SCIENCE AND TECHNOLOGY ORGANIZATION
CENTRE FOR MARITIME RESEARCH AND EXPERIMENTATION

Reprint Series CMRE-PR-2019-050

Toward the development of secure underwater acoustic networks

Chhagan Lal, Roberto Petroccia, Konstantinos Pelekanakis,
Mauro Conti, João Alves

May 2019

Originally published in:

IEEE Journal of Oceanic Engineering, volume: 42, issue: 4, October 2017, pp. 1075-1087, doi: 10.1109/JOE.2017.2716599

About CMRE

The Centre for Maritime Research and Experimentation (CMRE) is a world-class NATO scientific research and experimentation facility located in La Spezia, Italy.

The CMRE was established by the North Atlantic Council on 1 July 2012 as part of the NATO Science & Technology Organization. The CMRE and its predecessors have served NATO for over 50 years as the SACLANT Anti-Submarine Warfare Centre, SACLANT Undersea Research Centre, NATO Undersea Research Centre (NURC) and now as part of the Science & Technology Organization.

CMRE conducts state-of-the-art scientific research and experimentation ranging from concept development to prototype demonstration in an operational environment and has produced leaders in ocean science, modelling and simulation, acoustics and other disciplines, as well as producing critical results and understanding that have been built into the operational concepts of NATO and the nations.

CMRE conducts hands-on scientific and engineering research for the direct benefit of its NATO Customers. It operates two research vessels that enable science and technology solutions to be explored and exploited at sea. The largest of these vessels, the NRV Alliance, is a global class vessel that is acoustically extremely quiet.

CMRE is a leading example of enabling nations to work more effectively and efficiently together by prioritizing national needs, focusing on research and technology challenges, both in and out of the maritime environment, through the collective Power of its world-class scientists, engineers, and specialized laboratories in collaboration with the many partners in and out of the scientific domain.

NOTE: The CMRE Reprint series reprints papers and articles published by CMRE authors in the open literature as an effort to widely disseminate CMRE products. Users are encouraged to cite the original article where possible.

Toward the Development of Secure Underwater Acoustic Networks

Chhagan Lal, *Member, IEEE*, Roberto Petroccia, *Member, IEEE*, Konstantinos Pelekanakis, *Member, IEEE*, Mauro Conti, *Senior Member, IEEE*, and João Alves, *Senior Member, IEEE*

***Abstract*—Underwater acoustic networks (UANs) have been recognized as an enabling technology for various applications in the maritime domain. The wireless nature of the acoustic medium makes UANs vulnerable to various malicious attacks, yet, limited consideration has been given to security challenges. In this paper, we outline a hybrid architecture that incorporates aspects of physical layer security, software defined networking, node cooperation, cross-layering, context-awareness, and cognition. The proposed architecture envisions strategies at the node as well as at the network level that adapt to environmental changes, the status of the network and the possible array of attacks. Several examples of attacks and countermeasures are discussed while deployment and functionality issues of the proposed architecture are taken into consideration. This work is not intended to represent a whatsoever proven solution but mainly to suggest future research directions to the scientific community working in the area of UANs.**

***Index Terms*—Cognitive networks, context-aware security, cross-layering, denial-of-service (DoS) attacks, physical layer security (PLS), security, software-defined underwater networks, underwater acoustic networks (UANs).**

I. Introduction

UNDERWATER networks have become an important area of research with potential impact on a host of different applications, including monitoring and discovery of the marine environment, remote control of submarine oil extraction, coastline protection, and critical infrastructure surveillance [1], [2]. In the last decade, increasingly capable and reliable underwater communication technologies have been made available to users and researchers alongside the growth of the maritime robotics field. The state of the art in underwater communications has evolved from the deployment of few underwater communications assets from the same manufacturer, to that of networks composed by few tens of heterogeneous nodes, including teams of cooperating autonomous underwater and surface vehicles. The size expansion and the complexity of the network led to the problem of efficient delivery of the data to and from the network nodes.

Given the high attenuation of optical/radio waves in water, acoustic waves are currently the most reliable means to communicate underwater over large distances. However, the use of acoustic transmissions in water incurs several medium-specific challenges, such as long propagation delays, low data rate, and several temporal and spatial fluctuations affecting the quality of the received signals (multipath, attenuation, ambient noise, Doppler, to name a few), which complicate the implementation of reliable networks.

Considering the challenges imposed by the underwater acoustical channel, it has become clear that trying to simply reuse terrestrial solutions is not performing as expected. Many distributed and ad hoc solutions addressing channel reservation and message routing have been therefore proposed for UANs in the recent past [3]. From the wide spectrum of solutions, it is safe to say that there is no solution fitting all the possible scenarios, since the communication parameters (intrinsic and channel dependent) may significantly vary in space and time. Additionally, all aspects related to security have been marginally investigated (or not considered at all) leaving room for potential attackers, which might make a UAN unusable [4].

The properties of acoustic channels and underwater networks exposes UANs against a large array of malicious attacks. Novel scalable and efficient networking security solutions have to be explored to increase the level of flexibility and adaptation currently provided. To reach this goal and overcome the limitations imposed by the existing monolithic integrated modems and communications stacks, a software defined networking (SDN) system would be beneficial with the support for significant cross-layering, from physical coding to routing and application. Accurate context awareness at the node and network level can also help to forecast in real-time potential challenges and risks [5]. Not only reliability but also security should be a key metric that needs to be considered in the decision of the different networking protocols and node components. We therefore propose the inclusion of new underwater security techniques based on physical layer security (PLS), software-defined cognitive networks, and context-aware (or context-centric) networking to build the next generation of UANs architecture.

The rest of this paper is organized as follows. Section II describes the state of the art of security for UANs, it includes the attack vector, possible countermeasures and challenges. Future

Manuscript received January 24, 2017; revised May 24, 2017; accepted June 12, 2017. Date of publication July 6, 2017; date of current version October 11, 2017. This work was supported in part by the EU TagItSmart Project (agreement H2020-ICT30-2015-688061), in part by the projects "Physical-Layer Security for Wireless Communication," and "Content Centric Networking: Security and Privacy Issues" funded by the University of Padua, in part by the project CNR-MOST/Taiwan 2016-17 "Verifiable Data Structure Streaming," and in part by the NATO Allied Command Transformation. The work of M. Conti was supported by the Marie Curie Fellowship funded by the European Commission (agreement PCIG11-GA-2012-321980). *(Corresponding author: Roberto Petroccia.)*

Guest Editor: I. Akyildiz.

C. Lal and M. Conti are with the Department of Mathematics, University of Padova, Padova 35122, Italy (e-mail: chhagan@math.unipd.it; conti@math.unipd.it).

R. Petroccia, K. Pelekanakis, and J. Alves are with the NATO Science and Technology Organization, Centre for Maritime Research and Experimentation, La Spezia 19126, Italy (e-mail: roberto.petroccia@cmre.nato.int; konstantinos.pelekanakis@cmre.nato.int; joao.alves@cmre.nato.int).

Digital Object Identifier 10.1109/JOE.2017.2716599

TABLE I
LAYERED-BASED CLASSIFICATION OF SECURITY ATTACKS, INFORMATION SECURITY PRINCIPLES AFFECTED (CONFIDENTIALITY, AVAILABILITY, INTEGRITY, AUTHENTICATION), AND COUNTERMEASURES IN WIRELESS NETWORKS

OSI layer	Attacks	Issues	Countermeasures
Physical	Jamming	A	Spread spectrum techniques, multi-frequency communications, lower duty cycle, strong forward error correction codes
	Tampering	A+I	Encryption algorithms, memory erase
Datalink	Collision	A	Retransmission protocols
	Exhaustion	A	Limit number of retransmissions
	Unfairness	A	Small packets, scheduling protocols, rate limitation
Network	Sybil (multiple identities)	Auth	Authentication, secure positioning
	Wormhole	A	Secure location of nodes, traffic monitoring
	Sinkhole	C+A+I	Traffic monitoring, authentication, multipath routing
	Selective forwarding (message dropping)	A+I	Multipath routing (overhead), authentication (overhead), reputation and trust
Transport	Flooding	A	Limit broadcast range of nodes, non-contention based protocols
	Desynchronisation	A+Auth	Synchronisation protocols, authentication

research and way forward to achieve security in the underwater domain is discussed in Section III. In particular, this section discusses the key elements to consider for the development of a reliable and robust underwater networking system, including aspects of PLS, cross-layering, cognition, node cooperation, and context-awareness along with SDN paradigm to enhance the communication reliability and security in the network. Section IV describes the design and working methodology of our proposed SDN-based UAN architecture, making use of the aforementioned key elements. This section also describes potential deployment challenges and issues of the proposed hybrid architecture. Finally, concluding remarks are given in Section V.

II. ATTACKS, COUNTERMEASURES, AND CHALLENGES IN UANS

The focus of this section is to identify limitations in current security solutions and provide future research directions. The interested reader is directed to [6]–[8], for an in-depth survey of attacks and countermeasures in UANs. Following the radio paradigm, Table I classifies the security attacks based on the open systems interconnection (OSI) protocol stack as well as according to the following information security principles:

1) confidentiality, i.e., information is concealed from unauthorized nodes;
2) availability, i.e., information must be available when it is needed;
3) integrity, i.e., the contents of the transmitted data have not been tampered with or modified;
4) authentication, i.e., reliability of information by identifying its origin;

The most common yet highly destructive denial-of-service (DoS) attack is the jamming attack performed at the physical layer. During a jamming attack, a malicious node continuously floods the channel with illegitimate signals to deny services to legitimate users. In [9] and [10], Zuba *et al.* introduce and analyze the effects of jamming on UANs using real-world field tests. Due to the long and time-varying multipath of underwater acoustical channels, spread spectrum jamming mitigation approaches used in the terrestrial domain are less effective in UANs. Multipath routing, used to avoid the jammed area of the network [11] is difficult to implement due to the typically sparse deployments of underwater sensors.

Another widely studied attack in UANs is a wormhole. In a wormhole attack, the colluding attackers create a virtual high-quality tunnel between two distant legitimate nodes making them believe they are neighbors. Wormhole attacks pose severe obstacles in the discovery of any routes other than the wormhole. In [12], Wang *et al.* use a multidimensional scaling technique, which allows each node to reconstruct the network topology up to two hops, thus preventing the wormhole attack. However, the dependency on secure distance estimation is very challenging in the underwater domain due to the relatively short time changes of the sound speed and so it limits its applicability. Another approach to mitigate the wormhole attack is proposed in [13], which uses the direction of arrival (DoA) of acoustic signals for secure neighbor discovery. The complexity and latency in true neighbor discovery using DoA is high, thus consuming the scarce network bandwidth and node energy.

Location spoofing and sybil attacks are performed by impersonating false node location and identity (ID). These kinds of attacks target multipath routing and topology maintenance. A secure pressure routing protocol using cryptographic techniques, implicit acknowledgments, geographic constraints, and randomization is proposed in [14] to mitigate location spoofing. In [15]–[18], the authors present a complete security suite to protect integrity and confidentiality of received messages using cryptographic-based authentication, thus securing from internal attacks such as spoofing, replay, and sybil. Additionally, in [19], Ibragimov *et al.* proposed an energy-efficient secure message authentication code (MAC) protocol using counter with cipher block chaining-message authentication code along with the advanced encryption standard techniques, to achieve data integrity, confidentiality, data authentication, and replay attack prevention in UANs. However, the use of encryption and authentication processes increases the size of the communication messages, thus reducing the limited network resources. Furthermore, the scalability of such solutions is questionable due to high computational complexity, energy consumption, and overhead for the one-to-one key and group key maintenance and distribution. The cryptographic technique and configuration parameters to use should be carefully selected considering the tradeoff between performance and resilience of the system.

In a sinkhole attack, network traffic is directed into a node, which typically advertises itself as a zero-cost node. The aim of this attack is to drop all or a selection of the received data packets. To mitigate such attacks in UANs, multilevel trust and reputation-based solutions have been proposed [20], [21]. However, the tradeoff between the estimation of accurate trust values and the introduced overhead should be considered carefully when applying these solutions. Another possible attack is represented by the silent monitoring of UAN communications without causing any disruption, i.e., eavesdropping attack. In some cases, the deployed UAN needs to stay undetected (e.g., military, coastguard, and homeland security applications) and procedures have to be put in place to avoid the eavesdropping by an adversary or a group of adversaries. Ling *et al.* [22]

and Yang and Yang [23] exploit the benefits of direct-sequence spread-spectrum (DSSS) modulation to achieve covert UAN communications. On a similar note, Kulhandjian *et al.* [24] concentrate on the problem of securely transmitting a confidential message in the presence of eavesdropping attacks by keeping the communication covert but not undetectable. The proposed solution relies on cooperative friendly jamming scheme, which is implemented using code-division multiple access based analog network coding.

It is clear that attacks at different layers will affect different security principles and require different countermeasures. Independent (layered) countermeasures could result in conflicting requirements leading to network performance degradation. For instance, the use of more robust waveforms at the physical layer and more sophisticated encrypted transmissions can be effectively used to secure the communication channel between two nodes, however, many other DoS attacks (such as wormhole or sinkhole) can render the network unusable. Recently, Martin and Rajasekaran [25] proposed a possible way to detect and mitigate DoS attacks in UANs by using information centric networking (ICN) techniques. The ICN requires that each node collects information about neighboring nodes and overall nearby transmissions, and uses machine learning tools on the collected information to identify possible malicious nodes. Another approach to efficiently counteract the DoS attacks is through the use of cross-layer information (see Section III-B). For instance, information about the quality and reliability of the underwater links need to be collected and provided at the upper layers over time. Additionally, upper layers need to be able to set key physical layer parameters (transmission rate, transmission power, and modulation scheme) according to the protocol strategies and to various metrics, such as data priority, lifetime of the generated information, required quality-of-service (QoS), node and network status and resources. However, cross-layer solutions are challenged by the fact that current technology is based on rigid, closed, proprietary all-in-one implementations of acoustic modems, and protocol stacks. A promising way forward is to develop a software-defined architecture (see Section III-C) that will provide the required mechanisms to share vital information among the different layers of the stack.

III. Fostering Security in Underwater Networks

To provide strong security measures against various internal and external attacks in UANs, we present envisaging solutions based on PLS, software-defined cognitive networking with the support for cross-layering communications [26], [27] and context-aware networking. Along this line, we propose an architectural design for next-generation UANs and discuss its potential in counteracting possible DoS attacks in the underwater domain (major features of the proposed design are displayed in Fig. 1). The features shown in the lower part of the Fig. 1 are mandatory for all the nodes in the proposed UAN design, while the one shown in the upper part (i.e., dashed box) are optional. Only a reduced set of nodes, equipped with more resources (i.e., controllers) will execute these additional tasks (all or a subset of them).

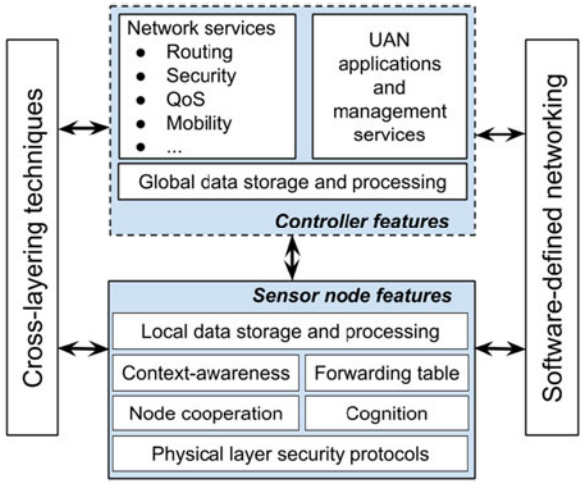

Fig. 1. Major features running at the nodes depending upon their role(s) and resources in the next-generation UAN architecture.

An underwater network composed by mobile and static nodes (underwater and surface) bridging underwater and terrestrial networks, and a command and control station (C2S) is considered. The C2S can be placed onshore or onboard a ship. Commands and data are transmitted in and out of the network. The proposed underwater network can be employed in various operational scenarios, including distributed surveillance, and monitoring systems. When available, mobile surface, and underwater nodes can be used for various purposes such as data muling, replacement of damaged sensors, filling short-term connectivity holes, and adjusting the network topology to counteract any on-going attacks.

In what follows, we discuss the main security concepts, the design and the challenges of the proposed architecture.

A. Physical Layer Security

Security of information (authentication, confidentiality, and privacy) is typically handled by a higher-network-layer utilizing crypto-based methods. However, increasing the key length and/or the frequency of the key updates are not viable solutions in UANs due to the severely limited bandwidth available. In addition, any cryptographic algorithm is at stake with the advent of quantum computers [28].

A fundamentally different approach to security has emerged from the area of information theory under the term PLS. It relies on the characteristics of the physical layer, i.e., the channel itself, to provide confidentiality. The generation of a secret key among two legitimate users through public conversation is possible even when the communication channel among the latter is worse than the eavesdropper's [29]. Information-theoretic approaches for key generation based on sharing a common source of randomness, e.g., impulse response of the reciprocal channel, frequency selectivity, received signal strength, to name a few, in the wireless channel can be found extensively in the literature [30], [31]. In [32], secret keys are obtained by direct sampling of the channel impulse response. In [33]–[35], delay profiles of ultrawideband channels are processed for key genera-

TABLE II
PACKET FORMAT FOR SECURE UANS

Header	Packet sequence number	Payload
Nonencrypted	Encrypted	

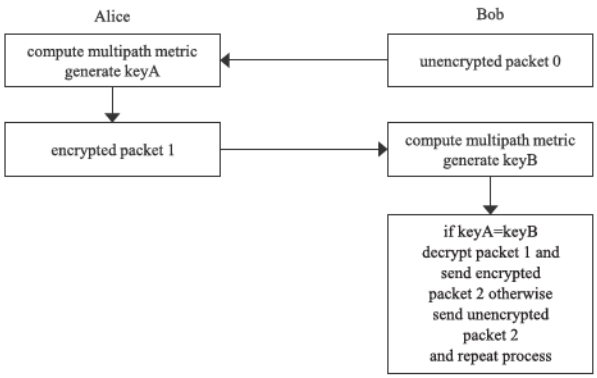

Fig. 2. Physical layer key management protocol.

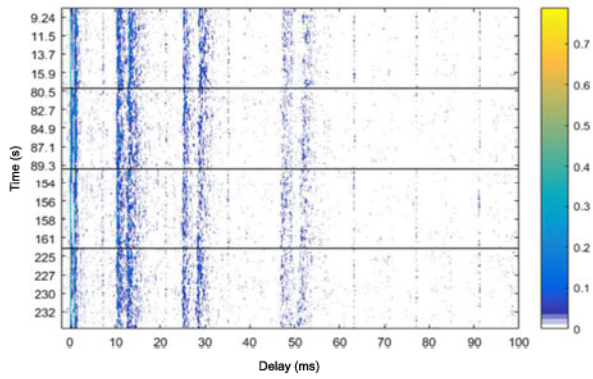

Fig. 3. Snapshots of a shallow water time-varying channel response. The x-axis shows multipath delay, the y-axis shows absolute time, and the z-axis shows the channel amplitude in linear scale. The black horizontal lines are used to visually separate different transmission times. The data processed here was recorded during REP16-Atlantic at-sea trial on July 21, starting at 8:28 coordinated universal time (UTC).

tion. The impact of sparsity on the secret key capacity is studied in [36]. In the underwater domain, Luo *et al.* [37] investigated secret key generation exploring the received signal strength, while in [38], a protocol that generates secret keys dynamically based on the channel frequency response is proposed.

Based on the reciprocity theorem, our idea is to exploit the unique multipath characteristics between two nodes to generate a cryptographic key. Let us assume that the packet structure is composed by three parts: header, sequence number, and payload (see Table II). The header is used for synchronization and channel estimation purposes. The sequence number is used to prevent replay attacks and becomes an integral part of the key generation process. The payload carries the data. The key is independently generated between the receiver and the transmitter and is the combination of a measured channel multipath metric and a pseudo number. This multipath metric is fed to a k-bit quantizer. To further enhance the randomness of the key, a pseudorandom m-bit string is appended at the end of the k-bit channel metric. The pseudorandom bit string is a function of the packet sequence. The key length, $k + m$, dictates the strength of the encryption against a brute force attack. The possibility to add (e.g., by performing XOR addition) the physical-layer key into state-of-the-art cryptographic techniques (e.g., Galois counter mode [39]) for enhanced security can be considered.

For example, let us assume that (authenticated) node Bob is requesting to secretly talk to (authenticated) node Alice. The key negotiation protocol between Bob and Alice is seen in Fig. 2. First, Bob sends an unencrypted packet. Second, Alice measures the multipath metric of the link from the header, generates keyA and sends an encrypted packet based on that key. Third, Bob measures the multipath metric of the link and generates keyB. If keyA = keyB, successful packet decryption is possible otherwise Bob transmits an unencrypted packet.

It is vital that the considered multipath metric remains invariant for a period longer than the time of a two-way communication transaction. From Fig. 3, there is evidence that a metric depending only on the relative multipath delays could serve our purposes. This figure was generated after processing four transmissions of a 10-s-long binary phase-shift keyed (BPSK) channel probe (9.6–15.3 kHz) though a shallow water channel (100-m depth). After stacking the respective channel responses in time, one observes that the total reception interval lasts about 4 min (234 s). The 0-ms delay corresponds to the fastest arrival and the observed multipath spread is about 55 ms. Note that the multipath delay (not the amplitude) structure between the two nodes remains constant for a period of 4 min, which is long enough to cover a typical two-way communication transaction. In the unfortunate event of rapid multipath delay fluctuations, an exception rule accounting for the maximum time allowed for a key confirmation can be implemented. If that maximum time elapses, the nodes must revert back to the previously established key. In case the nodes did not manage to establish any key, a preinstalled common key will be applied.

B. *Cross Layering*

Recent trends in protocol design show that cross-layer techniques can impact protocol performance positively, especially in networks with limited resources and/or deployed in challenging environments, such as UANs [40], [41].

Separately addressing secure actions at each layer of the stack, as traditionally done in the OSI stack, can lead to less secure and sometimes conflicting overall strategies, which can potentially result in an overall degradation of the network performance. Sharing all the relevant information across the stack would make possible to have a better picture of the status of the network and to have the different layers working as a single and coordinated unit. This empowers each layer to adapt and react in the best way possible to the changes and attacks occurring in the network. The use of physical layer information about the quality of the links to reach neighbor nodes (in terms of signal-to-noise ratio, bit error rate, to name a few) is a key element for the selection of the modulation and coding scheme to use, according to the required transmission rate and the supported transmission power. Sharing this information with the upper layers of the protocol stack

would make possible to adjust the use of control messages,[1] and the selection of the next hop and route to follow for message delivery. Similarly, the upper layers of the stack need to share QoS data, e.g., message priority and maximum delivery time, to drive the selection of lower layers parameters.

A possible way to implement this flexible exchange of information is through the definition of a cross-layer messaging channel, as presented in [27] and [42]. This messaging channel can be used by all modules and layers, which are locally available on the underwater node, to share contextual data regarding their operation and status. A publish-and-subscribe mechanism can be adopted. Using this mechanism, each module can publish individual messages on a variable, parameter or topic that may be read by any module that subscribes to update for that information. This mechanism automatically provides the published data to the subscribed modules. Similarly, each module can notify the other ones about the data it can provide and the data are interested in. This makes possible to have all the modules and layers informed about the full set of provided and requested information and to better plan the activities to perform. This publish-and-subscribe mechanism represents an efficient solution to have all systems components sharing the full picture about the data that can be used to enhance the robustness and security of the system [27], [42].

C. Software Defined Networking

The use of a rigid and inflexible communication system in UAN imposes significant challenges when trying to adopt new management services, communication designs, and networking protocols. Additionally, it negatively affects the utilization of resources, deployment cost, communication robustness, and network security. In designing the next generation of UANs, the use of a SDN paradigm is a promising way forward, enabling to select in real time the most suitable communication protocols to use at all the different layers of the stack, thus addressing the lack of adaptiveness, security, and heterogeneity in current underwater communication systems.

SDN enables the network control to be programmable and the underlying infrastructure to be abstracted for applications and network services. It was initially introduced for data center networks for the purpose of efficient management and processing of the huge amount of data generated in such networks [43]. Latter, SDN has been extended to support the next-generation wireless networks, such as Internet of Things [44] and 5G [45]. Recently, for the first time in [46], Akyildiz *et al.* discussed an SDN-based next-generation architecture for underwater communication systems called "SoftWater." SoftWater architecture shows that the use of SDN techniques can easily incorporate new underwater communication protocols, thus maximizing network capacity while achieving network robustness and energy efficiency. However, the work uses few bold assumptions such as resourceful sensor nodes, and specialized hardware devices. Furthermore, the proposed SoftWater architecture partially covers the analysis of the critical issues such as routing, security, energy efficiency, and deployment feasibility.

[1]The use of control messages can be more intense over reliable links, while it could introduce a bottleneck over less reliable links.

D. Cognition

Selecting the best way to communicate among possible solutions has been widely addressed in terrestrial RF transmission systems with the use of software defined radio and cognitive radio systems. In simple terms, cognitive radio is the smart engine behind the configuration of the software defined radio system. It consists in the capability to decide how to program and configure dynamically the radio transceiver to use the best available wireless channels. Very little work has been published on applying the cognitive radio paradigm to the underwater acoustical channel. Adopting such a solution would have a significant impact on the capability to select appropriate modulation methods and receiver parameters that will maximize the usable bandwidth.

Recent at sea experiments in [47]–[49], have shown the capability to perform adaptive modulation for underwater acoustical channels. Pelekanakis *et al.* in [47] focused on single-carrier modulation and a machine learning approach based on decision trees is used. In [48], the focus is on orthogonal frequency-division multiplexing (OFDM) and different modulation and power levels are achieved based on efficient channel estimation and prediction. In [49], a modem with real-time adaptation between OFDM and DSSS was implemented and tested in a lake environment. The above approaches pave the way for smart, adaptable solutions to be employed at the physical layer, offering reactive solutions to tackle the dynamic challenges of the underwater acoustical channel.

While in the terrestrial domain the cognitive paradigm has been adopted mainly on programming and configuring dynamically the radio transceiver, recent works in UANs address a more extended use of the cognitive component across the protocol stack. In [27] and [42], the use of decision modules at all the layers of the communication stack is presented as a key component to select the most suitable protocol to use, depending on the channel and network conditions. In [50], a decision module selecting the most suitable medium access control protocols is presented.

With the design of more flexible and capable communication solutions, cognitive modules can be used at the physical layer, as well as for channel reservation, message routing, network coding, packet fragmentation, and reassembling. All the cross-layer information, collected locally at the node or coming from the network, can be used to construct a better picture of the status of the system. The cognitive component can then use this information to configure the SDN modules and to ensure that the decisions and actions taken at node level reflect the strategies and the needs of the overall network. These decision and actions have to consider security as a key metric, thus enabling a reliable and robust data exchange in the network.

E. Context Awareness

Context-aware solutions [51] aims at exploiting the context in the proximity of a node, when possible, to derive information and similarities or dissimilarities about the network nodes. In UANs, nodes deployed in different areas of the network that are able to communicate using long range acoustic transmissions (in the order of several kilometers) might not be similar in terms of depth, temperature, salinity, conductivity, and other external features (such as marine life and bathymetric profile), as shown

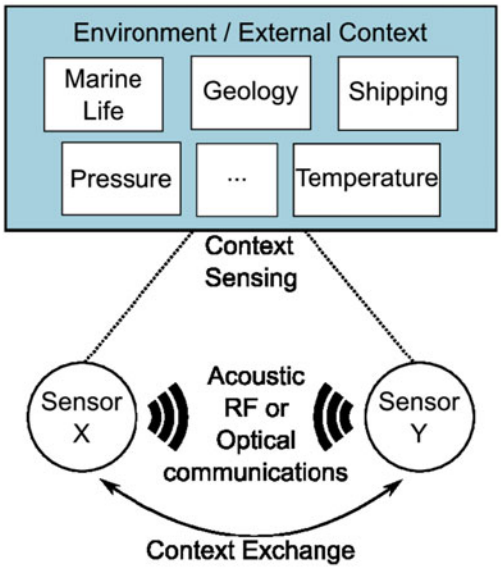

Fig. 4. Context-awareness for neighbor verification.

in Fig. 4. Similarly, the structure of the received signal may be different across various links.[2] This information can be used to detect anomalies in the information transmitted by nodes that claim to be neighbors, thus increasing the overall robustness and security of the system.

One of the examples where context-aware based solutions can be applied is the routes discovery process in a multihop UAN. Context information collected at a node can be then used to verify whether the claiming node(s) are in proximity (i.e., neighbors) during the context-aware route discovery phase. This way, context-aware routing can identify the true neighbors and reject routes that include suspected adversary nodes.

F. Adaptive Trust and Reputation Models

In a reputation system [53], each sensor node keeps a reputation value for all its neighbor nodes based on historical information such as the success of the past transmissions. The accuracy of such systems depends on the reliability of the collected information and on the metrics used for trust estimation. During the computation and assignment of reputation values to the neighbor nodes, the following aspects should be carefully considered: unreliability of underwater channels, possible involvement of security attacks, energy consumption, and node mobility.

To increase the security and accuracy of the reputation system, the use of context information and of cross-layer metrics needs to be integrated in the process of estimating trust values for neighbor nodes. A node using the context information can check whether the neighbor's current behavior is affected by a nearby adversary before assigning a reputation value. Different tradeoffs have to be explored between the use of an increasing number of cross-layer metrics and the introduced overhead and delays. Unlike the reputation systems used for terrestrial sensor networks, the following metrics should be considered in UANs:

1) trust calculations for sensors as well as the data they transmit (to handle data modification attacks);
2) unique characteristics of acoustic links such as multipath structure, packet error rate, or link loss rate; and
3) credibility of the third party recommendation (in cases where indirect trust measurements are included in the reputation system).

G. Node Cooperation and Mobility

To improve the efficiency of the described software defined cognitive system, the cooperation of static and mobile nodes is a key aspect to consider. Whenever possible, node mobility can be exploited in a dynamic way to adapt the network topology according to the ongoing attack and the quality of the communication channel. This would make it possible to avoid the presence of single point of failure and to enable efficient and energy-saving data delivery in the network. Data muling solutions can be explored to create mobile collection points, and to cover connectivity holes in the network in the presence of attacks such as jamming, sinkhole, and resource exhaustion.

Through the cooperation of the network nodes it is possible to monitor and keep track of neighbor node operations when reserving the channel and relaying messages, thus building trust and reputation metrics for the underwater nodes. Unexpected behaviors can then be detected. These include the following.

1) Too many/few packets getting in/out of a node, repeated transmissions of obsolete packets or repeated transmission requests addressed to the same node (replay and resource exhaustion attacks).
2) Continuous dropping of the received packets after requesting to be selected as relays (sinkhole attack).
3) Fake advertising of a node as the best relay or continuous forwarding of messages through the same node(s) while other good relays are available (packet redirection).
4) Nodes advertising themselves in different parts of the network (sybil and wormhole attacks).

IV. Proposed Architecture

In this section, we present our proposed hybrid UAN architecture with the objective of enhancing the robustness and security of UANs. We describe how the proposed SDN-based hybrid UAN architecture called "SUAN" will be benefited in terms of robust deployment, secure and reliable communication, and enhanced network management by using a combination of the various techniques explained in Section III.

A. Architecture Overview

Fig. 5 illustrates a high level layered structure of our proposed SUAN architecture. The architecture is divided into three planes: application, control, and data. The interaction between the three planes makes use of the north-bound application programmable interface (API) (between application and control plane) and the OpenFlow (OF) protocol (between control and data plane) [54]. The application plane is responsible for application-related tasks, e.g., data collection, QoS requirements definition, defining security policies. The control plane consists of logically centralized controllers called "primary OF-controller" configured

[2]Due the recent advancements [52] in hardware technologies for underwater sensors, collecting the aforementioned context information is not a difficult task.

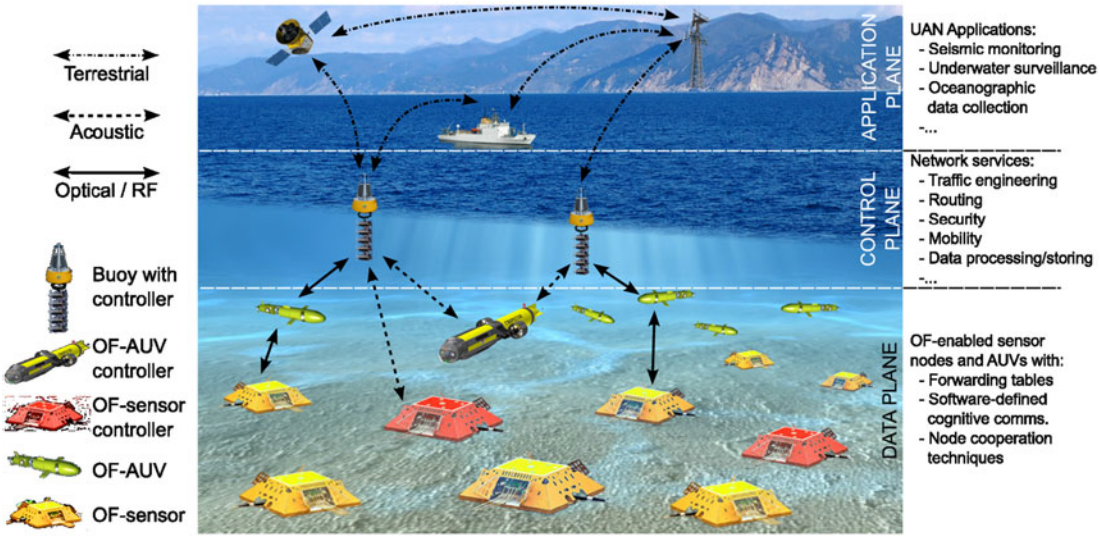

Fig. 5. SDN-based hybrid UAN architecture.

at surface buoys (or any other surface asset with radio capability acting as a gateway, e.g., autonomous surface vehicles). These controllers execute various networking services based on the requirements of UAN applications running at application plane. Finally, the data plane forms the networking infrastructure of UAN, and it consists of OF-enabled static underwater sensors nodes called "OF-sensors" and mobile autonomous underwater vehicles (AUVs) called "OF-AUVs." These nodes are used to perform data sensing and forwarding tasks. Additionally, controlling capabilities can be deployed on these sensors, thus implementing a secondary layer of control ("secondary OF-controller"). Apart from sensing and message forwarding, these secondary OF-controllers also executes a subset of primary OF-controller's functionalities. The size of this subset depends on the resource availability at each class of nodes.[3] The secondary OF-controllers are mostly used to perform the essential communication functions (such as installing forwarding rules on OF-nodes for routing) at data plane. However, if the primary OF-controller becomes unreachable, they can be used to select the strategy to perform the required tasks based on the local information they have.

In what follows, we detail the three planes of the proposed SUAN including their various elements (i.e., hardware and software), functionalities, and interactions with each other.

1) *Application plane:* This plane consists of a set of customized UAN applications such as seismic monitoring, underwater surveillance, and oceanographic data collection. With the help of the control plane, application plane is abstracted from the underlying network devices and communicating protocols, thus enabling the sharing of networking resources among multiple applications. The controller communicates with the network management service applications residing at surface buoys, and the customized UAN applications residing at the surface or onshore sink, by using a set of APIs called "SDN northbound APIs." With the help of these APIs, various UAN applications could use the same UAN network without interfering with the functionalities and performance of other UAN applications running in parallel.
2) *Control plane:* This plane consists of a centralized logical unit, and a set of network management service modules (please see Fig. 5), both residing at logically centralized primary OF-controller(s). The control plane objective is to allow various customized UAN applications to access and manage underlying networking infrastructure based on their set of requirements. In SUAN, the primary OF-controllers collect data from underlying OF-nodes and secondary OF-controllers, and it exhibits control logic to manage network elements and their functionalities at data plane by using OF protocols (also called "SDN southbound APIs"). For this purpose, in SUAN, the control plane should be able to differentiate between four types of messages, that it receives from the data plane.
   a) Routing messages that are sent when a route is required by an OF-node.
   b) Service messages that contain data collected using node cooperation and context-aware techniques. These techniques include contextual information, i.e., link or node behavioral information, and any other specific information required by network services running on OF-controllers.
   c) Topology update messages, i.e., periodic messages sent to OF-controllers. These messages includes the recent changes in network topology. To keep the overhead to minimum, an OF-node will not send these message, if no change in its neighbor set has been seen when compared to the previous update message.
   d) Data messages that contain data from sensors. In SUAN, multiple primary OF-controllers are deployed to enforce a more robust and distributed design. These controllers are equipped with more resources as they need to perform heavy processing tasks which includes large scale data collection,

[3]More controlling capabilities will be deployed on OF-nodes with more resources. Usually AUVs have more computational and storage capability with respect to regular sensors.

processing and storage, and the execution of various networking services such as QoS-aware routing, security policy enforcement and mobility handling.

3) *Data plane:* In SUAN, an OF-node is configured with following: 1) a forwarding table that consists of a set of forwarding rules required for the routing of messages, 2) a neighbor table that keeps information about neighbor (one or more hops away) nodes, and 3) the OF communication module (OF-COM) that facilitates data receiving and transmission operations with control plane devices. The OF-COM is configured with multiple software and hardware front-ends, thus it can simultaneously support other UAN communication technologies such as optical and radio communications along with the acoustic communications. The cognitive component at data plane devices make use of the software-defined modems to perform run-time switching between the available communication technologies. For instance, as shown in Fig. 5, the OF-COM could use acoustic channels for transmission of long-range single-hop messages (i.e., data communication between primary and secondary OF-controllers), while optical or radio channels could be preferred for short-range multihop transmissions (i.e., transmitting sensing data to sink). As mentioned before, few of the resourceful OF-nodes can be provided with a subset of controlling capabilities. These secondary OF-controllers are equipped with basic services required for minimal communication, such as evaluation and installation of forwarding rules on OF-nodes. Secondary OF-controllers can be also provided with enhanced controlling capabilities (depending on the node resources) to act as primary OF-controllers. This enables ensurance of the continuity of operations in the network when the communication with the surface stations is compromised.

B. Fault Tolerance, Mobility Management, and Overhead Minimization

Terrestrial SDN systems are mostly centralized solutions where all the decisions are offloaded to one or more controllers, which are able to communicate with each other. In SUAN, this original design is modified to cope with the channel unreliability typical of UANs. Different levels of control are assigned in the network in the form of primary and secondary OF-controllers. This helps in distributing the load in the network and in avoiding the presence of a single point of failure in the system.

In an ideal scenario, the primary OF-controller will always be able to collect the required data and to provide network OF-nodes[4] the optimal strategies and solutions to use, based on the acquired global view of the network. In scenarios where the communication channel is highly unreliable (due to the environmental conditions or to the on-going attacks) and communication with the primary OF-controllers is compromised for some time, the secondary OF-controllers have to take actions according to their local knowledge (i.e., existing information received by the other nodes and controllers). This may lead to suboptimal solutions ensuring however the continuity of operations in the network. Additionally, the presence of a distributed level of control makes it possible to reduce the number of control messages exchanged in the network. Each sensor node can communicate with the nearest OF-controller to obtain updated routes and to provide the collected measurements, without necessary reaching the primary OF-controllers all of the times. Moreover, the number of control messages exchanged in the SUAN can be proportional to the level of communication reliability and security required by the specific mission and application scenario. When reducing the number of services provided by the control plane in the network (see Fig. 5), fewer control messages need to be transmitted in the network at the cost of reducing the communication reliability and security of the network.

The distributed level of control is therefore used by SUAN to increase the robustness of the network and to minimize the introduced overhead. At the same time, SUAN uses the cross-layer design[5] to employ adaptive strategies that are able to select the best waveform, error correction algorithm, and other physical layer parameters to use. To minimize the exchange of control information, this selection can be performed locally at the node and near it, depending on the channel conditions and QoS requirements. Similarly, various medium access control solutions can be selected and configured in real-time (depending on physical layer information and QoS) to reduce the introduced overhead and delay, and to increase the probability of message delivery. This selection can be again performed locally at the node and near it. As soon as the global picture of the system can be built at the primary OF-controller, new and better decisions can be distributed in the network. These decisions may include network coding strategies, packet fragmentation and reassembling, level of redundancy for specific classes of data messages, cryptographic parameters, path planning for mobile nodes. Cluster-based solutions can be also considered to efficiently distribute the controlling capabilities in the network.

To avoid the presence of connectivity holes and a single point of failure in the network, moving nodes can be effectively used to adapt the network topology according to the needs. Mobile sinks can be used to improve the data collection process and mobile OF-controllers (underwater and surface vehicles) to increase the coverage on the other nodes of the network. However, due to node mobility and to channel unreliability, the available communication links may change over time. To effectively select the best strategies to use, the OF-controller requires an updated view of network topology and resources. For this purpose, the OF-nodes need to send periodic information update messages to the OF-controllers (control packets or control information in piggybacking to regular data packets), this may increase the control overhead in the network. Similarly, the secondary OF-controllers should receive periodic updates from primary OF-controllers to ensure that all the OF-controllers in the network have same view of the underlying network topology. Therefore, efforts to minimize the control overhead must be sought along with an adequate tradeoff between the QoS of the communi-

[4]OF-nodes refers to both static OF-sensors and mobile OF-AUVs.

[5]Note that usually underwater nodes are provided with good energy, memory, and computational resources. The exchange of many messages locally at the node between the different modules and layers of the protocol stack, as also presented in [27] and [42], does not seem to represent a bottleneck for the proposed architecture.

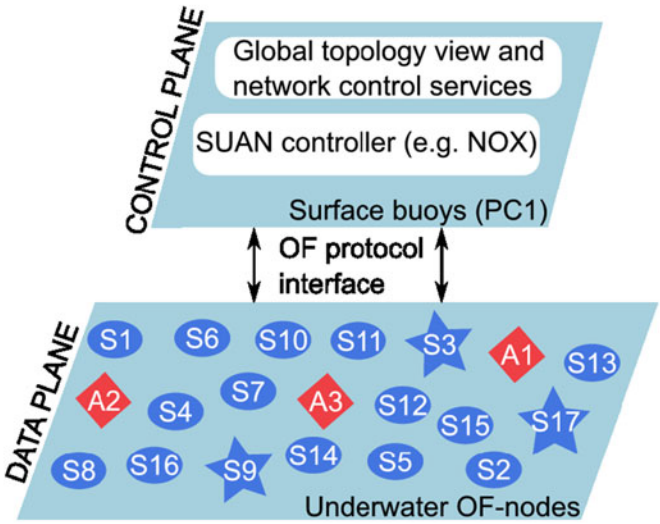

Fig. 6. SUAN example instance.

cation process and the control overhead in the network. The use of optimal number and placement of mobile nodes and OF-controllers in SUAN should be considered to effectively reduce the control overhead.

For all the scenarios presented so far, when no known routes are available, an alarm should be triggered and flooding or multipoint relay-based algorithm [55], [56] (i.e., traditional routing algorithms) should be employed, thus exploring node cooperation to deliver the intended data. This again comes at the price of an increased overhead and usage of resources in the network. Delay-tolerant networking (DTN) approaches [57], [58] can be also considered, depending on the application's QoS requirements. As a general rule, DTN strategies forward data opportunistically, typically exploiting the mobility of nodes, to have packets routed to otherwise unreachable portions of the network. The use of these strategies enables reduction of the usage of resources at the price of longer delays.

C. Security Analysis

We now discuss the effectiveness of our proposed SUAN architecture in tackling an array of security attacks in underwater networks. We suggest the possible strategies that use the cooperation of various approaches presented in Section III to detect and mitigate an attack in UAN. Let's assume a small SUAN scenario depicted in Fig. 6 to clearly understand the effectiveness of SUAN while addressing an attack. As shown in Fig. 6, the SUAN consists of 17 OF-nodes ($S1$, $S2$, ..., $S17$) out of which, three more capable (in terms of available resources) nodes (i.e., $S3$, $S9$, and $S17$) will act as secondary OF-controllers, three will act as adversary nodes ($A1$, $A2$, and $A3$), and one[6] will act as primary controller ($PC1$). Considering Fig. 6 as an example SUAN scenario, we now discuss various methods that can be adopted to detect and countermeasure a security threat in SUAN. In particular, we will explore possible ways to use the functionalities of SUAN to dynamically handle an attack at data plane.

1) *Jamming attack:* When node $S4$ wants to send data messages to a sink node (such as $PC1$), $S4$ checks its forwarding table for matching rules, and based on the search result, it sends the message to $S1$. Assume that $A2$ is performing a jamming attack on link $S4 \rightarrow S1$, therefore $S4$ will believe that $S1$ is no longer its neighbor, and it needs to send a routing message to $PC1$ to get a new route. In an ideal case, $S4$ knows how to reach $PC1$ (using a secondary suboptimal route through $S7$ or $S9$). Once $PC1$ receives the request, it can compute the new routes. A security service running at $PC1$ could raise an alarm at this point, as it will observe that the newly calculated best route is same as the old one (i.e., through $S1$), which has not been used. A number of such consecutive alarms for the routing messages received from $S4$ indicates malicious activity on link $S4 \rightarrow S1$. This information is then shared by $PC1$ with the secondary controllers operating in that area. While, in the case where $S4$ has no active route to reach the primary controller, novel routes can be obtained by the secondary controllers, similarly to what described for $PC1$. If no routes are available to reach any controller, $S4$ could use flooding or multipoint relay routing to inform the rest of the OF-nodes and find a path towards a controller (secondary or primary). At the same time, nodes in the jammed area can detect an increase noise level and exchange information (selecting the most suitable modulation and coding scheme) to determine if an alarm has to be triggered and reported to the OF-controllers. Furthermore, the node cooperation, the use of multiple communication interfaces and the availability of mobile nodes can be explored to deliver the intended messages in the network against the jammer. In particular, the use of SUAN architecture helps the OF-controller to make an optimal decision[7] to avoid or mitigate the jamming attack. For instance, the OF-controller might not use the multipath routing approach [11] to avoid the jamming link(s) as it detects higher overhead in its usage, and the controller suggests some other approach to handle the jamming such as the use of a spread spectrum technique or temporary muling data with a mobile AUV.
2) *Wormhole and ID-spoofing attacks:* In SUAN, launching a wormhole attack is not possible as the OF-controllers will not include the nodes $A1$ and $A2$ in any of the evaluated routes because these nodes are not registered[8] with the OF-controllers. An attacker can still perform the wormhole attack by spoofing the ID of genuine OF-nodes. However, the spoofing or impersonation attacks can be easily detected in SUAN with the help of the OF-controller, which can identify a possible ongoing attack during the next few updates of global network topology information. In particular, if the controller receives consecutive (to tackle mobility induced changes) topology update messages from the OF-nodes all indicating that a same ID node is in the neighbor set of two or more far away OF-nodes, it will raise a security alarm. For instance, in Fig. 6, if $A1$ imper-

[6] In practical scenarios, multiple primary OF-controllers needs to be deployed as shown in Fig. 5 to avoid a single point of failure.

[7] The decision is based on the recently available information that is gathered at different layers of SUAN architecture.

[8] In SUAN, the controllers keep details (such as ID) of each OF-nodes that is deployed at data plane.

sonate $S7$ then $S7$ will be shown as neighbor of $S4$ and $S13$. With the help of the global network view information, the security services at OF-controller will identify this anomaly (i.e., two far away OF-nodes have the same neighbor node), thus suspecting a possible malicious activity in the network. A similar anomaly, if detected, could also point towards an ongoing sybil attack in the networking infrastructure. Once this anomaly is detected, the controller can trigger the use of context-based technique discussed in Section III-E, to verify, whether the node claiming to be a neighbor is real or just impersonating. For this purpose, the OF-nodes have to collect context information and share it with the OF-controllers, or the OF-nodes can exchange the context with each other and perform the copresence detection locally. We believe that the proposed context-based technique can adequately tackle a relay attack in the presence of a dynamic topology (due to mobility) with long and varying propagation delays.

3) *Blackhole and sinkhole attacks:* An OF-node that is under the control of an adversary could perform a blackhole or sinkhole attack by discarding (all or few), the messages it receives for forwarding. In SUAN, such an attack not only cause packet drops, but it also disrupts the whole communication system by dropping the control messages, thus leaving the global topology view information at controllers in an inconsistent state. To detect this attack, node cooperation techniques installed on the neighbor nodes of the attacker should observe and report the malicious behavior of the attacker to the nearest OF-controller. Once detected, the OF-controller can isolate the attacker node from all the active routes. For instance, $A3$ is intentionally dropping all the packets that it receives for forwarding from $S14$. By using node cooperation, nodes $S7$ and $S12$ could observe and report the following anomaly to the controller: Messages sent from $S14$ with next hop $A3$ and destination $PC1$, but $A3$ performs no further action. To perform such node cooperation functions, the OF-nodes need to stay awake and do small processing continuously, this causes extra overhead on the resource limited OF-nodes. Therefore, we suggest that the primary OF-controllers should dynamically activate (or deactivate) various node cooperation functions based on the communication performance at data plane. Similarly, with the help of node cooperation and cross-layering techniques running on the OF-nodes, other attacks such as selfishness (i.e., denying forwarding of messages to save own resources) and misbehaving (i.e., disseminating false network control information) could be identified and reported to the controller to perform adequate countermeasures.
4) *Replay and resource exhaustion attacks:* The replay attack leads to network state inconsistencies and waste scarce network resources. The node cooperation techniques could be made responsible for monitoring, detecting, and reporting such anomaly (i.e., a node transmitting packets with very high frequency or same packets multiple times) to the OF-controller. The anomaly detection techniques should be lightweight due to the resource constrained nature of OF-nodes. Apart from the attacks on data plane, an adversary could also target the controller resources (i.e., processing power, memory, and energy). For instance, an adversary could send a large number of routing messages asking for new routes to various destinations to exhaust the resources of the controller, thus launching a DoS attack. The use of distributed and multiple layers of OF-controllers in SUAN helps in combating with resource exhaustion attacks. For instance, if the $PC1$ is not able to satisfy all the requests that it receives from OF-nodes due to resource exhaustion (either caused by an adversary or high network traffic), the secondary controllers (i.e., $S3$, $S9$, and $S17$) can temporary act as primary controllers for load balancing purposes. OF-nodes showing anomalies in the triggered requests can be put in quarantine (i.e., not considered in the network operations) for some time while addressing if further actions have to be taken. Once a node is proven to be not trusted anymore, it will be permanently isolated thus avoiding the waste of resources in the network.

The feasibility of the aforementioned possible solutions for various attacks in SUAN highly depends on the proper functioning of the security services running at OF-controllers, which in-turn depends on the correctness and reliability (i.e., quality and timeliness) of the control information received or gathered from the underlying OF-nodes. For instance, an adversary could hack an OF-node to perform the ID-spoofing or blackhole attack. Now, to detect an ongoing spoofing attack in SUAN, the OF-controller uses the network topology information that it receives from a set of consecutive topology messages. Similarly, to detect a blackhole node, the OF-controller relies on the neighbor nodes of the attacker that should observe and report the malicious behavior (i.e., void transmissions/forwarding from a node). In particular, the detection time and accuracy (i.e., false positives or false negatives) of attack detection solutions in SUAN relies on the availability of the required network control information at OF-controllers. As detailed in Section I, differently from terrestrial radio networks, the underwater communication channel is highly unreliable with high propagation delays and bit error rates. Gathering the required information to keep the global view at OF-controllers up-to-date is therefore a challenging task. However, we believe that the required control information can be acquired in SUAN as discussed in Section IV-B, thus enabling the use deployment of robust, secure and reliable UANs. In the case of a high degradation in the network communication capability, a suitable tradeoff between the level of security provided and the number of control messages required in the network can be defined according to the mission profile.

D. Design Challenges

The proposed SUAN architecture aims at providing reliable, secure, and controlled communication system for underwater networks. However, there are a set of issues that needs to be addressed in order to ensure proper deployment and functionality of SUANs. To this end, we identify the following design challenges.

1) *Controller robustness:* The placement and security of OF-controllers are major design challenges for SUAN architecture because the data plane relies on OF-controllers

for routing and other network services. In SUAN, the more demanding control capabilities resides on primary OF-controllers (surface stations) and a subset of more capable OF-nodes, acting as secondary controllers. The optimal placement of OF-controllers is required to minimize the initial routing delay caused in route calculation and installation processes used in SUAN, specifically for delay-sensitive UAN applications. Furthermore, the surface buoys are more vulnerable to physical attacks such as tempering. Along with the optimal placement, identifying the required number of OF-controllers has to be determined effectively by considering the tradeoff between communication reliability, cost, and delay. The actions performed by primary controllers have to be monitored as well to ensure that no malicious behavior has been injected on some of these controllers. However, this task is made easier by the possibility to use radio link to exchange control information between the various primary controllers and detect possible anomalies.

Depending on the considered application scenario, it could be also possible to make use of mobile underwater platforms to implement primary OF-controller capabilities. These mobile nodes could stay submerged, thus maintaining covertness of operations, and they could surface when it is required to communicate with the C2 station.

2) *Energy-aware networking:* In SUAN, the OF-nodes have limited energy resources, and these nodes have to perform routing for data as well as control messages (i.e., routing and topology packets), thus it is essential to develop the energy-aware traffic engineering solutions. Along with the information about global topology of underlying communication network, the OF-controller should also keep a global/local view of the residue energy and the link bandwidth. By using this information, the OF-controllers can take efficient routing decisions for individual dataflows, and at the same time, they can also ensure that the selected routes are energy-efficient, thus maximizing the network lifetime. In addition, the OF-nodes with lower remaining energy could be identified, and the OF-controller could send mobile platforms (e.g., AUVs) in the proximity to offload OF-nodes. This would make possible to balance the energy consumption and energy harvesting in the overall network. Furthermore, the distributed nature of SUAN should be efficiently exploited to keep the control overhead (between OF-nodes and OF-controllers) to the minimum. For instance, an OF-node could always be able to connect with its nearest OF-controller to get the desired services.
3) *Scalability:* Since the SUAN architecture uses a set of OF-controllers interfacing with multiple OF-nodes, this opens possibilities for the OF-controllers to become a communication bottleneck in situations, where the network scales in terms of traffic and number of OF-nodes. When few secondary OF-controllers are deployed, a large number of routing and topology control messages along with the data packets received from OF-nodes can overwhelm the controllers. An adversary can further escalate the situation by sending fake control messages to the OF-controllers, thus causing a DoS attack by exhausting controller resources. Even in the absence of an adversary, as the network size increases, the number of messages received by an OF-controller increases significantly, thus the bottleneck tightens and network performance degrades. Increasing the number of secondary OF-controllers enables creation of a decentralized control architecture to support the scalability. However, in this case additional challenges have to be considered and managed such as deployment cost, employment of aligned strategies, convergence, and an increasing number of controller instances.

V. Conclusion

In this paper, a hybrid UAN architecture is introduced to fortify security in UANs based on intelligent decision making at the node and network level. Aspects of PLS, SDN, node cooperation, cross-layering, context-awareness, and cognition are envisaged in the proposed architecture to tackle an array of possible security attacks. In particular, possible strategies that lead to the detection and countermeasure of various threats are presented and challenges related to energy efficiency, scalability, and control overhead are outlined. Since this work is mainly focused on identifying security challenges and suggesting possible solutions, many research issues remain wide open. Future work will address these issues as we move toward the implementation and validation of the proposed solutions through computer simulations and at-sea experimentation.

Acknowledgment

This work acknowledges the use of acoustic data that were made possible by the REP16-Atlantic sea trial, including as participants CMRE and PRT-N, FEUP, University of Padova, Atlas Elektronik. The authors would like to thank the CMRE Engineering Technical Division, the Captain and crew of *NRV Alliance* for the excellent support during the experiments.

References

[1] L. Lanbo, Z. Shengli, and C. Jun-Hong, "Prospects and problems of wireless communication for underwater sensor networks," *Wireless Commun. Mobile Comput.*, Special Issue Underwater Sensor Netw., vol. 8, no. 8, pp. 977–994, Aug. 2008.

[2] J. Heidemann, M. Stojanovic, and M. Zorzi, "Underwater sensor networks: Applications, advances, and challenges," *Royal Soc.*, vol. 370, no. 1958, pp. 158–175, May 2012.

[3] T. Melodia, H. Khulandjian, L.-C. Kuo, and E. Demirors, "Advances in underwater acoustic networking," in *Mobile Ad Hoc Networking: Cutting Edge Directions*, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Eds., Hoboken, NJ, USA: Wiley, Mar. 5 2013, ch. 23, pp. 804–852.

[4] E. Souza, H. C. Wong, I. Cunha, A. A. F. Loureiro, L. F. M. Vieira, and L. B. Oliveira, "End-to-end authentication in under-water sensor networks," in *Proc. 18th IEEE Int. Symp. Comput. Commun.*, Split, Croazia, Jul. 7–10, 2013, pp. 299–304.

[5] C. Lal, R. Petroccia, M. Conti, and J. Alves, "Secure underwater acoustic networks: Current and future research directions," in *Proc. 3rd IEEE OES Int. Conf. Underwater Commun. Networking*, Lerici, Italy, Aug. 30–Sep. 1, 2016.

[6] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54–60, Aug. 2015.

[7] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and privacy in localization for underwater sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 11, pp. 56–62, Nov. 2015.

[8] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Commun.*, vol. 18, no. 1, pp. 22–28, Feb. 2009.

[9] M. Zuba, Z. Shi, Z. Peng, and J.-H. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *Proc. 6th ACM Int. Workshop Underwater Netw.*, Seattle, WA, USA, Dec. 1–2, 2011, pp. 12:1–12:5.

[10] M. Zuba, Z. Shi, Z. Peng, J.-H. Cui, and S. Zhou, "Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks," *Security Commun. Netw.*, vol. 8, no. 16, pp. 2635–2645, Nov. 2015.

[11] M. Goetz, S. Azad, P. Casari, I. Nissen, and M. Zorzi, "Jamming-resistant multi-path routing for reliable intruder detection in underwater networks," in *Proc. 6th ACM Int. Workshop Underwater Netw.*, Seattle, WA, USA, Dec. 1–2, 2011.

[12] W. Wang, J. Kong, B. Bhargava, and M. Gerla, "Visualisation of wormholes in underwater sensor networks: A distributed approach," *Int. J. Security Netw.*, vol. 3, no. 1, pp. 10–23, Jan. 2008.

[13] R. Zhang and Y. Zhang, "Wormhole-resilient secure neighbor discovery in underwater acoustic networks," in *Proc. 29th IEEE Int. Conf. Comput. Commun.*, San Diego, CA, USA, Mar. 15–19, 2010, pp. 1–9.

[14] M. Zuba, M. Fagan, Z. Shi, and J.-H. Cui, "A resilient pressure routing scheme for underwater acoustic networks," in *Proc. 57th IEEE Global Commun. Conf.*, Austin, TX, USA, 8–12 Dec. 2014, pp. 637–642.

[15] G. Dini and A. Lo Duca, "A secure communication suite for underwater acoustic sensor networks," *Sensors*, vol. 12, no. 11, pp. 15133–15158, Nov. 2012.

[16] A. Caiti, V. Calabrò, G. Dini, A. Lo Duca, and A. Munafò, "Secure cooperation of autonomous mobile sensors using an underwater acoustic network," *Sensors*, vol. 12, no. 2, pp. 1967–1989, Feb. 2012.

[17] Y. Liu, J. Jing, and J. Yang, "Secure underwater acoustic communication based on a robust key generation scheme," in *Proc. 9th Int. Conf. Signal Process.*, Leipzig, Germany, May 10–11, 2008, pp. 1838–1841.

[18] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, "SecFUN: Security Framework for Underwater acoustic sensor Networks," in *Proc. MTS/IEEE OCEANS Conf.*, Genova, Italy, May 18–21, 2015, pp. 1–9.

[19] M. Ibragimov *et al.*, "CCM-UW security modes for low-band underwater acoustic sensor networks," *Wireless Pers. Commun.*, vol. 89, no. 2, pp. 479–499, Jul. 2016.

[20] A. Capossele, G. De Cicco, and C. Petrioli, "R-CARP: A Reputation Based Channel Aware Routing Protocol for Underwater Acoustic Sensor Networks," in *Proc. 10th ACM Int. Workshop Underwater Netw.*, Washington, DC, USA, Oct. 22–24, 2015, pp. 37:1–37:6.

[21] G. Han, J. Jiang, L. Shu, and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2447–2459, Dec. 2015.

[22] J. Ling, H. He, J. Li, W. Roberts, and P. Stoica, "Covert underwater acoustic communications: Transceiver structures, waveform designs and associated performances," in *Proc. MTS/IEEE OCEANS Conf.*, Seattle, WA, USA, Sep. 20–23, 2010, pp. 1–10.

[23] T. C. Yang and W. B. Yang, "Low probability of detection underwater acoustic communications for mobile platforms," in *Proc. OCEANS Conf.*, Quebec City, QC, Canada, Sep. 15–18, 2008, pp. 1–6.

[24] H. Kulhandjian, T. Melodia, and D. Koutsonikolas, "Securing underwater acoustic communications through analog network coding," in *Proc. 11th Annu. IEEE Int. Conf. Sensing, Commun. Netw.*, Singapore, Jun. 30–Jul. 3, 2014, pp. 266–274.

[25] R. Martin and S. Rajasekaran, "Data centric approach to analyzing security threats in underwater sensor networks," in *Proc. MTS/IEEE OCEANS Conf.*, Monterey, CA, USA, 19–23 Sep. 2016, pp. 1–6.

[26] G. Toso, D. Munaretto, M. Conti, and M. Zorzi, "Attack resilient underwater networks through software defined networking," in *Proc. 9th Int. Conf. Underwater Netw. Syst.*, Rome, Italy, Nov. 12–14, 2014, pp. 1–2.

[27] J. Potter *et al.*, "Software defined open architecture modem development at CMRE," in *Proc. Underwater Commun. Netw.*, Sestri Levante, Italy, Sep. 3–5, 2014, pp. 1–4.

[28] J. Chu, "The beginning of the end for encryption schemes?" 2016. [Online]. Available: http://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303

[29] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[30] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.

[31] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, Nov. 2013.

[32] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Security*, Alexandria, VA, USA, Oct. 29–2 Nov. 2007, pp. 401–410.

[33] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[34] A. Kitaura, T. Sumi, K. Tachibana, H. Iwai, and H. Sasaoka, "A scheme of private key agreement based on delay profiles in UWB systems," in *Proc. IEEE Sarnoff Symp.*, Princeton, NJ, USA, Mar. 27–28, 2006, pp. 1–6.

[35] A. Kitaura, T. Sumi, T. Tango, H. Iwai, and H. Sasaoka, "A private key sharing scheme based on multipath time delay in UWB systems," in *Proc. Int. Conf. Commun. Technol.*, Guilin, China, Nov. 27–30, 2006, pp. 1–4.

[36] T. H. Chou, S. C. Draper, and A. M. Sayeed, "Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1751–1764, Sep. 2013.

[37] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: Advantages, challenges and performance improvements," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 32–38, Feb. 2016.

[38] Y. Huang, S. Zhou, Z. Shi, and L. Lai, "Channel frequency response-based secret key generation in underwater acoustic systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 5875–5888, Sep. 2016.

[39] M. J. Dworkin, "Recommendation for block chiper modes of operation: Galois/counter mode (GCM) and GMAC," Nat. Inst. Std. Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-38D, 2007.

[40] R. Jurdak, A. G. Ruzzelli, and G. M. P. O'Hare, "Design considerations for deploying underwater sensor networks," in *Proc. Int. Conf. Sensor Technol. Appl.*, Valencia, Spain, Oct. 14–20, 2007, pp. 227–232.

[41] Y. Cong, G. Yang, Z. Wei, and W. Zhou, "Security in underwater sensor network," in *Proc. Int. Conf. Commun. Mobile Comput.*, Shenzhen, China, Apr. 12–14, 2010, pp. 162–168.

[42] C. Petrioli, R. Petroccia, J. R. Potter, and D. Spaccini, "The SUNSET framework for simulation, emulation and at-sea testing of underwater wireless sensor networks," *Ad Hoc Netw.*, vol. 34, no. C, pp. 224–238, Nov. 2015.

[43] S. Jain *et al.*, "B4: Experience with a globally-deployed software defined wan," *SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 3–14, Aug. 2013.

[44] N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the internet of things: A survey," *IEEE Access*, vol. 4, pp. 5591–5606, Sep. 2016.

[45] S. Sun, L. Gong, B. Rong, and K. Lu, "An intelligent SDN framework for 5G heterogeneous networks," *IEEE Commun. Mag.*, vol. 53, no. 11, pp. 142–147, Nov. 2015.

[46] I. F. Akyildiz, P. Wang, and S.-C. Lin, "SoftWater: Software-defined networking for next-generation underwater communication systems," *Ad Hoc Netw.*, vol. 46, no. C, pp. 1–11, Aug. 2016.

[47] K. Pelekanakis, L. Cazzanti, G. Zappa, and J. Alves, "Decision tree-based adaptive modulation for underwater acoustic communications," in *Proc. IEEE OES 3rd Underwater Commun. Netw. Conf.*, Lerici, Italy, Aug. 30–1, Sep. 2016, pp. 1–5.

[48] A. Radosevic, R. Ahmed, T. M. Duman, J. G. Proakis, and M. Stojanovic, "Adaptive OFDM modulation for underwater acoustic communications: Design considerations and experimental results," *IEEE J. Ocean Eng.*, vol. 39, no. 2, pp. 357–370, May 2014.

[49] E. Demirors, G. Sklivanitis, G. E. Santagati, T. Melodia, and S. N. Batalama, "Design of a software-defined underwater acoustic modem with real-time physical layer adaptation capabilities," in *Proc. Int. Conf. Underwater Netw. Syst.*, Rome, Italy, Nov. 12–14, 2014, pp. 1–8.

[50] V. Di Valerio, F. Lo Presti, C. Petrioli, L. Picari, and D. Spaccini, "A self-adaptive protocol stack for underwater wireless sensor networks," in *Proc. MTS/IEEE OCEANS Conf.*, Shanghai, China, Apr. 10–13, 2016, pp. 1–8.

[51] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Using contextual co-presence to strengthen zero-interaction authentication: Design, integration and usability," *Perv. Mobile Comput.*, vol. 16, Part B, pp. 187–204, Jan. 2015.

[52] E. Demirors, G. Sklivanitis, T. Melodia, S. N. Batalama, and D. A. Pados, "Software-defined underwater acoustic networks: Toward a high-rate real-time reconfigurable modem," *IEEE Commun. Mag.*, vol. 53, no. 11, pp. 64–71, Nov. 2015.

[53] A. Capossele, G. De Cicco, and C. Petrioli, "R-CARP: A reputation based channel aware routing protocol for underwater acoustic sensor networks," in *Proc. 10th Int. Conf. Underwater Netw. Syst.*, Washington, DC, USA, Oct. 22–24, 2015.
[54] N. McKeown *et al.*, "OpenFlow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.
[55] S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, "CARP: A channel-aware routing protocol for underwater acoustic wireless networks," *Ad Hoc Netw.*, vol. 34, no. C, pp. 92–104, Nov. 2015.
[56] J. Alves, R. Petroccia, and J. R. Potter, "MPR: multi-point relay protocol for underwater acoustic networks," in *Proc. 9th ACM Int. Conf. Under water Netw. Syst.*, Rome, Italy, Nov. 12–14, 2014.
[57] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proc. 2003 Conf. Appl., Technol., Archit., Protocols Comput. Commun.*, Karlsruhe, Germany, Aug. 25–29, 2003, pp. 27–34.
[58] D. Merani, A. Berni, J. Potter, and R. Martins, "An underwater convergence layer for disruption tolerant networking," in *Proc. 2011 Baltic Congr. Future Internet Commun.*, Riga, Latvia, Feb. 16–18, 2011, pp. 103–108.

Chhagan Lal (M'13) received the B.S. degree in computer science and engineering from MBM Engineering College, Jodhpur, India, in 2006, the M.S. degree in information technology with specialization in wireless communication from Indian Institute of Information Technology, Allahabad, Allahabad, India, in 2009, and the Ph.D. degree in computer science and engineering from Malaviya National Institute of Technology, Jaipur, India, in 2014.

He is currently a Postdoctoral Fellow in the Department of Mathematics, University of Padua, Padua, Italy. His current research interests include security in wireless networks, software defined networking, underwater acoustical networks, and context-based security solutions for internet of things networks.

Dr. Lal received the Canadian Commonwealth Scholarship in 2012 under the Canadian Commonwealth Scholarship Program to work at the University of Saskatchewan, Saskatoon, SK, Canada.

Roberto Petroccia (M'10) received the Laurea degree (with the highest honors) in 2006 and the Ph.D. degree in 2010, both in computer science, from Rome University "La Sapienza," Rome, Italy.

Until 2015, he was a Research Staff. Since 2015, he has been a Research Scientist at the NATO STO Centre for Maritime Research and Experimentation, La Spezia, Italy. He is currently an Invited Lecturer of the Master's in ocean engineering at the University of Pisa, Pisa, Italy, and has supervised the work of several master thesis and Ph.D. students. He has participated in several EC projects including the EC IP projects E-SENSE, SENSEI, the FP7 STREP CLAM, and the FP7 SUNRISE. For the two latter projects on underwater networking, he was in charge of coordinating all underwater experimental activities. In the last five years, he participated in more than 20 experimental campaigns at sea, where innovative underwater solutions he developed have been extensively tested. He has been actively collaborating with several acoustic modem and underwater vehicle manufacturing companies and research labs to design novel technologies supporting cooperative underwater acoustical networks. He is also a member of ACM. His research interests include wireless sensor networks design, underwater communications and networking, where he has contributed more than three dozens papers published in leading venues (h-index = 14, i10-index = 21, Google Scholar, June 2017).

Dr. Petroccia was in the organizing committee of the 2016 IEEE Underwater Communications and Networking Conference the 2014, ACM International Conference on Underwater Networks and Systems (WUWNet), and 2012 ACM WUWNet.

Konstantinos Pelekanakis (S'06–M'09) received the Diploma degree from the Department of Electronic and Computer Engineering, Technical University of Crete, Chania, Greece, in 2001, and the M.Sc. and Ph.D. degrees in mechanical and ocean engineering from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2004 and 2009, respectively.

From 2009 to 2015, he was a Research Fellow at the Acoustic Research Laboratory, National University of Singapore. He is currently a Scientist at NATO Science and Technology Organization, Centre for Maritime Research and Experimentation, La Spezia, Italy. His current research include robust signal processing, security, and adaptive modulation for underwater acoustical communications.

Dr. Pelekanakis received the MIT Presidential Fellowship in 2001. He was the Secretary (2013) and the Vice-Chairman (2014) of the IEEE OES (Singapore chapter) and was with the organizing committee of the IEEE Underwater Communications and Networking 2016. He was also a Reviewer for many international conferences and journals.

Mauro Conti (SM'14) received the Ph.D. degree in computer science from Sapienza University of Rome, Rome, Italy, in 2009.

In 2011, he joined the University of Padua, Padua, Italy, as an Assistant Professor, where since 2015, he has been an Associate Professor. After his Ph.D., he was a Postdoctoral Researcher at Vrije Universiteit Amsterdam, Amsterdam, The Netherlands. In 2017, he obtained the national habilitation as a Full Professor for computer science and computer engineering. His main research interests include the area of security and privacy. In this area, he has published more than 170 papers in topmost international peerreviewed journals and conference.

Dr. Conti was a Visiting Researcher at GMU (2008, 2016), UCLA (2010), UCI (2012, 2013, 2014), TUDarmstadt (2013), UF (2015), and FIU (2015, 2016). He received the Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). He was the Program Chair of TRUST 2015, ICISS 2016, WiSec 2017, and the General Chair for SecureComm 2012 and ACM SACMAT 2013. He is an Associate Editor for several journals, including the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

João Alves (SM'17) received the B.Sc. and M.Sc. degrees in electrotechnical engineering, control and robotics from the Technical University of Lisbon, Lisbon, Portugal,

Since 1995, he has been working in underwater robotics and associated technologies. He had a key role in the development of the hardware and software architectures for the INFANTE AUV and DELFIM ASV developed at the Technical University of Lisbon. In 2003, he cofounded a private start-up company, Blue Edge Systems Engineering, offering services and conducting R&D activity in the maritime domain. In 2007, he took scientific leadership for the underwater communications activities of the EC project GREX, where pioneering maritime cooperative robotics was demonstrated. In late 2009, he joined the NATO Undersea Research Centre, now the Centre For Maritime Research and Experimentation (CMRE) as a Scientist to work on underwater communications. He led studies in support of establishing the first underwater communications standard and developed innovative protocols for underwater ad hoc networking. In 2014, became a Principal Scientist responsible for the underwater communications activities at CMRE. He conducted several trials as Scientist-in-Charge, leading teams of several tens of people during long sea-going campaigns. During this period, he was also a PI for different European commission projects (such as MORPH and SUNRISE). He is currently an Invited Lecturer of the Master's in ocean engineering at the University of Pisa, Pisa, Italy.

Mr. Alves was the General Chair of the IEEE OES Underwater Communications and Networking 2014 (UComms14) and UComms16 conferences. He is a Guest Editor of the IEEE JOURNAL OF OCEANIC ENGINEERING. He is also with the AUVSI subcommittee for the international regulations for preventing collisions at sea, dealing with the challenging issues of adding robots to our oceans.

Document Data Sheet

Security Classification		Project No.
Document Serial No.	**Date of Issue**	**Total Pages**
CMRE-PR-2019-050	May 2019	13 pp.

Author(s)

Chhagan Lal, Roberto Petroccia, Konstantinos Pelekanakis, Mauro Conti, João Alves

Title

Toward the development of secure underwater acoustic networks

Abstract

Underwater acoustic networks (UANs) have been recognized as an enabling technology for various applications in the maritime domain. The wireless nature of the acoustic medium makes UANs vulnerable to various malicious attacks; yet, limited consideration has been given to security challenges. In this paper, we outline a hybrid architecture that incorporates aspects of physical layer security, software defined networking, node cooperation, cross-layering, context-awareness, and cognition. The proposed architecture envisions strategies at the node as well as at the network level that adapt to environmental changes, the status of the network and the possible array of attacks. Several examples of attacks and countermeasures are discussed while deployment and functionality issues of the proposed architecture are taken into consideration. This work is not intended to represent a whatsoever proven solution but mainly to suggest future research directions to the scientific community working in the area of UANs.

Keywords

Cognitive networks, context-aware security, cross-layering, denial-of-service (DoS) attacks, physical layer security (PLS), security, software-defined underwater networks, underwater acoustic networks (UANs).

Issuing Organization

NATO Science and Technology Organization
Centre for Maritime Research and Experimentation

Viale San Bartolomeo 400, 19126 La Spezia, Italy

[From N. America:
STO CMRE
Unit 31318, Box 19, APO AE 09613-1318]

Tel: +39 0187 527 361
Fax:+39 0187 527 700

E-mail: library@cmre.nato.int