INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

# A NOVEL APPROACH TO DETECT BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK

**Kamalpreet Singh[1], Gaganjot Kaur Aulakh[2]**

[1,2]Baba farid college of engineering and technology, Bathinda.
[1]kamalbathinda@yahoo.com, [2]er.gaganaulakh@gmail.com

***Abstract:*** *Networking is used to share information like data communication. A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium. Under Water acoustic Networks term is refers to a kind of networking that do not requires cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level. In the underwater sensor study the different characteristics of quality of water, temperature, density, salinity, acidity, chemical conductivity, hydrogen, dissolve methane gas and turbidity. In this paper, we are going to prevent the black hole attack. With this prevention we can enhance the lifetime and performance of network.*

***Keywords:*** *Acoustic Network, Wireless Sensor Network, black hole attack, AODV.*

## 1. INTRODUCTION

Ocean bottom sensor nodes are deemed to enable applications for oceanographic data collection, pollution monitoring, offshore exploration, disaster prevention, assisted navigation and tactical surveillance applications. Multiple Unmanned or Autonomous Underwater Vehicles (UUVs, AUVs), equipped with underwater sensors, will also find application in exploration of natural undersea resources and gathering of scientific data in collaborative monitoring missions. To make these applications viable, there is a need to enable underwater communications among underwater devices. Underwater sensor nodes and vehicles must possess self-configuration capabilities, i.e., they must be able to coordinate their operation by exchanging configuration, location and movement information, and to relay monitored data to an onshore station.

Wireless underwater acoustic networking is the enabling technology for these applications. Under Water Acoustic Sensor Networks (UW-ASN) consist 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.

**Underwater sensor:** Internal structure of underwater sensor it consist of main controller, it can be interfaced with oceanographic instrument through interface circuitry. Controller receives data from the sensor through a sensor interface circuitry after stored data processed it, and send it to other network devices by the acoustic modem. The electronics are usually mounted on frame which is protected by PVC housing. All sensor components are protected by bottom-mounted instrument frames that design to permit azimuthally Omni directional acoustic communications which prevent from the fishing activity. In the protecting frame is designed to deflect trawling gear by housing all components beneath a low profile pyramidal frame. In the underwater sensor study the different characteristics of quality of water, temperature, density, salinity, acidity, chemical conductivity, hydrogen, dissolve methane gas and turbidity [2].

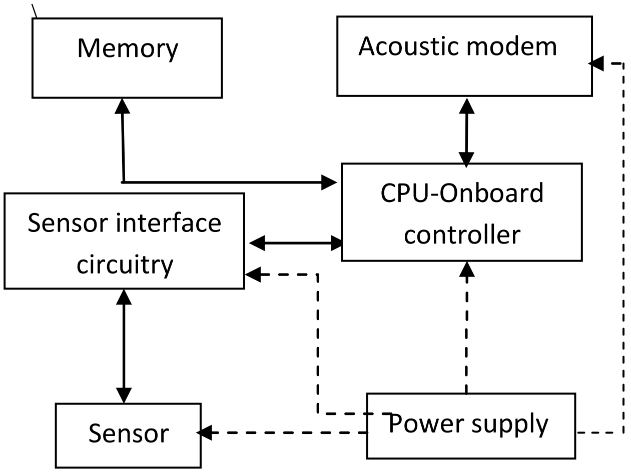

**Figure 1:** Internal architecture of an underwater sensor node

Underwater networking is a rather unexplored area although underwater communications have been experimented since World War II, when, in 1945, an underwater telephone was developed in the United States to communicate with submarines. Acoustic communications are the typical physical layer technology in underwater networks. In fact, radio waves propagate at long distances through conductive sea water only at extra low frequencies (30-300 Hz), which require large antennae and high transmission power. Optical waves do not suffer from such high attenuation but are affected by scattering. Moreover, transmission of optical signals requires high precision in pointing the narrow laser beams. Thus, links in underwater networks are based on acoustic wireless communications.

The traditional approach for ocean-bottom or ocean column monitoring is to deploy underwater sensors that record data during the monitoring mission, and then recover the instruments. This approach has the following disadvantages:

**Real time monitoring is not possible**. This is critical especially in surveillance or in environmental monitoring applications such as seismic monitoring. The recorded data cannot be accessed until the instruments are recovered, which may happen several months after the beginning of the monitoring mission.

**No interaction is possible between onshore control systems and the monitoring instruments.** This impede any adaptive tuning of the instruments, nor is it possible to reconfigure the system after particular events occur.

**If failures or mis-configurations occur, it may not be possible to detect them** before the instruments are recovered. This can easily lead to the complete failure of a monitoring mission.

**The amount of data that can be recorded during the monitoring mission by every sensor is limited** by the capacity of the onboard storage devices (memories, hard disks, etc.).

Therefore, there is a need to deploy underwater networks that will enable real time monitoring of selected ocean areas, remote configuration and interaction with onshore human operators. This can be obtained by connecting underwater instruments by means of wireless links based on acoustic communication.

Many researchers are currently engaged in developing networking solutions for terrestrial wireless ad hoc and sensor networks. Although there exist many recently developed network protocols for wireless sensor networks, the unique characteristics of the underwater acoustic communication channel, such as limited bandwidth capacity and variable delays, require for very efficient and reliable new data communication protocols.

Major challenges in the design of underwater acoustic networks are:

- Battery power is limited and usually batteries cannot be recharged, also because solar energy cannot be exploited;
- The available bandwidth is severely limited;
- Channel characteristics, including long and variable propagation delays, multi-path and fading problems;
- High bit error rates;
- Underwater sensors are prone to failures because of fouling, corrosion, etc.[1]

## 2. RELATED WORK

Pradeep kyasanur et. al. Proposed a protocol extension of 802.11 DCF protocol to detect the selfish behavior of the nodes in the infrastructure and ad hoc network topologies. Selfish nodes means the nodes which select the contentional window (CW) time in such a way so that the other nodes are keep on waiting to send the data and overall through put of the network degrade [3]. The proposed scheme has three components first one is that the receiver decides that whether sender is diverting form protocol or not. Second component is penalize ,in this scheme the receiver assigns the contentional window time to the sender if sender not sends data in that time period sender have to pay the plenty. Plenty means that in next time when sender sends that data they have to wait more to send data to receiver .The third component is the diagnosis scheme receiver decide whether the sender is selfish or not on the basis of the total data send by the sender and number of times the sender pay plenty .if no of plenty paid by the sender is more than the threshold value which is fixed then the sender is selfish and no more data is received form that sender.

Yixin Jiangand et. al In this paper they have proposed a new mutual authentication and key exchange protocol. The two main features of this protocol is identity anonymity and session key renewal. This protocol provides secure roaming services to the legitimate user between the home and visiting agent or in short, this protocol provides secure handoff to the legitimate user [4]. The proposed protocol is based on the secrete splitting principle and self-certified scheme. The protocol works in two phases: First phase is the mutual authentication with anonymity which hides the use's real identity when a legitimate user is roaming from the home agent to the visiting agent. This phase use the temporal identity (TID) instead of the user's real identity. Second phase is the session key renewal phase which renews the shared key which is shared between the legitimate user and the serving agent.

Sushma Yalamanchi and K.V. Sambasiva Rao, They had proposed a two stage authentication scheme for wireless networks. They discus that in wired network use the authentication protocol which is having large computations but in wireless networks we require less computation and energy efficient authentication protocol .Because in wireless networks the hand held devices are having limited battery and limited computational resources also wireless networks on suffer from packet losses and bit errors and offers low bandwidth [5]. In the paper, they presents a two-stage authentication scheme for wireless networks that uses a computationally intensive but highly secure strong authentication in Stage 1 and a lightweight symmetric key based protocol in Stage 2. The cost of the strong authentication adopted in Stage 1 is amortized over N sessions thus reducing the overall cost of the scheme. We adapt the Dual-signature based IKE authentication that we proposed in our earlier work and employ it as Stage 1 authentication. The Symmetric key protocol in Stage 2 authentication that we propose uses the symmetric keys that are generated in Stage 1.

## 3. PROPOSED WORK

In the acoustic sensor network integrated acoustic sensor nodes were deployed in the monitoring area all kind of targeted environment information gathered by the cooperative nodes. In this scenario mainly study the existing localization and different routing schemes in the sensor network. In this network also study about the different underwater sensor network is defined within the parameters. Use the different parametric approaches for nodes localization in the network. With the help of different aggregation and multicasting concept used to define the network. In this scenario also discuss some concept of black hole node. In the network when black hole node occur it does not pass the data to the destination at that position packet is drop and nodes energy also reduce. In this problem define the intermediate disseminate node which sent acknowledge to source regarding the data and pass to destination if some case not respond source find the other path to sent data from source to destination.  Whole scenario implemented on the network simulator.

## 4. METHODOLOGY

This method uses the fake RREQ message to attract the malicious node to respond the fake RREP message. In our scenario, there is more than one malicious node who will reply the fake RREQ packet.

a) In this mechanism, before discovering the actual route for data transmission in AODV, a fake RREQ packet is broadcasted which includes the target or destination address which does not exist in reality.
b) The multiple black hole nodes will immediately respond to the fake RREQ packet as they do not care about whether the fake target addressed node exists or not in the network. Then, the RREP packet will be sent by those black hole nodes.
c) The RREP packet is here enhanced by adding one more field as Record Field using the reserved bits of RREP packet. This field is used to contain the information about the identity of the node who replies the RREP packet to the source node. When any node in the network reply RREP packet, its identity will be recorded into Record field. So, if any intermediate node sends the RREP packet in response to the fake RREQ, it can be easily traced or detected.

In fig. 2, we have three black hole nodes located at different places in the network named as 1, 4 and 6. Before the initiating the actual route discovery process in AODV, the source node broadcast the fake RREQ message with fake target address of node T (non-existent node) to the neighboring nodes 1, 3 and 5.

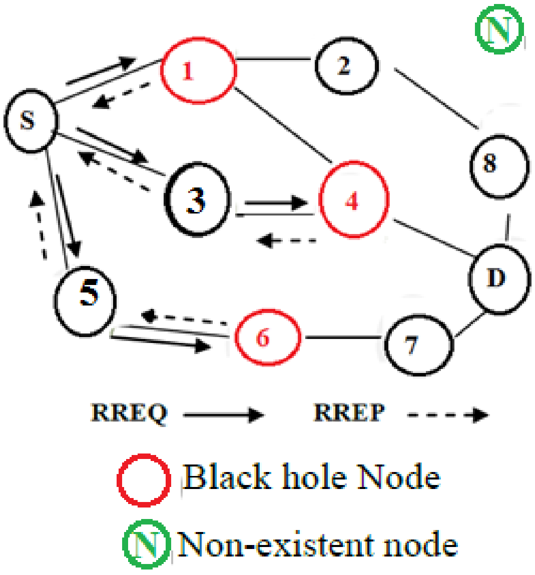

**Figure 2:** Sending fake RREQ packet

d) The normal nodes having no malicious behavior will not reply to the fake RREQ message as they have no route to that virtual node T.  The malicious nodes 1, 4 and 6 will reply the RREP packet as advertising the shortest path towards the destination node (T).
e) The identity of these nodes will be recorded into the Record field of the RREP packet. When the source node S receives the multiple RREP packets, from the Record field it will be able to trace the identity of malicious nodes.
f) These identities will be added to the black list and this list will be broadcast as an ALARM packet to all the nodes in the network. Then, these multiple black hole nodes will be isolated from the network. After isolating the multiple black hole nodes, the normal route discovery process in AODV will be initiated. The data is then routed to the destination.
g) If the packet delivery ratio is down to some threshold value that has been decided on the basis of average packet delivery ratio (threshold value).
h) Also, the end to end delay is checked if it is more than the average end to end delay of data packets, then there will be chances of attack.
i) The threshold values for packet delivery ratio and end to end delay is taken as the average of normal PDR and end to end delay of data packets respectively.
j) Normal Operation of AODV.
k) If(packet delivery ratio<threshold_value1 and end to end delay>threshold_value2)
l) Then, again the source node will restart the process of broadcasting fake RREQ packet to detect the single or multiple black hole nodes.

The detection of single or multiple black hole nodes have done early before initializing the route discovery process in AODV. It makes this method more effective. After the detection process, there is an additional check to find out the packets are again dropped or not during normal transmission of data packets after normal route discovery process. This additional check is calculating the packet delivery ratio, if it comes down to some threshold value (average PDR). And also, if end to end delay, the time taken for the data packets to transfer from source to destination, is more as compare to the average end to end delay of data packets (threshold_value2). Then, there is the maximum chance of existence of black hole nodes. Again, the detection mechanism will be started.

## REFERENCES

**[1] http://www.ece.gatech.edu/research/labs/bwn/UWASN/**

**[2] ABDUL HAIMID BASHIR MOHAMED, thesis, “ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS”2004**

**[3] Pradeep kyasanur “Selfish MAC layer Misbehavior in wireless networks”, IEEE on Mobile Computing,2005**

**[4] Yixin Jiang Chuang Lin, Minghui Shi, Xuemin Shen “Multiple Key Sharing and Distribution Scheme With (n; t) Threshold for NEMO Group Communications”, IEEE 2006**

**[5] Sushma Yalamanchi and K.V. Sambasiva Rao“TWO-STAGE AUTHENTICATION FOR WIRELESS NETWORKS USING DUAL SIGNATURE AND SYMMETRIC KEY PROTOCOL” International Journal of Computer Science and Communication (IJCSC), n Vol. 2, No. 2, July-December 2011, pp. 419-422.**