Wireless Personal Communications (2020) 113:1–15
https://doi.org/10.1007/s11277-020-07175-8

SAPDA: Secure Authentication with Protected Data Aggregation Scheme for Improving QoS in Scalable and Survivable UWSNs

Nitin Goyal[1] · Mayank Dave[2] · Anil Kumar Verma[3]

Published online: 20 January 2020

Abstract

Security is one of the main objectives while designing protocols for underwater wireless sensor networks (UWSN), since the sensors in UWSN are vulnerable to malicious attack. So it becomes easy for opponents to manipulate the communication channel of UWSN and its nodes. Authentication and data integrity play important roles in the context of security to make network scalable and survivable. Hence in this paper, a secure authentication and protected data aggregation method for the cluster based structure of UWSN is proposed as because cluster based arrangement produces a concise and stable network. In this technique, the cluster head in each cluster is authenticated by the gateway to ensure that all the clusters are being handled by valid nodes. Also, the data being communicated in the network will be securely handled to ensure that it will not get compromised during network operations. In this way, the security of all the nodes is ensured to maintain safe network communication. The proposed technique improves the data reliability in the network by reducing the energy consumption and delay. Here, the proposed method is moreover compared with the state of the art techniques to prove the validity and effectiveness.

Keywords Reliability · Cluster · Security · Aggregation · Communication · Underwater wireless sensor network

1 Introduction

Underwater Wireless Sensor Network (UWSN) is a network of self-governing sensor nodes which are distributed underwater to sense pressure, temperature etc. This sensed data can be utilized by the arrays of applications like in military surveillance, disaster

✉ Nitin Goyal
nitin.goyal@chitkara.edu.in

[1] Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India

[2] Department of Computer Engineering, National Institute of Technology, Kurukshetra, India

[3] Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala, India

avoidance, offshore exploration, pollution level examining, etc. that can be used for the benefit of humans [1]. UWSN face several issues like restricted bandwidth, greater propagation delay, random node mobility etc. which are yet to be handled appropriately. These issues give rise to new issues in each layer of the network protocol model [2]. One of the common issues faced in UWSN is the clock synchronization issue. For the appropriate functioning of the network, it is important to achieve a similar notion regarding time along with distributed aggregation of data, localization, time stamping of events, MAC, etc. UWSN is widely used for exploration of aquatic organisms, enemy tracing, discovery of possible resources, disaster prevention, underwater surveillance etc. [3]. A very important contribution of UWSN is automation of Water Quality Surveillance (WQS), since water is the fundamental need of a human being [4]. UWSN has enhanced the monitoring techniques to a great level and it also provides regular and promising surveillance. Since it is possible for an attacker to infuse false data into the network, it is critical to ensure the trustworthiness of the data being utilized for taking decisions.

Also, capability of the UWSN to handle issues and attacks in the real time environment remains an important field of exploration [5–8]. During the development of network protocols and techniques, security is considered as one of the critical aspects in UWSN. Here, sensors are prone to various attacks because of its cost factors, and also, it can be easily accessed since it is usually situated close to the event source. Moreover, it is possible for any random device to gain access to the information exchanged due to unrestricted nature of communication channel. Thus, attacking sensor nodes or channels in UWSN is an easy task. The security needs in UWSN are devised on the basis of factors are confidentiality, integrity, authentication, and re-authentication for secure acoustic communication. To ensure security in network, authentication is an important factor. For the conventional WSN which is designed for the land topology, several authentication protocols are developed like Blom’s symmetric matrix multiplication algorithm, RSA algorithm, etc. However, these protocols are not suitable for the UWSN because of the increased computation sophistication, low chances of correction, irreversible nature of network processes, etc. Hence, it is important to develop specialized authentication mechanisms for the UWSN.

To the best of author’s knowledge, very limited techniques have been suggested for security during data aggregation in UWSN. The advantages of our contribution in this paper of Secure Authentication and Protected Data Aggregation (SAPDA) are as follows:

- SAPDA is based on real-time parameters and the same are taken in experiments also.
- Multiple uses of sink nodes reduce delay, packet drop, and enhances packet delivery ratio.
- SAPDA proves to be reliable and secure by using trusted encryption schemes.
- Use of cluster based approach enhances network life time.

Here, the manuscript is abridged into six different sections; out of which, related work on existing security methods is described in Sect. 2. Further, the proposed scheme SAPDA is elaborated in Sect. 3. An analytical model for the proposed scheme is also shown in Sect. 4. The projected method is analyzed and compared with various techniques, whose outcomes are explicitly embodied in Sect. 5. The concluding remarks of the proposed scheme are described in Sect. 6.

2 Related Work

The use of encryption schemes improves the reliability of the system. Existing schemes were proposed to achieve forward or backward security by using hash function only but most of the techniques are not applicable to UWSN. Various existing schemes on reliability are as follows:

Karimi et al. [9] have utilized the techniques of machine learning for a fault tolerant, reliable, and secure framework. This technique suggests collection of information from the environment and passes its inconsistencies from events to actuators in the deployed network. A node has to follow specific rules in a network. This helps in building trust among the nodes. The trust is qualitative and asymmetric in nature [10]. If the rules are not followed by a node then it is identified as an errant node i.e. to be eliminated from the network to restrict further communication. CSLT is developed by Geetha et al. [11] for ensuring location security on the basis of trust model. The model divides the localization into five processes based on selection, localization and trust evaluation of a node. In this article a trust management system for WSNs is proposed that identified different parameters and trust based factors to influence trust variation. STKF a trust based framework is introduced by Kaur et al. [12] that relies on the past and present interaction between the nodes. In this framework the faulty node is isolated from the network route and a link is developed within remaining nodes.

Use of clustering improves the lifetime of the system [13–15]. Xu et al. [16] proposed a CLUster-based Secure Synchronization (CLUSS) protocol that guarantees synchronization security even under harsh underwater environments w.r.t. numerous malicious attacks such as sybil attack, delay attack, replay attack, and message manipulation attack. In the CLUSS protocol, the procedure of time synchronization is classified into 3 classes: authentication, inter-cluster synchronization, and intra-cluster synchronization phase. Proposed protocol enhances the accuracy involved in time synchronization. Verma [17] have proposed a Cluster based Key management Protocol (CKP), for hierarchical networks. This protocol is proposed based on the analysis made around the security and mobility issues in UWSN. CKP also presents a communication model to manage mobility effectively and also to reduce the node compromise effect on itself. CKP offers authentication, freshness, confidentiality and also integrity to the network. Based on the performance study, it is proven that CKP is energy efficient as well as storage efficient. Yuan et al. [18] presented a low computational complexity authentication mechanism on the basis of the vandermonde matrix. Matrix multiplication has been replaced by the matrix addition in order to minimize the overhead involved with computation. Also, the proposed mechanism is self-sustaining and irreversible. This improves the UWSN security to a greater extent. Yun et al. [19] developed an appropriate ticket based authentication mechanism for UWSN after analysing the type of tickets selected in the authentication protocol for WSN.

Yavuz et al. [20] have proposed a set of signature mechanism called as Hash-Based Sequential Aggregate and Forward Secure Signature (HaSAFSS). It permits the signer to create a fixed size and compact signature which can be verified publicly with minimum computation expense. Elliptic curve cryptography based HaSAFSS and symmetric HaSAFSS are the 2 HaSAFSS mechanisms proposed there. The proposed scheme combines the proficiency of MAC-based signatures as well as public verifiability signatures along with the preservation of forwards security through Timed-Release Encryption (TRE). Ren et al. [21] have presented a secure as well as reliable data distribution mechanism, capable of facilitating forward secrecy. In this scheme, an optimized data distribution technique was presented to enhance the probabilistic backward secrecy as well as data reliability. Du et al. [22] and Dargahi et al. [23] have provided solutions for routing attacks. Du et al. provided a secure and anonymous routing technique in which short signature algorithm is used in route structure for validation between source–destination node pair. Anonymity is achieved using trap-door system in routing the messages. Dargahi et al. presented a distributed detection and mitigation technique to mitigate routing attacks. The behavior of neighbors is monitored by storing their ongoing traffic details. Dini et al. [24] proposed a security suite that bears a protected routing protocol and a set of cryptographic primitives. It assures privacy and reliability in underwater communication.

In past, very few schemes were suggested for reliable communication in UWSN and there created a space for further enhancement in attaining energy efficient technique having decreased delay and packet drop [25–39]. In recent past investigators have proposed the work in WSN and have designed numerous techniques for secure data aggregation. The situation has also created the need to implement the existing techniques in underwater network to explore the consequences in a diverse environment.

3 Secure Authentication and Protected Data Aggregation (SAPDA)

In this paper, a secured authentication and protected data aggregation scheme for UWSN is proposed in cluster based environment. The proposed technique consists of two modules: Secure authentication of cluster heads (CHs) and protected data aggregation. In first module, CHs are authenticated to gateways (GWs). The authentication is required to ensure that the CH serving each cluster is a valid node and is not compromised. This confirms that the cluster is under safe operation. In second module, each sensor protects the data using symmetric encryption, before sending to the CH. The data is then aggregated in a secure manner and transmitted to the base station. Any compromised data, if detected through time stamp values, is handled to ensure secure network operation. Figure 1 shows this model of SAPDA through the block diagram.

3.1 System Model

The system model of UWSN is considered as made up of sensor nodes, CH, GW and base station (BS). Figure 2 shows the proposed system model of UWSN. Each sensor node is a part of minimum one cluster that itself is managed by a CH. The base station links CH with the GW through acoustic links. This GW has unlimited energy resources and perfect timing information. If there are 2 or more than 2 GWs, then they transfer information with each other through radio frequency (RF) links.

3.2 Module 1: Secure Authentication of Cluster Head

After route establishment among the clusters, all the CHs are authenticated to the GW. Here, every CH in the network initially generates secret key and registration request with GW. CH further creates hash value and signs it using secret key for sending the request to GW. The request is decrypted at GW using public key of CH and retrieves the time stamp. GW generates registration confirmation by using hash value received and time stamp. Both hash values are compared by ignoring small variation to authenticate CH. GW sends

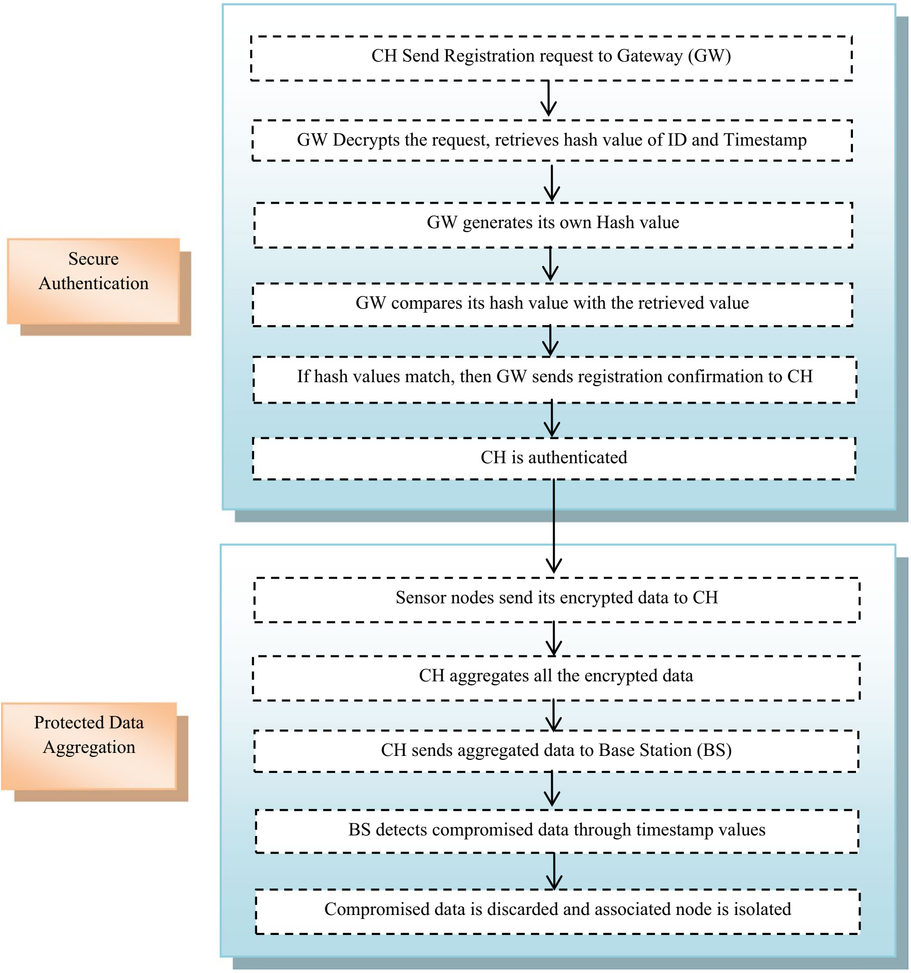

Secure Authentication
CH Send Registration request to Gateway (GW)
GW Decrypts the request, retrieves hash value of ID and Timestamp
GW generates its own Hash value
GW compares its hash value with the retrieved value
If hash values match, then GW sends registration confirmation to CH
CH is authenticated
Protected Data Aggregation
Sensor nodes send its encrypted data to CH
CH aggregates all the encrypted data
CH sends aggregated data to Base Station (BS)
BS detects compromised data through timestamp values
Compromised data is discarded and associated node is isolated

Fig. 1 Block diagram of SAPDA

registration response to CH after signing hash value using secret key of GW. CH determines that it has been authenticated by decrypting the registration response received using public key of GW. The process of CH authentication is also described in Algorithm 1.

Notations	Meaning
SK_{CH}	Secret key generated by CH
PK_{CH}	Public key of CH
CH_{id}	ID of the CH
GW_{id}	ID of the gateway
CH_RR	CH registration request
CH_RC	CH registration confirmation
M_{RREQ}	Registration request message
M_{RRES}	Registration response message

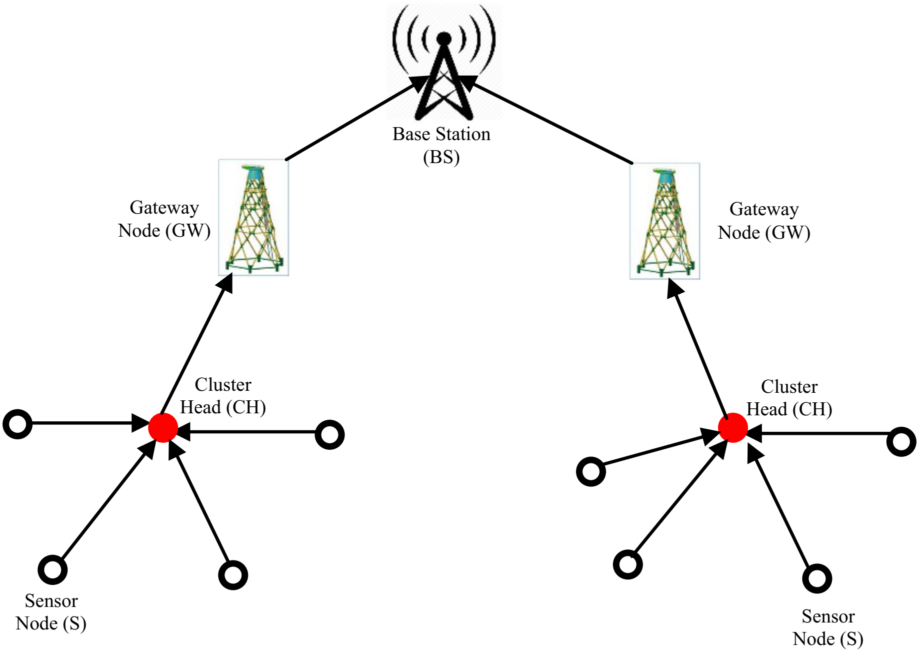


Fig. 2 System model

Notations	Meaning
H	Hash function
T_{s1}	Time stamp at which the request was generated at CH
T_{s2}	Time stamp at which the reply was generated at GW
SK_{GW}	Secret key of gateway
PK_{GW}	Public key of gateway

Algorithm 1

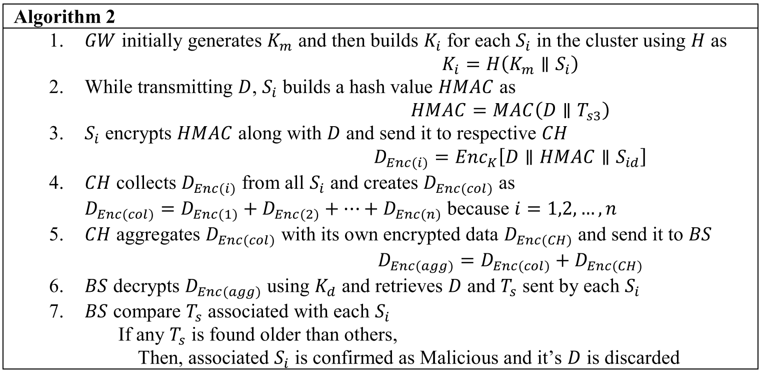
```
1.  Every $CH$ initially generates $SK_{CH}$
2.  $CH$ creates $CH\_RR$ which consists of $[CH_{id}, GW_{id}]$
3.  $CH$ generates $M_{RREQ}$ by creating hash value of $[CH\_RR, T_{s1}]$ and signs it using $SK_{CH}$ as
        $M_{RREQ} = SK_{CH}[H(CH\_RR, T_{s1})]$
4.  $CH$ sends $M_{RREQ}$ to $GW$
5.  $GW$ decrypts it using $PK_{CH}$ and retrieves $CH\_RR$ and $T_{s1}$
6.  $GW$ creates $CH\_RC$ as $[CH_{id}, GW_{id}]$
7.  $GW$ create hash value of $[CH\_RC, T_{s2}]$ as $[H(CH\_RC, T_{s2})]$
8.  $GW$ compare $[H(CH\_RR, T_{s1})]$ with $[H(CH\_RC, T_{s2})]$
        If $[H(CH\_RR, T_{s1})]$ does not match with $[H(CH\_RC, T_{s2})]$,
          Then, $GW$ discards $M_{RREQ}$
        Else $GW$ confirms that $CH$ is a valid node
9.  $GW$ signs $[H(CH\_RC, T_{s2})]$ using $SK_{GW}$ to create $M_{RRES}$ as
        $M_{RRES} = SK_{CH}[H(CH\_RC, T_{s2})]$
10. $M_{RRES}$ is sent to $CH$ by $GW$
11. $CH$ decrypts it using $PK_{GW}$ and retrieves $H(CH\_RC, T_{s2})$
12. $CH$ determines that it has been authenticated by $GW$
```

In this way, every CH is individually and securely authenticated by the GW to ensure that any malicious node is not controlling the cluster operation leads to safeguarding the cluster from being compromised.

3.3 Module 2: Protected Data Aggregation

After ensuring that the selected CH is authentic, the sensor nodes transfer data to its CH. Each sensor protects the data using symmetric encryption, before sending to the CH. The data at CH is aggregated securely and further transmitted to Base station where compromised data, if any detected, is handled accordingly. This process is described in Algorithm 2.

Notations	Meaning
S_i	Sensors
S_{id}	ID of S_i
T_{s3}	Time stamp at which the data is sensed at S_i
K_m	Master key
K_i	Encryption key
K_d	Decryption key
Enc_K	Encryption using K_i
D	Sensed data
$D_{Enc(i)}$	Encrypted data at S_i
$D_{Enc(col)}$	Collection of encrypted data from all S_i at CH
$D_{Enc(CH)}$	CH's encrypted data
$D_{Enc(agg)}$	Aggregation of encrypted data



```
Algorithm 2
1. $GW$ initially generates $K_m$ and then builds $K_i$ for each $S_i$ in the cluster using $H$ as
        $K_i = H(K_m \parallel S_i)$
2. While transmitting $D$, $S_i$ builds a hash value $HMAC$ as
        $HMAC = MAC(D \parallel T_{s3})$
3. $S_i$ encrypts $HMAC$ along with $D$ and send it to respective $CH$
        $D_{Enc(i)} = Enc_K[D \parallel HMAC \parallel S_{id}]$
4. $CH$ collects $D_{Enc(i)}$ from all $S_i$ and creates $D_{Enc(col)}$ as
   $D_{Enc(col)} = D_{Enc(1)} + D_{Enc(2)} + \cdots + D_{Enc(n)}$ because $i = 1,2,\ldots,n$
5. $CH$ aggregates $D_{Enc(col)}$ with its own encrypted data $D_{Enc(CH)}$ and send it to $BS$
        $D_{Enc(agg)} = D_{Enc(col)} + D_{Enc(CH)}$
6. $BS$ decrypts $D_{Enc(agg)}$ using $K_d$ and retrieves $D$ and $T_s$ sent by each $S_i$
7. $BS$ compare $T_s$ associated with each $S_i$
       If any $T_s$ is found older than others,
           Then, associated $S_i$ is confirmed as Malicious and it's $D$ is discarded
```

In this way, the data transmission is performed with high security and securely aggregated by the CH. The aggregated data is checked for its authenticity by the base station through its time stamp and detected compromised data is discarded to ensure the safety of the remaining aggregated data. The detected compromised/malicious node is then isolated from the cluster to maintain network security.

To show overall processing of information through process flow diagram of SAPDA Fig. 3 is depicted here. In this diagram, the process flows 1 and 2 indicate the CH authentication with its GW. Process flow 3 indicates the symmetric encryption of data by the sensor nodes and process flow 4 indicates decryption of received data by the BS.

4 Analytical Model

Due to packet drop of some control packets, signature mismatch may occur, leading to the false detection and isolation of honest node. The probability of false detection and isolation becomes necessary and can be derived as follows:

Let,P_r = probability, P_D = probability of packet drop, R = packet generation rate, t = time interval, SM_i = number of signature mismatches of node N_i among its neighbours.

Then the probability of SM exceeding the maximum threshold SM_{th} is given by

$$P_r\left(SM > SM_{th}\right) = 1 - \sum_{i=1}^{SM_{th}} \binom{Rt}{i} P_D^i \left(1 - P_D\right)^{Rt-i}$$

Let,W = number of warnings received by node N_i when any of its neighbour turns to be malicious.

The probability of W exceeding the maximum threshold W_{th} is given by

$$P_r\left(W\left(N_j\right) > W_{th}\right) = 1 - \sum_{i=1}^{W_{th}} \binom{NH}{i} P_{FD}\left(N_j\right)^i \left(1 - P_{FD}\left(N_j\right)\right)^{NH-i}$$

where,NH is the number of neighbours of node N_i, $P_{FD}\left(N_j\right)$ is the probability of False Detection of node N_j which is given by

$$P_{FD}\left(N_j\right) = 1 - exp\left[-2 \cdot \frac{\left(R \cdot t \cdot P_D - SM_{th}\right)^2}{R \cdot t}\right]$$

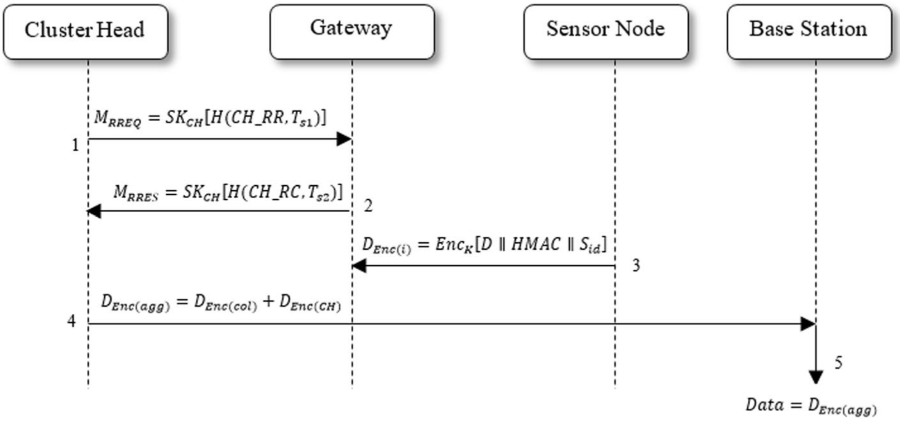

Cluster Head
Gateway
Sensor Node
Base Station
$M_{RREQ} = SK_{CH}[H(CH\_RR, T_{s1})]$
1
$M_{RRES} = SK_{CH}[H(CH\_RC, T_{s2})]$
2
$D_{Enc(i)} = Enc_K[D \parallel HMAC \parallel S_{id}]$
3
$D_{Enc(agg)} = D_{Enc(col)} + D_{Enc(CH)}$
4
5
$Data = D_{Enc(agg)}$

Fig. 3 Process flow of SAPDA

Then the probability of False Isolation P_{FI} is given by

$$P_{FI}(N_j) = 1 - exp\left[-2 \cdot \frac{\left(NH \cdot P_{FD}(N_j) - W_{th}\right)^2}{NH}\right]$$

5 Results and Analysis

The AquaSim tool of NS2 is used. To simulate the proposed scheme in UWSN, the UnderwaterChannel and UnderwaterPropagation model are used. We have used UnderwaterMac as the MAC layer protocol and considered area size as 1000×1000 m^2 region for a span of 100 s. Here, 200 sensor nodes are randomly deployed that remain static. The numbers of attackers varied from 1 to 10. The other parameters used are given in Table 1.

The proposed SAPDA is compared with HaSAFSS [20], ES [21], FDRT [25] and IDACB [27] schemes. Although HaSAFSS allows signer to produce a fixed-size and freely verifiable signature in sequence but, it requires asymmetry between the (distinguish characterised) senders and receivers. ES scheme applies RS code so that the encrypted data is encoded into n shares where the BS collects data, say m, shared by nodes and reconstructs data using (m, n) RS codes. Although this scheme ensures reliability of data but, it involves high computational cost and delay. FDRT uses scheduling (TDMA based) for collision free data transmission but it doesn't ensure secure data aggregation because when number of attackers is more it takes time to confront them. IDACB uses receiver oriented sleep scheduling mechanism with data fusion at cluster head but did not implement encryption during data transfer for secure communication.

The malicious nodes or numbers of attackers are taken randomly and varied from 1 to 10. The results so obtained of the proposed SAPDA and existing HaSAFSS, ES and IDACB named schemes are compared graphically below. The performance metrics considered for comparison are:

Average End-to-End Delay It is the total time consumed by data packet to arrive BS which includes encryption time at sensors, aggregation time at CH, transmission time from CH to BS, and decryption time at BS. Figure 4 displays the results of end-to-end average delay for the proposed and existing techniques.

Table 1 Parameters used

Name of parameter	Value of parameter
Number of nodes	200
Time span taken	100 s
Traffic source	CBR
Traffic rate	50Kbps
Attackers	1 to 10
Propagation	Two ray ground
Antenna	OmniAntenna
Initial energy	10000 J
Transmission power	2.0 W
Receiving power	0.75 W

When the attackers are increased from 1 to 10 the delay of proposed technique SAPDA increases from 0.0020 to 0.0034 whereas the delay incurred in existing ES scheme increases from 0.0053 to 0.023, the delay in existing HaSAFSS increases from 0.024 to 0.031, the delay in existing FDRT increases from 0.01209 to 0.030902 and the delay of existing IDACB increases from 0.002055 to 0.00743. Hence the delay of SAPDA is 91% lesser when compared to HaSAFSS, 72% less when compared to ES, 84% less when compared to FDRT and 41% less than IDACB. This is due to the fact that HaSAFSS necessitates an ExpOp to set each time and ES scheme requires RS encoding and decoding.

Average Data Delivery/Reliability Ratio It is said to be the ratio of data packages successfully received w.r.t. the entire sum of packages transmitted from source. It totally reflects the reliability and efficiency of the network. Figure 5 demonstrates the results of data reliability for the proposed and existing methods.

As attackers are increased from 1 to 10 the average delivery ratio of SAPDA decreases interestingly from 0.7186 to 0.5322 while the average delivery ratio of HaSAFSS decreases from 0.4274 to 0.3056, the delivery ratio of ES decreases from 0.5874 to 0.3542, the average delivery ratio of FDRT decreases from 0.4272 to 0.31205 and the average delivery ratio of IDACB decreases from 0.6186 to 0.4322. Hence the average delivery ratio of technique SAPDA is 12% greater than HaSAFSS, 20% higher than ES, 36% higher than FDRT and 14% higher than IDACB schemes.

Average Packet Drop It is counted as the number of packets dropped due to attacks. Figure 6 depicts the simulation results of average packet drop for the techniques under consideration.

As shown in the above graph, when the attackers are increased from 1 to 10, the packet drop of SAPDA increases from 15 to 23 however the packet drop of ES scheme increases from 16 to 57, the packet drop of HaSAFSS increases from 47 to 88, the packet drop of FDRT increases from 26 to 71 whereas the average packet drop of IDACB increases from 16 to 40. Hence the packet drop of SAPDA is 71% less when compared to HaSAFSS, 19% less when compared to ES, 57% less when compared to FDRT and 21% less in comparison

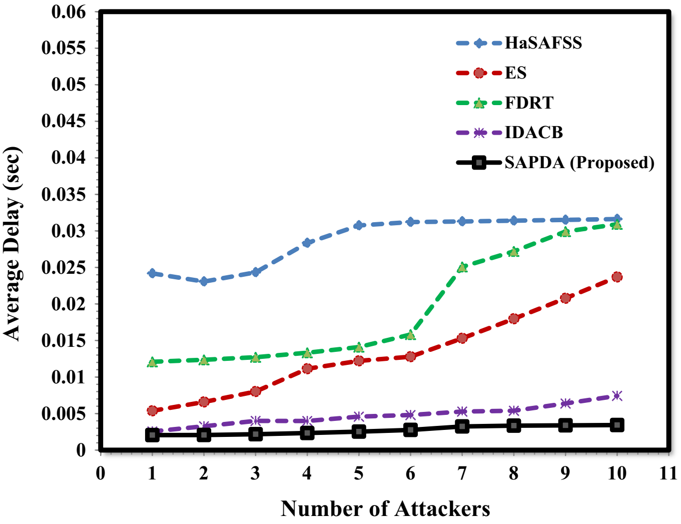


Fig. 4 Average end-to-end delay varying according to number of attacker nodes

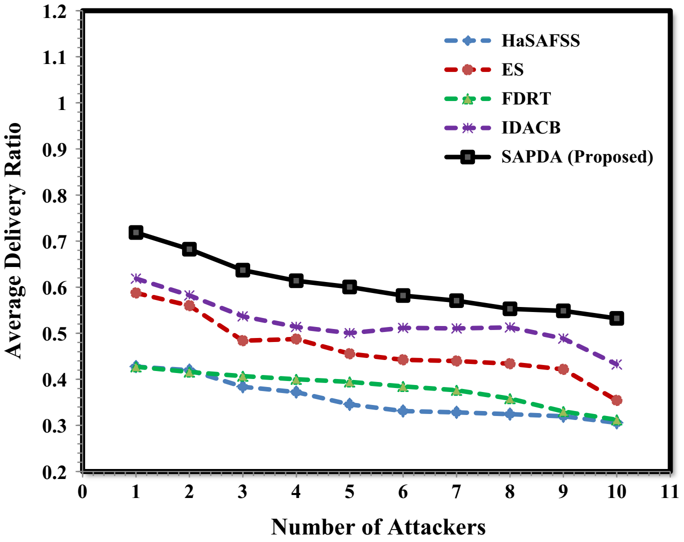


Fig. 5 Average data delivery ratio variation according to number of attacker nodes

to IDACB schemes. This is due to the fact that HaSAFSS, ES, FDRT and IDACB schemes did not possess strong authentication before the data reaches to BS. Hence data drop occurs at intermediate nodes along the path.

Average Energy Consumption It is analysed as the total amount of energy consumed by all the nodes during data packets transmission in the network. Figure 7 shows the effects of energy consumption for the proposed and existing techniques.

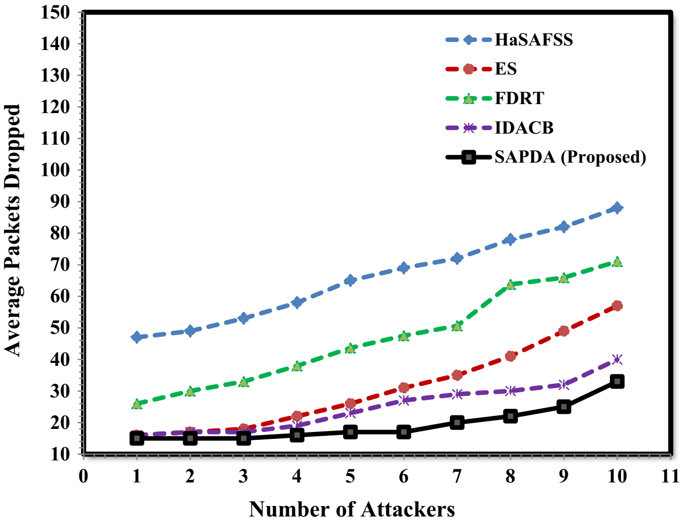


Fig. 6 Average packets dropped comparison with varying to number of attacker nodes

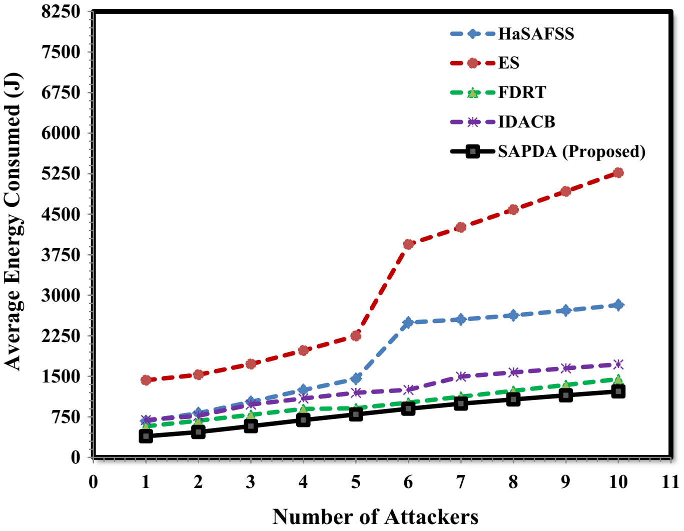


Fig. 7 Average energy consumed variation according to number of attacker nodes

The graph in Fig. 7 represents that with the increase in attackers from 1 to 10, the average energy consumption of SAPDA increases from 392 to 1222 joules, the average energy consumption of ES increases from 1429 to 5266 joules, the average energy consumption of HaSAFSS increases from 671 to 2820 joules, the average energy consumption of FDRT increases from 576 to 1449 joules and of IDACB increases from 492 to 1522 joules. Hence the delay of SAPDA is 43% lesser when compared to HaSAFSS, 67% lesser when compared to ES, 19% less when compared to FDRT and 17% less in comparison to IDACB schemes. This is due to the fact that HaSAFSS, ES and IDACB schemes involve high computational overhead as opposed by the proposed SAPDA technique.

6 Conclusion

A secured authentication and protected data aggregation mechanism is proposed for improving QoS in scalable and survivable cluster based underwater network. It works in two modules: authentication and data aggregation. In first module, the cluster head of each cluster is authenticated by the gateway. In the second module, the sensor node within the cluster secures its data through encryption. The base station analyses the data and detects compromised data using timestamp value. The compromised data thus detected is discarded. Its associated node referred as malicious node gets isolated from the network. In this way, the proposed scheme ensures data security and node authentication. Presented scheme is having application in marine and underwater vehicle communication security where energy efficiency is crucial requirement with lower packet drop. The performance of the proposed scheme is analysed in terms of data reliability ratio, packet drop, average energy consumption and end-to-end delay in UWSN and compared with existence techniques. The graphical representation of results states the outstanding performance of proposed scheme SAPDA in comparison to existing schemes.

References

1. Yoon, S., & Qiao, C. (2010). Cooperative search and survey using autonomous underwater vehicles (AUVs). *IEEE Transactions on Parallel and Distributed Systems, 22*(3), 364–379.
2. Goyal, N., Dave, M., & Verma, A. K. (2019). Protocol stack of underwater wireless sensor network: Classical approaches and new trends. *Wireless Personal Communications, 104*(3), 995–1022.
3. Zandi, R., Kamarei, M., & Amiri, H. (2016). Distributed estimation of sensors position in underwater wireless sensor network. *International Journal of Electronics, 103*(5), 853–867.
4. Hamilton, E. I., & Minski, M. J. (1972). Comments on the trace element chemistry of water: Sampling a key factor in water quality surveillance. *Environmental Letters, 3*(1), 53–71.
5. Das, A. P., & Thampi, S. M. (2015). Secure communication in mobile underwater wireless sensor networks. In *IEEE international conference on advances in computing, communications and informatics (ICACCI)* (pp. 2164–2173).
6. Han, G., Jiang, J., Sun, N., & Shu, L. (2015). Secure communication for underwater acoustic sensor networks. *IEEE Communications Magazine, 53*(8), 54–60.
7. Han, G., Liu, L., Jiang, J., Shu, L., & Rodrigues, J. J. (2016). A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks. *Sensors, 16*(2), 229.
8. Rezvani, M., Ignjatovic, A., Bertino, E., & Jha, S. (2014). Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks. *IEEE Transactions on Dependable and Secure Computing, 12*(1), 98–110. (2015).
9. Karimi, H., Medhati, O., Zabolzadeh, H., Eftekhari, A., Rezaei, F., & Dehno, S. B. (2015). Implementing a reliable, fault tolerance and secure framework in the wireless sensor-actuator networks for events reporting. *Procedia Computer Science, 73,* 384–394.
10. Xu, M., Liu, G., & Guan, J. (2015). Towards a secure medium access control protocol for cluster-based underwater wireless sensor networks. *International Journal of Distributed Sensor Networks, 11*(5), 325474.
11. Geetha, V., & Chandrasekaran, K. A. (2014). Distributed trust based secure communication framework for wireless sensor network. *Wireless Sensor Network, 6*(9), 173.
12. Kaur, J., Gill, S. S., & Dhaliwal, B. S. (2016). Secure trust based key management routing framework for wireless sensor networks. *Journal of Engineering, 2016,* 1–9.
13. Ahmed, M., Salleh, M., & Channa, M. I. (2018). CBE2R: Clustered-based energy efficient routing protocol for underwater wireless sensor network. *International Journal of Electronics, 105*(11), 1916–1930.
14. Goyal, N., Dave, M., & Verma, A. K. (2016). Energy efficient architecture for intra and inter cluster communication for underwater wireless sensor networks. *Wireless Personal Communications, 89*(2), 687–707.
15. Kumar, R. (2014). A survey on data aggregation and clustering schemes in underwater sensor networks. *International Journal of Grid and Distributed Computing, 7*(6), 29–52.
16. Xu, M., Liu, G., Zhu, D., & Wu, H. (2014). A cluster-based secure synchronization protocol for underwater wireless sensor networks. *International Journal of Distributed Sensor Networks, 10*(4), 398610.
17. Verma, S. (2015). A cluster based key management scheme for underwater wireless sensor networks. *International Journal of Computer Network and Information Security, 7*(9), 54.
18. Yuan, C., Chen, W., Zhu, Y., Li, D., & Tan, J. (2015). A low computational complexity authentication scheme in underwater wireless sensor network. In *11th IEEE international conference on mobile ad hoc and sensor networks (MSN)* (pp. 116–123).
19. Yun, C. W., Lee, J.H., Yi, O., & Park, S. H. (2016). Ticket-based authentication protocol for underwater wireless sensor network. In *8th IEEE international conference on ubiquitous and future networks (ICUFN)* (pp. 215–217).
20. Yavuz, A. A., & Ning, P. (2012). Self-sustaining, efficient and forward-secure cryptographic constructions for unattended wireless sensor networks. *Ad Hoc Networks, 10*(7), 1204–1220.
21. Ren, Y., Oleshchuk, V. A., & Li, F. Y. (2013). Optimized secure and reliable distributed data storage scheme and performance evaluation in unattended WSNs. *Computer Communications, 36*(9), 1067–1077.
22. Du, X., Peng, C., & Li, K. (2017). A secure routing scheme for underwater acoustic networks. *International Journal of Distributed Sensor Networks, 13*(6), 1550147717713643.
23. Dargahi, T., Javadi, H. H., & Shafiei, H. (2017). Securing underwater sensor networks against routing attacks. *Wireless Personal Communications, 96*(2), 2585–2602.
24. Dini, G., & Duca, A. L. (2012). A secure communication suite for underwater acoustic sensor networks. *Sensors, 12*(11), 15133–15158.

25. Goyal, N., Dave, M., & Verma, A. K. (2018). A novel fault detection and recovery technique for cluster-based underwater wireless sensor networks. *International Journal of Communication Systems, 31*(4), e3485.
26. Lee, S., Jeong, Y., Moon, E., & Kim, D. (2017). An efficient MOP decision method using hop interval for RPL-based underwater sensor networks. *Wireless Personal Communications, 93*(4), 1027–1041.
27. Goyal, N., Dave, M., & Verma, A. K. (2017). Improved data aggregation for cluster based underwater wireless sensor networks. *Proceedings of the National Academy of Sciences, India, Section A: Physical Sciences, 87*(2), 235–245.
28. Hamid, Z., & Hussain, F. B. (2014). QoS in wireless multimedia sensor networks: a layered and cross-layered approach. *Wireless Personal Communications, 75*(1), 729–757.
29. Kanthimathi, N. (2017). Balanced and multi-objective optimized opportunistic routing for underwater sensor networks. *Wireless Personal Communications, 94*(4), 2417–2440.
30. Zhao, X., Pompili, D., & Alves, J. (2017). Underwater acoustic carrier aggregation: Achievable rate and energy-efficiency evaluation. *IEEE Journal of Oceanic Engineering, 42*(4), 1035–1048.
31. Goyal, N., Dave, M., & Verma, A. K. (2019). Data aggregation in underwater wireless sensor network: Recent approaches and issues. *Journal of King Saud University-Computer and Information Sciences, 31*(3), 275–286.
32. Mohamed, R. E., Saleh, A. I., Abdelrazzak, M., & Samra, A. S. (2018). Survey on wireless sensor network applications and energy efficient routing protocols. *Wireless Personal Communications, 101*(2), 1019–1055.
33. Gomathi, R. M., & Manickam, J. M. L. (2018). Energy efficient shortest path routing protocol for underwater acoustic wireless sensor network. *Wireless Personal Communications, 98*(1), 843–856.
34. Ahmad, B., Jian, W., Enam, R. N., & Abbas, A. (2019). Classification of DoS attacks in smart underwater wireless sensor network. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-019-06765-5.
35. Mazinani, S. M., Yousefi, H., & Mirzaie, M. (2018). A vector-based routing protocol in underwater wireless sensor networks. *Wireless Personal Communications, 100*(4), 1569–1583.
36. Kim, S., & Yoo, Y. (2019). Practical multiple user system using heterogeneous frequency modulation for high data rate in underwater sensor network. *Wireless Personal Communications, 108,* 1–24.
37. Goyal, N., Sandhu, J. K., & Verma, L. (2019). Machine learning based data agglomeration in underwater wireless sensor networks. *International Journal of Management, Technology and Engineering, 9*(6), 240–245.
38. Gomathi, R. M., & Manickam, J. M. L. (2019). Energy efficient static node selection in underwater acoustic wireless sensor network. *Wireless Personal Communications, 107,* 1–19.
39. Krishnaswamy, V., & Manvi, S. S. (2019). Fuzzy and PSO based clustering scheme in underwater acoustic sensor networks using energy and distance parameters. *Wireless Personal Communications, 108,* 1–18.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Nitin Goyal is working as an Associate Professor in the department of CURIN (Chitkara University Research and Innovation Network), Chitkara University, India. He is having 11 years of teaching and academic experience. He obtained B.Tech and M.Tech degrees from Kurukshetra University and PhD from NIT Kurukshetra, India majoring in computer science. He is GATE and UGC-NET qualifier. He has published approximately 41 research papers in various SCI/SCIE/ESCI/SCOPUS/WoS Journals, Book Chapters and Conferences. He has guided 7 M.Tech and currently guiding 2 M.Tech and 2 Ph.D. candidates. He has delivered 1 Expert Lecture on NS2, 1 consultancy project completed, 2 patents filed. Also he has submitted 2 research projects in the field of internet of drones (IoD). He is IEEE, CSI member and also Associate Editor of 1 Reputed Journal. He has recently Edited a book titled "Energy Efficient Underwater Wireless Communications and Networking" to be published with IGI Global. His research interests include MANET, FANET, WSN, and UWSN.

Mayank Dave received the Ph.D. in Computer Science and Technology from IIT, Roorkee, India in 2002. He received B.Tech degree from AMU, Aligarh, India in 1989 and M.Tech degree in Computer Science and Technology from IIT Roorkee, India in 1991. He is a Full Professor in the Department of Computer Engineering at NIT, Kurukshetra, India since 2013. He has so far guided 15 Ph.Ds and has published over 200 research papers in various international/national journals and conferences. Prof. Dave has attended, presented papers and chaired technical sessions in national and international conferences and seminars in India and abroad including USA, Italy, Singapore, China and Thailand. He has also served as Dean (Research and Consultancy) at for 3 years. He has coordinated several research and development projects. He has recently co-edited a book titled "Security and Privacy Issues in Sensor Networks and IoT" published with IGI Global. He has also written a text book titled "Computer Networks" published by Cengage Learning. His research interests include mobile ad hoc and sensor networks, cyber security, cloud computing, SDN etc. He is a Senior Member of IEEE and the IEEE Computer Society, and Member of ACM and Computer Society of India.

Anil Kumar Verma is working as a Professor in the Department of Computer Science and Engineering at Thapar Institute of Engineering and Technology, Patiala, India since 1996. He received his B.S., and M.S. in 1991, and 2001 respectively, majoring in Computer Science and Engineering. He is PhD from IIT Roorkee in 2008. He has published around 220 papers in referred journals and conferences (India and Abroad). He has chaired various sessions in the International and National Conferences and seminars in India and abroad. Prof. Verma has also delivered many expert lectures in various conferences and seminars in India and abroad. He is active member of MACM, MISCI, LMCSI, MIETE, GMAIMA. He is group lead of mobile computing and communication research. Prof. Verma also serves as a regular reviewer for many prestigious journals and conferences. His research interests include wireless networks, routing algorithms and mobile clouds.