Proceedings of 20th International Congress on Acoustics, ICA 2010

23-27 August 2010, Sydney, Australia

Security Considerations of Underwater Acoustic Networks

Yangze Dong, Pingxiang Liu

Shanghai Marine Electronic Equipment Research Institute, Shanghai, China

PACS: 43.30Nb

ABSTRACT

Recent researches on Underwater Acoustic Network (UAN) mainly focused on the construction and management. Though these studies have covered nearly all the respects within the UAN infrastructure, few efforts have been made for its security, which is surely an important consideration when put into practices. This paper focuses to the security considerations of UAN. Within the paper, the characteristics of UAN are analyzed firstly, and comparisons between the common-used networks are performed. Thereafter, the application environments of UAN are studied and the goals and challenges of a secure UAN are investigated. Based upon the above studies, the security threats are classified according to their harm to UAN, and corresponding countermeasures against them are taken into considerations.

INTRODUCTION

Underwater Acoustic Network (UAN) has been studied for over three decades, and now there have been a number of experimental implementations developed by various research organizations for various purposes. It is believed that most of them will bring into relevant applications in the near future.

Recent researches corresponding to UAN mainly focused on its construction and management [1]. Though these studies have covered nearly all the respects within the UAN infrastructure, few efforts have been made for its security, which is surely an important consideration when put into practices.

Whether used in what kinds of applications, the robustness of UAN seems to be one of the most significant considerations. The network might be degraded via two ways: One is the natural destroy, such as the severe circumstances of the network locates; the other is from hostile attacks, which are performed purposedly by the adversary.

The performance of UAN is tightly linked to its intrinsic features, structure, environment, security measures, etc. Although there couldn't be an absolutely secure network, efforts should be made to the largest extent. And the endeavors are based upon thorough analysis of UAN.

In the foregoing sections, several problems are investigated.

The characteristics of UAN are analyzed started from underwater acoustic communication. Comparisons between UAN, WSN (Wireless Sensor Network in territory) and Ad hoc Sensor Network (ASN) are pursued, which states a more significant necessity for the security of UAN.

The application environments of UAN are analyzed. Both civil and military applications are prone to be destroyed, either by the nature or the intended artificial attackers. For example, the severe current and hostile attacks are the two main causations.

The goals and challenges of a secure UAN are analyzed. For different utilities, different requirements and difficulties would be confronted.

The security threats are analyzed. The study indicates that security problem might happen at all physical and protocol layers. Since the hardware weakness is a secondary problem, emphasis are put to the protocol attacks, which might arouse a large-scale paralysis of UAN.

The countermeasures against the attacks are studied. Based on the threat estimations, security measures are analyzed with respect to the adversary offensives.

CHARACTERISTICS OF UAN

The naissance of new technologies generally depends on two bases. One is the leading of the practical requirements, the other is the promotion of relevant techniques.

As for UAN, these two aspects are both at present. The motivation comes from environmental data collection and surveillance [2], while there also are two developed techniques – underwater acoustic communications and networking – as the support.

Underwater Acoustic Communications in UAN

Though it is the best means for communications in the water, 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 may result in low rate, near range, high BER (bit error rate), large time delay, etc.

From 1990's, with the application of coherent processing technique, there has been a shift in high-rate communications. With the rapid development of large scale integrated circuits, OFDM (orthogonal frequency division modulation), MIMO (multi-input multi-output) and TRM (time reversed modulation) techniques are gradually adopted in the study of underwater acoustic communications.

In UAN, communications are the most frequent happening events, from the beginning handshaking to the exchanging of information.

Comparison between UAN, WSN and ASN

Besides the transmission media, there are still many other differences between UAN, WSN and ASN.

Table 1 presents a simple comparison with a variety of parameters.

Table 1. Main Differences between UAN, WSN and ASN

Items	UAN	WSN	ASN
Cost	Expensive [a]	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	Distributed sensing	Cooperation engagement
Environment condition	Severe	Good	Good

[a] Including manufacturing, deployment, maintenance and recovery, etc.

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

APPLICATION ENVIRONMENT OF UAN

As one knows, the application environment may bring tremendous influences to the systems. From the point of view of the robustness of UAN, there are two factors should be taken into considerations.

Severe Natural Environment

Surely, UANs are deployed underwater, especially in the sea. An obvious fact is that most of the practical (experimental) UANs are in the littoral sea, which is one of the acknowledged difficult communication channels.

In such channels, the successful communication probability would be lowered to some extent. Thus the energy of the power supply (usually batteries) would consume rapidly.

Another impact of such environment to UAN is that the nodes might not be strictly static own to the water float, which would produce troubles for precise localization.

The third circumstance is that the erosion of the sea water to the nodes, which would accelerate their collapse extremely.

Hostile Attacks

Whether or not it is used in the civil fields, hostile attacks are potential threats to UAN for various purposes (e.g., by terrorists).

The attacks may be classified into three categories: attacks to nodes, to communication links, and to the network protocols. The embodied analysis will be performed in the foregoing parts.

In summary, UAN works in a dangerous environment, and it is prone to be destroyed by either natural or man-made breaks. To the former, it's a safety problem, and the latter is a problem of security. Together with the two assurances, we say that the UAN is a robust one.

A SECURE UAN – GOALS AND CHALLENGES

General Security Goals of Networks

Efficient information exchange among nodes is the main work of a network. To achieve such objective, there are several general goals of a network corresponding to the considerations of security [3].

- 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 communication information between nodes not leak to other nodes.
- Data Authentication: Allows the receiver to verify that the data was really sent by the claimed sender.
- Data Freshness: This implies that the data is recent, and it ensures that no adversary replayed old messages.
- Data Integrity: Ensures the receiver that the received data is not altered in transit by an adversary.

Embodied Requirements on Security in UAN

An illustration of a typical UAN is in Figure 1 [4].

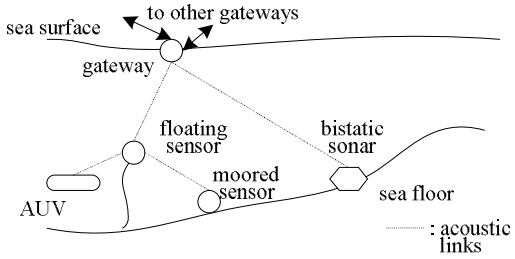

Figure 1. Illustration of a typical UAN

Here we can see that a typical UAN is made up of a number of static and/or dynamic sensor nodes via acoustic communications link. The fixed nodes (seabed moored sensors, bistatic sonars, etc. for instance) are often deployed in the interested region for information acquisition, while the dynamic ones (such as AUVs, sonars carried by ships, etc.) can join the network if necessary. Communications between the nodes use acoustic signals through multi-hopping. Usually, information collected by UAN will be sent to the commander centre, so a gateway (buoy usually) connecting other kinds of gateways is indispensable.

The aforementioned general goals of networks are also necessary to UAN. As stated in last section, there may be three embodied requirements on UAN security.

See Figure 1 again. Information exchanges between nodes in UAN are via acoustic links, i.e., acoustic communication. And the communications among the nodes are controlled by the network protocols.

Therefore, the security of UAN lies in three levels:

- Nodes security: This is the physical basis of UAN. Especially if the important nodes, such as the cluster heads or even the gateway are destroyed, the network won't work any longer.
- Communication security: This is the "nerves" in UAN. If it can't be assured, the network will degrade to an assembly of several individual devices.
- Protocol security: This is the control system of UAN. Without the arrangement of protocol, the operation would run into confusions.

Now it gets obvious that for the successful information exchanges, the three levels of security must be assured.

Challenges for UAN Security

Characteristics and application environment of UAN directly bring challenges for its security.

- Challenge 1: Though UAN nodes have stronger storage and processing capabilities compared to WSN and ASN, its power supply is limited and consumable. Apart from the regular functions, extra operation would bring 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 ASN (Ad hoc Sensor Network) 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 node due to the networking topology. Large scale and sparse structure makes the network easy to be attacked and hard to defense.

ATTACKS TO UAN

This section will present some attack measures to UAN. This is the reversed proposition of the security, which could supply thoughts to the security.

Detection of UAN

To achieve the aim of destroying the adverse UAN, the first step is to find the existence and scale of UAN.

UAN's operation can be active or passive. The difference between the two modes is that if there are signals transmitting from network nodes. In practice, most of UANs are in passive mode for stealthiness. This fact brings big difficulties to locate a UAN.

Fortunately, there still is some information to make use.

Figure 2 presents the scheme of Detection of UAN in practice [5].

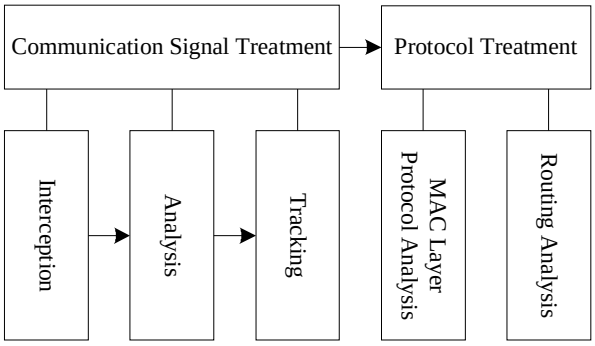

Figure 2. Practical scheme of detection of UAN

One can see from Figure 2 that during the UAN detection, communication signals and protocol information are taken into consideration.

Hard destroy to UAN

It seems that it is the most effective method to destroy UAN.

UAN is made up of various kinds of nodes. If any nodes are destroyed physically, the function of network would be degraded, or even collapse absolutely if important ones are ruined.

But this method is not so practical. Because of the large distance between UAN nodes, it's hard to simultaneously break several nodes. Thus the influence to UAN is not so vital, unless the node is right the sink node.

Suppressing to UAN communication

Communication is the most frequently happening action in UAN for information interchanging.

After analysis of the intercepted UAN communication signals, its basic parameters such as frequency, waveform, repeat period, power and so on are known. Under this circumstance, high-power signals at the same frequency point could be transmitted to suppress the communication of UAN.

A feasible scheme is to generate random noise using m-series, then modulate it into the assigned frequency. The amplitude of the noise should be uniform distributed.

Attack to UAN Protocols

If above method is not successful (for example, the UAN changes its communication signals' parameters), an advanced measure might be taken.

Protocols are the nerves of UAN. All the network behaviors abide by them. 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).

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 receivers. A corrupted ACK control message could induce costly exponential back-off in some MAC protocols.

In the routing layer, Attacks in this layer mainly include the following ones: wormhole attacks, black holes attacks, sybil attacks, flood attacks, detours and loops attacks, ring of evil attacks, etc.

And, a new kind of conceptual method worthy studying is the so-called underwater acoustic virus, which is illumined by the concept of computer virus.

In summary, the attack attempts to UAN may be classified into two measures – hard attacks and soft attacks. Thinking of the target, these measures drop into two targets – to nodes and to the network.

Figure 3 presents the attack methods to UAN.

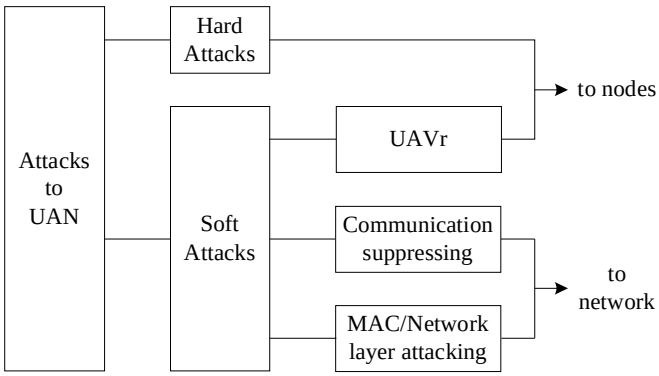

Figure 3 Attack methods to UAN

SECURITY CONSIDERATIONS OF UAN

Now, we have known that there are many challenges for the security of UAN, and many essential attack attempts to UAN. Hence, security measures of UAN must be taken into consideration.

How to Improve the Security Performances of UAN?

Security is one of the most significant respects of the robustness of UAN. As mentioned above, there are three kinds of main threats. So the security measures discussed here in this paper are pertinent to the counterparts.

A. Nodes Security

Though it seems impossible that all the nodes be ruined, important nodes' being destroyed would bring disaster to the network. Consequently, nodes security should be taken into account as well.

The first thought is that to reinforce the hardware themselves, which could make the nodes more solid; The other measure is to have cooperation with other devices to protect the nodes jointly.

B. Communications Security

While spread spectrum methods have been widely adopted in underwater acoustic communications, which bring rather extent security, additional measures should be taken for farther security.

With normal communication methods, encryption is a necessary measure. As to the used waveforms, some special components should be added to form complicated signals, thus not easy to be captured. Another thinking is to backup various styles of transmission signals, so that alternating could be implemented if the former used signals were uncovered by the attacker.

C. Protocols Security

There have been many secure protocols (especially routing protocols) developed in WSN and ASN. Some of their ideas could be absorbed in the investigation of the counterpart in UAN. For example, a underwater pairwise distance measuring method used in UAN is proposed in [6].

Another thought is that the network must have the ability of self-cure [2]. A simulation had proved its validity via a self-organization protocol [4].

D. Brief Discussion

The proposed measures on the security of UAN above all need extra resources in UAN. Since the resources in UAN are very limited, such as storage, processing, and power supply, etc., there must be a tradeoff between the security and consumptions.

When to Implement the Security Measures?

The lessons taught in Internet and other networks show that if security measures are added as mends when the problems have arisen, the cost will be enormous, together with limited effects [7].

Therefore, measures on security must be taken into consideration at the beginning of the construction of UAN, and be carried out simultaneously during the construction.

SUMMARY

The technologies of UAN have been studied for over 30 years. It has come to a pre-practical developing stage. But the security measures are not carried out simultaneously.

Based on the analysis of the related problems concerning the security of UAN, such as the intrinsic characteristics and the environments, the goals and challenges of a secure UAN put forward, and the security considerations are presented.

Since the security considerations are crucial to UAN, and measures on security must be taken into consideration simultaneously.

REFERENCES

1 Zaihan Jiang. "Underwater Acoustic Networks – Issues and Solutions" *International Journal of Intelligent Control and Systems*, **13**(3), 152-161 (2008)
2 Joseph A. Rice, Bob Creber, et al. "Evolution of Seaweb Underwater acoustic Networking" *Proceedings of Oceans Conference Record (IEEE)*, **v3**, 2007-2017 (2000)
3 Adrian Perrig, John Stankovic and David Wagner. "Security in Wireless Sensor Networks" *Communications of the ACM*. **47**(6), 53-57 (2004)
4 Dong Yangze, Liu Pingxiang. "Study on Security of Underwater Acoustic Networks" *Proceedings of International Conference for Intelligent Systems*, December 1 – 3, 2005, Kuala Lumpur, Malaysia
5 Dong Yangze, Liu Pingxiang. "On Countermeasures to Underwater Acoustic Network" *Proceedings of 19th International Congress on Acoustics*, September 2-7, 2007, Madrid, Spain
6 Jiejun Kong, Zhengrong Ji, et al. "On Denial-of-Service Attacks in Under-Water Sensor Networks" *www.engr.uconn.edu/~jhuang/DenialOfService.ppt*
7 Fei Hu. "Security considerations in ad hoc sensor networks" *Ad Hoc Networks*, **3**(5), 69-89 (2005)