environmental data collection, surveillance, etc.	Distributed sensing	Cooperation engagement
Environment Condition	Severe	Good	Good

In UAN, communications are the most frequent happening events, from the beginning handshaking to the exchanging of information. But the performance of underwater acoustic communications is limited by the distinct characteristics of sound channel, which lie in the following aspects: slow propagation speed, narrow bandwidth, frequency-selected attenuation, and severe multipath. These would result in low rate, near range, high bit error rate, large time delay, etc.

Besides the transmission media, there are still many other differences among UAN, WSN (Wireless Sensor Networks) and ASN (Ad hoc Sensor Networks).

Table I presents a simple comparison with a variety of parameters.

It can be seen from the table that UAN features are much distinguished from those of WSN and/or ASN, which would bring distinct problems on the security considerations.

C. Challenges of Secure UAN

Characteristics and application environments of UAN directly bring challenges for its security [12], [13]:

- **Challenge 1:** The UAN nodes have stronger storage and processing capabilities compared to WSN and ASN, however, the power supply of that is limited and consumable. Apart from the regular functions, extra operation would lead into a conflicting interest between minimizing resource consumption of UAN nodes and maximizing security performance.
- **Challenge 2:** The underwater acoustic communication characteristics within UAN render traditional wired-based security schemes and those for impractical. The large time delay, severe ISI (inter-symbol interferences), etc. limit complex measures to be taken.
- **Challenge 3:** Attacks to UAN can come from all directions and target at any nodes due to the networking topology. Large scale and sparse structure make the network easy to be attacked but difficult to defend.

D. Demands on Security of UAN

The aforementioned general goals of networks are also necessary to UAN.

Concerning the concrete constitution of UAN, the security of UAN lies in three levels [14]:

- **Node security:** If a node, which is the physical basis of UAN, is destroyed, such as the cluster heads or even the gateway, the network would not work any longer.
- **Communication security:** Communication is the "nerves" in UAN. If it cannot be assured, the network will degrade to an assembly of several individual devices.
- **Protocol security:** Without the arrangement of protocol, which is the control system of UAN, the operations would run into confusions.

The former two kinds of security considerations are the basic poles of secure network, while the latter one – protocol security is much more complex, which is mainly investigated in the consequence sections.

III. DoS Attacks Against UAN Protocols

A. Attacks Against UAN Protocols

To perform a complete destroy, one can aim at all of the network nodes; The second thought may be to lower the capacity of communication between network nodes. Besides, attacks to network protocols is another effective measure.

Protocols that all the network behaviors abide by are the nerves of UAN. Hence, if the protocols are broken, the network operations would go out of order.

The usually applied attacking measures to UAN include those to Data Link Layer (MAC layer) and Network Layer (Routing layer). But it should be known that each layer could suffer from outer or inner attacks.

B. DoS Attacks Against UAN

DoS attacks against UAN can be divided into two categories [14]:

- **Passive attacks:** Selfish nodes use the network but do not cooperate, saving battery life for their own communications: they do not intend to directly damage other nodes.
- **Active attacks:** Malicious nodes damage other nodes by causing network outage by partitioning while saving battery life is not a priority.

DoS attacks prevent the victim nodes from being able to use all or part of their network connection. DoS attacks may extend to all layers of the protocol stack [15].

- **Physical Layer:** DoS attacks can be launched against physical layer by using communication jamming device or by source of strong noise to interfere the physical channels and may compromise the service availability.
- **MAC Layer:** In the MAC layer, adversaries may only need to induce a collision in one octet of a transmission to disrupt an entire packet. A change in the data portion would cause a checksum mismatch at some other receiver. A corrupted ACK control message could induce costly exponential back-off in some MAC protocols.
- **Routing Layers:** DoS attacks against routing layer is with quite a few styles, which will be thoroughly discussed below.

C. DoS Attacks Against Routing Layer in UAN

Since this is the main topic of this paper, usual types are summarized as follows [12]-[16]

- **Flooding attack:** The attacker transmits a flood of packets toward a target node or to congest the network and degrade its performance. Flooding DoS attacks are difficult to handle. Attacker may use any types of packets to congest the network.
- **Wormhole attack:** In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network in order to create a shortcut (or wormhole) in the network through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker, and then replays them into the network from that point. The malicious node can use this position to maliciously drop packets in order to deny the services in the UAN.
- **Selective forwarding attack:** This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them.
- **Blackhole attack:** In this attack, the malicious nodes broadcast themselves as optimal node to select for data forwarding. The malicious nodes then drop packets and hence deny the service.
- **Jellyfish attack:** It is done by complying protocols for packet dropping in malicious way to deny the services.
- **Byzantine attack:** Attacks are referred to as Byzantine attacks, where the adversary has full control of an authenticated device and it can perform arbitrary behavior to disrupt the system.
- **Sybil attack:** A Sybil attack is essentially an impersonation attack, in which a malicious device illegitimately fabricates multiple identities, behaving as if it were a larger number of nodes (instead of just one). Malicious device additional identities are referred to as Sybil identities or Sybil nodes.

Though the attacks ways differ, the goals of them are the same. That is to deny information transferring to proper nodes, or to make obstacles during the procedure. Comparatively speaking, the former three kinds are more common and basic.

IV. Simulations on DoS Attacks Against UAN

To get a secure UAN, the possible attacks should be aware of. In this section, three kinds of DoS attacks (among above introduction) against UAN are simulated and analyzed.

A. Simulation Tool and Parameters Setup

As a popular network simulation tool, OPNET Modeler supplies an open development environment, which can define and simulate more details within networks. It can be used in any fields in network simulation, such as End to End Network Architecture Design, System level Simulation for Network Devices, Protocol Development and Optimization, and Network Application Optimization and Deployment Analysis [17].

OPNET Modeler 14.5 is selected to perform the simulations in this work. Since there is still not a right model for underwater acoustic channels, Radio Transceiver pipeline stage is modified to adapt UAN channel.

The relative parameters of UAN channel are [18]:

1). Ambient noises

The ambient noises are assumed to be 35dB.

2). Sound speed

The sound speed is set to 1500m/s.

3). Absorption coefficients

$$\alpha(f) = 0.11 \times \frac{f^2}{1+f^2} + 44 \times \frac{f^2}{4100+f^2} + 2.75 \times 10^{-4} f^2 + 0.003 \quad (1)$$

where f is signal frequency (kHz), α is absorption coefficient (dB/km).

So the transmission loss can be obtained as follows:

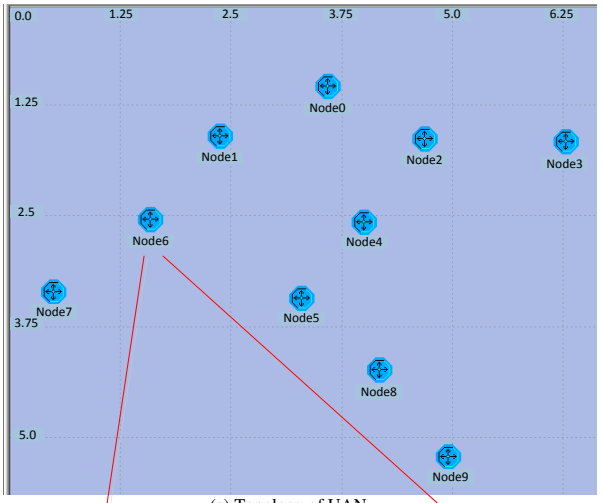
$$TL = 60 + 20 \log r + \alpha r \quad (2)$$

where r represents the range of communication (km), and TL represents transmission loss (dB).

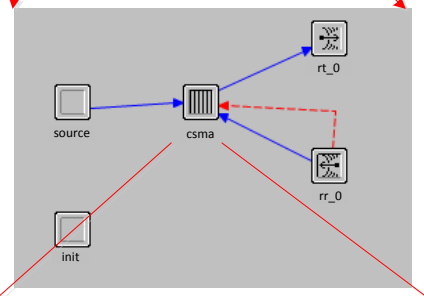
B. UAN Prototype and Performance Analysis

1). UAN prototype

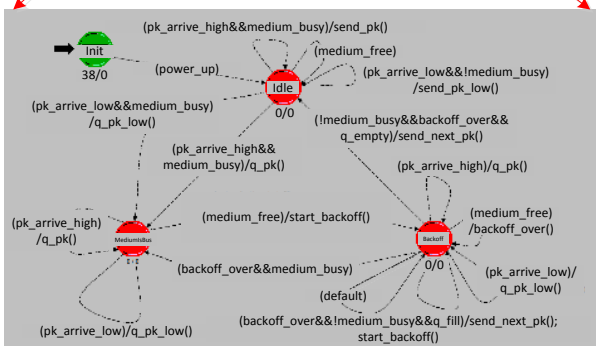
First, a prototype UAN model is constructed for later comparisons as in Fig. 1.



(a) Topology of UAN



(b) Network node model



(c) State transfer of CSMA

Fig. 1. The UAN prototype model

From the Fig. 1, it can be seen that there are 10 nodes within the multi-hop network. The communication range of each node is 1.5km.

The topology is given in (a), the node model is shown in (b), and (c) illustrates the state transferring of CSMA (Carrier Surveillance Multi Access) protocol in the MAC layer of the network.

Table II (on the top of next page) depicts the distances between nodes.

AODV (Ad hoc On Demand Distance Vector) is adopted as routing protocol with some adaptive modification [13][19].

Packets are generated with the distribution of uniform (1s, 30s), and the total simulation time is 1hour (60 minutes) during which 270,000 packets are transmitted. All simulations in this paper will abide by these parameters.

2). UAN prototype

To evaluate the performances of the network, two parameters are selected for comparison: packet loss probability and average ETE (end-to-end) time delay.

According to Fig. 2, it reflects the differences between two groups of transmitted and received packets within the network.

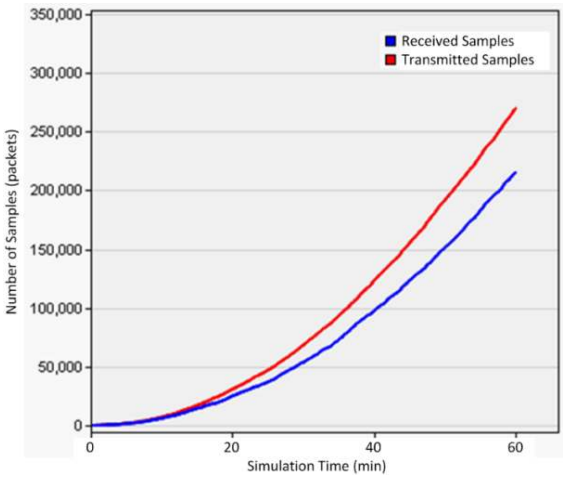


Fig. 2. The packet loss of the UAN prototype model

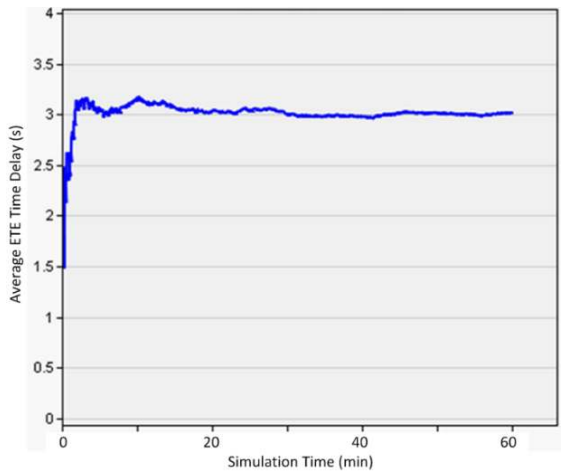


Fig. 3. The average ETE time delay of the UAN prototype model

It shows that 215,000 packets are received by proper nodes, which means that the packet loss probability is 20.4%.

Fig. 3 gives the average ETE time delay of the UAN. The value of the ETE time delay is around 3s.

Take the two values discussed above as references, the next parts will analyze the influences of flooding attack, wormhole attack and selective forwarding attack to the network performances.

TABLE II. DISTANCES BETWEEN NETWORK NODES (KM)

Node No.	0	1	2	3	4	5	6	7	8	9
0	0.00	1.46	1.36	2.47	1.67	2.71	2.70	3.94	4.06	5.42
1	1.46	0.00	2.53	3.69	2.14	2.65	1.27	2.48	4.06	5.46
2	1.36	2.53	0.00	1.16	1.10	2.24	3.57	4.85	3.28	4.53
3	2.47	3.69	1.16	0.00	1.96	2.85	4.69	5.97	3.47	4.47
4	1.67	2.14	1.10	1.96	0.00	1.17	2.86	4.11	2.41	3.76
5	2.71	2.65	2.24	2.85	1.17	0.00	2.85	3.93	1.43	2.82
6	2.70	1.27	3.57	4.69	2.86	2.85	0.00	1.29	4.12	5.42
7	3.94	2.48	4.85	5.97	4.11	3.93	1.29	0.00	5.02	6.21
8	4.06	4.06	3.28	3.47	2.41	1.43	4.12	5.02	0.00	1.40
9	5.42	5.46	4.53	4.47	3.76	2.82	5.42	6.21	1.40	0.00

C. Simulation on DoS Attacks Against UAN

1) Simulation on flooding attack

Fig. 4 illustrates the scenario of flooding attack.

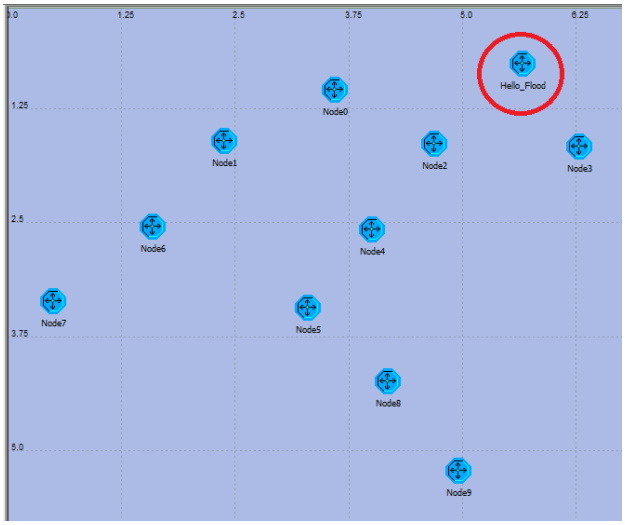


Fig. 4. The scenario of UAN suffering from flooding attack

The new node "Hello_Flood" is a malicious one. It transmits "Hello" message to the network at certain power which can be received by node0 – node6. These nodes then save the ID of "Hello_Flood" node into their neighbor lists as potential relay node. "Hello_Flood" node itself does not generate packets. If it receives packets from other nodes, it simply discards them.

In Fig. 5, when we compare the amount of sent and received packets, we see the packet loss probability is 96.2%. As expected, higher packed loss probability occurs. But it is still surprising the rate is so high. This is because of the strong transmission power of the attacking node, which makes it believable to many of other nodes, so that it attracts many data packets.

Fig.6 proves the dominance of the simulation of the average ETE time delay, which is around 1.1s.

Here we can see that the average ETE time delay decreases. The causation is that most of the packets are sent to "Hello_Flood" node, and then be discarded. Only those nodes bypassing "Hello_Flood" node can really accomplish the transmission.

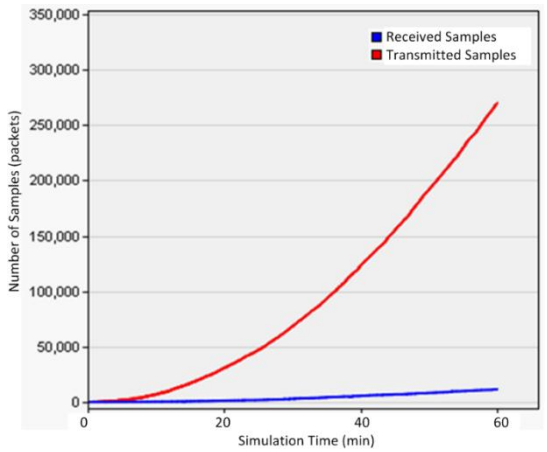


Fig. 5. The packet loss of the UAN suffering from flooding attack

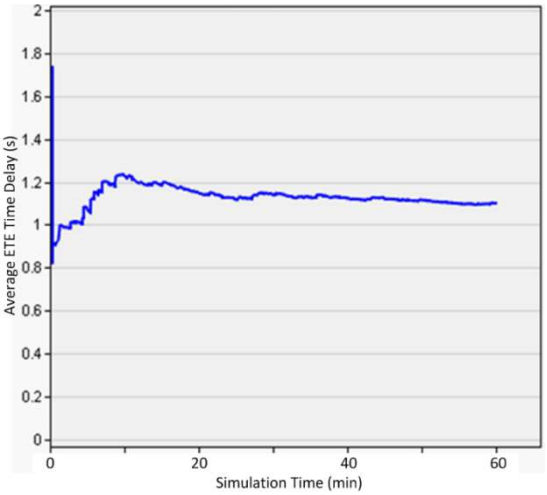


Fig. 6. The average ETE time delay of the UAN suffering from Flooding Attack

2) Simulation on wormhole attack

Fig. 7 illustrates the scenario of wormhole attack against UAN.

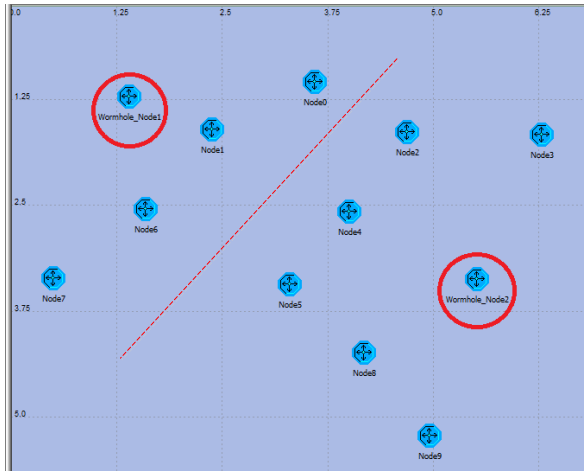


Fig. 7. The scenario of UAN suffering from wormhole attack

There appear two "new" nodes: "Wormhole_node 1" and "Wormhole_node 2". At the same time of transmitting "Hello" messages, they both claim that they themselves have sufficient power, thus attract some 2-hop (and upper) packets to come. And then, the packets are discarded.

Fig. 8 and Fig. 9 give the simulation results of such attack.

Fig. 8 reflects the great differences that exist between the packets in transmitted and received packets, where 97% of the packets lose.

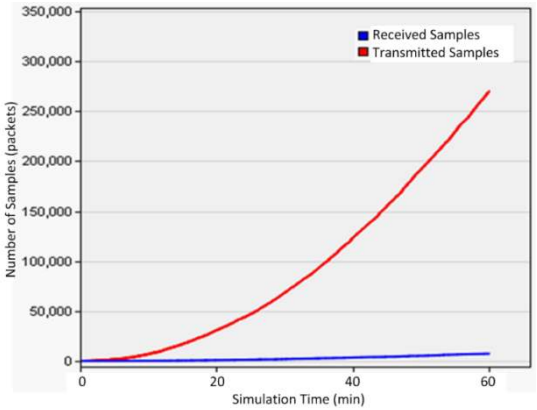


Fig. 8. The packet loss of the UAN suffering from wormhole attack

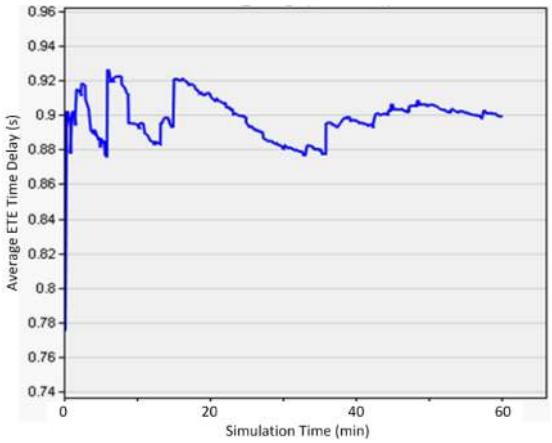


Fig. 9. The average ETE time delay of the UAN suffering from wormhole attack

Fig. 9 shows the average ETE time delay, which is around 0.9s.

Also, one can see that the performance of UAN is seriously degraded.

The reason why the average ETE time delay decreases is similar to that of flooding attack. But it is more serious since the two evil nodes could cooperate in a way.

3) Simulation on selective forwarding attack

Fig. 10 illustrates the scenario of selective forwarding attack against UAN.

The circled nodes called "Select_Forwarding node" are enemy nodes. They do not generate data packets, and act as only relay nodes. But they would not forward the packets on demands, only part of them can be sent out. Say the ratio is 50% in the simulation.

Fig. 11 and Fig. 12 give the simulation results of such attack against UAN.

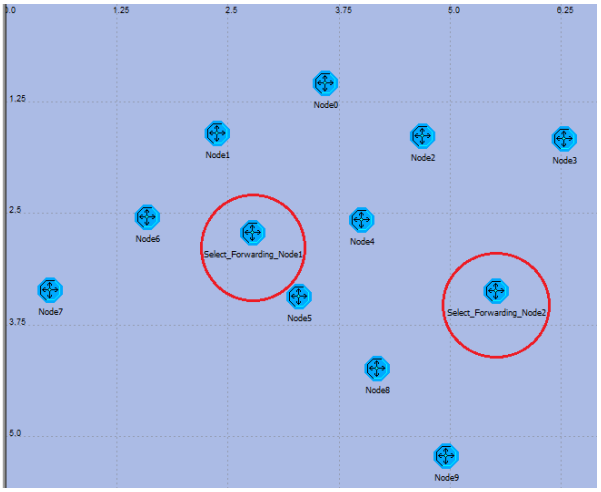


Fig. 10. The Scenario of UAN suffering from wormhole attack

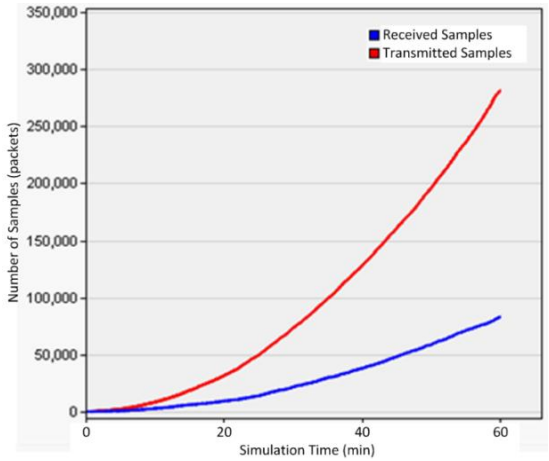


Fig. 11. Simulation Results of Selective Forwarding Attack

Fig. 11 is the comparison of sent and received packet amount. It shows that the packet loss probability is 69%. It seems better than above two attacks, because nearly half of the packets the enemy nodes received are forwarded.

Hence, this is a more deceptive method for discrimination.

Fig. 12 is the average ETE time delay, which is approximately 2s.

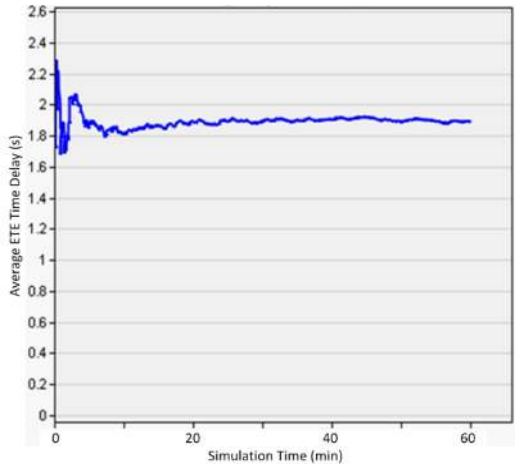


Fig. 12. Simulation results of selective forwarding attack

The reason for the average ETE time delay decreases is that the "Select_Forward" node acts as common relay node to some extent, thus shortens some of the routes.

V. Summary of the Simulation and Some Recommendations on Secure UAN

A. Summary of the Simulation

In previous section IV, we selected two parameters – packet loss probability and average ETE time delay – to describe the effects of DoS attacks against UAN.

Table III is a summary of the simulation results. Remember that here in the simulation, 270,000 packets were sent within the network.

TABLE III. Summary of Simulations

Attack Type	None	Flooding	Wormhole	Selective_ Forwarding
Packets Received	215,000	10,260	8,100	83,700
Packet Loss Possibility	20.4%	96.2%	97%	69%
Average ETE Time Delay	3s	1.1s	0.9s	2s

The second column of Table III is the simulation results of the prototype UAN. It shows that even without any attacks, UAN could not get ideal performances because of the serious operation environment.

The results explicitly show that DoS attacks can seriously aggravate the performances of UAN. For example, the packet loss probability of the network increases sharply, which means most of the data packets cannot be sent to the proper destination.

It is interesting that the average ETE time delay of UAN suffering from three attacks all decreases with the increasing of Packet Loss Possibility. But it is obviously meaningless at all under circumstances of little delivery of information.

It can be concluded that other kinds of attacks would have the similar effects.

B. Recommendations to Secure UAN

Security is one of the most important demands of UAN operation due to its significance and deploying environment.

It is strongly recommended that during the construction of UAN, security problems must be taken into account simultaneously to avoid later invalid mending. Otherwise, it will be costly and inefficient as proved in other kinds of networks.

The other critical reality is that security measures themselves would cost much and lead to sophisticated design. That is a problem that needs to compromise.

C. Countermeasure Considerations to DoS Attacks

Anyway, there should be some countermeasures against DoS attacks for secure UANs. To contrast DoS attacks, following two schemes could be considered [12], [20].

- **Watchdog scheme:** It is a necessary operation to overcome DoS attacks that identify and circumvent the abnormal nodes during the operation of UAN. Watchdog Scheme attempts to achieve this purpose through the using of two concepts: watchdog and pathrater. Each node implements a watchdog that constantly monitors the packet forwarding activities of its neighbors, and a pathrater that rates the transmission reliability of all alternative routes to a particular destination node, according to the reports of the watchdog.
- **Rating scheme:** It is a further investigation and extension of Watchdog Scheme. In Rating Scheme, the neighbors of any single node collaborate in rating the node, according to how well the node execute the functions requested from it.

Despite the security countermeasures, auto reorganization of UAN must be taken into account when UAN is destructed in some extent [21].

Generally, this should be regarded as one more measure for securing UAN. There may be three main steps:

- **UAN Destructing Extent Estimation:** In this period, the importance of destructed nodes should be analyzed before evaluation of the restoration possibility.
- **UAN Destruction Causation Analysis:** It is a necessary step to know why the nodes are invalid. The probable reason may include physical destruction, nodes become selfish or nodes become malicious, etc.
- **UAN Auto-reorganization:** The methods may be adjusting of network topology and adjusting of network protocols.

Together with the countermeasure schemes and an aftermath dealing auto-reorganization, a relative secure UAN can be expected.

VI. Conclusions

Due to the complicated operation environment of UAN, we have to overcome many difficulties on the construction and maintenance. Among them, security is one of the most important considerations.

UANs are prone to suffer from DoS attacks, especially in the Routing Layer. There are several types of DoS attacks against UAN, which are summarized in the paper. Three of them – Flooding, Wormhole and Selective-forwarding are selected to simulate, which show serious aggravation to UANs' performances.

To get secure UANs, some recommendations are put forward. At the same time, some possible countermeasure schemes are introduced. Additionally, a kind of aftermath dealing method when attacked by DoS is discussed to maintain the networking operation at the largest extent.

ACKNOWLEDGMENT

This work was supported in part by China Scholarship Council and partly sponsored within the project CAMOS by the Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology.

REFERENCES

[1] J. G. Proakis, E. M. Sozer, and Joseph A. Rice, "Shallow water acoustic networks," *IEEE Communications Magazine*, vol. 39, pp. 114-119, November 2001.

[2] D. P. Brady and J. A. Catipovic, "Adaptive multi-user detection for underwater acoustical channel," *IEEE Journal of Oceanic Engineering*, vol. 19, pp. 158-165, February 1994.

[3] A. Bessios, "Compound compensation strategies for wireless data communications over the multimode acoustic ocean waveguide," *IEEE Journal of Oceanic Engineering*, vol.21, pp. 167-180, February 1996.

[4] TNO innovation for life. [Online]. Available: http://www.tno.nl/instit/fel/roblink

[5] Mclink. Documento non trovato. [Online]. Available: http://www.mclink.it/com/swan

[6] G. Lapierre, L. Chevallier, and F. Gallaud, "Design of a communication protocol for underwater acoustic modems and networks", in *Proc. MTS/IEEE Oceans*, vol. 4, 2001, pp. 2220-2226.

[7] A. E. Adams, O. R. Hinton, and B. S. Sharif, "Experiments in sub-sea acoustic communication networks," in *Proc. MTS/IEEE Oceans*, vol. 4, 2001, pp. 2059-2064.

[8] A. Caiti, G. Dini, A. L. Duca, *et al.*. Secure cooperation of mobile sensors in an underwater acoustic network. [Online]. Available: http://t.cn/z8GDAf3

[9] M. A. Habib, J. Uddin, and M. M. Islam, " Safety aspects of enhanced underwater acoustic sensor," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, pp. 385-390, August 2012

[10] J. J. Kong, Z. R. Ji, W. C. Wang, *et al.*. "On wormhole attacks in under-water sensor networks: A two-tier localization approach," *UCLA Computer Science Department Technical Report 040051*, 2004

[11] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, pp. 53-57, June 2004.

[12] Y. Z. Dong and P. X. Liu, "Security considerations of underwater acoustic networks," in *Proc. 20th International Congress on Acoustics*, Sydney, 2010.

[13] Y. Z. Dong, G. Q. Zhang, and M. M. Yin, *Networked Underwater Acoustic Warfare*, Beijing: Publishing House of Electronic Industry, 2012.

[14] F. Hu and N. K. Aharma, "Security considerations in ad hoc sensor networks," *Ad hoc Networks*, vol. 3, pp. 69-89, March 2005.

[15] S. A. Soomro, "Denial of service attacks in wireless ad hoc networks," *Journal of Information / Communication Technology*, vol. 4, pp. 1-10, February 2011.

[16] W. Z. Khan, "The selective forwarding attack in sensor networks: Detections and countermeasures," *International Journal of Wireless and Microwave Technologies*, vol. 2, pp. 33-44, January 2012.

[17] C. Min, *OPNET Networking Simulation,* Beijing: Tsinghua University Press, 2004.

[18] Y. Z. Dong, G. Q. Zhang, and P. X. Liu, "A composite networking protocol for asymmetric underwater acoustic networks," in *Proc. 20th International Congress on Acoustics*, Sydney, 2010.

[19] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on demand distance vector (AODV) routing," IETF RFC 3561, 2003.

[20] Y. Z. Dong and L. Yao, "On infrastructure of networked underwater acoustic warfare," *Technical Acoustics*, vol. 26, pp. 1121-1128, November 2007.

[21] Y. Z. Dong and P. X. Liu, "Study and simulation on auto-reorganization of UAN," *Ship Science and Technology*, vol. 28, pp. 70-73, June 2006.

Yangze Dong received the B.Sc. degree in Applied Electronics from Northwestern Polytechnical University, Xi'an, China in 1994, and the M.Sc. degree in Communication and Electronic System from Shanghai University, Shanghai, China in 1999, the Ph. D. degree in Signal and Information Processing from Northwestern Polytechnical University, Xi'an, China in 2003, respectively.

From 2003 to 2005, he was a post doctorial fellow at Shanghai Jiaotong University, Shanghai, China. From 2008 to 2010, he was a post doctorial fellow at Xiamen University, Xiamen, China. From 2003, he was an Engineer, Senior Engineer and Professor of Shanghai Marine Electronic Equipment Research Institute, Shanghai, China. He is now a visiting scholar at Norwegian University of Science and Technology, Trondheim, Norway from 2013. His research interests include underwater acoustic signal processing, underwater acoustic communication and networking, and system simulation.

Prof. Dong is a senior member of the Chinese Society of Naval Architects and Marine Engineers, member of Acoustical Society of China and Chinese Association for System Simulation.

Hefeng Dong received the B.Sc. and the M.Sc. degrees in physics from the Northeast Normal University, Changchun, China in 1983 and 1986, respectively, and the Ph. D. degree in geoacoustics from the Jilin University, Changchun, China, in 1994.

From 1986 to 1994, she was a lecturer of physics at the Northeast Normal University, Changchun, China, where she was associate professor from 1995 to 2000. She was visiting scholar and post doctorial fellow at the Norwegian University of Science and Technology, Trondheim, Norway from 1999 to 2000 and from 2000 to 2001, respectively. From 2001 to 2002 she worked as a research scientist at the SINTEF Petroleum Research, Trondheim, Norway. Since 2002 she has been a professor with the Norwegian University of Science and Technology, Trondheim, Norway. Between 2008 and 2009, she was on a one-year sabbatical with the Underwater Acoustics Laboratory, University of Victoria, Victoria, BC, Canada. Her research interests include wave propagation modeling, geoacoustic inversion and signal processing in ocean acoustics and seismic.

Prof. Dong is a member of the Acoustical Society of America and a member of IEEE.

Gangqiang Zhang received the B.Sc. and the M.Sc. degrees in ocean physics from Xiamen University, Xiamen, China, in 2005 and 2008, respectively.

From 2008, he has been worked as an Engineer with Science and Technology on Underwater Acoustic Antagonizing Laboratory, Shanghai, China. He is also an engineer with Shanghai Marine Electronic Equipment Research Institute, Shanghai, China. His research interests include signal processing, underwater acoustic communication systems and networks.

Mr. Zhang is a member of Acoustic Society of China, and the Shanghai Society of Naval Architects & Ocean Engineers.