International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Special Issue 01 | 2020

Attacks in Underwater Sensor Network

[1]Suresh Wati (PhD Scholar), [2] Nitin Rakesh, [3] Parma Nand Astya , [4] Dr. Ashish Kumar

[1,2,3] Department of Computer Science & Engineering School of Engineering Sharda University
[4] Department of Computer Science & Engineering ITS Engineering collage Greater Noida, India

ABSTRACT

UWSNs are discovered to an advanced class of security malicious attacks. In this paper we explain two types of attack active and passive attack and explain which attack is more prominent in underwater sensor network. In during research deliberation has not taken security in UWSNs. WSN security cannot be direct use in UWSNs. Due to acoustic channel, incalculable environment and other communication issues in UWSNs. In this paper we explain all types of attack in UWSNs. UWSNs are unsafe to various attacks and solution of these attacks should be discussed. Some uniqueness and attacks of UWSNs and underwater acoustic channels are presented and discussed in detail.

Keywords - Underwater, Environments, Active Attacks, Passive Attacks, Security.

1. INTRODUCTION

In underwater different types of attacks, threats and vulnerabilities present to corrupt and break the underwater nodes security. These attack that compromise the security of the underwater nodes. The security attacks can be classified into two types there are active and passive attacks where the attacker gains illegal access to the underwater acoustic channel resources. In active attacks the attacker cut off the connection and convert the information, while in passive attack the attacker motive of reading and analyzing and convert the transmit information not for altering it is the big difference within active and passive attacks.

2. COMPARISON OF PASSIVE AND ACTIVE ATTACKS

Comparison Based	Active Attacks	Passive Attacks
Basic	In active attack the attacker can cut off the connection and convert the information, underwater acoustic channel resources or affect their operation.	In passive attack the attacker motive of reading, analyzing and convert the transmit information. It does not altering and do not affect the system resources.
Information modification	Occurs	Does not take place. It can't modify any information.
Nodes harmful	Always causes damage to the nodes.	Do not cause any harm.
Threat to	Availability and Integrity	Reliability
Attack awareness	When attack occurs the entity gets informed	The entity does not get informed.
The attacker perform task	The transmission is captured by physically controlling the portion of the link	Just need to observe the transmission
Emphasis is on	Detection	Prevention

3. ACTIVE ATTACKS

The active attacks the attacker cut off the connection and convert the information, while in passive attack the attacker motive of reading and analyzing and convert the transmit information attacks in which the attacker tries to modify the information or creates a false message. A broad range of software vulnerabilities, potential physical and network the prevention of active attacks is quite difficult. But prevention, it emphasizes on the detection of the attack and recovery from any disruption or delay caused by it. An active attack mostly requires more dangerous implication and more effort. When the hacker attempts to attack, the victim gets aware of it. Shown in fig.1

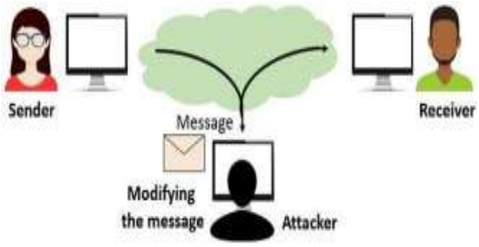


Fig.1 Active attacks

3.1 Types of active attack

Active attacks can be executed by internal or external malicious attackers. Internal attack if attacks come from an insider node, these kinds of attacks are internal attacks which can cause considerable damage to the network. It is unfeasible to detect a malicious node which is distinguished as a normal node and then prevent it from disrupting the network. Even worse, internal attacks may be launched by compromised nodes which are actually legitimate nodes before being compromised. The compromised node has legitimate ID and other privacy data (e.g., secret key, encryption algorithm, trust value), which would act as a legitimate node and cause continuous attacks. From the analyses above, it is obvious that internal attacks are more difficult to detect and may cause more severe damages than external attacks.

To prevent this problem, External attack if the attacks are carried out by nodes that do not belong to the network, these kinds of attacks are external attacks, which would be easier to detect and defend. The feasible solution is using security mechanisms such as encryption, authentication and trust management.

Various types of active attacks are:

- Node compromise attacks
- Repudiation attacks
- Packet-oriented attacks
- Protocol-oriented attacks
- Denial of service (Dos) attacks

Passive Attacks are the attacks where the attacker indulges in unauthorized eavesdropping. It just monitoring the transmission or gathering information. The eavesdropper does not make any changes to the data or the system. Passive attack is hard to detect because it does not involve any alteration in the data or underwater channel resources. The attacked entity does not get any clue about the attack. It can be prevented using encryption method in which the data is firstly encoded in the unintelligible language at the sender’s end and then at the receivers end it is again converted into human understandable language. In this way at the time of transmit the message is in an unintelligible form which could not under stood by attackers. it is the reason , in passive attack the prevention has more concern than detection .the passive attack entangle the open ports that are not protected by firewalls. The attacker continuously searches for the vulnerabilities and once it is found the attacker gains access to network and underwater acoustic channels. Passive attacks refer to the attempts that are made by malicious nodes to perceive the nature of activities and to obtain data transmitted in the network without disrupting the operation. Shown in fig.2

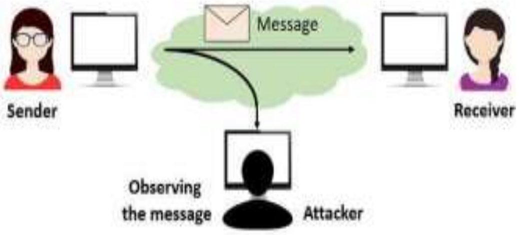
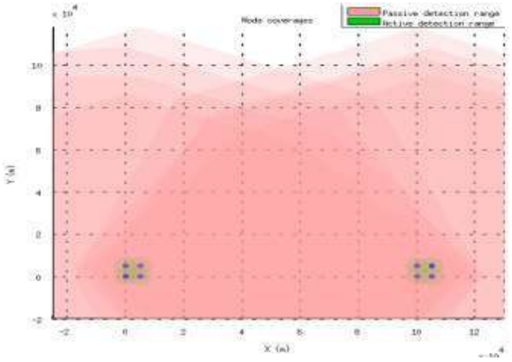


Fig.2 Passive attacks

For example Eavesdropping, Interfering, Leakage of secret information, Impersonation, Message replay and Message distortion.

3.2 Methods of passive and active attacks detection

There are two cases for determining the transmission range (*R*) of a point source in a particular direction.



In this figure top-down view of communication (passive detection) and echo-based detection (active detection) ranges for two sets of identical sensor nodes, each operating with a *TL* threshold of 150 dB at a depth of 3000 m. To eliminate unnecessary computational overhead, ranges are only calculated in the direction of every other node in addition to the 26 cardinal directions from each point source in 3D space.

3.3 Passive detection:

An acceptable loss in intensity level for node communication it is duplex communication between a pair of nodes requires each node to be in the other's one-way transmission range in its direction.

3.4 Active detection:

Acceptable-losses in intensity level for echo-based detection it is require taking into consideration the two-way transmission losses in a particular direction and back.

3.5 TL Active

Communication ranges are appreciably larger than echo-based detection ranges for a given node in a particular direction and under the same set of conditions D‖ it also improve the node mobility issues and it also improve the communication in as compare to other communication carrier. Bandwidth and frequency is in KHZ of acoustic communication career.

4. CONCLUSION

4.1 Conclusion and future work

The active and passive attacks can be differentiated on the basis of what they are. How they are performed and how much extent of damage they cause to the system. But majority the active attack modifies the information and causes a lot of damage to the system resources and can affect its operation. The passive attack does not make any changes to the system resources and therefore does not cause any damage. In this paper the threats and attacks in UWSNs are discussed. Firstly, a brief introduction about UWSNs is presented. In the second part, attacks, which were explained in details. These attacks prevent any part of UWSN from functioning correctly or in a timely manner. Such attacks can target the communication channel (e.g. jamming) or the life of the nodes themselves (e.g. power exhaustion). In this paper, a distributed detection and mitigation approach to routing attacks in UWSNs is presented. Our next steps target to elaborate on the detection and mitigation of other security attacks against UWSNs.

5. REFERENCES

[1] Walter.Nishit, Rakesh.Nitin, ―KRUSH-D approach for the solution to node mobility issue in UWSN,‖ Networking Communication and Data Knowledge Engineering (NCDKE), pp.89-98, 2018.

[2] Walter.Nishit, Rakesh.Nitin, ―SEE THROUGH Approach for the solution to Node Mobility in UWSN„‖ International Confrence on Smart System, Inovation and Computing(ICSSIC), pp. 19-29, 2018.

[3] emad felemban, faisal karim shaikh, umairmujtaba qureshi, adil a. sheikh,and saad bin qaisar3" underwater sensor network applications" article id 896832,2015.

[4] .KhalidMahmood Awan, Peer Azmat Shah ,1 Khalid Iqbal, Saira Gillani, Waqas Ahmad,and Yunyoung Nam" Underwater Wireless Sensor Networks: A Review of Recent Issues and Challenges" Volume 2019, Article ID 6470359,Wiley 2019.

[5] . P.Carroll, S.Zhou, K.Mahmood, H. Zhou,X.Xu, and J.-H. Cui,"On-demand asynchronous localization for underwater sensor networks," in *Proceedings of the IEEE Oceans*, pp. 1–4, IEEE, Hampton Roads, Va, USA, October 2012.

[6] Javier Lopez, Rodrigo Roman, and Cristina Alcaraz‖ Analysis of Security Threats,Requirements,Technologies and Standards in Wireless Sensor Networks‖2009.

[7] Ateniese, G., Capossele, A., Gjanci, P., Petrioli, C., Spaccini, D.: Secfun: Security framework for underwater acoustic sensor networks. In: OCEANS 2015-Genova, pp. 1–9. IEEE (2015)

[8] Tooska Dargahi, Hamid H.S.Javadi , Hosein Shafiei" Securing Underwater Sensor Networks against Routing Attacks"IEEE 2017.

[9] Rubal Bansal, Saurabh Maheshwari and Payal Awwal" Challenges and Issues in Implementation of Underwater Wireless Sensor Networks" Springer Nature Singapore Pte Ltd. 2018.

[10] Sidharth Iyer D. Vijay Rao, *Senior Member*, IEEE" Genetic Algorithm based Optimization Technique for Underwater Sensor Network Positioning and Deployment"2015.