Effective Security and Energy Aware Approach for Performance Augmentation of Underwater Sensor Networks

Pramod H B[1], Rajeev Kumar[2],

Abstract— Underwater Acoustic Networks are in research from a long time since the inception and integration of defense based applications. With the increasing terrorism based threats, it is mandatory to secure the submarines and underwater resources of national security so that the opponent adversary cannot damage or violate the region. This research work is having key focus on the security and integrity which is main aspects in any network based environment or distributed processing. A number of algorithms are devised so far for the integration of security and integrity so that the overall performance of underwater network can be enhanced still there is colossal scope of research as the vulnerability analysis is one of the domain that it taken by the cracking community. In this research work, a novel and effective cryptography approach is devised and implemented taking care of network defense and overall performance of underwater wireless network. The proposed system can be integrated on any type of network environment ensuring the security and effectiveness of data transmission. In this research work, a hybrid cryptography approach is devised to enrich and congeal the security during data transmission for security of defense submarines and merchant navy ships. In the proposed approach, the overall performance and security of system is extremely effective and giving better results than classical approach.

Keywords - Network Security, Dynamic Key Exchange, Network Defense

1. INTRODUCTION

A wireless network [1] comprises the set of virtually connected nodes for the key objective of data sharing or information dissemination. In wireless networks, there exist mobile nodes which are not physically connected but broadcast or share the resources to meet the common objectives.

Now days, the wireless networks are used everywhere including mobile phones, cloud applications, Internet of Things, personal digital assistants and many other applications related to personal, commercial and defense based domains.

The underwater sensor networks (UWSN) are used classically by the military bases or corporate navy (merchant navy) based applications.

Whenever, the transmission of goods or military objects are done there is need to make it secured so that any intruder cannot intercept the environment.

The modulation approaches in underwater acoustic communications includes Frequency Shift Keying (FSK), Phase Shift Keying (PSK), Frequency Hopped Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), Frequency and Pulse-position modulation (FPPM and PPM), Multiple Frequency Shift Keying (MFSK) and Orthogonal Frequency-Division Multiplexing (OFDM).

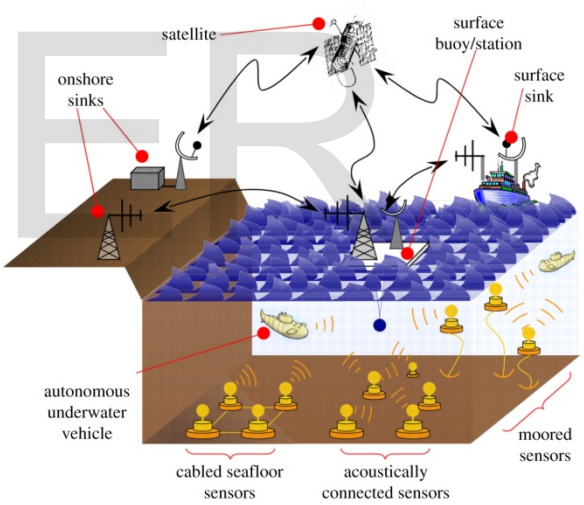

Figure 1 – Typical Flow of Information in Underwater Acoustic Networks

The wireless communication is typically processed and taken care using radio signals based transmission with higher efficiency and security.

This particular implementation is done at the physical layer in OSI reference model [2] of a classical network environment.

[1] *Research Scholar, Department of Computer Science & Engineering, Shri Venkateshware University,Gajroula,UP,INDIA*
hbpramod@gmail.com

[2] *Associate Professor, Department of Computer Science & Engineering, Shri Venkateshware University,Gajroula,UP,INDIA*
dr.r.kumar@ieee.org

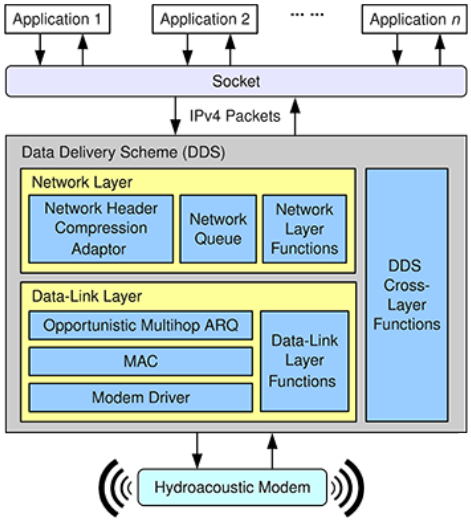

Figure 2 – Layered Approach of Underwater Acoustic Network

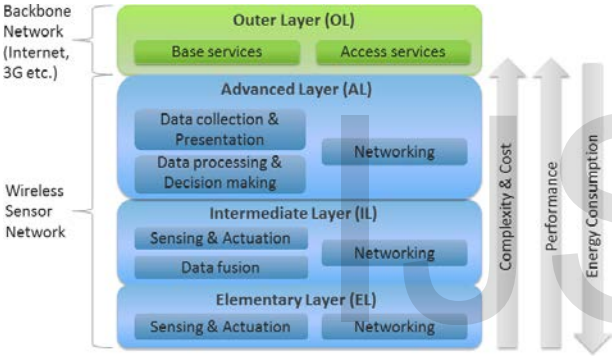

Figure 3 – Layered Approach of Services and Aspects in Wireless Networks [3]

The links and technologies associated with wireless networks include spread spectrum, cellular systems, communication satellites, microwave transmission, radio technologies, optical communications and many other technologies which work together in the secured and distributed environment.

2. FEATURES AND CHARACTERISTICS OF AN EFFECTIVE UNDERWATER WIRELESS NETWORK (UWSN)

- Expandable without Complexity
- Robustness and Autonomous
- Dynamic and Effective Load Balancing
- Scalability with Network Access Control
- Distributed, Arbitrary and Connected Operations
- Multihop based Routing
- Network Topology in Dynamic
- Network Scalability
- Light Weight Terminals
- Ease and Speed of deployment
- Decreasing dependency on infrastructure
- Mobility and Quality of Service
- Portability and Transportation

2.1 CHALLENGES AND RESEARCH ISSUES IN UNDERWATER WIRELESS ACOUNSTIC NETWORKS (UWSN)

- Interferences and Interceptions
- Hidden Node and Spy Problems
- Multipath Fading
- Resource Optimization
- Formation of Energy Aware Networks
- Capacity and Data Rate Issues

IEEE 802.11 STANDARDS

IEEE 802.11 [4] refers to a set of specifications devised by IEEE for the representation of **w***ireless* **LAN** (WLAN) technology. The standard 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. IEEE accepted this standard in year 1997.

Table 1- 802.11 Standards

Protocol / Standard	Classical Frequency (GHz)	Modulation
802.11 (Wireless LAN)	2.4	DSSS, FHSS
802.11 a (Wireless LAN)	5	OFDM
802.11 b (Wireless LAN)	2.4	DSSS
802.11 g (Wireless LAN)	2.4	OFDM
802.11 n (MIMO with Additional Transmitter and Receiver)	2.4/5	MIMO-OFDM
802.11 ac (MU-MIMO)	5	
802.11 ad Under Development with higher transfer rate	60	OFDM, single carrier, low-power single carrier
802.11 ah Wi-Fi HaLow	1	
802.11 r Fast Basic Service Set, VoIP, Vo-WiFi	5	Voice Over WiFi, VoIP Roaming

2.2 VULERABILITY AND SECURITY ISSUES

Wireless networks are susceptible and prone to assorted attacks at different layers from multiple sources and therefore it is required to understand the mechanism as well as taxonomy of attacks.

Using this approach, the effective system can be developed to guard the network against such attacks.

Following are the vulnerability aspects associated with the wireless network scenarios

3. ACCESS CONTROL ATTACKS

These assaults attempt to infiltrate a network by means of wireless or dodging WLAN access control measures, like AP MAC filters and 802.1X port access controls [5].

- War Driving
- Ad Hoc Associations
- Rogue Access Points
- MAC Spoofing
- 802.1X RADIUS Cracking

CONFIDENTIALITY ATTACKS

The network attacks of this type attempt to interrupt undisclosed information sent on the wireless channels, whether sent in the clear or encrypted by 802.11 or higher layer protocols [6].

- WEP Key Cracking
- Eavesdropping
- Evil Twin AP
- Man in the Middle
- AP Phishing

INTEGRITY ATTACKS

These attacks send counterfeited control, administration or data frames over wireless to mislead the recipient or facilitate another type of attack [7].

- 802.11 Data Replay
- 802.11 Frame Injection
- 802.1X EAP Replay
- 802.1X RADIUS Replay

AUTHENTICATION ATTACKS

Intruders use these attacks to steal legitimate user identities and credentials to access otherwise private networks and services [8].

- PSK Cracking
- Shared Key Guessing
- Application Login Theft
- VPN Login Cracking
- Domain Login Cracking
- 802.1X Identity Theft
- 802.1X LEAP Cracking
- 802.1X Password Guessing
- 802.1X EAP Downgrade

AVAILABILITY ATTACKS

- Queensland DoS
- AP Theft
- 802.11 Beacon Flood
- 802.11 TKIP MIC Exploit
- 802.11 Associate / Authenticate Flood
- 802.11 Deauthenticate Flood
- 802.1X EAP-Failure
- 802.1X EAP-of-Death
- 802.1X EAP-Start Flood
- 802.1X EAP Length Attacks

4. OBJECTIVES OF THE PROPOSED WORK

- The key objective of the research work is to provide high level security and integrity to the existing systems mainly on the network layer to prevent the attacks etc.
- To investigate and conclude the scope of multi layer attacks.
- To analyze the needs of above mentioned techniques in different network layers especially in the multi link layer.
- To propose a unique technique for different attacks using multilayered cryptography based hash key.
- Intelligent Wireless Sensor Network proposal to deal with all kinds of attacks.
- Validation of the approaches with dataset of dynamic and virtual wireless environment.

5. KEY POINTS AND FEATURES OF THE PROPOSED WORK

- The proposed approach is making use of dynamic key that is generated based on the current timestamp and location of the underwater nodes or submarines
- The hybrid cryptography based approach is security and performance aware as the data transmission is integrated without hindrance
- The dynamic key is fully secured and cannot be cracked by the interceptions. If there is any interception, the acknowledgement packet will be transmitted and intruding attempt can be identified.
- The key is generated with each simulation attempt at the time of data packet initialization so that the interceptions can be avoided with the analysis of historical patterns.

6. IMPLEMENTATION AND RESULTS

The proposed approach is dynamic in nature that makes use of dynamic key exchange. The parallel hybrid approach of multiple hash algorithms and implemented for higher security and integrity in the network.

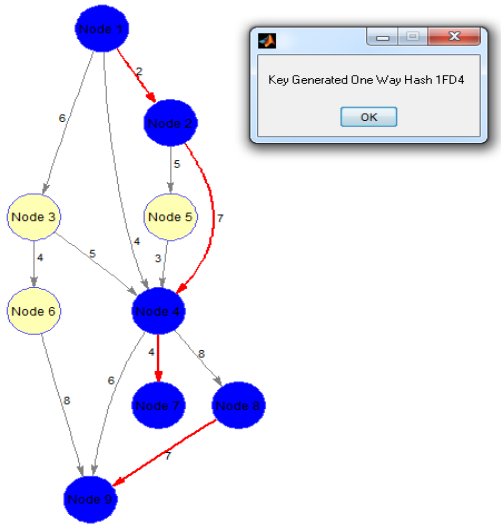

Figure 4 – Dynamic Formation of the Virtual Wireless Scenario for Simulation

In figure 3, there is simulation of dynamic wireless topology having assorted number of nodes. These nodes are virtually connected with other nodes using wireless transmission media. The data is set to be transmitted from node 1 to node 9 with the minimum distance and higher security. The classical approach is making use of shortest path with greedy based approach. In the greedy method, the minimum distance is selected and no global optimization is considered. In addition, the one way hash key is making use of keys which can be decrypted and damaged by the intruders. The proposed approach is highly secured with the integrated of multiple cryptography keys.

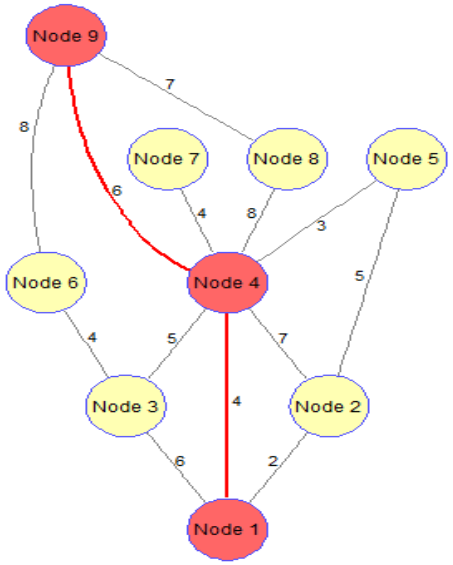

Figure 5 – Generation and Spawn of the Path from Source to Destination with Security Key

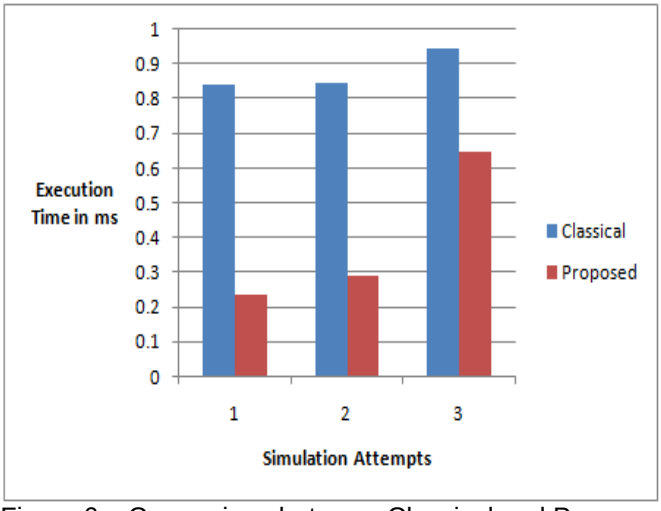

Figure 6 – Comparison between Classical and Proposed Approach in terms of Execution Time

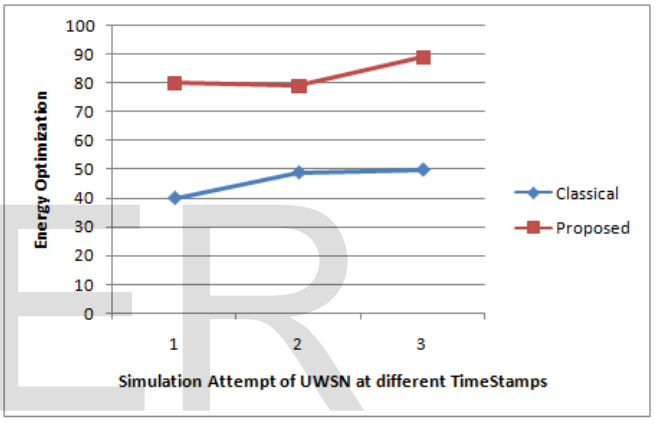

Figure 7 – Comparison between Classical and Proposed Approach in terms of Energy Optimization

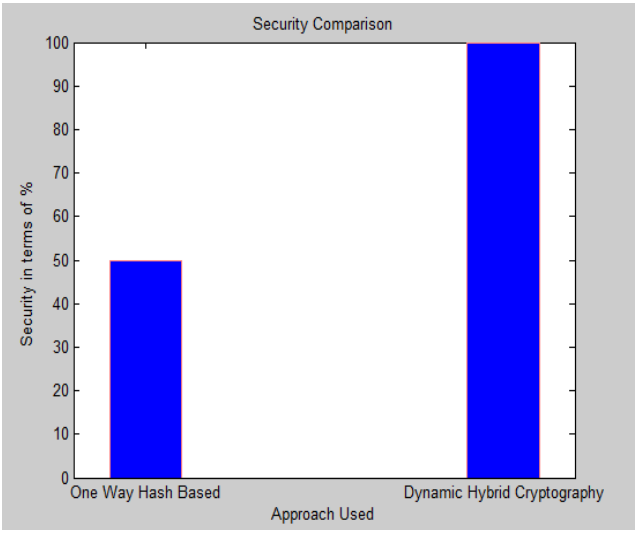

Figure 8 – Comparison between Classical and Proposed Approach in terms of Security

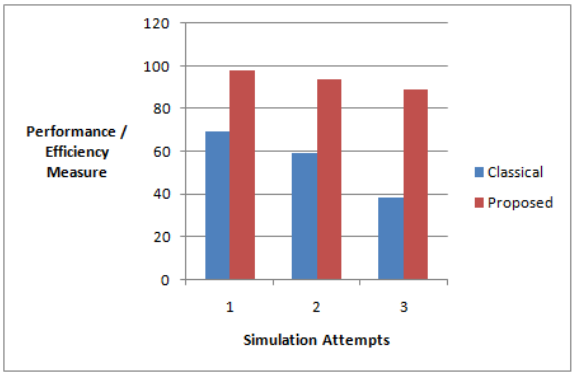

Figure 9 – Evaluation of Efficiency between classical and proposed approach

The proposed approach is better in terms of higher security and less cost factor which lead this approach efficiency aware. The cost factor and complexity in the algorithmic approach of dynamic hash is lesser than the one way approach.

7. CONCLUSION

As the underwater wireless networks established on the submarines or merchant navy ships are vulnerable from different types of attacks, there is need to develop and implement a secured mechanism with highly integrated keys so that the interceptions cannot be done. In this research work, a unique and effective approach is implemented for avoidance of interceptions and integration of security during data transmission in network environment. The proposed approach is effective and giving better results than the classical approach with less secured keys. The proposed system for underwater network scenarios can be implemented for any type of network and security can be integrated with dynamic keys.

REFERENCES

[1] Karygiannis, T., & Owens, L. (2002). Wireless network security. NIST special publication, 800, 48.
[2] Zimmermann, H. (1980). OSI reference model-the ISO model of architecture for open systems interconnection. IEEE Transactions on communications, 28(4), 425-432.
[3] Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), 1550-1573.
[4] Crow, B. P., Widjaja, I., Kim, L. G., & Sakai, P. T. (1997). IEEE 802.11 wireless local area networks. IEEE Communications magazine, 35(9), 116-126.
[5] Zhou, Y., Zhang, Y., & Fang, Y. (2007). Access control in wireless sensor networks. Ad Hoc Networks, 5(1), 3-13.
[6] Welch, D., & Lathrop, S. (2003, June). Wireless security threat taxonomy. In Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society (pp. 76-83). IEEE.
[7] Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. IEEE Pervasive Computing, 7(1), 74-81.
[8] Ning, P., Liu, A., & Du, W. (2008). Mitigating DoS attacks against broadcast authentication in wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 4(1), 1.