JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Security-Enhanced on Underwater Acquaintances Defend Verification

Babita Suryavanshi
M. Tech. Scholar
Department of CSE/IT
Patel College of Science & Technology, Indore
babitas9119@gmail.com

Er. Lokendra Jat
Designation -Asso. Prof.
Department of CSE/IT
Patel College of Science & Technology, Indore
lokendra.jat@patelcollege.com

Er. Megha Gupta Jat
Designation - Asst. Prof.
Department of CSE/IT
Patel College of Science & Technology, Indore
megha.guptajat@patelcollege.com

Abstract: The software-defined networking (SDN) paradigm is widely regarded as the one that will govern networking in the future generation. The software-defined architecture for underwater acoustic sensor networks, also known as SDUASNs, has recently emerged as an important subject of discussion. The research that is being done on SDUASNs at the moment is, however, still in its early stages and is mostly concentrating on network design, data transfer, and routing. The scope of the SDUASNs is tough to grow, and the security maintenance is seldom dabbled in. These are two of the many limitations that exist. As a result, this research presents a scalable software-definition architecture for underwater acoustic sensor networks, also known as SSDUASNs. It does this by realising an organic integration of the three levels of knowledge, control, and data. The new nodes are able to readily access the network, which may be beneficial to the implementation of a widespread system. Then, the fundamental security authentication mechanism, also known as BSAM, is created using our architecture as the basis. In order to take use of the benefits of being flexible and programmable in SSDUASNs, the security authentication mechanism with pre-push, abbreviated as SAM-PP, is being presented in the further. In today's UASNs, the nodes authentication protocol is inefficient due to its high consumption and lengthy latency times. In addition, it is challenging to adjust to the constantly shifting surroundings. The two approaches have the potential to successfully resolve these issues. In comparison to other systems that are currently in use, BSAM and SAM-PP are better able to differentiate between legal nodes and malicious nodes, significantly reduce the amount of storage space used by nodes, and enhance the effectiveness of the operation of the network. In addition to this, SAM-PP has an additional benefit in that it shortens the time it takes to authenticate.

Keywords: Software-Defined Underwater Acoustic Sensor Networks, Nodes Mobility, Identity Authentication, Autonomous Underwater Vehicle

I. INTRODUCTION

Major needs are put out for underwater acoustic sensor networks (UASNs) in monitoring the marine environment, developing the marine resources as well as preserving the marine rights and interests. At present, UASNs have played a significant role in marine hydrological data gathering, marine resource survey, seawater pollution monitoring, marine catastrophe warning, ship auxiliary navigation and military underwater surveillance [1], [2]. UASNs generally have the following three characteristics: broadly covered, dispersed management, and dynamic topology development. UASNs often employ large-scale heterogeneous sensor nodes for deployment in ocean monitoring environment; with the usage of unmanned management, the sensor nodes are clustered. The dispersed structure can better deal with a range of jobs and complicated scenarios; underwater ocean currents and marine life movements will affect the placement of underwater nodes, resulting in dynamic changes and instability in the network.

With the emergence of heterogeneous UASNs, sensors, hubs, anchor nodes, Autonomous Underwater Vehicles (AUVs) and different hardware gadgets bring up greater requirements for the architecture of UASNs, as well as voice communications, optical communications, radio communication and so on. However, the present distributed architecture is excessively inflexible. There are significant inadequacies in terms of network capacity, transmission performance, security protection and energy efficiency. Therefore, it is vital to innovate from the network architecture to overcome the cur- rent difficulties. Software-defined network (SDN), as the representation of the future generation of Internet, has been extensively deployed in conventional wired networks. Its separation of forwarding and control, centralised control and flexible programmable characteristics, may considerably enhance network resource consumption, simplify network administration, minimise operating costs, and stimulate the network innovation and evolution.

In recent years, a variety of wireless sensor networks linked with SDN, such as the Internet of things, vehicular network, were being researched. L Bertaux et al [3], pro- posed a software-defined architecture for WSNs to overcome the challenge of core component development. De Gante et al [4], listed many critical concerns that need to be solved by SDN- based WSNs, including OpenFlow applicability, distributed control, state synchronisation, and controller security. T Luo [5]used the software-defined framework to accomplish intelligent administration of WSNs, SDN controller function as a base station. The study [6]–[8] explored the major difficulties of UASNs coupled with SDN architecture, such as network design, communication connection, routing, et cetera. The findings reveal that with the fast development of different kinds of underwater hardware, incorporating SDN into the UASNs has become conceivable. However, the present software-defined UASNs investigations are still in their infancy, since several drawbacks still persist. First, the scalability of these networks is low. Software-defined UASNs explores primarily introduction SDN architecture into UASNs. It merely allocates the function of controllers, switches and hosts to UASNs, and does not fully reflect the complexity and dynamism of the undersea environment, making it difficult to be utilised in large-scale UASNs effectively. Second, the network security is insufficient. The present investigations are centred on network design, data transmission and routing. There is limited engagement in dynamic topology management, notably security management. The nodes displacement induced by Ocean current movement, and the nodes energy depletion will both lead to network hole. So new nodes need to be refilled in time for replacement healing. Even the extensible deployment of the network also requires the merging of additional nodes. As the inclusion of illegal nodes may quickly damage the whole network, the authenticity of the new node is the top concern of net- work security management. Therefore, this study examines the extensibility and security of software-definition UASNs in dynamic environment.

The remainder of the article is arranged as follows. The second chapter discusses the current investigations on software- defined UASNs, expounds the benefits and drawbacks of the present study outcomes and points out the existing challenges. The third portion proposes a scalable software-defined UASNs network architecture. The fourth portion focuses on the security authentication of software-defined UASNs, and two security authentication procedures, BSAM and SAM-PP, are presented. The fifth portion does the simulation and comparison tests be- tween the BSAM, SAM-PP protocol and other nodes access authentication technique for comparative analysis. Finally, the complete text is summarised.

II. RELATED WORKS

At now, the globe has viewed the ocean as the principal competing area of military. The coastal nations represented by the United States put high emphasis to the application and development of the UASNs. Preventing external intrusion is an essential responsibility of the acoustic network. To this purpose, the maintenance and preservation of sensors legitimacy and security has become a hot study. In order to compensate for deficiencies in current sensor network design, leveraging the benefits of software defines network, Akyildiz et al. [6] introduced the early notion of software-defined networking for underwater (Soft Water) (Soft Water). It reprogrammed responsibilities of surface fixed receiving station, surface mobile receiving station and ground information centre. The data transmission architecture and transmission performance were evaluated in depth. But there no particular trials carried performed. Ruolin Fan [7] built an underwater central network controller for underwater mobile network composed by AUV. The central network controller gives energy and control information for AUVs. Using this concept it was feasible to accomplish the project of AUV routing. But the central controller proved difficult to shift once installed, resulting in edge nodes relocation overhead. In [8], the new nodes USV (underwater Support Vehicle) as a controller were introduced. The dynamic software defined underwater network was developed. It suggested that the acoustic communication with omnidirectional, and optical communication with directivity. Control information transfer employed acoustic communication, whereas data transmission used optical communication. Water Com's test platform also verified performance. The network was modest, but it improved the rigidity of standard UASNs. Promotion was challenging. Soft Water [6] suggested QoS (Quality of Service) concerns for flawless route reconstruction in the event of network dynamic security authentication. Yan [9] presented a key management strategy for mobile heterogeneous networks based on clustering. Network only allowed moving cluster head. Mobile cluster head authentication uses asymmetric key and hash algorithm. High-security. Adapting to the underwater environment was tough. Verma S [10] analysed node mobility's security implications. Cluster-based key management protocol (CKP) offered varying degrees of security for different attack types. It didn't address authenticating nodes migrating across clusters. Zhang [11] transmitted local key to protect mobile nodes' channels. New network nodes might be verified. [12] introduced ECC encryption. The technique uses elliptic curve to encrypt asymmetrically. Ying Zhang [13] created a particle swarm optimization-based mobile node deployment methodology. It employed ECC encryption to authenticate mobile nodes travelling inside or between clusters. All network nodes must move, however. Nodes needed more hardware. Qi Jiang [14] reviewed the pros and cons of numerous encryption algorithms and noted that ECC is extensively utilised in UASNs due to its high security, small key, and simple generation. Existing research focuses on dynamic node authentication [15]. Existing large-scale self-organization networks cannot use these strategies. Disadvantages:

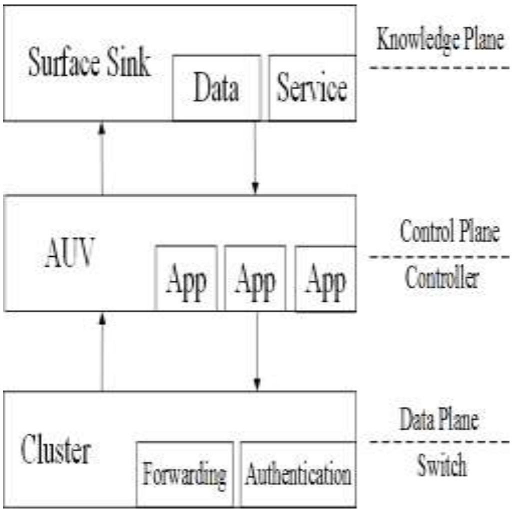
(1) Existing nodes authentication solutions for clustered networks employ asymmetric encryption, requiring the cluster head to maintain the global key. Head nodes require more storage.

(2) All nodes that contain global key information must update when a new node enters the network. The network is slow and inefficient.

III. THE SCALABLE SOFTWARE-DEFINITION ARCHITECTURE FOR UASNS

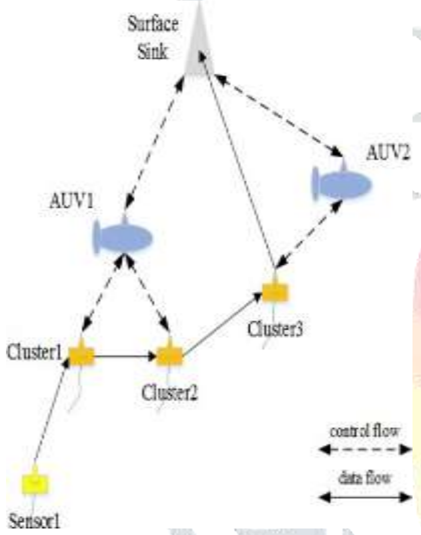
In the traditional IP network, network is becoming more and more rigid due to the complicated function of the router. This seriously hinders the development of new network technology and improvement of network performance. Therefore, SDN as the representative of the new network architecture hopes to leverage characteristics of centralized, separated data forwarding and control to eliminate the bottleneck of network development. However, in the study of software-defined UASNs, most of them use limited surface sink as a controller. This raises the problem of weak scalability and difficulty of application effectively in large-scale networks. Therefore, we have designed the scalable software defined architecture for UASNs (SSDUASNs) borrowing the idea of hierarchical, to

Improve the scalability of the network.



3.1 Architecture Design

An important feature of UASNs is its wide scope of coverage. So, it is unrealistic to implement the security authentication architecture by deploying single control node, which can't be applied in large-scale UASNs. Considering that UASNs itself has the characteristics of aggregating data from many sensors to surface sink, SSDUASNs partitions the network into three levels: data level, control level, and knowledge level.(Fig. 1) First of all, the common sensors are divided into several clusters according to traditional cluster idea. Each cluster consists of a cluster head node to authenticate the common sensors and collect the data of common sensors. All of these clusters constitute the network data level together which is responsible of data forwarding and security authentication. Then, partition the network into multiple independent control domains. Each control domain is composed of one AUV node as a controller and a number of clusters, which forms a SSDUASNs subnet. The control level of network is composed of AUVs, which mainly realizes the effective control of data forwarding and authentication in data level. Finally, at the top of the network, the surface sink is deployed to store overall information and provide service to the whole network, forming the knowledge level. This level is mainly responsible for the information distribution and decision-making of the whole network. Due to the independence and efficient interaction among three levels we achieve the centralized control of network forwarding and management. The additional benefit of this three level network architecture is the ability to get the utmost of existing vertical data aggregation channels to achieve effective control, without adding additional lateral interactions among different control domains.



3.2 Forwarding and Control

In SSDUASNs, the AUV as the controller can be centralized to obtain the current topology and information of entire control domain, while the surface sink in the knowledge level, can store the topology and information of entire network. Based on local and global information, the controller can manage the network effectively by running various control

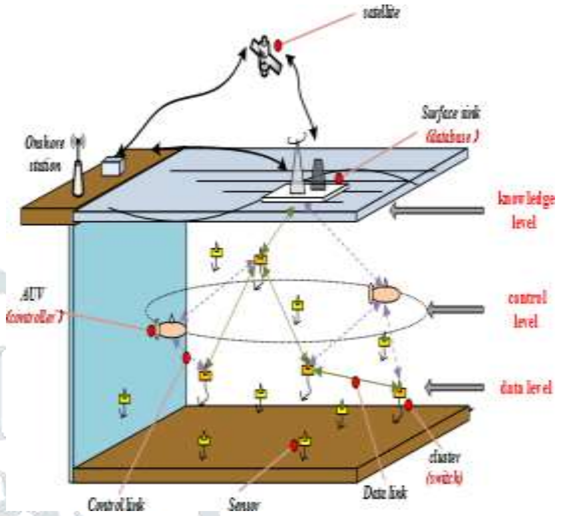


Fig. 1 The diagram of SSDUASNs

Fig. 2: The functions of different plane

Fig. 3: The channels of control flow and data flow

Components, such as routing, load balancing, access control and mobility management. As shown in Fig. 2, each cluster header node is merely responsible for forwarding data from sensors and security authentication for sensors. How to forward and authenticate the required key information are determined by the application components on the AUV controller. The application component running on the AUV can control the whole control domain autonomously. The AUV will initiate service requests to the surface sink, when the other control domain is involved, and make decision according to the service response. Take routing as an example, the data collected by sensors eventually converge to the surface sink. So all the Routing destinations are surface sink. Considering the physical scope and scale of the network, it is often necessary to transfer to the surface sink through multi-hop. As shown in Fig. 3, Sensor1 sends the collected data to the Cluster1 firstly. Then, AUV1, the controller of the Cluster1, initiates the routing query to the surface sink according to the source and the destination. The surface sink responds to the AUV1 according to the calculation path based on routing protocol and network topology. Finally, AUV1 distributes the routing rules to Cluster1 and Cluster2. The data of Sensor1 is forwarded to Cluster3 through Cluster1 and Cluster2. Cluster3 forwards data according to the control of AUV2.

IV. SECURITY AUTHENTICATION MECHANISM BASED ON SSD- UASNS

When a new sensor node wants to join the cluster, these authentication mechanisms will run. The two conditions as follows:

(1) The position of some nodes occur to offset due to the topological evolution of the network. Then they join the cluster again as the new identity.

a) Move within a cluster. After a node leaving its cluster due to environment, it returns again and needs to be authenticated by its cluster head. b) Move between clusters. A node belong to the A cluster transform to B cluster due to the topology dynamic evolution. It need to be authenticated by B cluster head node.

(2) The new node is added to UASNs.

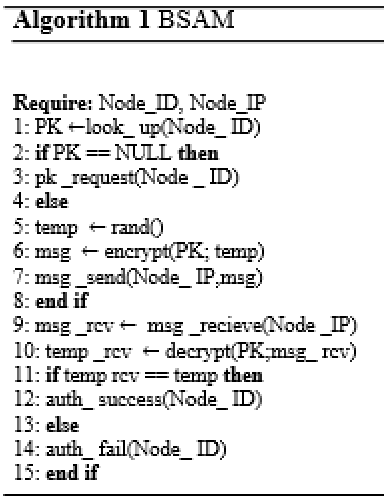
a) The New node is deployed underwater for optimizing network topology. b) Illegal nodes invade the network.

In the traditional security authentication mechanism for UASNs, the cluster head node which is composed of the common sensor node needs to complete all the authentication work independently. This greatly increases the over- head of cluster head nodes, which makes the network unable to flexibly deal with the problems of nodes mobility. In SS- DUASNs, due to the separation of data forwarding and control, the centralized control level and knowledge level can grasp the global information in real time. It can flexibly control the whole process of security authentication, and effectively reduce the authentication cost of cluster head nodes. In addition, programmable control level can provide convenient means for flexibly dispatching authentication process to improve the efficiency. Therefore, this paper studies the security authentication mechanism based on SSDUASNs.

4.1 Basic Security Authentication Mechanism (BSAM)

Because the nodes are frequently moved by the influence of the ocean currents and other factors in the UASNs, the new cluster header node need to be authenticated to maintain the security of the network when the nodes move from one cluster to the other. However, frequent nodes movements lead to frequent authentication processes. At the same time, because any node may move to different clusters, each cluster header node needs to store a large amount of authentication information, resulting in enormous storage overhead.

As shown in Algorithm1, when the cluster head finds a new node joined the networks, it queries Public key in the local storage according to the node ID (line 1). If the query result is empty, it indicates that the node is a newly added node, and sends the public key request to the controller (line 2-3). If the query hit in the local storage, it will Build the authentication message and sends to the new node (line 4-7). After received the authentication packet from the authentication node, the cluster head will perform analytical verification (line 9-10). If the authentication is successful, it enters the normal communication phase (line 11-12), otherwise, the data transmission is rejected (line 13-14). In this case, the controller will query the required key information from the surface sink when it receives the query request, and then return it to the corresponding cluster head node.



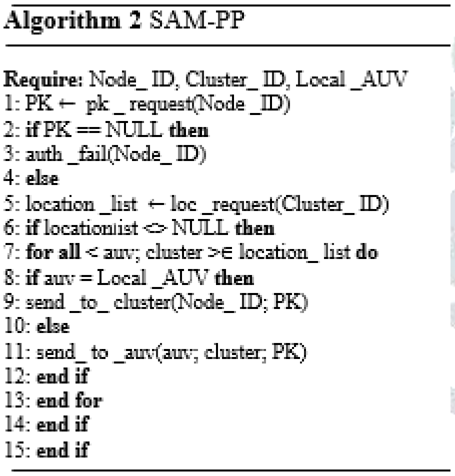
Algorithm 1 BSAM

```
Require: Node_ID, Node_IP
1: PK ←look_ up(Node_ ID)
2: if PK == NULL then
3:     pk _request(Node _ ID)
4: else
5:     temp ← rand()
6:     msg ← encrypt(PK; temp)
7:     msg _send(Node_ IP,msg)
8: end if
9: msg _rcv ← msg _recieve(Node _IP)
10: temp _rcv ← decrypt(PK;msg_ rcv)
11: if temp rcv == temp then
12:     auth_ success(Node_ ID)
13: else
14:     auth_ fail(Node_ ID)
15: end if
```

In the above-mentioned safety authentication process, the storage cost of the cluster head is limited to an acceptable stable range. It will not waste a lot of storage space be- cause of the uncertainty of newly added nodes. Compared with the traditional security authentication architecture, Authentication information only need to be stored by the surface sink, and not all cluster head nodes are stored. So the above architecture can be a good solution to the huge problem of storage costs. The larger the network size will be, the more benefit it will achieve. However, a fatal problem is that this architecture requires a roundtrip communication delay from the cluster head to the AUV, then to the AUV to the surface sink without reducing the time spent on the query. It just changes the cluster head local query to sink query. Considering the communication quality problem of the UASNs, this communication delay is much larger than the query de- lay, which makes it difficult for the security authentication process to be completed in a limited time. Therefore, the authentication process must be further improved in the security authentication architecture. It need to reduce the storage overhead while to reduce the authentication time.

4.2 Security Authentication Mechanism Based on Pre-push (SAM-PP)

The BSAM embodies the SDN centralized control idea, but not take full advantage of SDN's other features - flexible and programmable. In the SDN, the controller is the global manager. On the one hand it can easily access the entire network of information, on the other hand, it can flexible make decisions according to the entire network information. Therefore, to achieve some simple functions can be considered in the controller (AUV). Then, the various processes of security authentication can be scheduled more flexible. Another feature of UASNs is the dynamic topology. On the one hand, the nodes may unwork due to failure or energy depletion. On the other hand, the position of the nodes will be affected by the influence of ocean currents. However, for a cluster head, the newly discovered node may only have the following two kinds: (i) the new node is the newly deployed node; (ii) the new node moves from the other cluster. For (i), the deployed has inserted the authentication information of the node into the surface sink when the node is deployed, and the deployment location is determined. Therefore, when the new node is deployed, the surface sink can push the authentication information to the determined controller in advance. Then the controller push the information to the target cluster head, which completes the query process and the information request process in advance. The security authentication time can be greatly reduced. For (ii), the original cluster head can perceive the node to lose. The loss node can only move to the adjacent cluster in a finite time. The moving range of the node can be predicted according to the network topology. The main problem at this time is that the original controller can't push the authentication information to the cluster head node of the other domain, when the loss node moves beyond its original control domain. A viable solution is to add a simple communication protocol to the control level. The authentication information can be carried out between controllers. We named the security authentication process as SAM-PP. It is shown in Algorithm 2.



Algorithm 2 SAM-PP

```
Require: Node_ ID, Cluster_ ID, Local _AUV
1: PK ← pk _ request(Node _ID)
2: if PK == NULL then
3:     auth _fail(Node_ ID)
4: else
5:     location _list ← loc _request(Cluster_ ID)
6:     if locationiist <> NULL then
7:         for all < auv; cluster >∈ location_ list do
8:             if auv = Local _AUV then
9:                 send _to_ cluster(Node_ ID; PK)
10:            else
11:                send_ to _auv(auv; cluster; PK)
12:            end if
13:        end for
14:    end if
15: end if
```

The original cluster head of the mobile node reports the event to the controller after discovering the node loss. The controller initiates the authentication information query and the mobile range query to the surface sink according to the node identification and cluster identification (line 1-5). After the controller receives the authentication information and the mobile position prediction information, it is judged whether each possible moving position belongs to the control domain (line 7-8). If it belongs to the control domain, the authentication information is pushed directly to the tar- get cluster head (line 9). Otherwise the controller push the authentication information to the destination controller (line 10-11). The destination controller receives the push information and then pushes it to the corresponding cluster head to enable the push of the authentication information to all possible moving ranges.

The process of network security authentication can be divided into two parts: authentication information query and authentication interaction. The BSAM proposed in this paper will actually change the query process from traditional one-level query to one-level query (local query and remote query). The cluster head nodes cost smaller storage. What's more, SAM-PP cuts the multi-level query process. It makes the remote query with large time in the authentication process can be completed on the basis of the node movement prediction. Total delay in SAM-PP can be great reduced.

IV. SIMULATION AND PERFORMANCE ANALYSIS

5.1 Performance Analysis

The nature of the network is data transmission. So the evaluation of the network architecture can mainly be considered from the transmission efficiency. This paper mainly takes the effective throughput (good put) as the measure to analyze.

In UASNs, data is transmitted from the bottom to the surface sink. So the good put of the network refers to the amount of data received by the surface sink in the unit time. Obviously, the goodput is closely related to the network topology. Especially the node that communicates directly with the surface sink, its communication ability directly limits the goodput of the network. Secondly, the transmission efficiency and the transport protocol (routing protocol) also has a strong correlation. A good routing protocol can help improve network throughput. In Sect. 5.2, the detailed simulation experiments and results analysis will be provided.

In view of the shortcomings of the traditional security authentication mechanism, this paper mainly hopes to optimize the storage cost and authentication delay through the security authentication architecture in SSDUASNs. Two security authentication mechanism, BSAM and SAM-PP have been designed to reduce the additional energy loss as much as possible. The network storage overhead (M) consists of the storage overhead of the surface sink(M_S) and the storage overhead of each cluster head(M_{CH}).

$M = MS + MCH * NCH$ (1)

Where N_{CH} is the number of clusters. Without considering cluster overlap, the sum of the storage overhead of all cluster head is equal to the storage cost of the surface sink. The total delay of the authentication process is the length of time between the start of the authentication and the completion of the authentication. Therefore, in the BSAM, the total delay of the primary authentication is:

$T = TA + TB + TC$ (2)

Where T_A means the authentication interaction delay. T_Q means the authentication information query delay. T_C means the authentication information transmission delay. The authentication interaction is essentially the communication process between the cluster head and the node to be authenticated. So the magnitude of T_A and T_C is equivalent. Therefore, the query delay is the processing delay within the node, which is smaller than the magnitude of the transmission delay. In the SAM-PP, since the authentication process is separated, and the process of remote inquiry and information transmission is completed ahead. The total delay of the authentication is completed in:

$T=TA+TQ'$ (3)

Because the cluster head storage capacity is much smaller than the surface sink, so the local query delay (T'_Q) is slightly smaller than the remote query delay(T_Q).
The energy loss during network security authentication mainly includes three parts: energy consumption (E_{cpt}), storage energy consumption(E_m)and communication energy consumption(E_{com}).

E=Ecpt+Ecom+Em.(4)

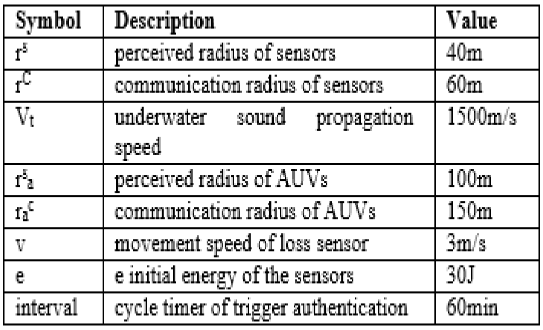
For cluster head nodes with limited capacity, BSAM and SAM-PP can effectively reduce the storage energy consumption of each cluster head. But they need to spend some communication energy consumption. Experiments show that in the two safety authentication mechanism, the increase in energy consumption in the proportion of 5% - 10% of the entire process of authentication. This energy cost is acceptable relative to its benefits in terms of storage and authentication latency.

5.2 Simulation Experiments

In order to verify the validity of the architecture (SSDUASNs) and two authentication mechanisms (BSAM and SAM-PP) proposed in this paper, the simulation experiments are carried out in the underwater monitoring area. The common sensors are affected by the current flow model [16]. Their positions will be changed. Table 1 shows the experimental parameters. After the node offset belongs to the cluster, the corresponding authentication mechanism is triggered. At the same time, one hour increments a new node to trigger the corresponding authentication mechanism. Four groups of experiments were performed.

Experiment 1: Comparison of goodput and control packets under different network architectures. The total size of nodes is set to 100, 200 and 300, respectively. The packet send rate for the node is set to 0.5pkt/s and 1pkt/s. In these cases, the Goodput under three different network architectures is compared. Among them, The SSDUASNs subnet consists of 5 clusters with 10 nodes per cluster. Multiple surface buoys are deployed in Soft Water, but too much buoys on the surface may affect running Ships and cause a variety of security risks. Due to the limited control range of buoys, they can be equivalent to one surface sink. In this experiment, the number of controllers is set to 1. The traditional distributed UASNs has no centralized control node. The size of each packet is 200bytes. The routing protocol uses the shortest path protocol, and the goodput and control packets is shown in Fig. 4 and Fig. 5. As shown in Fig. 4, goodput increases with the rate of packet generation and the expansion of network scale, under three different network architectures. Compared with the other two architectures, the larger the network scale, the more goodput of the SSDUASNS has. What's more, the gap is becoming more apparent as the scale increases. In traditional UASNs, data can only be forwarded through distributed routing while the convergence speed is slow and dynamic adaptability is poor in the data forwarding process.

Table 1: Experimental parameter settings



Symbol	Description	Value
r^s	perceived radius of sensors	40m
r^C	communication radius of sensors	60m
V_t	underwater sound propagation speed	1500m/s
r^s_a	perceived radius of AUVs	100m
r_a^c	communication radius of AUVs	150m
v	movement speed of loss sensor	3m/s
e	e initial energy of the sensors	30J
interval	cycle timer of trigger authentication	60min

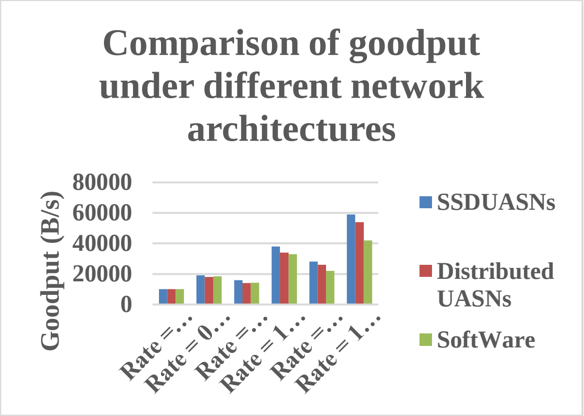


Fig. 4 Comparison of goodput under different network architectures.

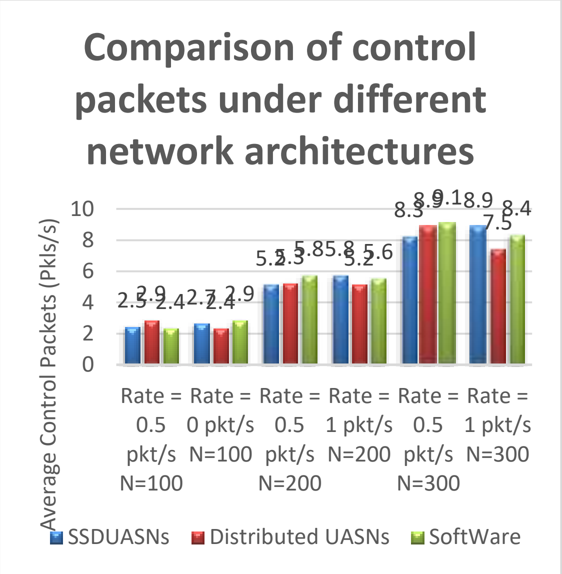


Fig. 5 Comparison of control packets under different network architectures.

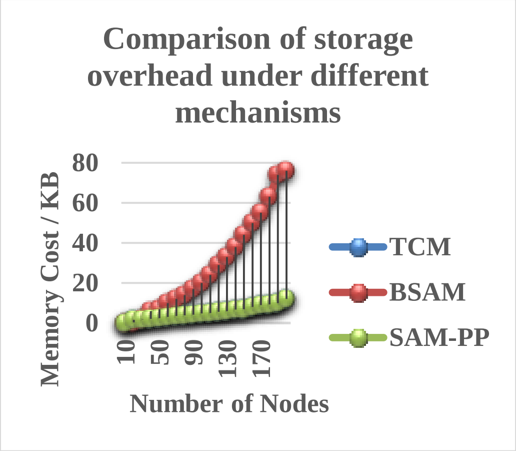


Fig. 6 Comparison of storage overhead under different mechanisms.

As a result, the transmission efficiency will be reduced with the increase of network scale. Figure 5 illustrates the average control packets under three network architectures. As shown in Fig. 5, the average number of control messages under different architectures is similar, and it only depends on the number of nodes. In fact, control messages of distributed UASNs are distributed evenly between nodes, while control messages of centralized SSDUASNs and Soft Water are mainly concentrated on the controller nodes. However, the Soft Water network is controlled only by surface sink. The control link is too long to lead to efficient control, and single controller is difficult to cope with large-scale requests. As the size of the network increases, its transmission efficiency is much lower than the distributed architecture. From the comparison, we can find that the SSDUASNS architecture proposed in this paper has good scalability and can work well in large-scale underwater networks.

Experiment 2: Comparison of storage overhead under different mechanisms. Discuss the nodes storage overhead with the size of network changes. Initially, the whole network has 10 nodes to form a cluster, belonging to an AUV. Follow up each time to add a cluster, we discuss the storage overhead changes in network. Adding an AUV after more than five new cluster joined in the networks. The two mechanisms proposed in this paper are compared with the TCM mechanism [13]. The storage overhead of each mechanism is shown in Fig. 6. As shown in Fig. 6, with the increase of network size, the network storage overhead of TCM mechanism is growing rapidly and the amplitude is very large. The two kinds of authentication mechanism proposed in this paper are relatively gentle in the storage cost, and the overall range is small. This is because each cluster head in the TCM needs to store the public key information of the global nodes. The more the number of nodes, the more the corresponding public key information will need to be stored. Then, the larger storage cost will be. In the two mechanisms proposed in this paper, the public key information of the whole network nodes are stored in the surface sink. The cluster head is only responsible for the public key information of the nodes in its cluster, which is less affected by the network size and has strong expansibility.

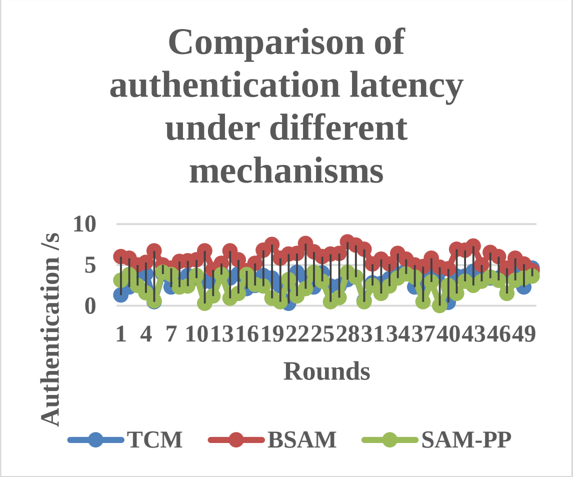


Fig. 7 Comparison of authentication latency under different mechanisms.

Experiment 3: Comparison of authentication latency under different mechanisms. The experiment 3 contrast are under the size of 200 nodes in UASNs. The average of 10 nodes to form a cluster, and the average of five clusters belong to an AUV. Using Monte Carlo method to run 50 rounds of simulation experiments. The experimental results are shown in Fig. 7. In Fig. 7, the of BSAM is about 6s. The average delay of TCM and SAM-PP delay are much smaller than BSAM, almost all about 3s. Because in BSAM, the global information is stored in the surface sink. When it needs to query the relevant node of the public key information in the certification process, the cluster head in BSAM requests the information to the AUV firstly, Then, AUV requests the information to the surface sink. The public key information of the relevant node is issued step by step. The communication process is long. A multilayer communication delay is added to local queries compared to TCM. While SAMPP will push the corresponding public key information after discovering the node lost. This parallel operating mechanism reduces the latency. The cluster head in SAM-PP storage range is much smaller than in TCM. Compared to TCM, the query process in SAM-PP is faster, and has a further advantage in the delay.

Experiment 4: Comparison of authentication energy consumption under different mechanisms. The experiment 4 contrast are under the size of 200 nodes in UASNs. The average of 10 nodes to form a cluster, and the average of five clusters belong to an AUV. In Fig. 8, compared with TCM, energy consumption differences in BSAM and SAM-PP are mainly reflected in the communication energy consumption and storage energy consumption. Total energy consumption growth is in less than 10%. The results show that BSAM and SAM-PP use additional communication to reduce storage overhead and delay overhead is feasible. The two mechanisms have little effect on network energy consumption and network life cycle.

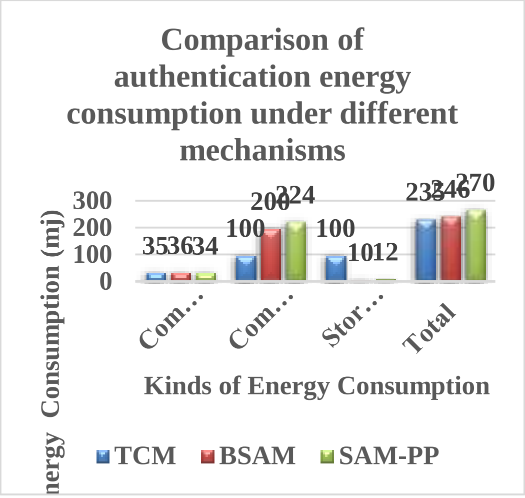


Fig. 8 Comparison of authentication energy consumption under different mechanisms.

V. CONCLUSION

The dynamic evolution of UASNs makes it difficult to expand the centralized SDN architecture in UASNs. And the frequent nodes movement and rapid topology change makes a great challenge to the security authentication between nodes. How to make full use of the characteristics of SDN and UASNs, effectively improve the scalability of the network, improve the efficiency of the node authentication, and reduce the influence caused by dynamic evolution of topology is an urgent problem to be solved. In this paper, a scalable software-definition architecture for UASNs (SSDUASNs) is introduced firstly. Then, two kinds of security authentication mechanism are designed based on SSDUASNs. One is named basic security authentication mechanism (BSAM). In order to reflect the advantages of flexible and programmable in this architecture, security authentication mechanism based on pre-push (SAMPP) is proposed in the further. The two mechanisms can guarantee the security access of new nodes, and reduce the network storage overhead and the information update delay. Next, we will further study the nodes communication problem.

References

[1] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, “SecFUN: Security framework for underwater acoustic sensor networks,” OCEANS 2015-Genova, pp.1–9, IEEE, 2015.

[2] Q. Wang, H.-N. Dai, X. Li, H. Wang, and H. Xiao, “On Modeling Eavesdropping Attacks in Underwater Acoustic Sensor Networks,” Sensors, vol.16, no.5, p.721, 2016.

[3] L. Bertaux, S. Medjiah, P. Berthou, S. Abdellatif, A. Hakiri, P. Gelard, F. Planchou, and M. Bruyere, “Software defined networking and virtualization for broadband satellite networks,” IEEE Commun. Mag., vol.53, no.3, pp.54–60, 2015.

[4] A. De Gante, M. Aslan, and A. Matrawy, “Smart wireless sensor network management based on software defined networking,” Proc. 2014 27th biennial symposium on communications, Kingston, ON, Canada, 1–4 June 2014, pp.71–75, IEEE, New York, June 2014.

[5] T. Luo, H.-P. Tan, and T.Q.S. Quek, “Sensor OpenFlow: enabling software-defined wireless sensor networks,” IEEE Commun. Lett., vol.16, no.11, pp.1896–1899, 2012.

[6] I.F. Akyildiz, P. Wang, and S.-C. Lin, “SoftWater: Softwaredefined networking for next-generation underwater communication systems,” Ad Hoc Networks, vol.46, pp.1–11, 2016.

[7] R. Fan, L. Wei, P. Du, C.M. Goldrick, and M. Gerla, “A sdncontrolled underwater mac and routing testbed,” MILCOM 2016 IEEE Military Communications Conference, pp.1071–1076, 2016.

[8] R. Fan, C.M. Goldrick, and M. Gerla, “An SDN architecture for under water search and surveillance,” 2017 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS), pp.96–99, IEEE, 2017.

[9] Yan, X., Li, B., Ye, X., “A key management scheme for mobile heterogeneous sensor networks,” J. Naval Univ. Eng., vol.29, no.1, pp.48–52, 2014.

[10] S. Verma and Prachi, “A Cluster based Key Management Scheme for Underwater Wireless Sensor Networks,” Int. J. Computer Network and Information Security, vol.7, no.9, p.54, 2015.

[11] X. Zhang, J. He, and Q. Wei, “Key managing for node mobility scenarios in wireless sensor networks,” J. Southeast Univ., vol.41, no.3, pp.227–232, 2011.

[12] V.S. Miller, “Use of Elliptic Curves in Cryptography,” Advances in Cryptology, CRYPTO85, pp.417–426, Springer, Berlin, Germany, 1986.

[13] Y. Zhang, W. Chen, J. Liang, B. Zheng, and S. Jiang, “A Network Topology Control and Identity Authentication Protocol with Support for Movable Sensor Nodes,” Sensors, vol.15, no.12, pp.29958–29969, 2015.

[14] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He, and N. Chilamkurti, “A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks,” Int. J. Network Management, vol.27, no.3, 2016.

[15] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, “Cloudaided Lightweight Certificateless Authentication Protocol with Anonymity for Wireless Body Area Networks,” J. Network and Computer Applications, vol.106, pp.117–123, 2018, DOI: 10.1016/j.jnca.2018.01.003.

[16] A. Caruso, F. Paparella, L.F.M. Vieira, M. Erol, and M. Gerla, “The meandering current mobility model and its impact on underwater mobile sensor networks,” INFOCOM, 771-779, Phoenix, USA, 2008.

[17] Sushama Singh ; Atish Mishra ; Upendra Singh , “Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm ” , Symposium on Colossal Data Analysis and Networking (CDAN) , 2016, pp. 1-5.

[18] Neeraj Arya ; Upendra Singh ; Sushma Singh , “Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm ”, International Conference on Computer, Communication and Control (IC4) , 2015, pp. 1-6.

[19] Jain, A.K., Tokekar, V., Singh, U., “Detection and avoidance of integrated attacks on MANET using trusted hyperbolic AODV routing protocol”. J. Mob. Comput. Commun. Mob. Netw. 3, 21–34 (2016)

[20] Singh, U., Samvatsar, M., Sharma, A., Jain, A.K., “ Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol”, In: Symposium on Colossal Data Analysis and Networking (CDAN), pp. 1–6 (2016)

[21] Mukesh Muwel ,Prakash Mishra ,Makrand Samvatsar, Roopesh Sharma , Upendra Singh , “Efficient ECGDH Algorithm Through Protected Multicast Routing Protocol In Manets” , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-7.

[22] Lokesh Baghel ,Prakash Mishra ,Makrand Samvatsar , Upendra Singh,“ Detection Of Black Hole Attack In Mobile Ad Hoc Network Using Adaptive Approach ”, Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.

[23] Amar Singh Chouhan ,Vikrant Sharma ,Upendra Singh, “A Modified AODV Protocol To Detect And Prevent The Wormhole Using Hybrid Technique ”,

Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.

[24] Roshani Verma ,Roopesh Sharma ,Upendra Singh, “New Approach Through Detection And Prevention Of Wormhole Attack In MANET”, Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.

[25] Vibhavarsha Prakaulya ,Neelu Pareek ,Upendra Singh, “Network Performance In IEEE 802.11 And IEEE 802.11p Cluster Based On VANET” , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.

[26] Vidya Kumari Saurabh ,Roopesh Sharma ,Ravikant Itare , Upendra Singh , “Cluster-Based Technique For Detection And Prevention Of Black-Hole Attack In Manets” , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.

[27] Ravi Parihar ,Ashish Jain ,Upendra Singh , “Support Vector Machine Through Detecting Packet Dropping Misbehaving Nodes In MANET” , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.

[28] Divyanshu Wagh ,Neelu Pareek ,Upendra Singh, “Elimination Of Internal Attacks For PUMA In MANET” , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.