Channel-Based Trust Model for Security in Underwater Acoustic Networks

Alberto Signori *Student Member, IEEE*, Filippo Campagnaro *Member, IEEE*, Ivor Nissen, Michele Zorzi *Fellow, IEEE*

***Abstract*—Underwater acoustic networks are often used in mission-critical scenarios, such as military underwater networks and assets deployed for tsunami prevention, hence an attack performed against these types of networks can easily lead to disastrous consequences. Nevertheless, countermeasures to possible network attacks have not been widely investigated so far. A reputation system, where a node gains trust each time it exhibits a good behavior, and loses trust each time it behaves suspiciously, is an effective way to identify possible attackers in the network. The main challenge when applying a reputation system in an underwater network is to understand whether the network performance degrades because a node is acting maliciously intentionally, or because of changed channel conditions causing a large packet drop. For instance, when a ship travels close to an underwater network deployment, it causes an increased packet loss, and so does the change of environmental conditions, such as a drop of temperature, the presence of rain or the increase of the wind speed. This behavior of the acoustic channel can be characterized with a Hidden Markov Model, whose parameters are obtained observing the time evolution of the acoustic channel in a sea experiment.**

This paper presents a trust model based on the knowledge of the channel state, inferred from the perceived noise and received signal strength, in which misbehavior and correct behavior are differently considered according to the actual channel state. We evaluate the model both analytically and through simulations, implementing the trust mechanism in the DESERT Underwater Network framework.

***Index Terms*—Hidden Markov Models, trustworthiness, underwater acoustic communications, security in underwater networks, reputation**

I. Introduction

Communication under the sea is gaining more and more interest in the last years, due to the development of new applications enabled by sophisticated sensors and underwater unmanned vehicles that follow pre-loaded missions or are remotely controlled by a central station. Due to the challenges imposed by the underwater channel, electromagnetic signals propagate for only a few meters under the sea, while optical communications suffer from water turbidity and need alignment between transmitter and receiver [1], and can be used only for some very specific scenarios [2]. Acoustic signals, instead, propagate up to a few kilometers, a communication range that suits well the needs of an underwater deployment, at the price of low bandwidth and datarate, large propagation delay, and poor performance in scenarios where the combination of noise and multipath can significantly affect the network operation [3]. In addition, the change of the weather conditions can suddenly affect the quality of the acoustic links, and, therefore, the network coverage. Due to the disruptive nature of acoustic networks, in the last two decades scientists focused their efforts on designing routing [4]–[6] and Medium Access Control (MAC) protocols [7]–[10] able to contrast the challenges imposed by the acoustic channel, and self-adapting physical layers able to change frequency and/or Modulation and Coding Scheme (MCS) according to the channel conditions, for example using a more robust modulation and adding more coding redundancy when the communication is facing a poor channel link [11], [12], or switching transmission frequency to reach a longer range or a higher throughput [13].

Security aspects of underwater wireless acoustic networks, instead, have not been widely studied so far and require a dedicated effort, due to the fact that the countermeasures used in wireless terrestrial networks cannot be directly applied to the underwater domain. For instance, a freshness index based on the generation time of a data packet, used to check if a malicious node is performing a replay attack [14], is a valid countermeasure in a wireless network, where the packet header already contains the packet generation timestamp, but is not a valid countermeasure in underwater networks, where only few bytes are used for the packet header, as the communication overhead needs to be minimized due to the low datarate. In addition, such countermeasure, that restricts the time validity of a packet transmitted in an underwater network, can result in the drop of legitimate packets, as underwater networks may be characterized by a very large Packet Delivery Delay (PDD), of the order of up to a few minutes.

In order to defend against a Denial of Service (DoS) attack (Figure 1) there are two possible strategies. The first consists in providing a countermeasure to specific attacks, analyzing how the network behaves when these attacks are performed [14], [15]. On the one hand, this solution is very effective, as it usually allows to both detect an attacker and avoid the DoS; on the other hand, it requires the knowledge of the attacker setup, and an extended simulation study where different variations of the attack are performed and analyzed. In case a different attack is applied, a different countermeasure needs to be taken. The second strategy, instead, consists in using a trust mechanism,

A. Signori (email: signoria@dei.unipd.it), F. Campagnaro (email: campagn1@dei.unipd.it), and M. Zorzi (email: zorzi@dei.unipd.it) are with the Department of Information Engineering, University of Padova, 35131 Padova, Italy. F. Campagnaro and M. Zorzi are also with Wireless and More srl, 35131 Padova, Italy. I. Nissen (email: ivornissen@bundeswehr.org) is with Bundeswehr Technical Center for Ships and Naval Weapons, Maritime Technology and Research, D-24340 Eckernförde, Germany.

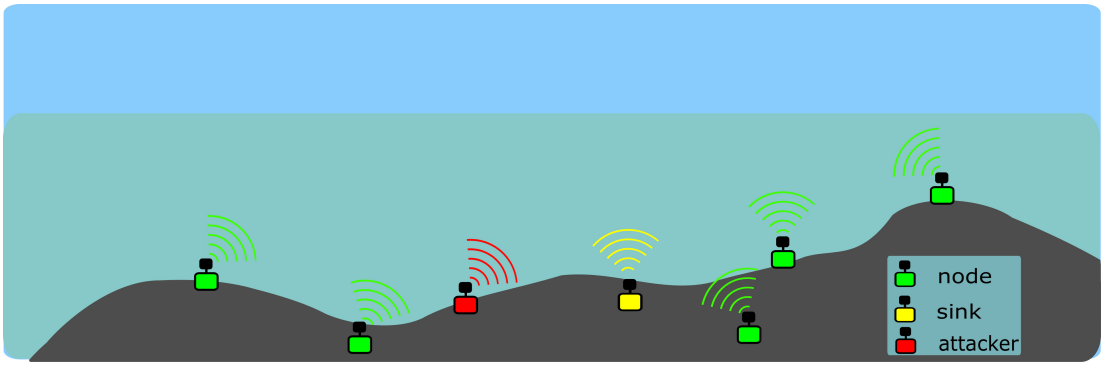


Fig. 1: Example of an underwater acoustic network, with nodes (green nodes) sending data to a sink (yellow node), while a malicious node (red node) tries to attack the network

based on the reputation of the nodes [16], [17], to identify whether or not a node can be expected to follow the protocol rules of the underwater network. Indeed, a trust mechanism can be applied whenever the definitions of correct behavior and misbehavior are stated precisely and can be detected through the overhearing of the packets. For instance, in a sinkhole attack the neighbors of a malicious node can mark it as untrustworthy if they do not overhear the correct forwarding of the packets, while in a replay attack a node is not trusted if it retransmits the same packet more times than expected by the protocol stack [18]. In the case of a spoofing attack, instead, if a node observes in a short amount of time the transmission of two packets with the same source node identifier but with a completely different received power (and/or SNR), it can suspect that an attacker is stealing the identity of a legitimate node and can mark this as a misbehavior. If it has already collected enough information about the legitimate node, it can also identify who is the attacker observing the received power and the channel impairments, otherwise it can still detect that there is an ongoing attack and notify this event to the other nodes in the network. While this strategy is limited to identifying the attacker rather than limiting its effect, its main advantage is that it can be applied to many different attacks, thus providing a general defense solution. For instance, a node marked as untrustworthy can be excluded from the packets' route, and the packets coming from that node can be discarded by the other nodes. In addition, the untrustworthy node can be localized via triangulation, and eventually removed from the network.

To infer the reputation, a node needs to observe the behavior of its neighbors by overhearing transmissions by the other nodes. This solution is widely used in terrestrial wireless networks, where a node can exploit the broadcast nature of the channel to understand the behavior of its neighbors, by overhearing the packets they transmit. This mechanism can be referred to as watchdog [19], implicit ack, or overhear forwarding mechanism. In this paper we present a trust mechanism for underwater networks, where we adapt approaches used in terrestrial wireless networks to the disruptive nature of the acoustic channel by using subjective logic [20] to take into consideration the uncertainty caused by the acoustic channel quality evolution. The use of subjective logic to provide a trust measure for the nodes of a network has been already employed in terrestrial networks [16], [21], however the peculiarity of the acoustic channel poses a further challenge in the analysis of the node trust. Indeed, bursts of packet errors characterize acoustic communications due to the multipath, high delay spread and ambient noise of the acoustic channel. For these reasons the trust models designed for the terrestrial counterpart do not take into account channel measures to compute the reputation. On the other hand, other methods based on bayesian models, often employed to compute the trust in terrestrial networks [22], [23], are not applicable to underwater networks because they do not consider any link disruption caused by the variability of the acoustic channel. The risk of this approach is to estimate the reliability of the channel rather than the trustworthiness of a node.

The main contribution of this paper is the design of a trust module that provides a measure of trust of the one-hop neighbors. Our proposed framework is: *i)* general enough to deal with different types of attacks; *ii)* specifically tailored for underwater acoustic networks; *iii)* independent of the network topology and of the number of nodes joining the network. Indeed, as soon as the concepts of correct behavior and misbehavior are well defined, the model can be employed to discover different attacks, such as sinkhole and resource exhaustion. Moreover, the unique characteristics of the underwater acoustic channel are taken into account in the trust model by considering channel based metrics, such as noise and Signal to Noise Ratio (SNR), and modeling the acoustic channel variability with a Hidden Markov Model (HMM) [24]. The proposed system is evaluated both analytically and through simulations based on real field measurements, using the flooding network protocol in the DESERT Underwater network simulator [25]. The trust model can also be used in real-field applications such as in underwater acoustic networks employed for coast surveillance that make use of the Gossiping in Underwater Acoustic Mobile Ad-hoc Networks (GUWMANET) protocol [5], [18] specifically tailored for military networks. In this paper we focused on analyzing the feasibility of the trust model, assessing whether or not a node can make a decision on the trustworthiness of its neighbors based on its own observations. At this stage, we do not consider the possibility that a node shares its information with its neighbors. Although this

could help avoid misdetections, it would also pose two main other challenges: sharing the information without increasing the overhead too much and avoiding the spreading of false information from malicious nodes. Thus we decided to leave this study for future works.

II. Related Work

Trust is a measure of the belief that a given subject will behave according to what is expected. This measure can be applied to many different fields [26], from sociology to science, academia, journalism, economics, medicine and, finally, wireless terrestrial and underwater networks, the last being the focus of this paper. The trust of a node can be based either on authentication certificates and cryptographic keys [27], or on a reputation-based system, the latter being more relevant to Mobile Ad Hoc Networks (MANET) [26]. Although lightweight authentication schemes for vehicular ad hoc networks exist [28]–[30], they usually rely on broadband communication links: this assumption is not applicable in underwater acoustic networks, where the characteristics of the acoustic channel, such as high latency and low datarate, can make the authentication process last several seconds or minutes, especially in case of congested networks or in case of retransmissions due to packet loss.

Also distributed blockchain-based authentication schemes [29] imply a high message overhead to distribute the information among the nodes; furthermore they are computationally demanding and may cause the battery depletion of underwater nodes. Many works in the literature propose a reputation-based system for terrestrial wireless networks [16], [17], [31], but only a few papers address the aspects of underwater acoustic networks, and most of them only propose a preliminary analysis [32], [33].

The authors in [31] demonstrate how a watchdog-based reputation system applied to the Ad-hoc On-demand Distance Vector (AODV) routing protocol in a wireless mesh network provides significant benefits in terms of network performance when the network is under attack. This reputation extension of the AODV protocol, called AODV-REX, has been tested against malicious nodes performing blackhole and grayhole attacks. The reputation of a node computed by one of its neighbors increases when it correctly forwards received packets according to the network protocol. Conversely, if this does not happen within a certain time interval, the reputation decreases. This observation can be performed by means of the watchdog mechanism, i.e., the neighbors of a node can overhear the packets it transmits even if these packets are not for them. The more interactions a node `A` performs with a node `B`, the more the reputation of `B` computed by `A` is considered solid. The reputation of a certain node is finally shared among the nodes of the network: the more the reputation values for that node differ, the less the node is trusted. While the watchdog mechanism can also be applied to our scenario, the proposed reputation system cannot be directly applied to underwater networks due to the disruptive nature of the acoustic channel and the overhead introduced by the signaling of the AODV-REX routing.

The authors in [16] propose an extension of the AODV routing protocol, called Trusted AODV (TAODV), where the trust of the nodes is performed using watchdog. The protocol has been designed for secure MANET. In this work, the trust among nodes is represented by opinion, which is an item derived from subjective logic. An opinion can be interpreted as a probability measure containing secondary uncertainty: specifically, a node may be uncertain about another node's trustworthiness because it does not collect enough evidence. For this reason, in subjective logic an opinion is modeled using belief, disbelief and uncertainty. Subjective logic is also used in the trustworthiness model presented in [17], where the authors used the uncertainty to model the error probability of the channel, that is assumed to be constant. They also use federated learning for distributed model training using local datasets from large-scale nodes, but this method applies well to terrestrial networks where large datasets can easily be collected by observing the traffic of cellular networks, rather than to acoustic networks where only a few network deployments can be observed in reality. Conversely, subjective logic can be applied to our security system, in order to model the case where the transmission of a forwarded packet is not observed due to adverse conditions of the acoustic channel rather than the intentional misbehavior of a node. We extended the model presented in [17] addressing the nature of the acoustic channel, where the error probability is not constant in time but changes during the day.

Sharing the trust metrics among nodes can help build a reputation system in a cooperative way. The drawback of this solution is that it is prone to attacks where the malicious node transmits wrong reputation scores of the other nodes, causing severe damage to the network. However, in [22] the authors prove that, as soon as all nodes share enough reputation information, the effect of a malicious node sharing wrong information on purpose is mitigated. A Bayesian approach is used to update the reputation, taking into account the possibility that the reputation value may be received from a malicious node. In their paper they also use a discount factor to weigh recently observed events more than events occurred in the past, thus addressing the case when a node changes its behavior after a certain amount of time.

Security aspects of underwater acoustic networks have been partially addressed, since only recently have researchers started focusing their work on these aspects. The simulation study in [33], for instance, uses trust in underwater networks to enhance location privacy rather than to detect intruders and malicious nodes. ITrust [32], instead, is an anomaly-resilient trust model based on isolation forest for underwater acoustic sensor networks. ITrust is composed of two sequential stages: data fusion – by aggregating various trust metrics – and defective node detection through the trust model. The model has been evaluated via simulation, with the simplistic assumption that the acoustic noise power spectral density can be computed with the analytical formulas presented in [3].

Conversely, in our work we model the acoustic channel according to the statistics of sea trial measurements. Indeed, in the last fifteen years researchers [24], [34]–[36] demonstrated that the time evolution of underwater acoustic channels can

be statistically well characterized with two- and four-state Markov models [37] and with a two-state HMM [38]. Specifically, in [35], they proved that a three state Markov model is a good candidate to describe the correlated underwater acoustic channel dynamics. More recently, in [36] a two-state Markov chain trained with the KAM'11 sea trial data [39] has been used to model the evolution of the acoustic channel. Finally, in [24] the authors demonstrated, using the SubNet'09 sea trial data [40], that an HMM is able to track well long term channel behaviors, outperforming both two- and four- state Markov models. The use of Markov models to characterize the behavior of the channel is well-known also in terrestrial networks [38], [41]–[43] where the transition probabilities from the states of the Markov Chain are usually obtained exploiting well-established statistical channel characterizations such as Rayleigh fading or Rician fading channel models [44]. In underwater acoustic networks, instead, there is no commonly accepted statistical model for the channel behavior, since the channel is strongly affected by the local environmental conditions of the network deployment. Therefore, in acoustic networks the parameters of the Markov model are often inferred from experimental measurements. An evaluation of the three Markov models (the two Markov models of [37] and the HMM of [38]) compared with sea trial measurements is presented in [24]. The discussion on which model best fits the experimental data is carried out considering relevant metrics for networking, i.e., packet error rate (PER), length of error bursts and correlation of errors after a given number of packet transmissions. Results show that HMMs yield an accurate reproduction of the channel metrics, tracking well long term channel behaviors. For this reason, we decided to model the acoustic channel with a two-state HMM.

III. Channel Model

Given the disruptive nature of the acoustic channel, where an acoustic link between two nodes may present only a small packet loss for several hours, then present a high packet loss for a few hours, and then return stable again, it is not trivial to understand when a drop of performance of an acoustic network is caused by a DoS attack or by bad channel conditions. The increase of packet loss can be caused by several factors [3], for example the increase of noise caused by a ship travelling close to the network deployment, by the presence of strong rain and wind, or by the presence of shadow zones caused by a temperature drop and the consequent change of sound speed profile [45].

In this work we characterize the acoustic channel quality evolution by using a two-state HMM, following the work presented in [24]. The trust model presented in this paper is built on top of the Markov channel model. In an HMM, the observable events stay on top of a non-observable structure, the Markov Chain (MC). The underlying, non-observable link model is a two-state MC that defines two states for the goodness of the channel, specifically a GOOD (g) and a BAD (b) state, collected in the set $\mathcal{S} = \{g, b\}$. The probability of receiving a transmitted packet is o_g in GOOD state, and o_b in BAD state, with $o_g > o_b$. The MC is described through the transition probability matrix $\boldsymbol{P}$

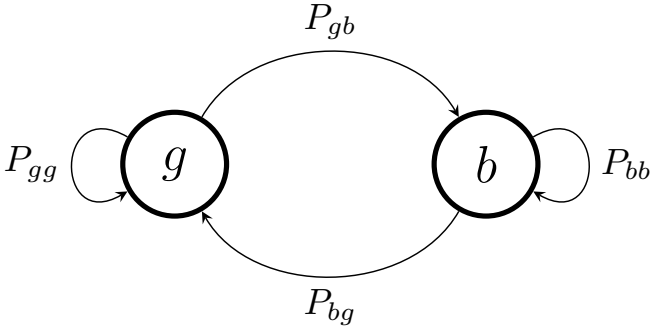


Fig. 2: Two-state MC.

$$\boldsymbol{P} = \begin{pmatrix} P_{gg} & P_{gb} \\ P_{bg} & P_{bb} \end{pmatrix}, \tag{1}$$

where P_{ij} is the probability of moving from state i to state j in one step, with $i, j \in \mathcal{S}$. Figure 2 shows the two-state MC, where $P_{bb} = 1 - P_{bg}$ and $P_{gg} = 1 - P_{gb}$.

The n-step transition matrix $\boldsymbol{P}^n$, can be computed as described in [46]

$$\begin{aligned} \boldsymbol{P^n} = & \frac{1}{P_{gb} + P_{bg}} \begin{pmatrix} P_{bg} & P_{gb} \\ P_{bg} & P_{gb} \end{pmatrix} \\ & + \frac{(1 - P_{gb} - P_{bg})^n}{P_{gb} + P_{bg}} \begin{pmatrix} P_{gb} & -P_{gb} \\ -P_{bg} & P_{bg} \end{pmatrix}, \end{aligned} \tag{2}$$

with n the number of steps after which the system described by the MC is observed again. We denote the state visited at step n as $X_n = s \in \mathcal{S}$. The steady state probability vector $\boldsymbol{\pi} = [\pi_g, \pi_b]$, with $\pi_g + \pi_b = 1$, does not depend on the initial state, and can be computed from the transition probability matrix, specifically,

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} \pi_g & \pi_b \end{pmatrix} = \lim_{n \to \infty} \boldsymbol{P^n} = \frac{1}{P_{gb} + P_{bg}} \begin{pmatrix} P_{bg} & P_{gb} \\ P_{bg} & P_{gb} \end{pmatrix} \tag{3}$$

where the last equality holds because $1 - P_{gb} - P_{bg}$ is smaller than 1 and therefore the second term in Equation (2) goes to 0, thus obtaining $\pi_b = \frac{P_{gb}}{P_{gb}+P_{bg}}$ and $\pi_g = \frac{P_{bg}}{P_{gb}+P_{bg}}$. P_{gb}, P_{bg}, o_g and o_b can be either set manually, in order to study the system in a synthetic channel, or obtained from sea trial measurements [24].

IV. Trust models

A. Subjective Logic

The trust model presented in this paper is based on the observation of the behavior of the neighbors, through the so called watchdog mechanism. In general, when a node of the network receives a packet, it needs to perform a task. For example, if node `A` sends a packet to node `B`, and `B` is not the final destination, `B` could be required to forward that packet either once or several times, depending on the routing protocol used in the network stack. The packet forwarded by `B` will be overheard by all of `B`'s neighbors, including `A`. From `A`'s point of view, `B`'s task will be correctly accomplished if `A`

overhears B's packet, or result in a misbehavior if A does not. Depending on the running protocols and applications, tasks can be different, from the forwarding of a single packet, to the transmission of a series of packets whose number and inter-transmission times depend on the running application. Independently of the task, the final result will always be a decision by node A about whether B's action corresponds to a correct behavior (C) or a misbehavior (M). In this work, a misbehavior is defined as the observation (or the lack of an observation) by a node about an action from the neighbor not compliant with the protocol rules, regardless of whether the action was intentionally carried out by the neighbor or caused by bad channel conditions. For example, if a neighbor is required to forward a packet and the node does not overhear its neighbor's transmission, this will be considered as a misbehavior regardless of whether the packet was intentionally dropped by the neighbor or it was actually transmitted by the neighbor but not overheard by the node because of bad channel condition. The goal of the trust model is to be able to distinguish between intentional misbehavior and unintended misbehavior caused by channel loss that in principle are not discernible by the overhearing node. The model can be applied in networks with tethered nodes as well as networks with non-tethered nodes. While in the former scenario the network nodes have almost fixed position, so that the topology does not change over time, in the latter the nodes slowly drift during time. As long as the nodes remain within transmission range, the node drifting is captured by the dynamics of the channel quality metrics used to determine the channel state (GOOD or BAD) employed in the trust model. In addition, if a new node A comes into B's transmission range because of drifting, B starts to compute A's trustworthiness as for the other nodes, as soon as the node is detected as a new neighbor (and vice versa). In our scenario we do not consider mobile nodes, such as Autonomous Underwater Vehicles (AUVs), leaving the study of this type of scenario for future works.

In an underwater environment, directly applying the output of the watchdog mechanism to compute the trustworthiness of a node could cause misleading conclusions due to the variability of the channel described in Section III. Indeed, a result purely based on the observation of a neighbor without any distinction on the channel quality could lead to a judgement related to the channel quality rather than to the actual node behavior.

In our model, we distinguish when a certain behavior occurs in GOOD and BAD channel state, weighing the two cases differently to obtain an opinion about the node's behavior according to subjective logic [20]. Considering the channel model described in Section III, we model the behavior of a neighbor node through an HMM in which the observable events are the correct behavior (C) or the misbehavior (M) of a node and we denote this set as $\mathcal{E} = \{C, M\}$. For each state $s \in \mathcal{S}$ and each observable event $e \in \mathcal{E}$, the probability of observing the event e in state s is defined as $o_s(e)$, with the constraint $\sum_{e\in\mathcal{E}} o_s(e) = 1$ for each value of $s \in \mathcal{S}$. We emphasize that for a well behaving node, the values of $o_s(M)$ and $o_s(C)$ are related to the probability of not overhearing the packet transmitted by the neighbor, and therefore depend on the packet error probability. Consider as an example a node that has to forward a packet due to the routing protocol rules: $o_g(C)$ is the probability of overhearing a packet transmitted by a legitimate forwarding node in GOOD channel conditions, and $o_b(C)$ is the probability of overhearing a packet transmitted by a legitimate forwarding node in BAD channel conditions.

To compute the trustworthiness of a node we use subjective logic. Subjective logic deals with uncertainty and can be used to represent an *opinion* about a given statement (in our case whether a node can be trusted or not). The opinion is defined as the tuple $\mathbf{o} = \{b, d, u\}$, where $b, d, u \in [0, 1]$ and $b + d + u = 1$. Specifically, the three terms refer to belief, disbelief and uncertainty, respectively. The main idea is to update belief, disbelief and uncertainty based on the outcome, i.e., a correct behavior or a misbehaviors, of the analyzed nodes. The opinion depends on the number of misbehaviors $m = m_b + m_g$ and correct behaviors $c = c_b + c_g$, where m_i and c_i with $i \in \mathcal{S}$ are the number of correct behaviors and misbehaviors observed by a node in channel state i. Belief, disbelief and uncertainty can be computed as:

$$\begin{cases} b = \dfrac{w_{cg}c_g + w_{cb}c_b}{c+m} \\ d = \dfrac{w_{mg}m_g + w_{mb}m_b}{c+m} \\ u = \dfrac{(1-w_{cg})c_g + (1-w_{cb})c_b}{c+m} + \\ \qquad \dfrac{(1-w_{mg})m_g + (1-w_{mb})m_b}{c+m} \end{cases} \tag{4}$$

where $w_{ij} \in [0, 1]\ \forall i \in \{M, C\}\ \forall j \in \{b, g\}$ are the weights to use for a correct behavior (C) or a misbehavior (M) in a GOOD (G) or a BAD (B) channel state.

In addition, the weights used to compute belief, disbelief and uncertainty can be composed by a fixed part, decided a priori, and a variable part that takes into account the trend of the behaviors of the neighbor to adjust the overall weights for correct behaviors and misbehaviors. Specifically, the weights related to a misbehavior, in both GOOD and BAD channel, are defined as

$$w_{mi} = \alpha\tilde{w}_{mi} + (1-\alpha)w_{var} \qquad i \in g, b, \tag{5}$$

where w_{var} is a function of the behaviors of a neighbor, whose goal is to grasp some signs about anomalous behavior (e.g., number of misbehaviors in GOOD channel higher than number of misbehaviors in BAD channel) that could be the manifestation of a misbehaving node, and therefore to penalize that neighbor increasing the weight for each misbehavior. Similarly, the weights for the correct behavior, in both GOOD and BAD channel, can be defined as

$$w_{ci} = \alpha\tilde{w}_{ci} + (1-\alpha)(1-w_{var}) \qquad i \in g, b. \tag{6}$$

B. Trustworthiness

We define a random variable T to describe whether a node is trustworthy ($T = 1$) or not ($T = 0$). Based on subjective logic and on the trust model described in Section IV-A, we can decide if a node is trustworthy by observing belief,

disbelief and uncertainty. These three values can be differently combined to infer trustworthiness, e.g., by considering in different ways the role of the uncertainty. For example, in the following we will use

$$\begin{aligned} T &= 1 \qquad \text{if } b + \beta u > d + (1-\beta)u \\ T &= 0 \qquad \text{otherwise,} \end{aligned} \tag{7}$$

with $\beta \in [0, 1]$. Based on the HMM we can compute the probability that a node is considered trustworthy after N_t observations. We compute

$$P[T = 1 \mid N_t] = P[b + \beta u > d + (1-\beta)u \mid N_t]. \tag{8}$$

We define $\mathcal{M}$ as the set of all the m_g values for which $T = 1$, for a given number of misbehaviors in BAD channel and for a given number of visits to the BAD state (N_b)

$$\mathcal{M} = \{m_g : b + \beta u > d + (1-\beta)u\} \tag{9}$$

We remember that the number of visits to the GOOD state (N_g) can be obtained from the equation $N_t = N_b + N_g$, and that $N_s = m_s + c_s$ with $s \in \mathcal{S}$.

The probability in Equation (8) can be computed by conditioning on the number of misbehaviors in the BAD channel m_b and on the number of visits either to the GOOD state (N_g) or to the BAD state (N_b).

$$\begin{aligned} P[T = 1 \mid N_t] = \sum_{N_b=0}^{N_t} \sum_{m_b=0}^{N_b} \sum_{m_g \in \mathcal{M}} P\Big[m_g \;\Big|\; N_t, m_b, N_b\Big] \\ P\Big[m_b \mid N_b, N_t\Big] P\Big[N_b \mid N_t\Big]. \end{aligned} \tag{10}$$

where m_g and m_b follow a binomial distribution: $m_g \sim \text{Bin}(N_g, o_g(M))$ and $m_b \sim \text{Bin}(N_b, o_b(M))$, respectively. Therefore, the trust probability becomes

$$\begin{aligned} P[T = 1 \mid N_t] = \sum_{N_b=0}^{N_t} \sum_{m_b=0}^{N_b} \sum_{m_g \in \mathcal{M}} \binom{N_t - N_b}{i} o_g(M)^i \\ (1 - o_g(M))^{(N_t - N_b - i))} \binom{N_b}{m_b} o_b(M)^{m_b} \\ (1 - o_b(M))^{(N_b - m_b)} P\Big[N_b \mid N_t\Big]. \end{aligned} \tag{11}$$

The last step is to compute the probability of visiting the BAD state N_b times, in a given number of steps N_t (or equivalently the number of visits in the GOOD state). We define $\phi_s(k, n) = P[k \text{ visits to B in } n \text{ steps} \mid X_0 = s]$ as the probability of visiting k times the BAD state in n steps, given that we start in the initial state $s \in \mathcal{S}$. We can recursively compute $\phi_s(k, n)$ exploiting the properties of a MC by conditioning on the first step

$$\begin{aligned} \phi_g(k, n) &= P_{gg}\phi_g(k, n-1) + P_{gb}\phi_b(k, n-1) \\ \phi_b(k, n) &= P_{bg}\phi_g(k-1, n-1) + P_{bb}\phi_b(k-1, n-1), \end{aligned} \tag{12}$$

with the initial conditions $\phi_s(0, 0) = 1$ and $\phi_s(k, n) = 0$ if $k > n$, with $s \in \mathcal{S}$. In the first row only the number of steps is decreased because, starting from the GOOD state, there is no visit to the BAD state in the first step. On the other hand, in the second row, given that we start from the BAD state both the number of remaining visits and the number of steps are decreased by one. Finally, $P[N_b \mid N_t]$ can be computed as

$$P[N_b \mid N_t] = \pi_g \phi_g(N_b, N_t) + \pi_b \phi_b(N_b, N_t) \tag{13}$$

C. Variable weights

To compute the set $\mathcal{M}$ for which the node is considered trustworthy, we need to define w_{var}. If we consider a scenario with both GOOD and BAD channel states, we define w_{var} as a function of the estimated misbehavior probability in GOOD and BAD channel, $p_{m,g} = m_g/N_g$ and $p_{m,b} = m_b/N_b$, respectively. A GOOD channel should be characterized by a small number of misbehaviors, while in BAD channel misbehaviors are more likely to be observed due to the higher packet error rate. Comparing the misbehavior rate in GOOD and BAD channel, we can gain some insight about the behavior of the neighbor. Indeed, a number of misbehaviors in the GOOD channel comparable or even higher than the number of misbehaviors in the BAD channel could be the manifestation of an attacking node, and therefore the weights for the misbehavior should be increased, while the weight for the correct behavior should be decreased. We define

$$\begin{aligned} w_{var} &= \frac{2p_{m,g}}{p_{m,g} + p_{m,b}} \qquad \text{if } p_{m,g} < p_{m,b} \\ w_{var} &= 1 \qquad \text{otherwise.} \end{aligned} \tag{14}$$

Using this definition, w_{var} is equal to 1 when the misbehaviors in GOOD channel are much higher than the misbehaviors in the BAD channel, and close to 0 when there are only few misbehaviors in GOOD channel as would be expected by a node behaving normally. This definition needs to be slightly modified for those scenarios in which the channel quality is favorable, and thus the channel always remains in GOOD state (i.e., $N_b = 0$). In this case, since $p_{m,b}$ cannot be computed, we consider a target value equal to 0.5, therefore the definition becomes:

$$\begin{aligned} w_{var} &= \frac{2p_g}{p_g + 0.5} \qquad \text{if } p_g < 0.5 \\ w_{var} &= 1 \qquad \text{otherwise.} \end{aligned} \tag{15}$$

The last step is to find the set $\mathcal{M}$, i.e., the number of misbehaviors in GOOD channel for which the node can be trusted, by solving the inequality

$$b + \beta u > d + (1-\beta)u\,. \tag{16}$$

Substituting the expressions for belief and disbelief defined in Equation (4), remembering that $u = 1 - b - d$, and considering that $c_s = N_s - m_s$ with $s \in \mathcal{S}$, we obtain the following inequality

$$\begin{aligned} m_g((1-\beta)w_{cg} + \beta w_{mg}) + m_b((1-\beta)w_{cb} + \beta w_{mb}) < \\ (1-\beta)w_{cb}N_b + (1-\beta)w_{cg}N_g - N_t(1/2 - \beta) \end{aligned} \tag{17}$$

In addition, we assume equal weights for the correct behaviors with GOOD and BAD channel, i.e., $\tilde{w}_{cb} = \tilde{w}_{cg} = \tilde{w}_c$ and

therefore $w_{cb} = w_{cg} = w_c$. Considering that $N_t = N_g + N_b$, the inequality becomes

$$m_g((1-\beta)w_c + \beta w_{mg}) + m_b((1-\beta)w_c + \beta w_{mb}) < N_t((1-\beta)w_c + \beta - 1/2) \quad (18)$$

Substituting Equations (5) and (6) in the previous inequality, we obtain

$$a_g m_g + a_b m_b + k_1 w_{var}(m_g + m_b) + k_2 w_{var} - k_3 < 0 \quad (19)$$

with the coefficients defined as

$$\begin{aligned} a_g &= \alpha((1-\beta)\tilde{w}_c + \beta\tilde{w}_{mg}) + (1-\alpha)(1-\beta) \\ a_b &= \alpha((1-\beta)\tilde{w}_c + \beta\tilde{w}_{mb}) + (1-\alpha)(1-\beta) \\ k_1 &= (1-\alpha)(2\beta - 1) \\ k_2 &= N_t(1-\alpha)(1-\beta) \\ k_3 &= N_t(\beta - 1/2 + \alpha(1-\beta)\tilde{w}_c + (1-\alpha)(1-\beta)) \end{aligned} \quad (20)$$

The last step is to substitute the value of w_{var} in the two cases as defined in Equation (14), $p_{m,g} < p_{m,b}$ and $p_{m,g} \geq p_{m,b}$, obtaining

$$c_1 m_g^2 + c_2 m_g + c_3 < 0 \quad (21)$$

with

$$\begin{aligned} c_1 &= \frac{a_g + 2k_1}{N_g} \\ c_2 &= a_g p_{m,b} + \frac{2k_1 m_b + 2k_2 + a_b m_b - k_3}{N_g} \\ c_3 &= a_b m_b - k_3 \end{aligned} \quad (22)$$

with $p_{m,g} < p_{m,b}$, and

$$m_g < \frac{k_3 - k_2 - m_b(a_b + k_1)}{a_g + k_1} \quad (23)$$

with $p_{m,g} \geq p_{m,b}$. This inequality holds for the general case with both GOOD and BAD channel. If we consider the case with only GOOD channel, the solutions can be obtained by substituting $N_b = 0$ (and therefore $m_b = 0$) and $p_{m,b} = 0.5$.

In addition to variable weights, in principle also different values of β could be used for different scenarios. As an example, where the channel remains always in the GOOD state ($N_b = 0$) the role of uncertainty would be different since less uncertainty is expected from a node experiencing good channel condition. In such a scenario β could be set to a low value (or at least lower than in the general case with both GOOD and BAD channel condition), to help discover malicious nodes performing weaker attacks (e.g., not performing the intended task only occasionally).

D. Malicious node

In the case of a malicious node the trust model remains the same, with the only exception of the probability of behaving correctly or maliciously. An attacker intentionally acts to damage the network, therefore the probability of misbehaving is not only related to the channel quality but also to the strength and type of attack the node is going to perform. If we consider a malicious node that performs an attack not accomplishing intentionally its task with a given probability p_d, e.g., does not forward the packet according to the protocol rules, the probability of behaving correctly becomes

$$\tilde{o}_s(C) = o_s(C)(1 - p_d) \qquad \forall s \in \mathcal{S} \quad (24)$$

and therefore, the probability of misbehaving is

$$\tilde{o}_s(M) = 1 - \tilde{o}_s(C) \qquad \forall s \in \mathcal{S} \quad (25)$$

By substituting $o_s(M)$ with $\tilde{o}_s(M)$ in Equation (11) we obtain the trust probability of an attacker acting maliciously with probability p_d.

V. Scenario Description and Parameter Settings

We analyze the trust model, both through an analytical formulation based on HMM and through simulation with the DESERT Underwater Network simulator [25].

The HMM described in Section III is characterized by the transition probabilities $P_{gg} = 0.87$ and $P_{bb} = 0.72$. For the theoretical analysis we compare the results with different probabilities of observing a misbehavior ($o_s(M)$) or a correct behavior ($o_s(C)$) for each channel state $s \in \mathcal{S}$, which correspond to different channel qualities experienced by a node. We assess the trust probability of both a normal node and a malicious node performing attacks of different strength, i.e., with different values of p_d. In the scenario with GOOD and BAD channel states we assume a value of $\beta = 0.7$, meaning that uncertainty is mostly considered as part of the trustworthiness of the node. In the scenario with only GOOD channel state we consider $\beta = 0$, therefore the uncertainty computed with the subjective logic is considered as the sign of an untrustworthy node. Indeed, in this second case, the channel condition is favorable and in principle the possibility of observing a misbehavior is lower, therefore each misbehavior needs to be carefully taken into account in the trust model. A value of $\beta = 0$ allows us to better detect attackers in such a scenario.

As a second step we test the trust model in an underwater network. We assess our model in topologies similar to the one depicted in Figure 3. Specifically, the network is composed by 10 nodes, 9 of them generating data and sending it to the sink placed in the center of the network using flooding as the routing protocol. Each node receiving a packet and running the flooding protocol is expected to forward the data to all its neighbors, until reaching the sink node. At the beginning of the mission the count of correct behaviors and misbehaviors is set to 0, and is updated during the mission. When a node overhears the packet forwarded by the neighbor a correct behavior is considered, while if the forwarding is not overheard within a predefined time interval a misbehavior is counted. We remark that the observed misbehaviors can in principle be either intentionally caused by an attacker, or unintended due to the channel condition. The count of correct behaviors and misbehaviors will be used to compute the trust of a node considering Equations (4) and (7). To test our trust model we select one of the nodes close to the sink to act as the attacker. Specifically, the attacker does not always forward the packets received from its neighbor, but drops them with a given probability p_d. In the network simulator the channel

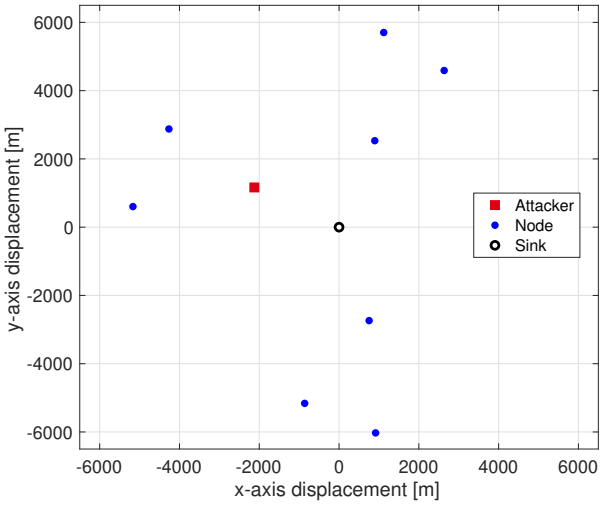


Fig. 3: Example of topology with normal nodes (blue circles), attacker (red square) and sink node (black circle).

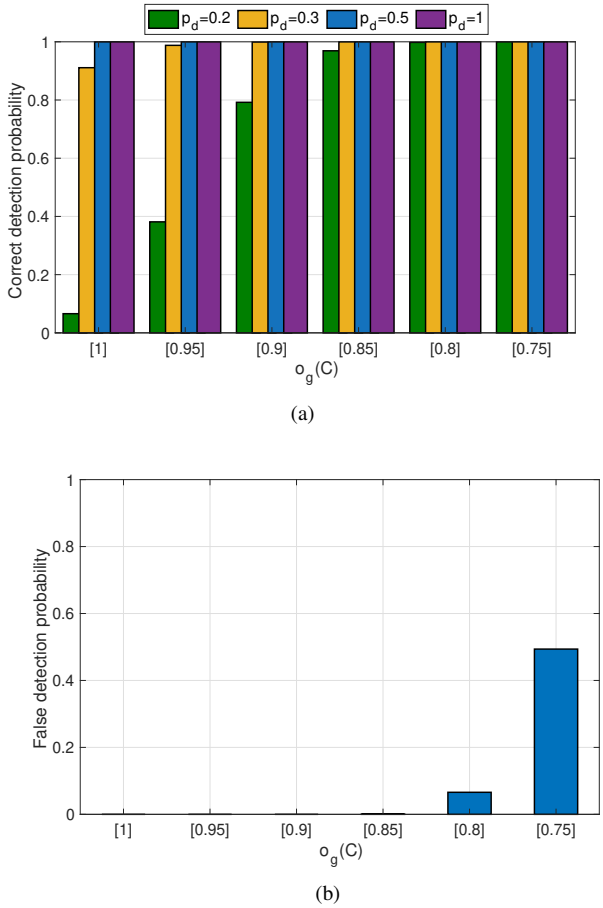


Fig. 4: (a) correct detection and (b) false detection probabilities as a function of the correct behavior probability for GOOD channel scenario.

state is obtained by looking at the Signal to Interference plus Noise Ratio (SINR) of each received packet or at the noise level when the node does not overhear the forwarding of a packet by one of its neighbors. We use two thresholds to detect the channel state, one for the transition from GOOD state to BAD state $S_{th,g}$, and the second one for the transition from BAD state to GOOD state $S_{th,b}$. The hysteresis is useful to avoid continuous jumps from one state to the other with small changes in the SINR value. In our scenario we set $S_{th,g} = 6.3$ dB and $S_{th,b} = 7$ dB. In an actual deployment, mathematical analysis can be performed before the mission to choose the SINR threshold used to define GOOD and BAD channel states. The goal is to set the threshold based on the performance, in terms of false detection and correct detection probabilities, that best suits the mission needs. The SINR threshold can be retrieved from the correct reception probabilities in GOOD and BAD state which can be easily varied in the mathematical analysis.

To simulate the behavior of a two-state channel model as that described in Section III, in the simulator we use the Urick propagation model [45], changing the noise level every $T = 180$ s between two values, according to the transition probabilities of a MC. For consistency, we set the same transition probabilities used in the theoretical analysis.

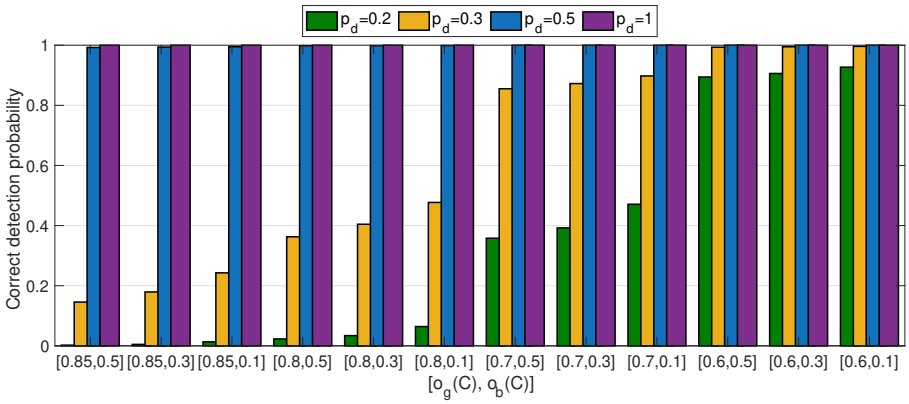
In the simulated scenario, each node generates a packet of 24 Bytes every 100 s, on average. The transmission power is equal to $P_{tx} = 180$ dB re μPa, the central frequency used for the transmission is $f_0 = 26$ kHz and the bandwidth is $B = 16$ kHz.

VI. Results

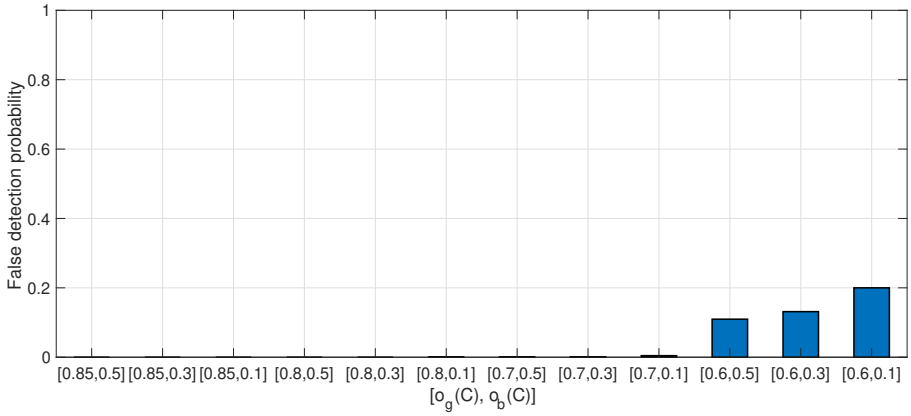
A. Analytical results

In this Section we present the results obtained from the theoretical trust model described in Section IV. We compute the probability of correct detection for a malicious node, i.e., the probability of not trusting the attacker (a node with $p_d > 0$), and the probability of false detection, i.e., the probability of not trusting a correctly behaving node (with $p_d = 0$), after $N_t = 150$ steps. We computed the correct detection and false detection probabilities in two different scenarios: the first one in which the channel always remains in GOOD state, with the goal of analyzing the trustworthiness of a node under very favorable channel conditions, the second one with a more general behavior where both GOOD and BAD channel states are considered.

Figures 4a and 4b show the correct detection and false detection probabilities in the scenario with only GOOD channel. The analysis has been carried out as a function of the probability of observing a correct behavior $o_g(C)$ (that is related to the packet delivery ratio) in a GOOD channel state and considering different attack strengths (i.e., different probabilities p_d of intentional misbehavior). For each analyzed channel quality, an attacker behaving intentionally maliciously with a probability of performing an attack of $p_d \geq 0.3$ can be easily identified and marked as an untrustworthy node. However, when the correct behavior probability $o_g(C)$ drops to 0.75, the false detection probability rapidly increases to 0.5, meaning that well behaving nodes are marked as untrustworthy half of the time. This is due to the fact that $\beta = 0$ is used in the case of only GOOD channel state, as stated in Section V. This



(a)



(b)

Fig. 5: (a) correct detection and (b) false detection probabilities as a function of the correct behavior probability for GOOD and BAD channel scenario

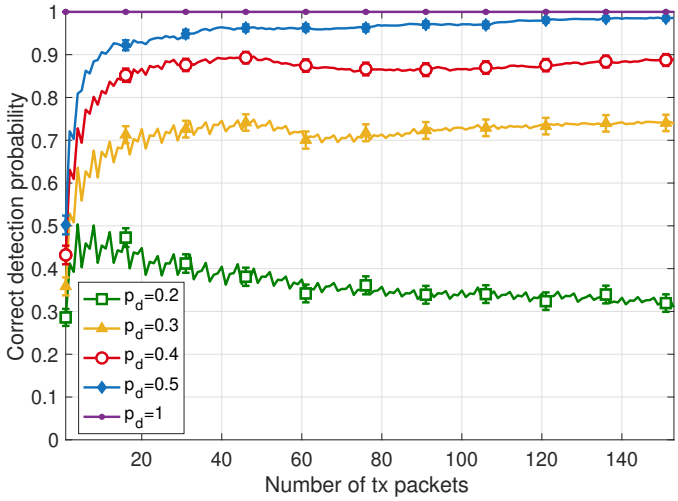
setting indeed highly penalizes misbehaviors since uncertainty will be only summed to disbelief in Equation (7).

The performance improves if the packet reception probability is higher, as is expected for this particular scenario with only GOOD channel conditions. Indeed, for better channel conditions the false detection probability remains lower than 0.1 and even close to 0 for a correct behavior probability less than or equal to 0.85.

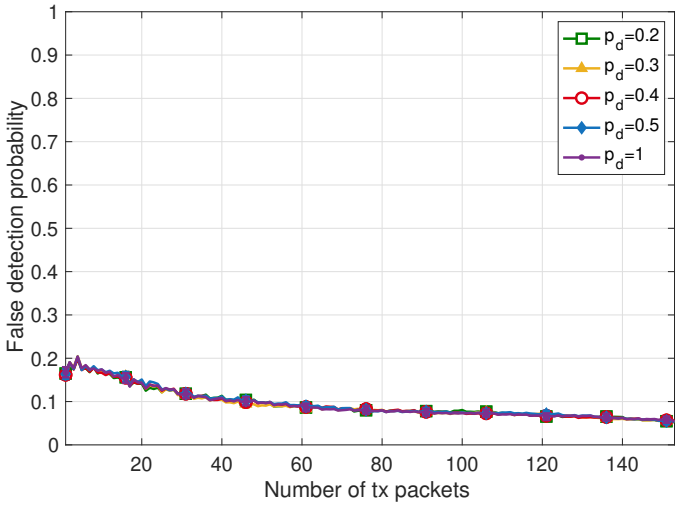
Figures 5a and 5b show the correct detection and false detection probabilities in the scenario with both GOOD and BAD channel. The analysis has been performed as a function of the correct behavior probabilities in both GOOD and BAD channel $[o_g(C), o_b(C)]$, and considering different attack strengths p_d. In this scenario, since the channel quality is lower than in the previous scenario with only GOOD channel, the detection of attackers with a low p_d becomes more difficult. Indeed, when $p_d \geq 0.5$ the attacker is always detected after 150 steps, while for $p_d \leq 0.3$ the correct detection depends on the channel quality. An increasing error probability due to channel losses seems to help in detecting attackers with lower strength. This is also followed by an increment of the false detection probability (Figure 5b), however the increment in the false detection probability in our scenario is limited when $o_g(C) = 0.6$ and always remains lower than 0.2.

B. Simulation results

In this Section we present the results obtained through simulation of the scenario described in Section V. We assessed the trustworthiness of the nodes, considering 50 runs for each of the 20 analyzed topologies, similar to that presented in Figure 3. Specifically, we considered the trust computed by each node in the most external set with respect to its neighbor closer to the sink. Figures 6a and 6b show the correct detection (for an attacker) and false detection (for a normal node) probabilities as a function of the number of transmitted packets and for different drop probabilities p_d, taking into account the results obtained for each run and each topology. Figure 6a shows the same trend observed with the theoretical results. We want to highlight that, depending on the topologies and thus on the actual distance between neighbors, the performance takes into account both nodes with favorable conditions (i.e., with only GOOD channel) and nodes with more unfavorable conditions (i.e., nodes that alternate GOOD and BAD channel states). For a drop probability $p_d = 0.2$, the system cannot easily identify an attacker because the drops caused intentionally by the malicious node can be confused with the losses caused by bad channel conditions or collisions with other transmissions. With $p_d \geq 0.3$ the overall performance improves, going from a correct detection

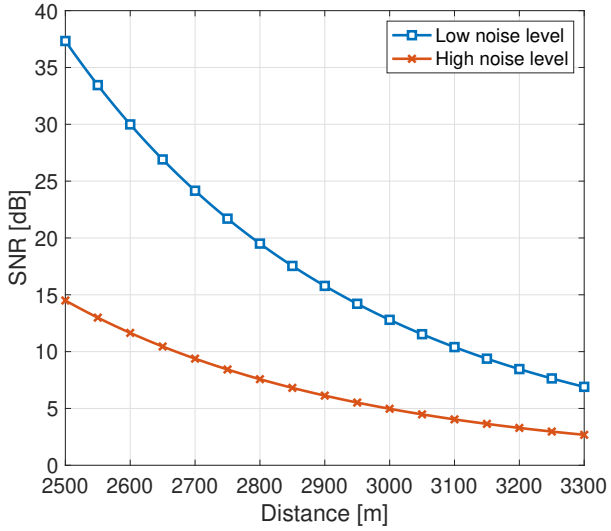


(a)

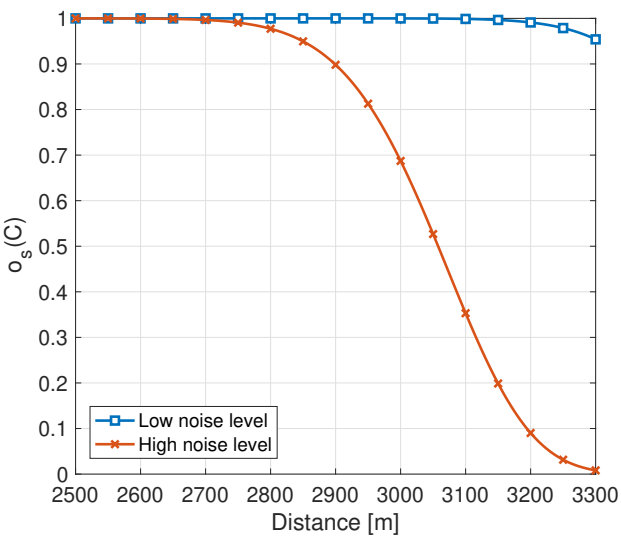


(b)

Fig. 6: (a) correct detection and (b) false detection probabilities as a function of the number of transmitted packets and for different attack strength p_d.



(a)

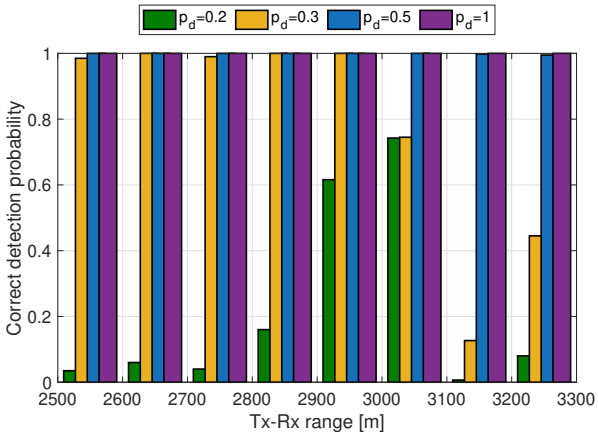


(b)

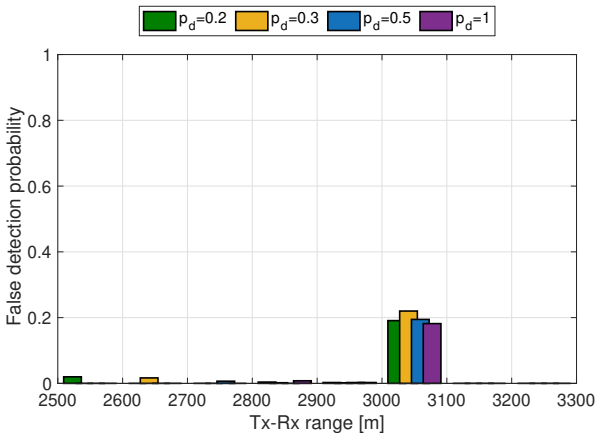
Fig. 7: (a) SNR and (b) probability of observing a correct behavior as a function of the distances for low (blue) and high (red) noise level.

probability of 0.7 with $p_d = 0.3$ to a detection of almost 100% with $p_d \geq 0.5$. On the other hand, Figure 6b shows the estimated false detection probability for a normal node as a function of the number of transmitted packets. As expected, the result does not depend on the drop probability p_d of the attacker. The false detection probability is close to 0.2 at the very beginning of the simulations, when few packets have been exchanged, while it decreases to 0.05 when more information becomes available. In addition, we can observe that the correct detection probability rapidly converges within 60 transmitted packets. With this fast convergence shown in the results, slow environmental condition changes, for example caused by day-night or tidal cycles, will have little effect on the trust model not causing the trustworthiness value to continuously change within short periods.

As mentioned before, this analysis considers all topologies, therefore it takes into account different channel qualities for both attackers and normal nodes. For a better understanding of the behavior of the trust model for different simulated channel qualities, we plot the estimated correct and false detection probabilities at the end of the simulation as a function of the distance between the node and its neighbors. Figures 7a and 7b are showing the SNR experienced by a node as a function of the distance for low and high noise level and the probability of observing a correct behavior from the neighbor based on the channel, respectively. Since different distances correspond to different channel qualities, this allows us to understand the behavior of the trust model for different channels. Figures 8a and 8b depict the estimated correct and false detection probabilities, respectively. According to the propagation model used in the simulator, a node placed at a distance lower than 3 km is always in GOOD channel, since the SNR is higher than the threshold $S_{th,g}$. In this scenario the trend obtained for the correct detection is similar to the trend observed with the analytical results with always GOOD channel condition (Figure 4a), where an attacker with $p_d \geq 0.3$ is correctly detected with a probability close to 1. Considering $p_d = 0.2$, the correct detection probability is very low for closer nodes,



(a)



(b)

Fig. 8: (a) correct detection and (b) false detection probabilities as a function of the number of transmitted packets and for different attack strength p_d.

but increases as the distance increases because the packet losses due to channel errors help in the attacker identification. At the same time, for a distance lower than 3 km the false detection probability is close to 0, meaning that the normal nodes are not wrongly marked as attackers. Nodes within a range of 3 to 3.1 km can experience both situations, i.e., either always GOOD channel condition or both GOOD and BAD channel. In this case attackers dropping packets with $p_d \geq 0.5$ are always correctly detected, while for an attack strength of $p_d = 0.2$ and $p_d = 0.3$ the correct detection probability is 0.7. In this range of distances the false detection probabilities increase up to 0.2, due to those nodes that are always in GOOD channel conditions but with an increased packet error rate. When the distance is bigger than 3.1 km the nodes always experience both GOOD and BAD channel conditions. Also in this case the trend for correct detection and false detection is similar to what observed in the theoretical analysis. For the considered distances, a lower attack strength is more difficult to detect, therefore the correct detection probability with $p_d \leq 0.3$ is lower than 0.5, while it remains close to 1 for $p_d \geq 0.5$. In this situation the estimated false detection probability is close to 0.

VII. Conclusions

In this paper we presented a trust model for underwater acoustic networks to detect suspicious behaviors of possible attackers. The main problem in acoustic communication is to understand whether a misbehavior is due to channel loss conditions or to a malicious behavior. The dynamic quality of an acoustic channel can be described through a two-state HMM and we exploited this characteristic to weigh differently misbehaviors in GOOD and BAD channel conditions. We analyzed the trust model both analytically and through simulations. Specifically, we computed the correct detection and false detection probabilities for different attack strengths p_d, observing that when $p_d \geq 0.5$ the malicious node is always detected, while for lower values of p_d in scenarios with both GOOD and BAD channel states the detection is more challenging since the intentional misbehavior is difficult to distinguish from a misbehavior caused by a channel drop. If the channel quality is more favorable, i.e., with only GOOD channel, even a value of $p_d = 0.3$ can be detected. The simulations of the trust model with the flooding routing protocols confirm the same trend observed with the analytical results.

As future work, we will extend the trust model by letting nodes exchange information about their trust level of a node, thus combining local information with the received information and obtain a more accurate result. In addition, we will design and evaluate countermeasures to exclude the attacker from the network which will exploit the trust model as a base for the detection of malicious nodes, and evaluate the trust model in a scenario composed of both fixed and mobile nodes.

Acknowledgment

This work has been partially supported and funded by the Bundeswehr Technical Center for Ships and Naval Weapons, Maritime Technology and Research, (contract 728053 - E/E71S/K1291CF081), and by the European Union - FSE REACT EU, PON Research and Innovation 2014-2020 (DM 1062/2021).

References

[1] F. Campagnaro, R. Francescon, P. Casari, R. Diamant, and M. Zorzi, "Multimodal underwater networks: Recent advances and a look ahead," in *Proc. ACM WUWNet*, Halifax, Canada, Nov. 2017.

[2] F. Campagnaro, A. Signori, and M. Zorzi, "Wireless remote control for underwater vehicles," *MDPI Journal of Marine Science Engineering*, vol. 8, no. 4, p. 55, Oct. 2019.

[3] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," *ACM Mobile Comput. and Commun. Review*, vol. 11, no. 4, pp. 34–43, Oct. 2007.

[4] G. Toso, R. Masiero, P. Casari, O. Kebkal, M. Komar, and M. Zorzi, "Field experiments for dynamic source routing: S2C evologics modems run the SUN protocol using the DESERT Underwater libraries," in *Proc. MTS/IEEE OCEANS*, Hampton Roads, VA, Oct. 2012.

[5] M. Goetz and I. Nissen, "GUWMANET — multicast routing in underwater acoustic networks," in *Military Communications and Information Systems Conference (MCC)*, 2012.

[6] R. Diamant, P. Casari, F. Campagnaro, O. Kebkal, V. Kebkal, and M. Zorzi, "Fair and throughput-optimal routing in multimodal underwater networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1738–1754, Mar. 2018.

[7] A. Signori, F. Campagnaro, F. Steinmetz, B.-C. Renner, and M. Zorzi, "Data gathering from a multimodal dense underwater acoustic sensor network deployed in shallow fresh water scenarios," *MDPI Journal of Sensor and Actuator Networks*, vol. 8, no. 4, p. 55, Dec. 2019.

[8] F. Guerra, P. Casari, and M. Zorzi, "A performance comparison of MAC protocols for underwater networks using a realistic channel simulator," in *Proc. MTS/IEEE OCEANS 2009*, 2009.

[9] M. Molins and M. Stojanovic, "Slotted FAMA: a MAC protocol for underwater acoustic networks," in *Proc. MTS/IEEE OCEANS 2006 - Asia Pacific*, 2006.

[10] F. Campagnaro, P. Casari, M. Zorzi, and R. Diamant, "Optimal transmission scheduling in small multimodal underwater networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 368–371, Apr. 2019.

[11] P. van Walree, H. Buen, and R. Otnes, "A performance comparison between DSSS, M-FSK, and frequency-division multiplexing in underwater acoustic channels," in *Underwater Communications and Networking (UComms)*, 2014.

[12] O. Kebkal, M. Komar, and K. Kebkal, "D-MAC: Hybrid media access control for underwater acoustic sensor networks," in *Proc. IEEE ICC*, Cape Town, South Africa, May 2010.

[13] H. Dol, M. Colin, P. van Walree, and R. Otnes, "Field experiments with a dual-frequency-band underwater acoustic network," in *Fourth Underwater Communications and Networking Conference (UComms)*, 2018.

[14] F. Campagnaro, D. Tronchin, A. Signori, R. Petroccia, K. Pelekanakis, P. Paglierani, J. Alves, and M. Zorzi, "Replay-attack countermeasures for underwater acoustic networks," in *Proc. MTS/IEEE OCEANS*, Virtual, Global, Oct. 2020.

[15] A. Signori, F. Chiariotti, F. Campagnaro, and M. Zorzi, "A game-theoretic and experimental analysis of energy-depleting underwater jamming attacks," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9793–9804, Oct. 2020.

[16] X. Li, M. R. Lyu, and J. Liu, "A trust model based routing protocol for secure ad hoc networks," in *Proc. IEEE Aerospace Conference*, vol. 2, Big Sky, MT, USA, 2004, pp. 1286–1295.

[17] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 700–10 714, Dec. 2019.

[18] A. Signori, E. Coccolo, F. Campagnaro, I. Nissen, and M. Zorzi, "Trustworthiness in the GUWMANET Protocol for Underwater Acoustic Mobile Ad-Hoc Networks," in *Proc. of ACM WUWNet 2021*, Shenzen, China, Nov. 2021.

[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM international conference on Mobile computing and networking (MobiCom)*, 2000, pp. 255–265.

[20] A. Jøsang, "Artificial reasoning with subjective logic," in *Proc. the second Australian workshop on commonsense reasoning*, vol. 48, 1997, p. 34.

[21] S. Dietzel, R. van der Heijden, H. Decke, and F. Kargl, "A flexible, subjective logic-based framework for misbehavior detection in v2v networks," in *Proc. IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Sydney, NSW, Australia, 2014.

[22] S. Buchegger and J. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Second Workshop on Economics of P2P Systems, Boston*, 2004.

[23] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Network*, vol. 4, no. 3, Jun. 2008.

[24] B. Tomasi, P. Casari, L. Finesso, G. Zappa, K. McCoy, and M. Zorzi, "On modeling JANUS packet errors over a shallow water acoustic channel using Markov and hidden Markov models," in *IEEE Military Communications Conference (MILCOM 2010)*, 2010, pp. 2406–2411.

[25] F. Campagnaro, R. Francescon, F. Favaro, F. Guerra, R. Diamant, P. Casari, and M. Zorzi, "The DESERT Underwater framework v2: Improved capabilities and extension tools," in *Proc. UComms*, Lerici, Italy, Sep. 2016.

[26] J. Cho, A. Swami, and I. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys Tutorials*, vol. 13, no. 4, pp. 562–583, Oct. 2011.

[27] A. Boukerche, L. Xu, and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Communications*, vol. 30, no. 11, pp. 2413–2427, 2007, special issue on security on wireless ad hoc and sensor networks. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366407001661

[28] X. Yang, X. Yi, I. Khalil, Y. Zeng, X. Huang, S. Nepal, X. Yang, and H. Cui, "A lightweight authentication scheme for vehicular ad hoc networks based on MSR," *Vehicular Communications*, vol. 15, pp. 16–27, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209618301785

[29] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, 2021, Early Access.

[30] S. Theodore, K. Gandhi, and V. Palanisamy, "A novel lightweight authentication and privacy-preserving protocol for vehicular ad hoc networks," *Springer Complex & Intelligent Systems*, Oct 2021.

[31] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in *IEEE Global Telecommunications Conference (GLOBECOM 2008)*, 2008.

[32] J. Du, G. Han, C. Lin, and M. Martinez-Garcia, "ITrust: An anomaly-resilient trust model based on isolation forest for underwater acoustic sensor networks," *IEEE Transactions on Mobile Computing (Early Access)*.

[33] M. M. Arifeen, A. A. Islam, M. M. Rahman, K. A. Taher, M. M. Islam, and M. S. Kaiser, "ANFIS based trust management model to enhance location privacy in underwater wireless sensor networks," in *International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2019.

[34] F. Pignieri, F. De Rango, F. Veltri, and S. Marano, "Markovian approach to model underwater acoustic channel: Techniques comparison," in *IEEE Military Communications Conference (MILCOM 2008)*, 2008.

[35] B. Tomasi, P. Casari, L. Badia, and M. Zorzi, "Cross-layer analysis via Markov models of incremental redundancy hybrid ARQ over underwater acoustic channels," *Ad Hoc Networks*, vol. 34, pp. 62–74, 2015, aDVANCES IN UNDERWATER COMMUNICATIONS AND NETWORKS. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870514001449

[36] B. Tomasi and J. C. Preisig, "Evaluating energy-efficient schedulers on underwater acoustic data," in *OCEANS 2019 - Marseille*, 2019.

[37] D. A. Sanchez-Salas and J. L. Cuevas-Ruiz, "N-states channel model using Markov chains," in *Electronics, Robotics and Automotive Mechanics Conference (CERMA 2007)*, 2007, pp. 342–347.

[38] W. Turin and R. van Nobelen, "Hidden Markov modeling of flat fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 9, pp. 1809–1817, Dec. 1998.

[39] B. Tomasi, J. Preisig, and M. Zorzi, "On the predictability of underwater acoustic communications performance: The KAM11 data set as a case study," in *Proc. ACM WUWNet*, Seattle, Washington, Dec. 2011.

[40] B. Tomasi, P. Casari, M. Zorzi, G. Zappa, and K. McCoy, "Experimental study of the acoustic channel properties during subnet 2009," University of Padova, Tech. Rep., 2010. [Online]. Available: {http://telecom.dei.unipd.it/pages/read/75/}

[41] E. N. Gilbert, "Capacity of a burst-noise channel," *The Bell System Technical Journal*, vol. 39, no. 5, pp. 1253–1265, Sep. 1960.

[42] M. Zorzi, R. Rao, and L. Milstein, "Error statistics in data transmission over fading channels," *IEEE Transactions on Communications*, vol. 46, no. 11, pp. 1468–1477, Nov. 1998.

[43] M. Zorzi, R. Rao, and L. Milstein", "On the accuracy of a first-order Markov model for data transmission on fading channels," in *Proc. IEEE International Conference on Universal Personal Communications*, Tokyo, Japan, 1995, pp. 211–215.

[44] J. G. Ruiz, B. Soret, M. C. Aguayo-Torres, and J. T. Entrambasaguas, "On finite state Markov chains for Rayleigh channel modeling," in *Proc. 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology*, Aalborg, Denmark, May 2009.

[45] R. J. Urick, *Principles of Underwater Sound*, 3rd ed. McGraw-Hill, 1983.

[46] H. M. Taylor and S. Karlin, *An Introduction to Stochastic Modeling*, 3rd ed. Academic Press, 1999.

Alberto Signori [S'19] received the B.Sc. degree in information engineering and the M.Sc. degree in telecommunication engineering from the University of Padova, Padua, Italy, in 2015 and 2017, respectively. In January 2018, he joined the SIGNET research group, within the Department of Information Engineering of the same university, as a research engineering. In October 2021, he completed the Ph.D program at the University of Padova, under the supervision of Prof. M. Zorzi. His studies during the Ph.D. include the design, the analysis and the implementation of novel communication protocols and architectures for underwater networks, and network security for underwater communications. He has been involved in the software development of the DESERT Underwater framework. He collaborated with the MarTERA RoboVaaS project and with the European Defence Agency project SALSA. In 2019, he received the Best Student Paper Award at International Conference on Underwater Networks & Systems (WUWNet). In 2020, he received the Best Paper Award at IEEE INFOCOM International Workshop on Wireless Communications and Networking in Extreme Environments (WCNEE).

Filippo Campagnaro [M'19] received the B.Sc. and the M.Sc. degrees from the University of Padova, Italy, in 2012 and 2014, respectively. In 2014, he joined the SIGNET Group, within the Department of Information Engineering of the same university, as a Research Engineer. In October 2019 he completed the Ph.D. program in Information Engineering and joined the same department as a post-doctoral researcher and lecturer of ICT master courses. His Ph.D. thesis involves the design and the evaluation of multimodal underwater optical and acoustic networks, with a particular focus on simulation and field experimentation (defence scheduled for February 2020). Filippo has joined many sea trials with the NATO STO CMRE (La Spezia, Italy), EvoLogics GmbH (Berlin, Germany), ENEA (Rome, Italy), the IMDEA Network Institute (Madrid, Spain), and the University of Haifa (Israel). He is the Technical Manager of the MarTERA RoboVaaS project, and collaborates with the European Defence Agency project SALSA. His current work involves software development for the DESERT Underwater framework as well as the design of novel communication stacks and architectures, with special attention to cross-layer and multi-technology designs. His research interests revolve mainly around the design, analysis, implementation, and field evaluation of multimodal underwater networks. Since 2017, he collaborates with Wireless and More srl, a spin-off company of the University of Padova, which he joined as a part-time employee in October 2019. In January 2022 he became a Research Fellow and a faculty member of the Information Engineering Department at the University of Padova.

Ivor Nissen (MCN founder and advisory council member, Ivor.Nissen@t-online.de), point of contact for underwater communications, obtained a PhD in the field of numerical mathematics and optimization at the University of Kiel in 1997. His research interests changed from numerical modelling to signal processing and digital communications for acoustics in shallow water during two years of Post doc research on a Fraunhofer grant. Then he started a career in underwater acoustics at FWG in Kiel. He serves as an underwater communication expert for the German Navy since 1999, is the leader of the underwater communication team at WTD71, holds lectures at the University of Kiel and Gdynia in this field, and is involved in the analysis of international underwater activities. In the EDA RACUN and SALSA project he was the GER technical coordinator.

His main interest is the underwater information management. He is working for DIN, Berlin, in the ISO/IEC SC41 panel Internet of Things (IoT) for underwater issues and standards like JANUS (ANEP 87). His long-term goal is the development of information supply concepts for a robust fault-tolerant co-operation, coordination and coalition in the water column.

Michele Zorzi [F'07] received his Laurea and PhD degrees in electrical engineering from the University of Padova, Italy, in 1990 and 1994, respectively. During the academic year 1992-1993 he was on leave at the University of California at San Diego (UCSD). In 1993 he joined the faculty of the Dipartimento di Elettronica e Informazione, Politecnico di Milano, Italy. After spending three years with the Center for Wireless Communications at UCSD, in 1998 he joined the School of Engineering of the University of Ferrara, Italy, where he became a professor in 2000. Since November 2003 he has been on the faculty of the Information Engineering Department at the University of Padova. His present research interests include performance evaluation in mobile communications systems, WSN and Internet of Things, cognitive communications and networking, 5G mmWave cellular systems, vehicular networks, and underwater communications and networks.

Dr. Zorzi received several awards from the IEEE Communications Society, including the Best Tutorial Paper Award in 2008 and 2019, the Education Award in 2016, the Stephen O. Rice Best Paper Award in 2018, and the Joseph LoCicero Award for Exemplary Service to Publications in 2020. He was the Editor-in-Chief of the IEEE Wireless Communications magazine from 2003 to 2005, the IEEE Transactions on Communications from 2008 to 2011, and the IEEE Transactions on Cognitive Communications and Networking from 2014 to 2018. He has served the IEEE Communications Society as a Member-at-Large of the Board of Governors from 2009 to 2011 and from 2021 to 2023, as the Director of Education from 2014 to 2015, and as the Director of Journals from 2020 to 2021.