Security Analysis and Issues in Underwater Wireless Sensor Auditory and Multipath Network

Syed Mohtashim Mian
Department of Computer Science
Shri Venkateshwara University
Amroha, India
syedmohtamshim15@gmail.com

Dr. Rajeev Kumar
Faculty of Engineering and Computing Science
Teerthanker Mahaveer University
Moradabad, India
dr.r.kumar@ieee.org

***Abstract*— UWSNs is an auspicious technology for marine, the first underwater communication device was underwater phone which is used for US Navy after the World War 2. Now these techniques have been under research over a last half century. However, the securities of underwater sensor networks are those which help to provide a secure network because there are so many security issues and malicious attacks are presented. Security of UWSNs is a critical issue with increasing the need for security of application of underwater sensor network for example malicious attacks of military exercise, assisted navigation, intrusion and simulation nodes are the major security threats. In this paper we introduce only security issues in UWSN because there are large numbers of applications require deploying the security issues.UWSNs is an auspicious technology for marine, the first underwater communication device was underwater phone which is used for US**

Keywords*— *UWSNs, Security Threats, Security Attacks

Introduction

In any organization of entire world the security issue is most important field. In UWSNs the security appeared in various applications in underwater like military applications, disaster prevention, oil & mineral exploration. There are many research is under process related to security issue and it is a challenging task due to special constraints of underwater environment because the nodes have limited battery power and limited bandwidth. Therefore, security services help to improve the network life and protect the useful information.[1]

Security Requirement

Authentication: Verifying that communicating nodes are who they claim to be. It can be achieved by Massage Authentication Code (MAC).

Confidentiality: Hidden the data from everyone except for those who are authorized. It can be achieved by the use of encryption.

Security Threats

In UWSN the nodes is not physically protected and the attackers may attacks the nodes with help of various type of security threats. There are two major attacks are Passive attacks & Active attacks.[2]

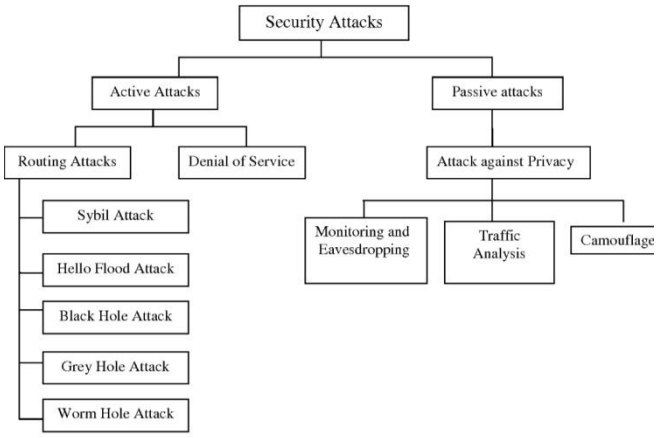

Figure 1: Security attacks in UWSNs.

Passive Attack – Passive attacks are those which attacks against Privacy and it can obtain the useful information while transmitted data and it can analyze the traffic.

Active Attack – Active attacks involves to create a wrong packet and to control the data send by the nodes it generated a fake message and to attack the network.

There are some different types of attacks which behave like malicious way and to control the node, generated a fake message, etc.

Sinkhole Attack – The adversary places malicious node to the closest sink. The malicious node tries to look very attractive for other nodes.[3]

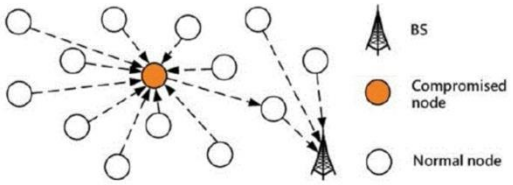

Figure 2: Sinkhole attacks in UWSNs.

Selective Forwarding Attacks – When receiver is not receive the data and information due to selective forwarding attacks then that time multipath routing protocol can effectively defence these attacks.

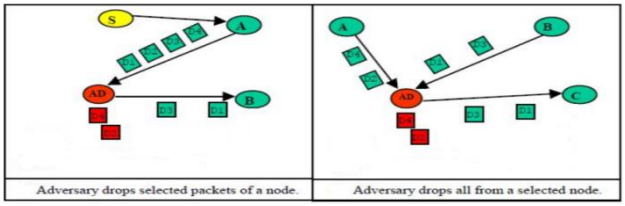

Figure 3: Selective Forwarding attack in UWSN.

Sybil Attack – Sybil attacks are those in which the several malicious nodes with multiple identities can attacks the multiple places at the same time.[4]

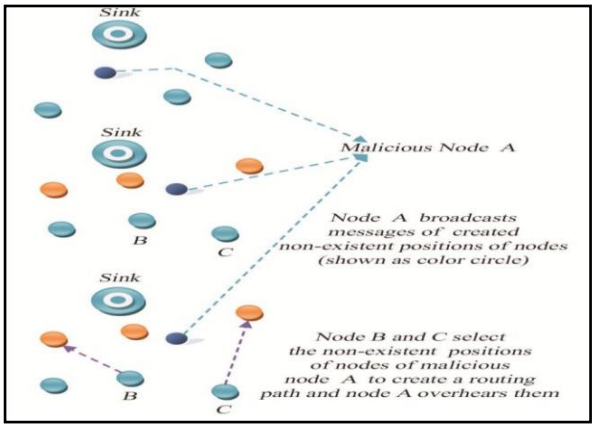

Figure 4: Sybil attacks in UWSN.

Homing Attack – Homing attacks are those in which they attack the cluster head node or a sink node to control the network. So once these nodes failed the whole network become useless.

Wormholes Attack – Two malicious nodes directly connected, receive packets at one node and tunnels them to other node. This creates a man in the middle attack and dropping the packets.

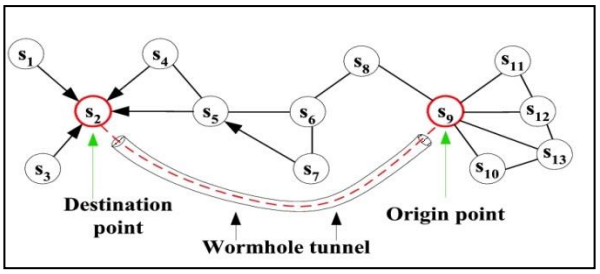

Figure 5: Wormhole attacks in UWSN.

Jamming Attack – Jamming attack can injects unwanted signals into the communication channels with the help of jammer and it can determines the frequency of communication.[5]

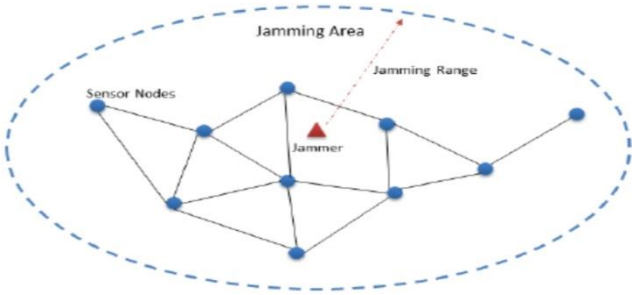

Figure 6: Jamming attack in UWSNs.

Tampering – An attacker can attack the underwater nodes which is in enemy zone and it can damage or modify nodes physically.[6]

Conclusion

In this paper, we discuss general introduction about the various security issues and threats in underwater wireless sensor network.

Acknowledgement

I would like to express my special appreciation and thank to my guide Professor Dr. Rajeev Kumar for always supporting also thankful to Shri Venkateshwara University.

References

[1] M.R Ahmed, X. Huang and H. Cui, "Mrakov Chain Carlo Based Internal Attack Evaluation for Wireless Sensor Network" Int.J. Comput.Sci. Netw.Secur., vol.13, no.3, no.3, pp. 23-31, Mar. 2013.

[2] Salvador Climent, Juan Vicente Capella, Nirvana Meratnia and Juan José Serrano, 'Underwater Sensor Networks: A New Energy Efficient and Robust Architecture', Sensors 2012, 12, pp.704-731.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in

Sensor Network Protocols and Applications, 2003., Berkeley, CA, USA, 2003, pp.113-127.

[4] Sihem Souiki, Maghnia Feham, Mohamed Feham and Nabila Labraoui, 'Geographic Routing Protocols for Underwater Wireless Sensor Networks: A Survey'International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 1, February 2014, pp.69-87.

[5] S. M. Manas Khatua, "CURD: Controllable reactive jamming detection in underwater sensor networks," Pervasive Mob. Comput., 2014.

[6] K. Jensen, L. Kristensen and L. Wells, "Coloured Petri Nets and CPN Tools for Modelling and Validation of Concurrent Systems", International Journal on Software Tools for Technology Transfer (STTT), Springer-Verlage, 2007.