Topology-based Secret Key Generation for Underwater Acoustic Networks

Roee Diamant, Paolo Casari, and Stefano Tomasin

***Abstract*—We propose a method to let a source and a destination agree on a key that remains secret to a potential eavesdropper in an underwater acoustic network (UWAN). We generate the key from the propagation delay measured over a set of multihop routes: this harvests the randomness in the UWAN topology and turns the slow sound propagation in the water into an advantage for the key agreement protocol. Our scheme relies on a route discovery handshake. During this process, all intermediate relays accumulate message processing delays, so that both the source and the destination can compute the actual propagation delays along each route, and map this information to a string of bits. Finally, via a secret key agreement from the information-theoretic security framework, we obtain an equal set of bits at the source and destination, which is provably secret to a potential eavesdropper located away from both nodes. Our simulation results show that, even for small UWANs of 4 nodes, we obtain 11 secret bits per explored topology, and that the protocol is insensitive to an average node speed of up to 0.5 m/s.**

***Index Terms*—Underwater security; Underwater acoustic networks; Secret key agreement; Sound speed.**

I. Introduction and Related Work

ADVANCES in underwater acoustic communications and the improving cost of acoustic sensor technology are progressively turning underwater acoustic networks (UWANs) into a feasible tool for undersea operations such as seabed monitoring, contamination control, and search-and-survey operations. These applications require multiple cooperative submarine sensors to communicate with one another. When defence-related or mission-critical communications are involved (e.g., with devices monitoring marine infrastructure such as oil and gas rigs), ensuring secure communications is a fundamental requirement. With the adoption of the JANUS standard [1] for the interoperability of heterogeneous underwater acoustic communication devices, cyber-security challenges will become more apparent and pressing for UWANs.

A requirement of many security solutions based on cryptography is the availability of some secret information, shared by two legitimate parties but unknown to other devices. This information is typically a key used, e.g., for encryption or authentication purposes. The key must be refreshed from time to time, in order to prevent attacks based on the long-term observation of encrypted messages exchanged by legitimate nodes. In this paper, we focus on the generation of a key shared by two legitimate parties, which must remain secret to a potential eavesdropper. This procedure is known as secret key generation, or secret key agreement. We generate the key from a random source, common to both the source and the destination, but only partially observed by the eavesdropper.

In the context of UWANs, the acoustic channel can be used as a source of randomness, exploiting features that can be independently measured by both the source and the destination, but are significantly different for the eavesdropper (named Eve in the following). For UWANs, secret-key agreement has been first considered in [2], where the exploited channel feature is the received signal strength (RSS). In [3], it is suggested to use the signal strength at different frequencies to increase the secret key rate. This idea has been applied to an OFDM system in [4] using Bose-Chaudhuri-Hocquenghem (BCH) codes for information reconciliation; the proposed approach has been tested on a transmission in a lake. This solution has been further investigated in [5], with the introduction of adaptive pilot signals to estimate and compensate for channel dynamics, and in [6] with the use of a turbo code for information reconciliation. Another solution based on a suitable multistage channel sounding protocol is discussed in [7] to deal with channel variations and large underwater acoustic propagation delays. Channel impulse response (CIR) features, such as its norm, a smooth sparseness measure and the root-mean-square (RMS) delay spread are exploited for key generation in [8], and demonstrated through experimental results. The work in [9] investigates multipath-based features for secret key generation, with experimental results collected in a shallow-water experiment off the coast of Portugal.

In our secret key generation procedure, we specifically rely on the sparsity of typical UWAN topologies, induced by the significant acoustic power attenuation under water. Topology sparsity ensures that Eve only hears a fraction of the data transmitted by legitimate nodes. Thus, the network topology can serve as a random source of bits observed by the source and destination, and partially hidden to Eve. Our simulation results show that, even for small networks of four nodes, our key generation scheme can extract 11 secret bits per UWAN topology. These can be accumulated over time as topology changes, in order to obtain longer keys. We also show that our approach is very robust to node mobility, as even for node speeds of up to 1 m/s (hence relative speeds of up to 2 m/s) the source and destination can agree with high probability on 11 secret bits that remain secret to Eve, and the agreement rate is 100% for node speeds of up to 0.5 m/s.

R. Diamant (roee.d@univ.haifa.ac.il) is with the Dept. of Marine Technologies, Univ. of Haifa, Israel. P. Casari (paolo.casari@unitn.it) is with DISI, Univ. of Trento, Italy. S. Tomasin (tomasin@dei.unipd.it) is with the Dept. of Information Engineering, University of Padova, Italy.

This work was supported in part by the Center for Cyber Law & Policy at the University of Haifa in conjunction with the Israel National Cyber Directorate in the Prime Minister's Office, and by MIUR (Italian Minister for Education) under the initiative *Departments of Excellence* (Law 232/2016).

II. System Model

We design our protocol around a generic underwater network deployment, whose topology is assumed to be unknown and to change slowly over time, e.g., as network nodes may drift slowly with the water current. Instead, we make no assumption about the flow of messages in the network: our secret key generation scheme applies equally to a mesh network and to, e.g., a converge-casting network. An eavesdropper (Eve) is located in the network area at an unknown location. The source and destination communicate through a publicly known physical layer scheme such as the JANUS standard [1]: therefore, all network nodes and Eve can detect the bits of any received packet. No secret information is shared in advance of network operations, except for mechanisms to ensure the authenticity of the packet source, and rule out the chance that a transmission comes instead from an impersonating attacker. We also assume that a) the nodes have means to estimate the hardware and software delay introduced by their modem, b) at least the source and destination are synchronized, and c) Eve has sufficient capabilities to also synchronize with them. We finally assume an underlying scheduling mechanism that ensures correct packet reception via automatic repeat queries (ARQ), whose delay can be determined by each receiver.

III. Channel-based Key Agreement for UWANs

Our algorithm utilizes the estimation of the per-route packet time-of-arrival (ToA), as well as a topology discovery method to generate secret keys. The latter is implemented by letting the source and the destination flood signaling packets through the network to record existing routes and measure the delay over each of them. Based on this information, both the source and destination can infer the network topology. Note that we do not require the discovery process to reveal the entire network: in fact, depending on the location of the source and destination, different, possibly partial sets of links may be probed. To prevent Eve's capability to infer additional topology data from node IDs, we let all nodes choose a temporary local ID (changed between uplink to destination and downlink to source) for each network discovery session and for all subsequent communications. In this way, Eve's knowledge about the network topology remains local to the nodes involved in the discovery process.

Fig. 1 shows the block diagram of the proposed algorithm. The process starts anew at each key generation/renewal attempt. First, the source floods a request-to-send (RTS) packet, including the actual ID of the source, the transmission time T_s, and a field δ_i to store the accumulated hardware and software delay over the i-th route. Each receiver of the RTS adds its own temporary local ID to the packet, updates δ_i, and forwards the packet such that no loops occur, i.e., only if the current node does not find its own temporary ID already logged in the packet. After receiving a packet at time T_r, the destination extracts the temporary IDs of nodes forming route i and δ_i. It then computes the *net route delay* as

$$D_i = T_r - T_s - \delta_i \ . \tag{1}$$

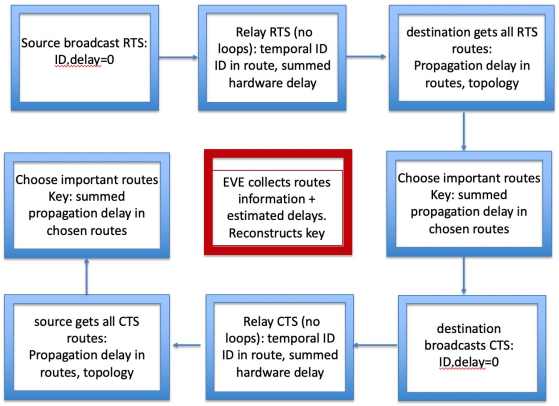

Fig. 1. Block diagram of the proposed algorithm.

We remark that our scheme does not depend on channel characteristics, but only assumes that the propagation delay from source to destination is equal on both ways.

The destination waits to receive additional RTSs, up to a pre-defined, globally known time T_c. It then reconstructs the UWAN topology matrix, and singles out a set $\mathcal{S}$ of $|\mathcal{S}| = N_c$ routes through some function $\mathcal{F}$, where both N_c and $\mathcal{F}$ are public, i.e., known to all nodes including Eve. Each chosen D_i is quantized down to a propagation delay resolution ρ, and transformed into a sequence of N_r bits, where N_r depends on the maximum delay in the UWAN. In turn, the maximum delay depends on the underwater modem's transmission range, the sound speed, and by the (public) maximum accepted number of nodes along a route. The bit sequences obtained from all quantized delay values $\{\hat{D}_i\}$, $i \in \mathcal{S}$ are concatenated in order of increasing RTS arrival time at the destination.

Once this process is finalized, the destination sends a clear-to-send (CTS) message back to the source that, similarly, contains the destination's actual ID, the transmission time, and the used delay quantization resolution ρ. Following the same procedure used by the destination for the RTSs (but with different temporal IDs of the intermediate nodes), the source will extract a sequence of bits slightly after time $2T_c$ from the RTS transmission.

The source and destination process the resulting sequences of N_cN_r bits to derive the actual secret key, which will be composed of $n < N_cN_r$ bits, in general. In particular, following the steps in [10, §4.3], the processing involves a) the *information reconciliation* step by which, through coding techniques, the source and destination remove differences in their sets of N_cN_r bits; and b) the *privacy amplification* step, by which a smaller set of bits that are really secret to Eve is extracted (typically using hash functions). We will assume that the random bit sequence obtained at the source and the destination are identical, thus step a) is not necessary. We assume the presence of a link-level mechanism to correct packet failures, e.g., by means of repeated transmissions or acknowledgments. In this case, the nodes are required to measure the time elapsed between retransmissions and accumulate this as part of the hardware delay field of the packet.

Note that the obtained secret bits can be accumulated over time by waiting for a change of topology and performing a new secret-key agreement protocol: this will provide longer keys. Moreover, the secret bits can be used to partially and progressively renew already existing keys (also initialized in some other ways), thus strengthening security. Another possibility is to use the secret bits obtained with our technique to establish a first secure channel over which traditional cryptography keys are then exchanged: this will provide a further level of security, on a different basis (physical layer parameters, in this case), making attacks harder to succeed.

A. Attack Model

The objective of the attacker Eve is to observe the RTS/CTS exchange used for key agreement, in order to infer the same key derived by the source and destination. For this purpose, Eve intercepts RTSs and CTSs by promiscuously listening to underwater acoustic transmissions in its proximity, and estimates route delays. This exposes to Eve both the route traveled by these packets, and the accumulated processing delay stored therein. Further, we assume that Eve knows all public information, such as the function $\mathcal{F}$, N_c, ρ, N_r, T_c, and the algorithm of Fig. 1. Yet, Eve is located at a random location, and overhears only a subset of the transmissions.

During the RTS forwarding phase, Eve logs all intercepted RTS packets and their reception times, and reconstructs routes by merging RTSs with CTSs. Unless only either the source or destination appear in the ID list of the RTS or CTS, Eve only merges packets with mutual intermediate nodes it is connected to. Consider Fig. 2, where Eve is connected to the destination and to the node of temporary address 2: an RTS with route information S→2 will be merged only with the CTSs reporting the routes D→2, D→4→2, and D→6→4→2. Like the source, Eve computes the delay D_i^{Eve} of each reconstructed route by accumulating the ToA of the intercepted RTSs and CTSs and by subtracting the transmission times and accumulated delays.

The difference between D_i^{Eve} and D_i is due to the propagation time from Eve to the route relays it is connected to. In the above example, this difference would be twice the delay between Eve and node 2. Note that Eve does not know the time when relays transmit, hence it can not discover the range to those relays. Still, Eve can attempt to estimate this mismatch if more information is known, such as the maximum range of the used modem, or the source level used by node 2: in this case, measuring the received level and using a propagation model can bound node 2's distance. Moreover, Eve can localize a relay via methods akin to matched field processing, e.g., [11], if it knows both the bathymetry and the sound speed, and the bathymetry is sufficiently diverse around it. In any event, Eve can only detect locally overheard packets, and may thus fail to gather enough information, if the UWAN topology is sufficiently sparse.

B. Secrecy Performance Evaluation

Let $\boldsymbol{X}(k) = [x_1(k), \ldots, x_M(k)]$, be the sequence of identical bits obtained at the source and destination at round k after the reconciliation process, assumed here to remove all differences among the sequences at the two devices.Let also $\boldsymbol{Y}(k) = [y_1(k), \ldots, y_M(k)]$, be the corresponding sequence obtained by Eve, which represents all the information available to Eve on sequence $\boldsymbol{X}(k)$. From sequence $[\boldsymbol{X}(0), \ldots, \boldsymbol{X}(k)]$ of all rounds up to round k, the source and destination will obtain the *secret key* $\mathcal{K}(k)$. This is the *source model* for secret-key generation [10, §4.3], where the source, the destination, and Eve observe realizations of random, correlated bit sequences. In our particular scenario, the source and the destination observe the same realization $\boldsymbol{X}(k)$, whereas Eve observes the (correlated) sequence $\boldsymbol{Y}(k)$. Secrecy here refers to the fact that the (normalized) mutual information between the key and the sequences obtained by Eve $[\boldsymbol{Y}(0), \ldots, \boldsymbol{Y}(k)]$ goes to zero as k goes to infinity, i.e.,

$$\lim_{k\to\infty} \frac{1}{k}\, \mathbb{I}(\mathcal{K}, [\boldsymbol{Y}(0), \ldots, \boldsymbol{Y}(k)]) = 0, \tag{2}$$

where $\mathbb{I}(\boldsymbol{a}; \boldsymbol{b})$ is the mutual information between the two random sequences $\boldsymbol{a}$ and $\boldsymbol{b}$. If $\mathcal{K}(k)$ includes n bits, and the k rounds took time kT, the rate of the key (in bit/s) is $R = n/(kT)$. The *weak secret-key capacity* is the maximum rate R of the key that remains secret to Eve, i.e., the maximum rate for which (2) still holds.[1] The following theorem provides bounds of the secret-key capacity [10, Theorem 4.1]:

Theorem 1: The weak secret-key capacity C_s of a source model $(\boldsymbol{X}, \boldsymbol{Y})$ satisfies

$$\mathbb{H}(\boldsymbol{X}) - \mathbb{I}(\boldsymbol{X}; \boldsymbol{Y}) \le C_s \le \mathbb{H}(\boldsymbol{X}|\boldsymbol{Y}) \,. \tag{3}$$

Now, by the definition of mutual information, we have

$$\mathbb{I}(\boldsymbol{X}; \boldsymbol{Y}) = \mathbb{H}(\boldsymbol{X}) - \mathbb{H}(\boldsymbol{X}|\boldsymbol{Y}) \,, \tag{4}$$

hence the bounds (3) coincide, yielding the identity

$$C_s = \mathbb{H}(\boldsymbol{X}|\boldsymbol{Y}) \,. \tag{5}$$

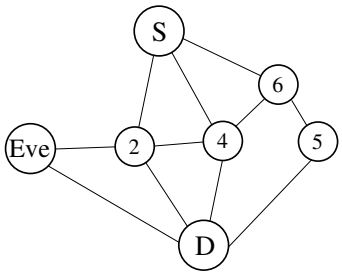

Fig. 2. Sample network topology showing the source S, the destination D, the attacker (Eve) and some relay nodes.

IV. Performance Analysis

Our simulation includes a set of N nodes, deployed uniformly at random over an area of 3 km×3 km. The nodes are separated by artificial blocks of 100 m length, also placed in the area uniformly at random: communications between any two nodes are possible only if their line-of-sight link is

[1] In addition to (2) reliability and weak uniformity constraints must also hold (see [10, Definition 4.3] for details): these are satisfied in our context.

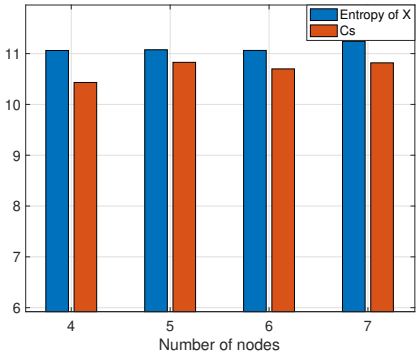

Fig. 3. Entropy of $\boldsymbol{X}$ and $\hat{C}_S$ as a function of the number of nodes.

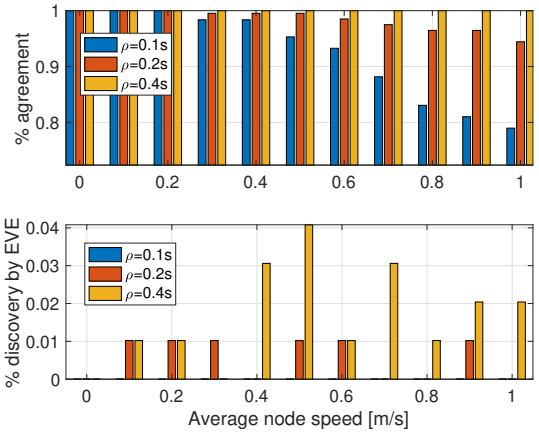

Fig. 4. The fraction of successful key agreements between the source and the destination, and of successful key discoveries by Eve, as a function the node speed v, for different values of the quantization resolution ρ.

unblocked. The result is a sparse network topology. For each simulation run, the source and its destination are randomly selected among the N network nodes. RTSs from the source and CTSs from the destination are propagated through the network by assuming a sound speed of 1500 m/s, and a hardware/software delay randomly distributed between 0 and 1 s for each node. We set the waiting time for the collection of RTSs and CTSs, T_c, to be 15 s. We assume that packet losses are corrected by an automatic repeat query scheme. Similarly, no attenuation model is considered and ToA errors are assumed handled by the PHY. From these simulations we obtain a set of pairs $(\boldsymbol{X}(k), \boldsymbol{Y}(k))$. As our sequences have a length of 16 bits, which is too large to directly estimate the conditional entropy of the bit sequence, $\mathbb{H}(\boldsymbol{X}|\boldsymbol{Y})$, we resort to well-known techniques to estimate the entropy of random variables from their samples [12], [13].

Fig. 3 shows $\hat{C}_s$ as a function of the number of nodes, N. We observe that more than 11 secret bits are obtained, and that this number only slightly increases with N, thereby suggesting that even for small networks with only four nodes the topology is a good feature for secret key generation. Note that these bits can be accumulated over time to obtain longer keys. Fig. 3 also shows the entropy $\mathbb{H}(\boldsymbol{X})$, thus the number of information bits of the string itself. We note that the entropy is very close to $\hat{C}_S$ (although obviously it holds that $\mathbb{H}(\boldsymbol{X}) > \hat{C}_S$): therefore, we conclude that almost all bits of the sequence $\boldsymbol{X}$ are indeed secret to Eve: this is a further confirmation that the topology provides a source of secret randomness. Lastly, note that sequences $\boldsymbol{X}$ are 16-bit long. However, they are partially correlated, and only $\mathbb{H}(\boldsymbol{X}) \approx 11$ bits are truly independent, and thus completely secret to Eve.

While we rely on the network operation to handle the loss of packets across routes and account for any processing and scheduling delays already in the RTS/CTS packets, our security algorithm may be sensitive to physical link delay changes due to node movement. When these changes exceed the quantizer resolution ρ before the CTS reaches the source, the source and destination may experience a mismatch on the secret key $\boldsymbol{X}$. To explore this scenario, we arrange 12 nodes equally spaced along the 3-km sides of a square, three nodes per side, and let the nodes on opposite sides move towards each other at a speed v. The nodes invert their movement as soon as they reach the opposite side of the square, and go back to their initial square. We additionally simulate the drifting of all nodes with sea current by superimposing a random Gauss-Markov mobility process of correlation 0.75 to the above deterministic movement. The results in Fig. 4 show the fraction of successful key agreements between the source and the destination, and of successful key discoveries by Eve. Results are shown as a function of the nodes' nominal speed v and for several values of the key resolution, ρ.

We note that ρ works as a trade-off parameter between the likelihood of the agreement and that of the discovery: by increasing ρ it becomes less likely that a difference in the propagation delay between the RTS phase and the CTS phase negatively impacts key agreement; however, this also reduces the number of secret bits, making it easier for Eve to intercept the generated key. Still, results show that for $\rho = 0.1$ s, where 11 secret bits are obtained per topology and Eve was always unsuccessful, agreement between source and destination is perfect up until a speed $v = 0.5$ m/s. Moreover, agreement still occurs more than 90% of the times for speeds of 0.7 m/s.[2] This result demonstrates the robustness of our algorithm to Eve's locations and to mobility in the UWAN.

V. Conclusions

We presented a scheme that leverages UWAN topology sparsity as a source of secret randomness to enable the generation of a secret key shared by a source and a destination node, which communicate through multiple multihop routes. Simulation results show that even for small networks of four nodes, we obtain 11 secret key bits, and that the results are insensitive to node mobility up to an average speed of 0.5 m/s. Future work will extend the approach to intelligently choose the key-related routes and will demonstrate the method in a real sea environment.

[2]In such cases, the source and the destination can still reach agreement via the information reconciliation process [10].

REFERENCES

[1] J. Potter, J. Alves, D. Green, G. Zappa, I. Nissen, and K. McCoy, "The JANUS underwater communications standard," in *Proc. UComms*, Sestri Levante, Italy, Sep. 2014.

[2] Y. Liu, J. Jing, and J. Yang, "Secure underwater acoustic communication based on a robust key generation scheme," in *Proc. ICSP*, Beijing, China, Oct. 2008.

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

[4] Y. Huang, S. Zhou, Z. Shi, and L. Lai, "Experimental study of secret key generation in underwater acoustic channels," in *48th Asilomar Conference on Signals, Systems and Computers*, Nov 2014, pp. 323–327.

[5] ——, "Channel frequency response-based secret key generation in underwater acoustic systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 5875–5888, Sep. 2016.

[6] T. S. N. Murthy, G. S. Reddyka, and K. Padmaraju, "Adaptive secret key generation in underwater acoustic system," in *Proc. IEEE ICPCSI*, Sep. 2017, pp. 698–702.

[7] Z. Shen, J. Liu, and Q. Han, "A local pilot auxiliary key generation scheme for secure underwater acoustic communication," *Information Sciences*, vol. 473, pp. 1–12, 2019.

[8] K. Pelekanakis, C. M. G. Gussen, R. Petroccia, and J. Alves, "Towards physical layer cryptography for underwater acoustic networking," in *Proc. UACE2019*, Hersonissos, Crete, Greece, 2019.

[9] K. Pelekanakis, C. M. G. Gussen, R. Petroccia, and J. Alves, "Robust channel parameters for crypto key generation in underwater acoustic systems," in *OCEANS 2019 MTS/IEEE SEATTLE*, Oct 2019, pp. 1–7.

[10] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[11] E. Dubrovinskaya, P. Casari, and R. Diamant, "Bathymetry-aided underwater acoustic localization using a single passive receiver," *The Journal the of Acoustic Society of America, S.I. on underwater localization*, vol. 146, no. 6, pp. 4774–4789, Dec. 2019.

[12] L. F. Kozachenko and N. N. Leonenko, "A statistical estimate for the entropy of a random vector," *Problems of Information Transmission*, vol. 23, pp. 9–16, 1987.

[13] H. Singh, N. Misra, V. Hnizdo, A. Fedorowicz, and E. Demchuk, "Nearest neighbor estimates of entropy," *American Journal of Mathematical and Management Sciences*, vol. 23, no. 3-4, pp. 301–321, 2003.