Heena Ahuja, Er. Jyoti Gupta / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 4, July-August 2012, pp.967-971

Analysis of Malicious Data in Underwater Sensor Network

Heena Ahuja*, Er. Jyoti Gupta**
*(Student, Department of ECE, MMU Mulllana, Ambala, India)
** (Assistant Professor, Department of ECE,MMU Mullana, Ambala, India)

ABSTRACT

In this paper, we tackle the malicious attacks in Underwater Sensor Networks (UWSNs). Underwater Sensor Networks (UWSNs) consists of variable number of sensors and vehicles that are deployed to perform collaborative monitoring tasks over a given area. In this paper, we use a novel routing protocol, called vector-based forwarding (VBF) protocol, to provide robust, scalable and energy efficient routing to deploy an Underwater Sensor Network. VBF is essentially a position-based routing approach: nodes close to the "vector" from the source to the destination will forward the message. Then we introduce the malicious node in the network that hack the data of nodes when nodes undergoes Denial of Service attack (DoS). Thus in this paper we have compared the various parameters like Throughput, PDR, PLR and Checksum Errors for before and after attack and results are shown in this paper.

Keywords **- checksum error, denial of service, nodes, PDR, PLR.**

1. INTRODUCTION

1.1 Definition of Underwater Sensor Network

Underwater Sensor Networks (UWSN) consists of a variable number of sensors and vehicles that are deployed to perform collaborative monitoring tasks over a given area. To achieve this objective, sensors and vehicles self-organize in an autonomous network which can adapt to the characteristics of the ocean environment.
Major challenges in the design of underwater Sensor Networks are [1]:

- The available bandwidth is severely limited.
- The underwater channel is severely impaired, especially due to multi-path and fading.
- Propagation delay in underwater is five orders of magnitude higher than in radio frequency (RF) terrestrial channels, and extremely variable.
- High bit error rates and temporary losses of connectivity (shadow zones) can be experienced, due to the extreme characteristics of the underwater channel.
- Battery power is limited and usually batteries cannot be recharged, also because solar energy cannot be exploited.
- Underwater sensors are prone to failures because of fouling and corrosion.

Currently, many routing protocols are available for terrestrial wireless sensor networks. However, specific properties of underwater medium make existing routing protocols inappropriate for under water. The main challenges in developing efficient routing protocols for underwater environments are:

- High propagation delays: The radio signals do not work efficiently under water and this problem encourages use of acoustic communication instead. The main problems with the acoustic channel, however, are low bandwidths and long propagation delays.
- Node mobility: Due to water currents, nodes can fluctuate or move if they are not anchored at the bottom of the sea. This situation results in a dynamic network topology. Moreover, autonomous underwater vehicles and robots used for exploration and controls can be utilised to route and mulling data.
- Error prone acoustic underwater channels: Since the acoustic channels have very low bandwidth capacity, they suffer from high bit error rates.
- Limited energy: Like in terrestrial wireless sensor networks, majority of sensor nodes in UWSNs are battery powered.

1.2 Vector Based Forwarding Protocol (VBF)

In sensor networks, energy constraint is a crucial factor since sensor nodes usually run on battery, and it is impossible or difficult to recharge them in most application scenarios. In underwater sensor networks, in addition to energy saving, the routing algorithms should be able to handle node mobility in an efficient way [2].

Vector-Based Forwarding (VBF) protocol meets these requirements successfully. We assume that each node in VBF knows its position information, which is provided by some location algorithms. If there is no such localization service available, a sensor node can still estimate its

relative position to the forwarding node by measuring its distance to the forwarder and the angle of arrival (AOA) and strength of the signal by being armed with some hardware device.

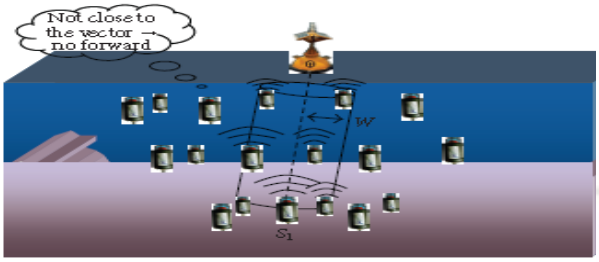

Fig.1: A high level view of VBF for UWSNs.

The position information can be calculated by measuring the AOA and strength of the signal. In VBF, each packet carries the positions of the sender, the target, and the forwarder (i.e., the node which transmits this packet). The forwarding path is specified by the routing vector from the sender to the target. Upon receiving a packet, a node computes its relative position to the forwarder. Recursively, all the nodes receiving the packet compute their positions. If a node determines that it is sufficiently close to the routing vector (e.g., less than a predefined distance threshold), it puts its own computed position in the packet and continues forwarding the packet; otherwise, it simply discards the packet. In this way, all the packet forwarders in the sensor network form a "routing pipe": the sensor nodes in this pipe are eligible for packet forwarding, and those which are not close to the routing vector (i.e., the axis of the pipe) do not forward. Fig. 1 illustrates the basic idea of VBF. In the above figure, node S_1 is the source, and node S_0 is the sink. The routing vector is specified by S_1S_0. Data packets are forwarded from S_1 to S_0. Forwarders along the routing vector form a routing pipe with a pre controlled radius (i.e., the distance threshold, denoted by W).As we can see, like all other source routing protocols, VBF requires no state information at each node. Therefore, it is scalable to the size of the network. Moreover, in VBF, only the nodes along the forwarding path (specified by the routing vector) are involved in packet routing, thus saving Security Issues and Solutions in UWSNs.

1.3 Various security parameters in UWSNs

Various security parameters are [3]:

Confidentiality: An attack on the confidentiality of information means theft or unauthorized access of data. This can be performed in lots of ways, such as the interception of data while in transit or it can be simply the theft of equipment on which the data might reside. The goal of compromising confidentiality is to obtain proprietary information, user credentials, trade secrets, financial or healthcare records or any other kind of sensitive information. Attacks on the confidentiality of wireless transmissions are created by the simple act of analyzing a signal travelling through the air.

Availability: Availability is allowing legitimate users access to confidential information after they have been properly authenticated. When availability is compromised, the access is denied for legitimate users because of malicious activity such as denial of service (DOS) attacks. Receiving RF Signal is not always possible, especially if someone does not want you to. Using a signal jammer to jam an RF signal is a huge problem that has been faced by national governments for years.

Integrity: Integrity involves the unauthorized modification of information. This could mean modifying information while in transit or while being stored electronically or via some type of media. To protect the integrity of information, one must employ a validation technique. This technique can be in the form of checksum, an integrity check, or a digital signature. Wireless networks are intended to function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system.

1.4 Various attacks in UWSNs

Denial of Service (DoS): A Denial of Service attack in sensor networks and networks in general is defined as any event that eliminates the network's capacity to perform its desired function. DoS attacks in wireless sensor networks may be carried out at different layers like the physical, link, routing and transport layers. [4], [5].This occurs by the unintentional failure of sensor nodes. The simplest DoS attack tries to exhaust the resources available to the victim node, by transmitting additional unwanted packets and thus prevents legitimate sensor network users from tapping work or resources to which these nodes are deployed [6]. Denial of Service (DoS) attack is means that not only for the adversary's attempt to subvert, disrupt, or destroy a sensor network, but also for any event that diminishes a sensor network's capability to provide a service [7].In WSNs, several types of Denial of Service attacks in different layers might be performed. i.e. at physical layer, the Denial of Service attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and resynchronizations.

Wormhole attacks: A devastating attack is known as the wormhole attack, where more than two malicious colluding sensor nodes does a

virtual tunnel in the wireless sensor network, which is used to forward message packets between the tunnel edge points. This tunnel establishes shorter links in the network. In which adversary documents forwards packets at one location in the sensor network, tunnels them to different location, and re-forwards them into the sensor network. In sensor network when sender node sends a message to another receiver node in the network [1].Then the receiving node tries to send the message to its neighboring nodes. The neighbor sensor nodes assume that the message was sent by the sender node (this is normally out of range), so they tries to forward the message to the originating node, but this message never comes because it is too far away. Wormhole attack is a great threat to sensor networks since, this type of attack will not require compromising a wireless sensor in the network instead; it could be performed even at the starting phase during the sensors initializes to identify its neighboring information [7]. This Wormhole attacks are very difficult to stop since routing information given by a sensor node is very difficult to check. The wormhole attack is possible even when the attacker has not compromised with any hosts nodes and even if all communication provides confidentiality and are authenticated also.

Sinkhole attack: In this case a compromised sensor node tries to influence the information to it from each and every neighboring node. Thereby, sensor node eavesdrops on each and every information is being communicated with its neighboring sensor nodes.

1.5 Intrusion Detection System

Information Systems and networks are vulnerable to electronic attacks. Underwater Sensor Networks are vulnerable to a large variety of attacks. To prevent a network, first and foremost important thing that is helpful is an Intrusion Detection System (IDS) which can be used for both wired as well as wireless networks. The challenges in designing an IDS for Underwater Sensor Network are much more than any other network due to the fact that it is dynamic in nature, decentralized nature, and access to radio medium. Thus the intrusion detection system of Underwater Sensor Network needs to be different from that of the wired networks.

The main purpose of Intrusion detection system is not to prevent attacks but to alert network administrator about the possible attacks so that they can be detected in time and hence their effect can be reduced. An IDS differentiates the aberrant activities from normal one and identifies the malicious activities from abnormal but non-malicious activities.

The accuracy of IDS is measured in terms of false positives i.e. the normal activities which have been reported as malicious and false negatives i.e. an attack which has not been detected by the IDS.

2. PROBLEM DEFINITION

The following two problems we have proposed here deal that can be linked together with them to give out the desired results:

1) Underwater sensor networks should be secure and reliable in such a manner that they do not defeat the purpose of data acquisition.

2) Underwater sensor networks are prone to malicious data attacks as they are based on sensing data which is RF based since they can be contacted/ communicated from any other signal in device which may be malicious in intent.

3. RESEARCH METHODOLOGY

This paper is based on the following research methodology. There are four main steps in UWSN's Threat Analysis:

1) Study of UWSN

2) Deploy a UWSN using VBF Protocol

3) Data transmission and correction

4) Compare the results before and after attack

Step One: In the first step study of Underwater Sensor Network is done. Various properties of Underwater Network are studied over the Terrestrial Network. These properties are Underwater Network is highly dynamic, prone to errors, low bandwidth and high latency. Above all there are various properties of Underwater Network like Environmental monitoring, undersea explorations, Distributed tactical surveillance, assisted navigation, Disaster prevention, Mine reconnaissance. Under the study of UWSN it has been studied that energy constraint is a crucial factor since sensor nodes usually run on battery, and it is impossible or difficult to recharge them in most application scenarios. In underwater sensor networks, in addition to energy saving, the routing algorithms should be able to handle node mobility in an efficient way. Various threats of UWSNs have also been studied like Denial of Service, Wormhole attacks, Sinkhole attack, Sybil Attack, Hello flood attack and the countermeasures against these attacks have also been studied. Various protocols of UWSNs has also been studied.

Step Two: After the study of UWSN, a network is deployed using VBF protocols. There are many other protocols of UWSNs and it has been studied

in the previous step that

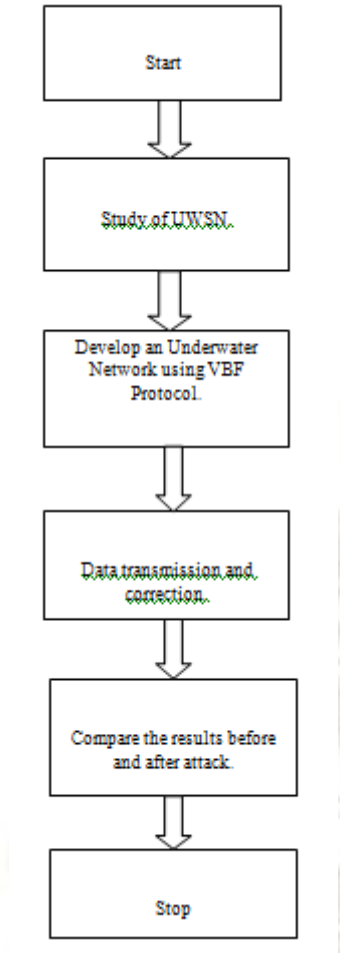

Fig. 2: Algorithm for the UWSN's Threat Analysis

VBF is the most robust, scalable and energy efficient. In VBF, each packet carries the positions of the sender, the target, and the forwarder (i.e., the node which transmits this packet). The forwarding path is specified by the routing vector from the sender to the target. Upon receiving a packet, a node computes its relative position to the forwarder. Recursively, all the nodes receiving the packet compute their positions. If a node determines that it is sufficiently close to the routing vector (e.g., less than a predefined distance threshold), it puts its own computed position in the packet and continues forwarding the packet; otherwise, it simply discards the packet. In this way, all the packet forwarders in the sensor network form a "routing pipe": the sensor nodes in this pipe are eligible for packet forwarding, and those which are not close to the routing vector (i.e., the axis of the pipe) do not forward.

Step Three: After the deployment of network, the network starts transmitting the data by checking the minimum Angle of Arrival and Desirable Factor. Then the network checks whether the channel is free or not. If the channel is free the sending and receiving nodes exchange keys and start sending data and receiving acknowledgement. There is a malicious node in the network which hacks the data and does not send any acknowledgement to the sending node when Denial of Service (DoS) occurs in certain nodes.

Step Four: When the attack occurs in the network, the various parameters like Packet Delivery Ratio (PDR), Packet Lost Ratio (PLR), Throughput and checksum errors have been studied, compared and plotted for before and after attack.

4. RESULTS AND DISCUSSION

Fig. 3 shows the Throughput vs. Message Arrival Rate for normal run or before attack and after attack. Throughput is the no. of bits per slot. It is shown in the following figure that no. of bits per slot for normal run is more than no. of bits per slot after the attack has been occurred.

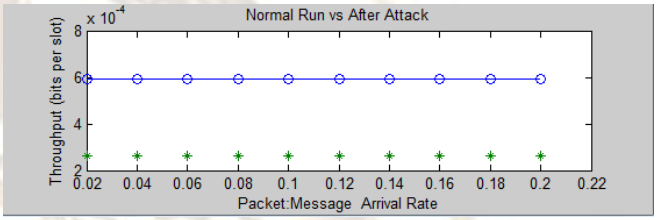

Fig. 3: Throughput vs. Message Arrival Rate

Fig. 4 shows the Packet Delivery Ratio (PDR) between two sensors. It is clear that packet delivery ratio is more in normal run condition and when the attack occurs the packet delivery ratio start decreasing.

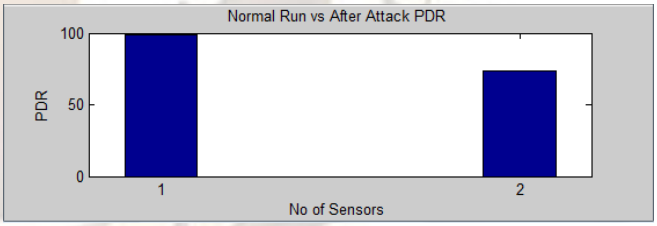

Fig. 4: Packet Delivery Ratio

Fig. 5 shows the Packet Loss Ratio between two sensors. It is exactly opposite of Packet Delivery Ratio. It is show in the figure that there is loss in packets when the attack occurs.

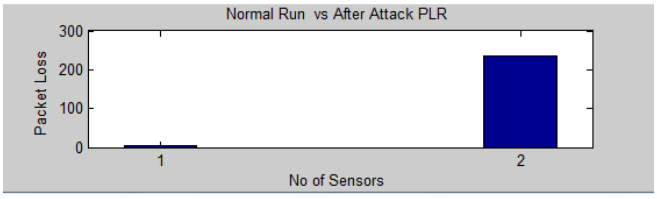

Fig. 5: Packet Loss Ratio

Fig. 6 shows the Check Sum Errors for normal run and after attack. It is clear from the following fig. that checksum errors are more in after attack condition.

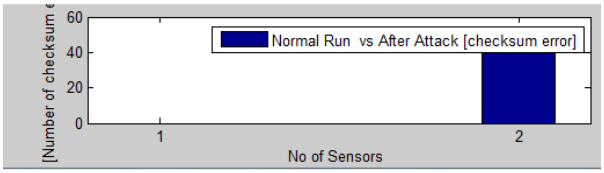

Fig. 6: Checksum Errors

6. CONCLUSION

In this paper it has tried to explore the possibility of threats of Underwater Sensor Network, as we progress we found the most prominent attack which might occur in Underwater Sensor Network which might occur in Underwater Sensor Network might be related to resource constraints. These resource constraints are natural due to nature of Underwater Sensors which cannot be supplied with recharging of power/energy. Therefore when nodes communicate with each other even in an efficient routing protocol like VBF, there is a possibility that a node might behave maliciously or may indefinitely continue to communicate with each other and at the same time deny services to other nodes. In this simulation it has been demonstrated the same scenario and observed before and after attacks on the network. These before and after attack observation were made by recording the trace of each event occur in simulation. By using this trace we identified few parameters based on which we could identify abnormal behavior in the network. These include Check Sum error, Packet Delivery Ratio, Packet Lost Ratio and Throughput. It is apparent from the bar graph shown above that these values drastically change if an attack is accused which shows abnormal behavior in the network.

7. FUTURE SCOPE

The research for detection of such scenarios which are related to the attack on services are limited due to resource constraints or external manipulations of the node which turns maliciously in nature. For future scope it has been suggested that more scenarios must be considered and some Intrusion Detection System must be designed so that we can have secure Underwater Sensor Networks.

REFERENCES

[1] J. G. Proakis, E. M. Sozer, J. A. Rice, and M. Stojanovic, "Shallow water acoustic networks," *IEEE Communications Magazine*, pp. 114–119, Nov. 2001.

[2] Peng Xie et.al," Efficient Vector-Based Forwarding for Underwater Sensor Networks", *EURASIP Journal on Wireless Communications and Networking Volume 2010*, Article ID 195910, 13 pages.

[3] J.-P. Hubaux,S. C˘apkun, and J. Luo. The Security and Privacy of Smart Vehicles. *IEEE Security & Privacy*, pages 49–55, 2004.

[4] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer, vol. 35*, no. 10, pp. 54–62, October 2002.

[5] M. Lee, E. J. Kim, and C. W. Lee, "Source identification scheme against DoS attacks in cluster interconnects," in *Proc. International Workshop on Network Design and Architecture*, Montreal, Quebec, August 2004, pp. 354–362.

[6] A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," *Computer, vol. 35*, no. 10, 2002, pp. 54–62.

[7] David R. Raymond and Scott F. Midkiff, (2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, 2008, pp. 74-81.

[8] Adrian Perrig, John Stankovic,," Security in wireless sensor networks". *ACM Communication*, 47(6): 2004, pp. 53-57.

[9] Zaw Tun and Aung Htein Maw,(2008)," Worm hole Attack Detection in Wireless Sensor networks", proceedings of *world Academy of Science, Engineering and Technology Volume 36*, December 2008, ISSN 2070-3740.

[10] Denning D.(1987) "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, Vol.SE-13, No 2, pp. 222-232.