Trustworthiness in the GUWMANET+ Protocol for Underwater Acoustic Mobile Ad-Hoc Networks

Alberto Signori[‡], Emanuele Coccolo[‡], Filippo Campagnaro[‡],
Ivor Nissen[*], Michele Zorzi[‡]
[‡] University of Padova, Department of Information Engineering (DEI)
Italy
{signoria,coccoloe,campagn1,zorzi}@dei.unipd.it
[*] Bundeswehr Technical Center for Ships and Naval Weapons, Maritime Technology and Research, Eckernförde
Germany
ivornissen@bundeswehr.org

ABSTRACT

Security in underwater networks is a crucial aspect to maintain correct network operations, but has only partially been investigated so far. Most of the applications of an underwater network are related to military or public safety scenarios, which should exhibit a high robustness to attacks and failures in order to avoid disastrous consequences even with simple Denial-of-Service attacks. The defense mechanisms and countermeasures are usually tailored to specific types of attacks. Albeit this procedure allows to obtain very effective defense mechanisms, it requires the development of different countermeasures for each possible attack. Another possible solution is to use reputation systems to identify the attackers; hence, in this paper we design a trust model able to tackle a wide range of attacks. The idea of the trust model is to observe the behavior of the nodes overhearing the neighbors' transmissions and use this information in a subjective logic framework to assign a trust metric to each of the neighbors. In addition, in order to take into account the unique characteristics of the underwater acoustic channel, which alternates periods of high packet loss to periods with low errors, we include the channel state in the trust model to avoid to erroneously mark as not trustworthy nodes that correctly forwarded the packets, but could not be overheard due to an unreliable channel.

KEYWORDS

Underwater acoustic networks; trustworthiness; security in underwater networks.

ACM Reference Format:
Alberto Signori[‡], Emanuele Coccolo[‡], Filippo Campagnaro[‡],, Ivor Nissen[*], Michele Zorzi[‡]. 2021. Trustworthiness in the GUWMANET+ Protocol for Underwater Acoustic Mobile Ad-Hoc Networks. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3491315.3491316

1 INTRODUCTION AND RELATED WORKS

In the last twenty years Underwater Acoustic Mobile Ad-Hoc Networks (UMANETs) have gained more and more interest by both industry and the research community, as they enable several applications [12], such as coastal monitoring, tsunami prevention, oil pipeline inspection and diver coordination during complex rescue or maintenance missions. The underwater acoustic channel is characterized by a long propagation delay, a narrow bandwidth and a high packet error rate due to multipath, signal attenuation and environmental acoustic noise [21]. In this scenario, the application of countermeasures designed for attacks in terrestrial wireless networks is not possible, due to scarce resources and the lack of a public key infrastructure and its certification authority. Given the broadcast nature of Underwater acoustic Sensor Networks (USNs), they are prone to Denial-of-Service (DoS) attacks, where the malicious node can easily affect the network performance even without being able to generate packets according to the network protocol [13]. An underwater jammer, for instance, can reduce the Packet Delivery Ratio (PDR) of the surrounding nodes [20], while a replay attack can be used to fill the nodes queues and saturate the network [6]. Generic countermeasures can be applied against these attacks: for instance, a game theory approach can be used against a jammer in order to maximize the PDR [20], while a freshness index based on the hash of the packet and

WUWNet'21, November 22–24, 2021, Shenzhen, Guangdong, China
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-9562-5/21/11…$15.00
https://doi.org/10.1145/3491315.3491316

its generation time can provide a valid defence against all classes of replay attacks [6]. Conversely, defending against more sophisticated attacks is much harder and often requires specific solutions that depend on the protocol stack. For instance, if the malicious node is aware of the protocol stack and exploits weaknesses of the protocols by transmitting selected signaling packets, it can cause a DoS without being detected. Sinkhole [11] and wormhole attacks [26, 27], for instance, can cause severe performance loss to the network just transmitting few packets and often requires distributed countermeasures based on node cooperation [26]. In order to protect the network, a first solution is to design each of the protocols keeping in mind that it should be resistant to all possible attacks [18]. This solution is not always applicable, because not all possible attacks can be easily foreseen, and its main drawback is that it requires to apply specific countermeasures for each network protocol. This calls for a more general solution easily applicable to different protocols and that allows the security system to scale up when different attacks are applied.

In this paper we analyze the effect of a reputation-based security mechanism in a UMANET where each of the nodes in the network gains trust when it behaves correctly, and is no longer trusted when it has a bad reputation due to its wrong behavior. The considered network makes use of the Gossiping in Underwater Acoustic Mobile Ad-hoc Networks plus (GUWMANET+) network protocol, which realizes medium access and routing functionalities specifically tailored to UMANET. The paper focuses on the trust assessment of the nodes in the network rather than on the action performed by the network when a malicious node is detected, being the latter a separate task that can be performed in different ways, such as ignoring packets incoming from the intruder and/or localizing the attacker for a physical exclusion, and is left for future work.

The concept of trust can be applied to different fields, from economics to sociology, and to communication networks as well [7]. In terrestrial networks the trustworthiness of a node can be regulated through certifications released by appointed authorities. However, this solution is mostly suited for networks with an infrastructure (wired or wireless) [10] and not for terrestrial ad hoc and underwater sensor networks, where the lack of an infrastructure does not enable the use of certification authorities. For these types of networks, a lighter solution, based on reputation built on the observation of the packets transmitted by the neighboring nodes, is more appropriate. However, most of the literature is focused on the analysis of terrestrial networks [3, 16, 19, 25] and only partially on underwater networks [2, 8]. In addition, in underwater networks a hostile communication environment and the limited capacity of the nodes make the trust assessment of a node, based on reputation, more challenging. For instance, if some packets are not received it is very hard to understand whether the packet loss is caused by bad channel conditions or by the presence of some anomalies in the network, such as the presence of a malicious node.

Most of the reputation systems used in wireless networks are based on the so-called watchdog mechanism [17, 19], i.e., each node overhears and analyzes the packets transmitted by its neighbors. The overhearing of a packet sent according to the networking protocol rules causes the increase of the reputation of the node that transmitted the packet; conversely, if the overheard packet is not transmitted following the protocol stack or if an expected packet is not transmitted at all, the reputation of the node involved in the transmission decreases. The main problem of this system, when applied to underwater networks, is the variability of the acoustic channel that can result in long periods of bad channel conditions making communication and, consequently, the overhearing of the packets, difficult. Therefore, the lack of overheard packets by a node may lead to a wrong understanding about the reputation of the node.

In our model, we propose a trust mechanism based on subjective logic [14] to consider the observed behavior of a neighbor in good and bad channel conditions differently. Subjective logic and channel conditions are also considered in the trustworthiness model presented in [15], where the error probability of the channel is assumed to be constant. We extended this model addressing the nature of the acoustic channel, where the error probability often changes during the day, hence modeling the channel with a Hidden Markov Model (HMM) on top of a non-observable 2-state Markov Chain (MC) [22].

The rest of the paper is organized as follows: Section 2 describes the trust model implementation into the GUWMANET+ protocol. Section 3 presents the simulated scenario and Section 4 shows the effectiveness of the trust mechanism in discovering misbehaving nodes. Finally, Section 5 draws some conclusions.

2 TRUSTWORTHINESS IN THE GUWMANET+ ROUTING PROTOCOL

In this section, after briefly describing the GUWMANET+ protocol and the Generic Underwater Application Language (GUWAL) application (Section 2.1), we present details of the trust model used to identify potential malicious nodes (Section 2.2).

2.1 GUWMANET protocols

The GUWMANET+ network protocol is designed to transmit packets generated according to the GUWAL language [9], in order to minimize the packet transmission overhead and therefore reduce packet length and packet error probability.

GUWAL defines an operational address of 6 bits composed as follows. The first 2 bits are used to identify the group to which the node belongs, while the last 4 bits are used to identify the specific node within the group. This address is not a unique identifier, i.e., the same operational address can be used by more than one node at the same time in the same network. The GUWMANET+ protocol is in charge of routing and medium access functionalities. While the former is based on flooding, the latter is a random access protocol. GUWMANET+ defines a network address, called nickname, that is a 5 bits address unique in the 2-hop neighborhood.

The GUWAL application layer defines 4 packet types that can be sent: strings, command, data request and data. To counteract the high error rate that can characterize the acoustic medium, the GUWMANET+ protocol transmits each packet 2 or 3 times, unless a node overhears its own packet transmitted by one of the neighbors. The number of per-packet transmissions depends on the priority of the packets. Two priority levels are defined: a low level, which implies one additional repetition of the periodical packet, and a high priority level for which two additional repetitions are required for the event packet.

According to the GUWMANET+ protocol, each node is required to participate in the routing process by forwarding each packet not intended for itself, and repeating it the proper number of times.

2.2 Trust model

The main goal of the trust model presented in this paper is to discover non-cooperative nodes inside the network, marking them as not trustworthy. In general, the trust model aims to detect different types of non-cooperative nodes, as long as the definitions of *CORRECT BEHAVIOR* and *MISBEHAVIOR* is given. We highlight that in this work we defined a misbehavior as the observation by a node of a behavior of a neighbor not compliant with the protocol rules, independently of whether it happens because of an intentional malicious action or because of the impossibility of overhearing the packet due to bad channel conditions. The trust model only counts the number of correct behaviors and misbehaviors observed by a node for one of its neighbors, and distinguishes those observed with a good channel state from those observed with a bad channel state, and uses them in a subjective logic framework. The subjective logic aims to compute an *opinion* about a neighbor. The opinion is defined as the tuple $\mathbf{o} = \{b, d, u\}$, representing belief, disbelief and uncertainty, where $b, d, u \in [0, 1]$ and $b + d + u = 1$. These values are then used to obtain a binary statement for the trustworthiness. In this specific scenario with the GUWMANET+ protocol, a node is behaving correctly if it participates to the forwarding process, while a misbehaving node does not forward the packets (or at least the forwarding of the packet has not been overheard by the other nodes) or forwards them too many times trying to overload the network. The general trust model is described a follows.

Once a node transmits a packet, generated by itself or received from a neighbor, it expects all the neighbors, except for the destination, to forward it the proper number of times defined by the packet priority. Through the watchdog mechanism, the node counts the number of packet repetitions overheard from each neighbor, and counts a correct behavior of the node if the overheard number of repetitions is within the allowed range, or a misbehavior if the node overhears either no repetitions or more repetitions than the maximum number allowed for that packet. In addition, the model distinguishes between correct behaviors in good channel c_g and bad channel c_b, and between misbehaviors in good channel m_g and bad channel m_b. This distinction helps in avoiding to mark as untrustworthy a node whose repetitions have not been overheard only because of bad channel and not because of an intentional misbehavior.

After the transmission of a packet, the node updates the counters for each neighbor. These values are then used to compute the opinion based on subjective logic, i.e., belief (b), disbelief (d) and uncertainty (u). Subjective logic deals with uncertainty which in our case represents the possibility that a misbehavior is caused by bad channel and not by a non-cooperative node. Belief, disbelief and uncertainty can be computed as:

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

where $w_{cg}, w_{cb}, w_{mg}, w_{mg} \in [0, 1]$ are the weights given to each counter, while $c = c_g + c_b$ and $m = m_g + m_b$ are the overall number of observed correct behaviors and misbehaviors, respectively. For example, a misbehavior under good channel conditions will have a higher weight than a misbehavior in bad channel, because it can be a hint of intentional misbehavior by an attacker, since it is less likely not to overhear a packet when the channel state is considered good. A neighbor is considered trustworthy if $T = 1$, where

$$\begin{aligned} T &= 1 \qquad \text{if } b + \beta u > d + (1 - \beta)u, \\ T &= 0 \qquad \text{otherwise,} \end{aligned} \tag{2}$$

and $\beta \in [0, 1]$ defines how the uncertainty is balanced between belief and disbelief. For example, $\beta = 1$ considers the uncertainty as belief to avoid false detections (i.e., good nodes marked as attackers), while $\beta = 0$ helps in avoiding misdetections (i.e., attackers marked as good nodes).

In GUWMANET+ the weights used to compute belief, disbelief and uncertainty can be set to either fixed or variable values. In the latter, the final weight is computed as a convex combination of the initial value and the variable part obtained from the observed behavior. Specifically, for the weights related to a misbehavior, the final weights are computed as

$$\begin{aligned} w_{mb} &= \alpha \tilde{w}_{mb} + (1-\alpha) w_{var} \\ w_{mg} &= \alpha \tilde{w}_{mg} + (1-\alpha) w_{var}, \end{aligned} \tag{3}$$

where $\tilde{w}_{mb}$ and $\tilde{w}_{mg}$ are the initial values, while w_{var} is the variable part. Similarly, for the weights related to a correct behavior the final weights are computed as:

$$\begin{aligned} w_{cb} &= \alpha \tilde{w}_{cb} + (1-\alpha)(1-w_{var}) \\ w_{cg} &= \alpha \tilde{w}_{cg} + (1-\alpha)(1-w_{var}), \end{aligned} \tag{4}$$

where $\tilde{w}_{cb}$ and $\tilde{w}_{cg}$ are the initial values. The variable part is computed as

$$\begin{aligned} w_{var} =& \frac{2p_{m,g}}{p_{m,g}+p_{m,b}} && \text{if } p_{m,g} < p_{m,b} \\ w_{var} =& 1 && \text{otherwise.} \end{aligned} \tag{5}$$

where $p_{m,g}$ is the ratio of misbehaviors in good channel and $p_{m,b}$ is the ratio of misbehaviors in bad channel. The idea is that the number of misbehaviors for a good node should be in principle higher in bad channel than in good channel. A different behavior could be the sign of a malicious node.

3 SIMULATION SCENARIO AND SYSTEM SETTINGS

In our scenario we assess the trustworthiness of nodes by looking at their cooperation in the forwarding process. We analyzed the trust model using the DESERT Simulator [4] integrated with the GUWMANET+ protocol [5] updated with the new trust module to implement the model described in Section 2.

The scenario, presented in Figure 1, is composed of 10 nodes: the sink, depicted with a blue circle and placed in the center of the network, eight legitimate nodes, identified with green squares, and an attacker, depicted with a red cross. Positions of both the nodes and the attacker are drawn at random for each considered network deployment, while the sink is always placed in the center of the network. The maximum transmission range is approximately 3.5 km, with fluctuations up to ±200 m according to the channel state: in the considered topology, each node is at most two hops from the sink. The constraints used to draw the positions of the nodes ensure that the same network topology is kept in all considered deployments. The constraints are described as follows:

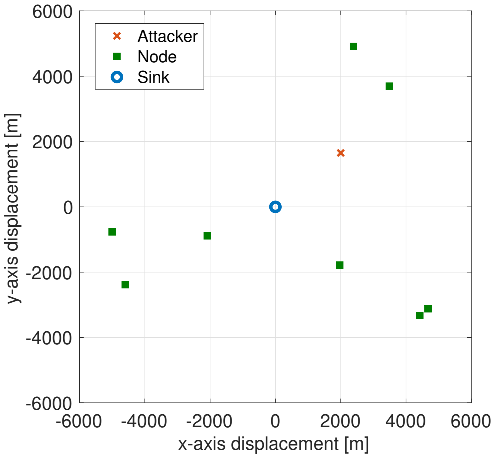


Figure 1: A realization of the network deployment used to test the trust model with normal nodes (green squares), attacker (red cross) and sink (blue circle).

- the maximum distance between a node and the sink is less than 6 km;
- 2 legitimate nodes and the attacker are always at 1-hop distance from the sink: each of these three nodes is always in range with 2 external nodes and the sink;
- the remaining 6 legitimate nodes are at 2-hop distance from the sink.

Every 800 s, on average, the sink broadcasts a data request to all the nodes in the network. Consequently, the receiving nodes reply to the sink with a data packet. In addition, every node transmits to the sink a data packet every 400 s. Each packet is transmitted twice according to the GUWMANET+ protocol rule. The only exception is represented by the attacker (red node) which decides the number of packets to transmit based on the misbehavior probability p_m. With probability p_m the attacker transmits the packets 4 times, while with probability $1-p_m$ it acts according to the protocol rules transmitting the packets twice. Each node transmits packets of 16 Bytes, the default packet size of GUWAL, and is equipped with a modem having a bitrate of 4800 bit/s with a central frequency of 26 kHz and a bandwidth of 16 kHz, mimicking the performance of the EvoLogics S2C 18/34 modem [1]. The transmission power is set to 170 dB re μPa.

The channel model used in our simulations is based on Urick's model [23]. To simulate different channel states during the simulations, we change the noise level every T = 180 s according to a 2-state MC with transition probabilities p_{gg} = 0.87 and p_{bb} = 0.72, where p_{gg} is the probability of remaining in the state with low noise, while p_{bb} is the probability of remaining in the state with a high noise level. The actual state is computed based on the Signal to Noise Ratio (SNR) of the received packets.

The trustworthiness of a node is computed using Equation (2) with $\beta = 0.7$ when both good and bad channel conditions have been registered in the past. If only good channel has been experienced, the value of β is set to 0. Indeed, in good channel state the uncertainty due to the channel should be reduced and therefore counted as disbelief.

4 SIMULATION RESULTS

In this section we evaluate the trust model presented in this paper with the DESERT Underwater network simulator. The results have been obtained by averaging over 20 different realizations of the network deployment, where the nodes positions are drawn at random as described in Section 3, and on 50 runs for each simulated deployment: the corresponding confidence intervals are very small and could not be visualized in the plots, hence they are not depicted in the figures. We assess the performance of the trust model computing the F-score (F) [24]. The F-score combines precision (P) and recall (R): the former describes the number of nodes marked as attackers that are actually malicious nodes, while the latter describes how many actual attackers have been correctly discovered. Specifically,

$$P = \frac{t_p}{t_p + f_p}, \qquad R = \frac{t_p}{t_p + f_n} \tag{6}$$

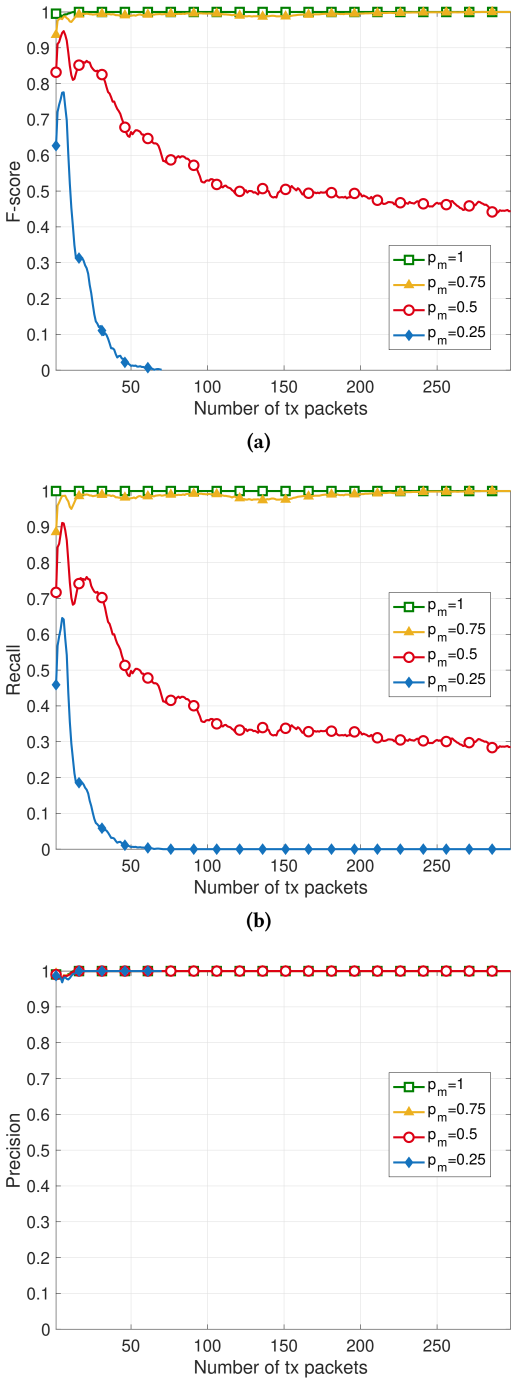
where t_p are the true positives (attackers marked as non-trustworthy), f_p are the false positives (normal nodes marked as non- trustworthy), and f_n are the false negatives (attackers marked as trustworthy). The F-score is then computed as

$$F = \frac{2PR}{P + R}. \tag{7}$$

In addition to the F-score, we plot also the recall and precision values, in order to understand whether a low F-score value is mainly due to attackers not discovered properly or to normal nodes erroneously marked as malicious.

We analyzed the performance of the model, varying the attack strength, i.e., varying the probability that a node behaves maliciously (p_m) as described in Section 3.

Figure 2 shows the results when fixed weights are used to compute belief, disbelief and uncertainty. Considering a misbehavior probability $p_m = 1$ or $p_m = 0.75$ the malicious nodes is easily identified, as confirmed by the F-score value close to 1 (Figure 2a). In addition, precision and recall values are also close to 1, meaning that all the attackers are correctly identified and no normal nodes are erroneously marked as attackers. When decreasing the misbehavior probability to 0.5, i.e., the attacker behaves correctly half of the time, the F-score drops to 0.5 due to a decrease in the recall value, while the precision always remains close to 1. In this case



(a)

(b)

(c)

Figure 2: F-score (a), recall (b) and precision (c) values with fixed weights, for different misbehavior probabilities.

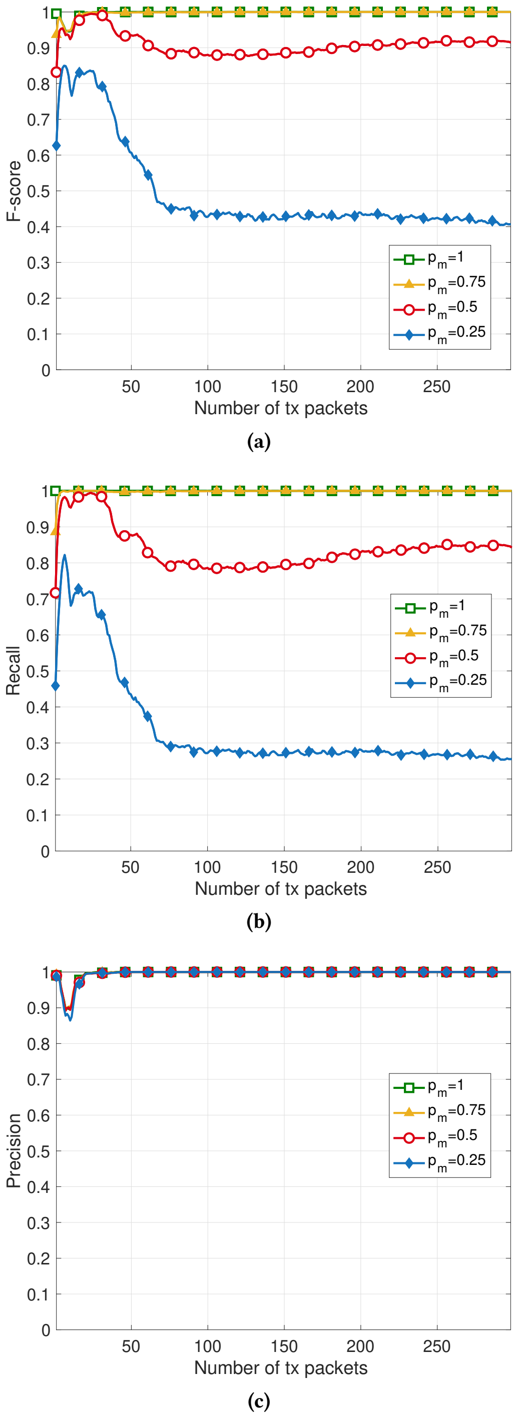
the good behaviors of the attacker cause an increment in the belief value making it more difficult to detect the attacker. Further decreasing the misbehavior probability to 0.25, the F-score drops, and most of the time no attackers are found in the simulations.

The performance improves using variable weights to compute belief, disbelief and uncertainty. Similarly as before, Figure 3 shows the F-score, the recall and the precision in the scenario with variable weights. When the misbehavior probability p_m is equal to 1 or 0.75, the attacker is always identified correctly, obtaining an F-score equal to 1. In addition, the precision value is 1 thus good nodes are never identified erroneously as attackers. Differently from the scenario with fixed weights, when the attack strength is lower, i.e., lower misbehavior probability, the attacker can still be correctly identified. With a misbehavior probability equal to 0.5 the F-score is close to 0.9. This is due to the improved capacity in identifying the attacker properly, as suggested by the recall values equal to 0.85 (Figure 3b). The precision remains high also in this case, therefore good nodes are rarely erroneously marked as malicious. The improvement is due to the use of variable weights, which allows to weigh less the correct behavior for the attackers, and to be able to identify them even in the cases where the attacker behaves properly more often because of the lower misbehavior probability. In the last case, with $p_m = 0.25$, the F-score drops to 0.4. In this case the main problem is to correctly detect the attacker since most of the time it is acting according to the protocol rules. This is confirmed by the recall value equal to 0.3. Also in this case, the precision is 1. However, in this particular situation, the attacker is also causing a lower overload effect to the network, making the misdetection less dangerous for the network.

In addition to the improvement of the performance on the attacker identification, in our scenario the use of variable weights helps the system identify sooner the attacker than in the case with fixed weights. For example if $p_m = 0.5$ the system converges after 50 analyzed packets when the variable weights are used, while it takes more than 100 packets with fixed weights (for higher p_m values both systems are fast in the identification of the attackers).

5 CONCLUSION AND FUTURE WORK

We presented a trust module implemented in the GUWMANET+ protocol and analyzed using the DESERT simulator. The trust module computes the trustworthiness of a node based on a subjective logic framework, considering the channel quality while computing the node's trust. This allowed us to take into consideration the uncertainty due to possible misbehavior caused by poor underwater acoustic channel conditions and not by malicious nodes. The trust module is designed to be as general as possible, computing trust based on the observed correct behavior and misbehavior as



(a)

(b)

(c)

Figure 3: F-score (a), recall (b) and precision (c) values for the scenario with variable weights, for different misbehavior probabilities.

defined by the employed protocol. We analyzed the trust of a node by assessing its cooperation in the forwarding process as defined by GUWMANET+ in the presented scenarios. Specifically, we considered a malicious node inside a network, whose goal was to overload the network transmitting each packet more than what is allowed by the GUWMANET+ protocol.

Using variable weights to compute the trust of a node, the trust module is able to detect most of the time all attackers with a misbehavior probability higher than or equal to 0.5. For lower values, there is a drop in performance of the trust mechanism caused by the fact that the attacker is actually behaving properly most of the time and therefore also causes less damage to the network.

ACKNOWLEDGMENTS

This work was mostly funded by the Bundeswehr Technical Center for Ships and Naval Weapons, Maritime Technology and Research (WTD 71), Eckernförde, Germany.

REFERENCES

[1] 2021. EvoLogics S2C Acoustic Modems. https://evologics.de/acoustic-modems. (2021). Last time accessed: Jul. 2021.

[2] M. M. Arifeen, A. A. Islam, M. M. Rahman, K. A. Taher, M. M. Islam, and M. S. Kaiser. 2019. ANFIS based Trust Management Model to Enhance Location Privacy in Underwater Wireless Sensor Networks. In *International Conference on Electrical, Computer and Communication Engineering (ECCE)*. https://doi.org/10.1109/ECACE.2019.8679165

[3] S. Buchegger and J. L. Boudec. 2004. A Robust Reputation System for P2P and Mobile Ad-hoc Networks. In *Second Workshop on Economics of P2P Systems, Boston.*

[4] Filippo Campagnaro, Roberto Francescon, Federico Favaro, Federico Guerra, Roee Diamant, Paolo Casari, and Michele Zorzi. 2016. The DESERT Underwater Framework v2: Improved Capabilities and Extension Tools. In *Proc. UComms*. Lerici, Italy.

[5] Filippo Campagnaro, Alberto Signori, Roald Otnes, Michael Goetz, Dimitri Sotnik, Arwid Komulainen, Ivor Nissen, Federico Favaro, Federico Guerra, and Michele Zorzi. 2021. Simulation Framework for Smart Adaptive Long-and Short-range Acoustic Networks. In *Proc. MTS/IEEE OCEANS*. San Diego, USA.

[6] Filippo Campagnaro, Davide Tronchin, Alberto Signori, Roberto Petroccia, Konstantinos Pelekanakis, Pietro Paglierani, João Alves, and Michele Zorzi. 2020. Replay-Attack Countermeasures for Underwater Acoustic Networks. In *Proc. MTS/IEEE OCEANS*. Virtual, Global.

[7] J. Cho, A. Swami, and I. Chen. 2011. A Survey on Trust Management for Mobile Ad Hoc Networks. *IEEE Communications Surveys and Tutorials* 13, 4 (Oct. 2011), 562–583.

[8] J. Du, G. Han, C. Lin, and M. Martinez-Garcia. [n. d.]. ITrust: An Anomaly-resilient Trust Model Based on Isolation Forest for Underwater Acoustic Sensor Networks. *IEEE Transactions on Mobile Computing (Early Access)* ([n. d.]). https://doi.org/10.1109/TMC.2020.3028369

[9] Michael Goetz and Ivor Nissen. 2012. GUWMANET - Multicast Routing in Underwater Acoustic Networks. In *Proc. MCC*. Warsaw, Poland.

[10] Minaxi Gupta, Paul Judge, and Mostafa Ammar. 2003. A reputation system for peer-to-peer networks. In *Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video*. 144–152.

[11] E. C. H. Ngai, J. Liu, and M. R. Lyu. 2006. On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. In *IEEE International Conference on Communications*, Vol. 8. 3383–3389.

[12] John Heidemann, Milica Stojanovic, and Michele Zorzi. 2012. Underwater sensor networks: applications, advances and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 370, 1958 (Jan. 2012), 158–175.

[13] Shengming Jiang. 2019. On Securing Underwater Acoustic Networks: A Survey. *IEEE Communications Surveys and Tutorials* 21, 1 (Jan. 2019), 729–752.

[14] Audun Jøsang. 1997. Artificial reasoning with subjective logic. In *Proc. of the second Australian workshop on commonsense reasoning*, Vol. 48. 34.

[15] Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. 2019. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal* 6, 6 (Dec. 2019), 10700–10714.

[16] Xiaoqi Li, Michael R Lyu, and Jiangchuan Liu. 2004. A trust model based routing protocol for secure ad hoc networks. In *IEEE Aerospace Conference Proceedings (IEEE Cat. No. 04TH8720)*, Vol. 2. 1286–1295.

[17] Sergio Marti, Thomas J Giuli, Kevin Lai, and Mary Baker. 2000. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*. 255–265.

[18] Annie Mathew and J Sebastian Terence. 2017. A survey on various detection techniques of sinkhole attacks in WSN. In *International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 1115–1119.

[19] F. Oliviero and S. P. Romano. 2008. A Reputation-Based Metric for Secure Routing in Wireless Mesh Networks. In *IEEE GLOBECOM 2008 - IEEE Global Telecommunications Conference*. https://doi.org/10.1109/GLOCOM.2008.ECP.374

[20] Alberto Signori, Federico Chiariotti, Filippo Campagnaro, and Michele Zorzi. 2020. A Game-Theoretic and Experimental Analysis of Energy-Depleting Underwater Jamming Attacks. *IEEE Internet of Things Journal* 7, 10 (Oct. 2020), 9793–9804.

[21] M. Stojanovic. 2007. On the Relationship Between Capacity and Distance in an Underwater Acoustic Communication Channel. *ACM SIGMOBILE Mobile Computing and Communications Review* 11, 4 (Oct. 2007), 34–43. https://doi.org/10.1145/1347364.1347373

[22] B. Tomasi, P. Casari, L. Finesso, G. Zappa, K. McCoy, and M. Zorzi. 2010. On modeling JANUS packet errors over a shallow water acoustic channel using Markov and hidden Markov models. In *MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*. 2406–2411. https://doi.org/10.1109/MILCOM.2010.5680327

[23] Robert J. Urick. 1983. *Principles of Underwater Sound* (3rd ed.). McGraw-Hill.

[24] C Van Rijsbergan. 1979. *Information retrieval* (second ed.). Buttersmiths.

[25] B. Wang, S. Soltani, J.K. Shapiro, and P.-N. Tan. 2005. Local detection of selfish routing behavior in ad hoc networks. In *8th International Symposium on Parallel Architectures,Algorithms and Networks (ISPAN'05)*.

[26] W. Wang, J. Kong, B. Bhargava, and M. Gerla. 2008. Visualisation of Wormholes in Underwater Sensor Networks: A Distributed Approach. *International Journal of Security and Networks* 3, 1 (Jan. 2008), 10–23.

[27] R. Zhang and Y. Zhang. 2010. Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks. In *Proceedings of 29th IEEE International Conference on Computer Communications (INFOCOM'10)*. San Diego, CA, USA, 1–9.