Improvisation of underwater wireless sensor network's efficiency for secure communication

Kotari Salini[1] **and M.B Mukesh Krishnan**[2]

[1]Student, SRM Institute of science and technology, Chennai, India
[2] Asst. Professor (Sr.G), SRM Institute of Science and Technology,
Chennai, India

*Corresponding Author: kotarisalini@gmail.com

Abstract. Earth is covered with land and water in that 2/3 rd of earth is covered by water bodies which includes both salt water and fresh water as well. Since water is a major component of the earth, it is necessary to understand about the water bodies and under water sensors will be helpful for it. Under water wireless sensor networks are used widely for oceanographic data collection such as abnormalities which cause natural calamities, to track other submarines (navigation and surveillance) and also pollution level in water. The major limitations of underwater wireless sensor networks are battery power, limited bandwidth, multi-path, fading problems, high bit error rates, propagation delays and also they are more prone to corrosion, foul forming etc., these limitations prove that they have fewer lifetimes compared to TWSN's. Due to the limitations and requirements of these UWSN's, are required to use Ultra light weight components. The major physical layer attacks of underwater wireless sensors are jamming and eavesdropping [4]. Due to eavesdropping data not only losses confidentiality but further may leads to other malicious attacks which losses both availability and integrity of data. The fundamental problem of underwater wireless sensor networks is to provide security which is highly efficient but uses less space, less computations and low bit rates. Therefore the security techniques used for terrestrial wireless sensor networks based on all the above stated reasons are not at all suitable for UWSN's.

Researchers are still trying to provide better security using an encryption technique with limited computations and less storage space. As far as now the latest efficient ultra lightweight encryption schema provides the better security with lower computations by using chaotic theory to generate the random key but it requires high storage space which is not accurate for underwater sensor network communication. So we do implement basic block cipher with combination of left, right shift, substitution and XOR operations for lower computations with key generated randomly using Pseudo Random Number Generator in order to reduce the storage space for key spaces and also splitting the process of encryption rounds according to the number of hops required to transmit from source node to destination node in between the sensor and the base station onshore, provide security for the data communication through underwater wireless sensor networks. Thus for decrypting the data, an attacker needs to know about the number of hops also along with the keys used for encryption which makes the process of encryption better secured than existing in UWASN.

Keywords: Underwater · Sensors · Acoustics · Encryption ·Ultra-Lightweight · Wireless network · UIoT

1. Introduction

Underwater sensor networks are group of separate sensor nodes, which are distributed deep inside the water bodies to sense the anomalies in the water and sends data to intended nodes. 75% of this earth's surface is covered by water in various forms like ponds, rivers, canals, seas and oceans. In order to explore the vast area underwater we are using this new technology implementation of IOT underwater. Many research's are going on to develop UNWSN's that increases the application which are used to get details regarding pollution, surveillance, disaster management, military usage etc., underwater[6,13,18]. Sensors are very small electronic devices which detects the change in the environment around it to a specific distance based on its programming. In general sensors are specialised to detect aspects like light, temperature, climatic change, motion, pressure, sound etc[19] A wireless network uses wireless data connections between network nodes. Due to its small size and wireless communication terrestrial wireless approaches to transfer and secure data in UWSN is not suitable.

Terrestrial wireless sensor networks uses radio frequency waves to transmit data where UWSN uses Acoustic waves to transfer data. Due to the limitation of UWASN like lower battery, higher bit error, lower bandwidth, Acoustic Communication, lower memory space, energy efficiency, more vulnerable to attacks etc., existing work for TWSN unsuitable for UWAN challenges for security [7,14]. So ultra-lightweight encryption schema evolved [12,17] which encrypts the contents of communication in UWASN. It provides integrity and confidentiality in between nodes using less space and provides high security with lower computations. The encryption schema should satisfy challenges of underwater like it should be adoptable for underwater transmission, lower computation with less overhead, cost and energy efficient and ensure high security [9].

2. Related Work

2.1. Architecture of sensors underwater

Basic internal architecture of underwater sensors is shown below. This has components like controller, sensor interface circuitary, memory, acoustic modem, power supply and sensor [11].

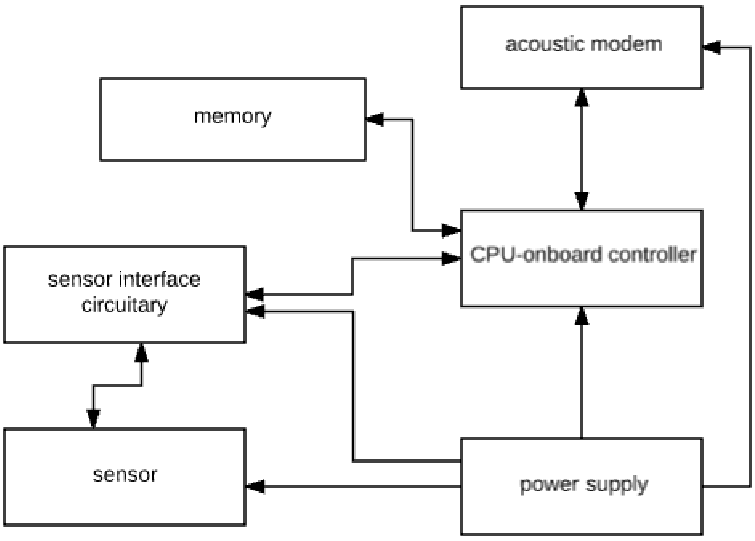

Figure 1. Architecture of underwater sensor

The CPU controller will get the information from sensor through sensor interface circuitry which are stored in memory and process it and sends to another sensor through acoustic modem.

2.2. Network Architecture of Underwater Sensors

UWSN has different types of architectures based on different aspects. One classification based on static, semi-mobile and mobile network. Other popular classification is based on dimensions i.e., two-dimensional and three dimensional. UWSN also classified based on hops like single hop, multi-hop or hybrid. Fig2 shows the UWSN 3D architecture, which are used to detect the phenomena that cannot be accurately done using two-dimensional architecture. In 2D architecture nodes or sensors are anchored to ocean bottom where as in 3D architecture sensors are hanged from ocean bottom with different length of strings anchored to ocean beds which considers the depth as third dimension [12].

The below network include sensors which are placed in underwater and classified in clusters with one cluster head for each which has higher battery power and computational strength. These cluster heads connected with master nodes and underwater sinks and these underwater sinks and master nodes can be connected to base nodes which are onshore, thus the transmission in UWASN is done.

Group of sensors are clustered and communicates with its cluster heads. Each cluster head has two acoustic transceivers, vertical and horizontal transceiver. Horizontal transceiver communicates with sensors using horizontal acoustic modes either in single hop or multi hop where vertical transceivers communicates with base stations by underwater sinks.

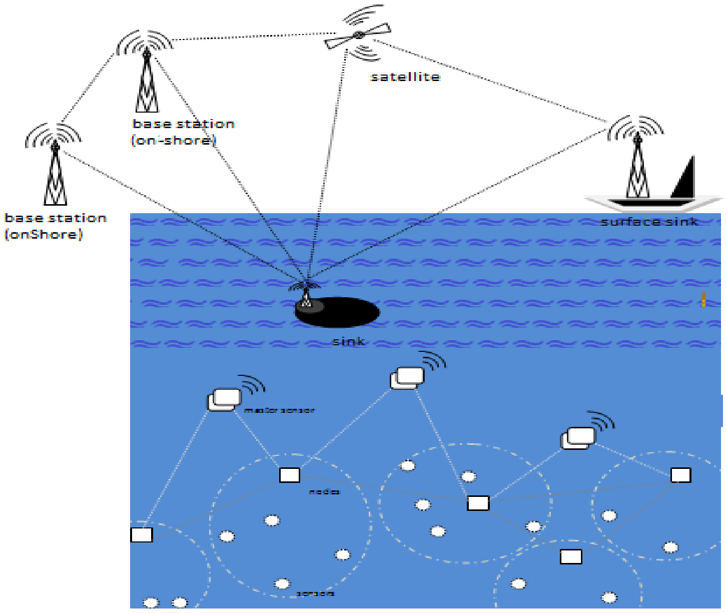

Figure 2. 3D architecture of underwater sensors

Sensors communicates with cluster heads to sink to base station (parallel communication) using these transceivers. Cluster heads sends commands and configures data to sensors, collects the monitored data from sensors. Use of these transceivers and hops results in energy saving and to increase the network capacity [6].

2.3. Challenges in underwater sensors

Expensive devices.

Underwater sensors are costly compared to terrestrial sensors because of limited supply.

Physical damage.

UWSN is more expensive so need to be physically protected from fouling, corrosion, marine animals etc.

Battery power.

The lifetime of USWN is much shorter compared to TWSN and they are not chargeable which increases replacement costs.

Higher bit error.

UWSN has high bit error ratio due to its environment and wireless network.

Propagation delay.

In order to transmit the data from node to node if network chooses the optimal path, sensors of UWSN are not suitable because it need more energy to transmit the data from more distance so it opts to choose to send to nearest node which leads to maximum hops increases the time taken to reach destination.

Limited Bandwidth.

Bandwidth is the bit rate available. UWSN have very less bandwidth due to the use of acoustic signals.

Localization.

If the place of node changes or node at a point damaged whole UWSN data communication effects so reliability and security are the major issues here [4,10,14].

3. Proposal Statement

Water is the most dominant part of earth. So it is necessary to know about what is happening underwater. Underwater wireless sensors are building up now a day's which are highly useful for developing application that collects the data underwater such as oceanographic data which might be useful to know the pollution condition and marine life underwater, for military purpose and submarines, for details regarding natural calamities etc., UWSN are not suitable with the protocols, encryption and transmission scheme of TWSN's, because TWSN uses ad-hoc network where underwater uses acoustic network for signal transmission, TWSN's uses light weight encryption scheme's which are heavy for UWSN's which has very lower memory space, low powered batteries, high bit error rates, propagation delays and soon, so after many experimental researches they came up with ultra-light weight encryption scheme which will reduce computational and storage space and also reduce battery consumption by providing security and lowering error bit rates comparatively.

UWSN uses ultra light weight encryption schema .In the existing block encryption algorithm, S-box it is more unsuitable for resources-constrained UANs because it consumes more energy. A lightweight, n-round iteration block cipher algorithm for UANs communication which did not reduced the storage space is been used instead of S-box .So we use an ultra lightweight encryption scheme which generates key using general PSRG and perform n-round substitution and row shift of block cipher algorithm, as number of rounds of iteration depends on the number of hopes required to transmit the data from source to destination data is secured better and the computation power required to encrypt the data is also shared by different nodes which reduces the storage space required for encryption process.

4. The Encryption Algorithms of UWASN

Recently many lightweight ciphers which use less storage space and memory space for computations and key management, low power consumption. Lightweight ciphers like piccolo, Simon and Speck, present are having the robust design and gate equivalence (GE) needs less than 2200 for implementation. simon & speck cypers are considered to be most ultralight weighted ciphers till today which are been launched by National security agency (NSA) because of their robust design and key scheduling. We aimed at compact design and robust network cipher which not only needs less storage space or memory but also need to take care of the other factors like battery utilized, throughput and the attacks. Present ultra light weight cipher has the bit permutations as its P- layer which only requires wires for its hardware implementation [2,3,8,18]. The encryption scheme of ultra light weight is discussed here which is suitable for underwater wireless sensor network which consumes lower energy and lower space required to perform computation and key management respectively.

The design of this algorithm has 32 bit pseudo random key and 64 bit plain text and 4 rounds of iteration at every node in the transmission path.

4.1. Dataflow diagram

The data sensed by the sensors by data loggers are been broad casted to the sensors in the cluster. The other sensors gets the id and group id of the sensor and if that id belongs to the sensor group the link is setup and data is transmitted between the sensors in a cluster.

Similarly data is transmitted between all the nodes in the sensor based on the path selected by the beacon signals generated by the tinyOS [16]. The routing protocol for selection of nodes is done using ENMR protocol [14] which is stated as best routing protocol to today for Underwater wireless sensors acoustic network.

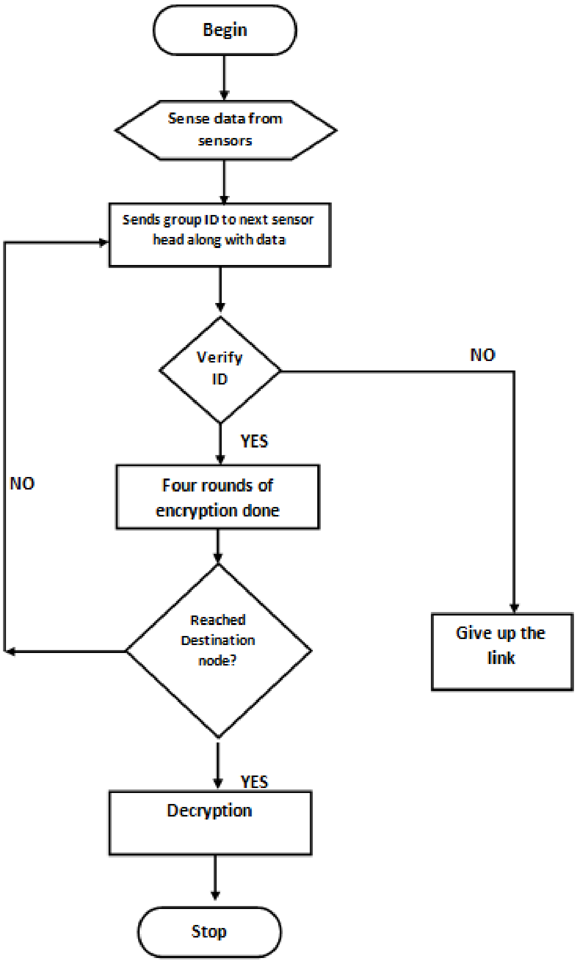
Begin
Sense data from sensors
Sends group ID to next sensor head along with data
Verify ID
NO
YES
Four rounds of encryption done
NO
Give up the link
Reached Destination node?
YES
Decryption
Stop

Figure 3. Data Flow diagram for process of authentication of cluster head

4.2. Block diagram

Message is divided in 64 bit of each block and added with the round key generated by Pseudo Random key generator[8] and 4-rounds of iteration is done which has XOR of random number, substitution by s-box and row shift then again round key will be added and cipher text is forwarded to next node.

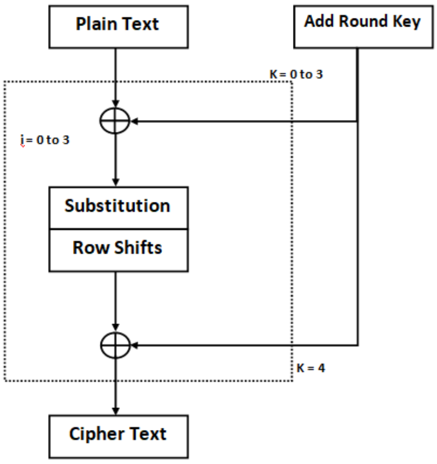

Figure 4. Encryption process

4.3. Algorithm

Plain text of 64 bit is written in 8-bytes from P0 to P63and is done XOR with 4-byte Random number which are been generated by the PRNG algorithm called by the function Roundkeys() and the continuous four rounds of XOR of random number , substitution of bytes by S-box and shift rows will happen at one node in the routing path from source to destination.

```
Step 1: select the next node in path.
Step 2: plain text is splited into 64 bits, let it be Pi, Where i=0 to 63
Step 3: call Round keys function
        Step 3.1: At every node, for 4 rounds do,
                Step 3.1.1: add a round key
        Step 3.1.2: substitution by using standard S-box.
Step 3.1.3: Shift rows
Step 4: add round key
Step 5: cipher text obtained and check whether it is destination node. If yes go to step 6, if no go to step 1.
Step 6: end
```

Along with the key pair required to perform encryption and decryption, the hop count is also added to key set and the key management can be done by either RSA or Diffie-Hellman [1].

5. Conclusion

An Ultra-lightweight encryption scheme is presented which results in decreasing the memory space, computational power consumption. This is very reliable for the UWASN’s which uses resource constraint devices or sensors.

6. References

[1] Alvarez R, Caballero-Gil C, Santonja J and Zamora A 2017 *Algorithms for Lightweight Key Exchange Sensors*, 17(7), 1517

[2] Bansod G, Patil A, Sutar S and Pisharoty N 2016 An ultra lightweight encryption design for security in pervasive computing In Big Data Security on Cloud (BigDataSecurity), *and IEEE International Conference on High Performance Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2nd International Conference on* (pp 79-84)

[3] Bogdanov A, Knudsen L R, Leander G, Paar C, Poschmann A, Robshaw M J, and Vikkelsoe C 2007 PRESENT: An ultra-lightweight block cipher Vol 4727 (In *CHES)* pp 450-466

[4] Cong Y, Yang G, Wei Z and Zhou W 2010 Security in underwater sensor network *In Communications and Mobile Computing (CMC), 2010* Vol 1 pp 162-168

[5] DiCarlo D F 2012 *Random number generation: Types and techniques*

[6] Das A P and Thampi S M 2015 Secure communication in mobile underwater wireless sensor networks *In Advances in Computing, Communications and Informatics (ICACCI)* pp 2164-2173

[7] Du X, Li M and Li K 2018 *Reliable Transmission Protocol for Underwater Acoustic Networks In Computer and Network Security Essentials* (Cham: Springer) pp 173-187

[8] Engels D, Fan X, Gong G, Hu H, and Smith E M 2010 Hummingbird: ultra-lightweight cryptography for resource-constrained devices *In International Conference on Financial Cryptography and Data Security* (Berlin, Heidelberg: Springer) pp 3-18

[9] Han G, Jiang J, Sun N and Shu L 2015 Secure communication for underwater acoustic sensor networks *IEEE communications magazine,* 53(8), 54-60

[10] Hu F, and Sharma N K 2005 *Security considerations in ad hoc sensor networks Ad Hoc Networks*, 3(1), 69-89

[11] Jadhav R 2017 Security Issues and Solutions in Wireless Sensor

Networks *International Journal of Computer Applications*, **162(2)**

[12] Kavar J M and Wandra K H 2012 *Survey paper on Underwater Wireless Sensor Network*

[13] Kim D, Cano J C, Wang W, De Rango F and Hua K 2015 *Underwater wireless sensor networks 2015*

[14] Li H, He Y, Cheng X, Zhu H and Sun L 2015 Security and privacy in localization for underwater sensor networks *IEEE Communications Magazine,* 53(11), 56-62

[15] Li Y, Jin Z, Su Y, Yang M and Xiao S 2017 An Environment-Friendly Multipath Routing Protocol for Underwater Acoustic Sensor Network *Journal of Sensors,* **2017**

[16] Nanda A, Rath A K and Rout S K 2010 Node sensing & dynamic discovering routes for wireless sensor networks *arXiv preprint arXiv:10041678*

[17] Pavithra S and Ramadevi M E 2012 Study and performance analysis of cryptography algorithms *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 1(5), pp-82

[18] Peng C, Du X, Li K and Li M 2016 An ultra-lightweight encryption scheme in underwater acoustic networks *Journal of Sensors,* **2016**

[19] Sensing and sensors : Acoustic Sensors : refered from Fraden : *Handbook of Modren sensors, Drafts, Acoustic Wave Sensors*

[20] Shi Y, Wei W, He Z and Fan H 2016 An ultra-lightweight white-box encryption scheme for securing resource-constrained IoT devices *In Proceedings of the 32nd Annual Conference on Computer Security Applications* ACM pp 16-29