Akustische Authentifizierung in Unterwassernetzwerken durch Hydro-Schlüssel

Ivor Nissen
Wehrtechnische Dienststelle für Schiffe und Marinewaffen, Maritime Technologie und Forschung
Eckernförde, Deutschland, Email: IvorNissen@Bundeswehr.org

Einleitung

Eine erfolgreiche Authentifizierung innerhalb von Identifikationsprozessen ist immer mit dem Erstkontakt zum Fremden verbunden. Eine hierfür notwendige Nennung einer Losung respektive Parole bedarf einer sicheren Verbindung. Die gemeinsame Schlüsselabsprache bei diesem Erstkontakt ist die Achillesferse jeder Kommunikation mit symmetrischer oder asymmetrischer Verschlüsselung. Diese muss über einen sicheren Kanal ggf. im Vorwege erfolgen, das schloss vorerst Ad-hoc-Aktivitäten aus. Ab den 80ern ermöglichte es z.B. die Diffie-Hellman-Merkle-Schlüsselvereinbarung, dass zwei Kommunikationspartner (Alice und Bob) über einen öffentlichen, abhörbaren Kanal einen gemeinsamen geheimen Schlüssel vereinbaren können, den nur diese beiden kennen und ein potenzieller Lauscher (Eve) nicht berechnen kann. Doch bei beschränkten Schlüsselräumen aufgrund beschränkter Transfervolumen im Netzwerk unter Wasser mittels Akustik ist das nicht mehr sicherzustellen, insbesondere wenn der Angreifer bei einem Man-in-the-Middle-Angriff (Mallory) Datenpakete verändern kann respektive die Übertragung stark fehleranfällig ist.

Die Hydroakustik mit ihrer verglichen zu dem Funk multiplen, variablen und langsamen Schallgeschwindigkeiten hilft, Schlüssel weder preiszugeben noch kopieren zu können, beugt Besitzerwechsel oder -verfälschungen vor. Vor über 40 Jahren wurden bereits für die Funk-Kommunikation zwischen Alice und Bob Szenarioparameter wie Laufzeit und Dopplershift als Schlüsselindikatoren in einem deutschen Patent veröffentlicht, die nur den beiden Kommunikationsteilnehmern bekannt sind. Insbesondere für die Unterwasserkommunikation im Netzwerk, bei denen eine fehlerfreie Nachrichtenübertragung nicht garantiert werden kann, bietet sich dieser Weg an, da bekanntlich Doppler-Verschiebung und Laufzeiten um Größenordnungen höher sind als in terrestrischen Anwendungen. In der Hydroakustik sind durch Eve konkrete Empfangszeitpunkte der Teilnehmer und damit diese ,,Hydroschlüssel" nicht schätzbar.

In diesem konzeptionellen Beitrag wird ein Experiment, geplant für diesen Monat, aus den Sichtweisen von Alice, Bob, Eve und Mallory vorgestellt.

Der erste Kontakt

Am 5. April 2063 findet bekanntlich der erste Kontakt mit Vulkan statt, doch wie ist die Prozedur hierfür definiert? Ist es wirklich Vulkan? Es ist zu klären, wie und was übertragen werden muss. Ob nun bei der Kontaktaufnahme der Wikinger in Nordamerika oder der Südeuropäer in Südamerika - sicherlich wurde in beiden Fällen mit den Indianern mittels Zeichensprache der erste Kontakt gestartet, Namen wurden ausgetauscht, der Sprachraum versucht zu erweitern. Auch bei den interstellaren Raumsonden-Plaketten von Pioneer 10 und 11 wurde intensiv diskutiert, was wie mitgeteilt werden soll; bei den Voyager-Sonden 1 und 2 sind sogar akustische Formen als ,,Golden Records" hinzugekommen.

Unter Wasser ist die Situation anders. Beim Disaster der K-141 Kursk im Jahr 2000 fehlte eine digitale Kontaktaufnahme und das führte zu einer Kette von Fehlinterpretationen. Siebzehn Jahre später wurde dann die Erstkontakt-Sprache JANUS durch die NATO als STANAG 4748 standardisiert. JANUS ist mittels Frequency-Hopping die erste digitale, weltweit offene Unterwasserwellenform und derart ausgelegt, dass in einer Standard-Übermittlungsschablone von 64 bit Anwendungsdaten mit ausgetauscht werden können. In 2017 wurde mit Studenten der technischen Fakultät der Universität Kiel eine Erst-Kontakt-Nachricht ,,Hello, I am the new one" definiert [1], die nun in die offizielle Klassenliste als User-Class 12 (First Contact) mit der Anwendungsnachricht 50 als Discovery request eingetragen wurde. Es wird hier das Alice-Bob-Modell zur Beschreibung herangezogen [2].

```
<JANUS UserClass="FirstContact" Application="Hello, I am the new one"> % Discovery request
 <Wakeup type=BIT[1] choice={disable}/>
 <Baseline>
  <Version      type=BIT[4] value2="0011" />
  <MobilityFlag type=BIT[1] choice={0=static} />
  <Schedule     type=BIT[1] choice={0=off} />
  <TxRxFlag     type=BIT[1] choice={1=Tx/Rx} />
  <Forwarding   type=BIT[1] choice={0=No} />
  <ClassUserID  type=BIT[8] value10=12 />
  <Application  type=BIT[6] value10=50 />
   <AppDataBlock type=BIT[34]>
    <ownName        type=BIT[4] value2="1001" /> % last nibble of name / operative address
    <knownNeighbors type=BIT[16] value2="1001111110011111" /> % of my neighborhood 1=known
    <mainPhyConfiguration type=BIT[4] value2="1001" /> %
    <secondPhyConfiguration type=BIT[4] value2="1101" /> %
    <NetConfiguration type=BIT[3] value2="101" /> %
    <WSSUS          type=BIT[2] value2="01" /> % 0 no WSS but 1 US
    <inWaterColumn  type=BIT[1] value2="1" /> % 0 no (Gateway), 1 yes
   </AppDataBlock>
  <CRC type=BIT[8] />
 </Baseline>
 <Cargo></Cargo>
</JANUS>
```

Beschreibung 1: Innerhalb von 34 bit werden eigener (Vor)name, die Nachbarschaftsbeziehungen, Haupt- und Nebensprache sowie das Netzwerkprotokoll, dem das kontaktierende Subjekt unterliegt, ergänzt um Kanalinformationen nach [3] mitgeteilt. Diese XML-Beschreibung wird nicht übertragen, dient nur der Präsentation; es wird nur die Bit-Allocation mit insgesamt 64 bit ausgestrahlt.

Wie kann nun eine Authentisierung der Entität Alice oder Bob bezüglich der behaupteten Echtheit durch den Besitz der Information erfolgen?

Wir gehen davon aus, dass Subjekte, deren Namen bei Gleichheit von anderen genannt werden, sich ebenfalls

melden, um einem akustischen Ein-Hop-,,Enkel-Trick" vorzubeugen *(Voraussetzung E)*.

I: Standardform: Alice sendet nun diese Nachricht No. 50 aus, verrät von sich den Eigennamen, die Nachbarschaftsbeziehungen und Modulations- und Dekodierfähigkeiten. Bob muss nun entscheiden, ob er antwortet. Denn in der dunklen Wassersäule könnten sich auch die Kommunikationsteilnehmer Eve und Mallory verbergen.

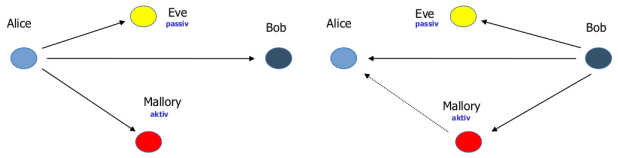

Figure 1: Erweiterung des einfachen Alice-Bob-Modells um die beiden Teilnehmer Eve (passiver Aufklärer) und Mallory als aktiver Angreifer, links bei Aussendungen von Alice und rechts der Antwort durch Bob respektive Mallory.

Neben den ,,First Contact"-Kommunikationsteilnehmer Alice und Bob ist Eve (eavesdropper) ein passiver Lauscher/Aufklärer/Intercepter und Mallory (malicious, als heimtückisch) ein aktiver Angreifer, der bei einem Man-in-the-Middle-Angriff die von Alice und Bob gesendeten Nachrichten abfängt und aktiv zu seinem Vorteil in den Prozess durch falsche Nachrichten inkooperativ eingreift.

Wie kann eine Authentifizierung durchgeführt und Vertrauen bei Bob und dann bei Alice aufgebaut werden? In einem symmetrischen Kryptosystem verwenden die Teilnehmer im Kommunikationsverbund die gleiche Schlüsselgrundlage, um mögliche Chiffrate aus dem Klartext zu berechnen. Gerade bei der Identifikationen (Identification of Friendly Submarine) stehen beim ersten Kontakt keine gesicherten Kanäle und synchronisierten Zeitstempel zur Verfügung. Zudem bedarf es einer aufwändigen Registrierung zum Verwerfen benutzter Schlüssel für bestimmte Teilnehmer, aktuelle Schlüssel zu identifizieren und gespeicherte zuzuordnen. Die gemeinsame Schlüsselgenerierung bei diesem Erstkontakt ist dabei die Achillesferse; auch bei der Schnorr-Identifikation. Diese muss über einen sicheren Kanal ggf. im Vorwege erfolgen, das schloss vorerst Ad hoc-Aktivitäten aus. Ab den 80ern ermöglichte es die Diffie-Hellman-Merkle-Schlüsselvereinbarung, dass die beiden Kommunikationspartner Alice und Bob über einen öffentlichen, abhörbaren Kanal einen gemeinsamen geheimen Schlüssel vereinbaren können, den nur diese beiden kennen und ein potenzieller Lauscher (Eve) nicht berechnen kann. Das Prinzip der Diffie-Hellman-Merkle-Schlüsselvereinbarung ist dabei geben durch:

- Allen Netzwerkteilnehmern sei die Schlüsselgeneratorvorschrift mit den Parametern f (Fundament) und p (Modulus) bekannt.
- Alice hat den privaten nur ihr bekannten Schlüssel a und generiert den public Key $K_A := f^a \mod p$.
- Diesen Wert K_A transferiert Alice im Netzwerk auch zu Bob. Jeder kennt diesen nun.
- Bob hingegen generiert seinen öffentlichen Schlüssel $K_B := f^b \mod p$ aus dem privaten Wert b.
- Beide können sich den gemeinsamen Schlüssel K_C (Common) generieren, denn $K_C = K_B^a \mod p$ (bei Alice) ist gleich $K_C = K_A^b \mod p$ (bei Bob). Es gilt: $K_C = K_A^b \mod p = (f^a \mod p)^b \mod p = f^{ab} \mod p = (f^b \mod p)^a \mod p = K_B^a \mod p = K_C$.

Ein akademisches Beispiel:

```
f  (fundament)         :257
a  (privateKey Alice)  :257
p  (modulus)           :79228162514264337593543950336
K_A (publicKey Alice)  :115528331576001985333257953537
b   (privateKey Bob)   :241
K_B (publicKey Bob)    :42647337879835750842114830593
K_C (commonKey Alice)  :51581421767670882238697435393
K_C (commonKey Bob)    :51581421767670882238697435393
```

Dabei ist der diskrete Logarithmus eine sogenannte ,,Einwege-Funktion", von der man ausgeht, dass die Parameter bei Kenntnis des public keys nicht geschätzt werden können. Jedoch bedarf es nur einer einfachen Brute-Force-Herangehensweise; diese hat in kurzer Zeit die Parameter für die empfangenen 96-Bit-Schlüssel gefunden. Der Suchraum muss entsprechend groß sein ($N >> 128$), nicht wie hier beim akademischen Beispiel.

```
function
    findPrivateParametes(publicKey::BigInt,p::BigInt)
    result      = big(0); fundament   = big(0);
    privateKey  = big(0); _fundament  = big(0);
    _privateKey = big(0);

    for _fundament = 0:N
      for _privateKey = 0:N
        result = mod(
          big(2*_fundament+1)^big(2*_privateKey+1),p)
        if (result == publicKey)
           println([2*_fundament+1, 2*_privateKey+1])
           fundament = 2*_fundament+1
           privateKey = 2*_privateKey+1
        end
      end
    end
    return [fundament, privateKey]
end
```

Skript: Mit der Programmiersprache Julia auf einem handelsüblichen ATOM-Netbook erhält man bei N=128 mittels [@time findPrivateParametes() 0.0069 seconds (74.41 k allocations: 1.330 MiB)] innerhalb von Sekundenbruchteilen die Schlüssel aus der Diffie-Hellman-Merkle-Schlüsselvereinbarung aus dem Netzwerk.

Ein symmetrischer Zugang ist gegeben durch die dieses Jahr veröffentlichte Blockchiffre-Klasse 17 in JANUS:

```
<JANUS UserClass="Venilia">
 <Wakeup type=BIT[1] choice={disable}/>
 <Baseline>
  <Version     type=BIT[4] value2="0011" />
  <MobilityFlag type=BIT[1] choice={1=mobile} />
  <Schedule    type=BIT[1] choice={1=on} />
  <TxRxFlag    type=BIT[1] choice={1=Tx/Rx} />
  <Forwarding  type=BIT[1] choice={0=No} />
  <ClassUserID type=BIT[8] value10=17 />
  <Application type=BIT[6]/> # Time slot
   <AppDataBlock type=BIT[34]>
    <EncryptedField type=BIT[27] />
    <InitialVector  type=BIT[5] />
    <EpochID        type=BIT[2] />
   </AppDataBlock>
  <CRC type=BIT[8] />
 </Baseline>
 <Cargo></Cargo>
</JANUS>
```

Beschreibung 2: Venilia-Nachricht (User-Class 17) mit einer 27-Bit-Blockchiffre dekodierbar mittels eines vorgegebenen Codebooks.

In diesem Bereich befindet sich die Klartext-Nachricht in einer 27-bit-Blockchiffre verborgen, das durch eine zusätzliche 5-bit-CRC-Prüfzahl verborgen ist.

Hydroschlüssel

Die kleinen Übertragungsvolumen der akustischen Unterwasserkommunikation mit Schlüssellängen von 27 bis 96 bit ermöglichen das Ausprobieren der möglichen Kombinationen durch Eve und Mallory. Übertragungsfehler führen zu Irritationen beim Prozess und für den Schlüsselwechsel im Netzwerk muss aufwendig Buch geführt werden, da diese möglichst pro Link nur einmal verwendet werden sollten - eine Herausforderung bei unterschiedlicher Teilnehmerzuordnung im Netzwerk.

Gesucht ist daher eine Schlüsselregel aus wenigstens einem lediglich für die aufzubauende Verbindung (zwischen Alice und Bob) signifikant abzuleitenden Parameter, die unmittelbar aus aufeinander folgenden Meßvorgängen an beiden von der Verbindung beteiligten Stellen getrennt gemessen und bewertet werden. Der Schlüssel soll pro Link individuell aus den hydroakustischen Gegebenheiten des Übertragungskanals abgeleitet werden. Dieser soll im Weiteren als Hydroschlüssel bezeichnet werden. Hydroschlüssel werden damit gemessen, NICHT übertragen. Die zugehörige Prozedur soll als Individual Link Encryption bezeichnet werden.

Da die Schallgeschwindigkeit in der Wassersäule von der Tiefe, der Temperatur und dem Salzgehalt abhängt, geospatial variabel und von den Subjekten meist nur an der eigenen Position bekannt ist, sind die Übertragungszeit und die Doppler-Verschiebung zwei sehr gute Kandidaten für die linkbasierte Messung. Auf diese haben nicht kooperative Teilnehmer wie Eve und Mallory keinen Zugriff, Alice und Bob müssen gemeinsam diese Größen ausmessen - hierfür kooperieren.

Diese Vorgehensweise ist für den Funk nicht neu. In dem Patent [4] hat Helmut Logemann diese Parameter (Laufzeit und Dopplerverschiebung) bereits vor 40 Jahren als Patentanspüche 2 und 4 formuliert; jedoch hat sich dieser Ansatz als Schlüsselregel im Funk nicht durchgesetzt. Im Unterwasserbereich hingegen würde sich bei nichtsynchronisierten Netzwerken folgender Prozess herausbilden:

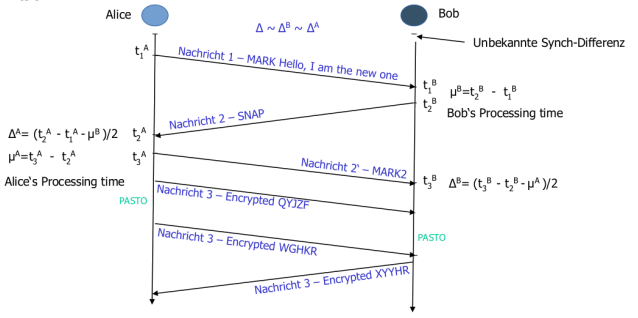

Figure 2: Vorgehensweise zwischen Alice und Bob mit vorgeschalteten First-Contact und Bestimmung der Hydro-Schlüssel. Als Individual Link Encryption-Prozess wäre das jedoch nicht weise, daher wird dieses in zwei getrennte Prozesse geteilt auf Kosten einer weiteren Transmission.

Bob würde bei Vertrauen (und wenn keine weitere Nachricht von einer anderen Alice eingeht) mit einer ,,Let's talk"-Nachricht (Nummer 53) antworten. Neben dem eigenen Namen wird auch die CRC-Prüfzahl der initialen Nachricht von Alice angegeben, damit eine Block-Verbindungskette aufgebaut werden kann. Besonders an dieser Nachricht ist, dass Bob die Bearbeitungszeit mit angibt, also die Zeitspanne in Millisekunden vom Eintreffen der Nachricht bei t_1^B von Alice bis zum Ausstrahlen dieser zur Zeit t_2^B. Diese als Mark-Snap-INRES-Interaktion (INRES - Initiator - Responder) bezeichnete Vorgehensweise fuktioniert in unsynchronisierten Netzwerken, in denen jedes Subjekt nur seine eigene unabgestimmte Zeitmessung benötigt.

```
<JANUS UserClass="FirstContact" Application="Hello, I am not compatible, lets talk!"> % INRES
 <Wakeup type=BIT[1] choice={disable}/>
 <Baseline>
   <Version     type=BIT[4] value2="0011" />
   <MobilityFlag type=BIT[1] choice={0=stati1=mobile} />
   <Schedule    type=BIT[1] choice={0=off} />
   <TxRxFlag    type=BIT[1] choice={1=Tx/Rx} />
   <Forwarding  type=BIT[1] choice={0=No} />
   <ClassUserID type=BIT[8] value10=12 />
   <Application type=BIT[6] value10=53 />
    <AppDataBlock type=BIT[34]>
     <ownName   type=BIT[4] value2="1001" /> % last nibble of name / operative  address
     <yourCRC   type=BIT[8] value2=CRC("I am the new one/not compatible") /> % Block chain
     <SNAP_MARK type=BIT[1] choice={0=SNAP, 1=MARK2} /> % response
     <processingTime type=BIT[11] value10=&z1999" /> % ms MARK / SNAP2; MARK2
     <watchword type=BIT[4] value2="1101" /> % first name/surname initials of common friend
     <NetConfiguration type=BIT[3] value2="101" /> %
     <WSSUS            type=BIT[2] value2="01" /> % 0 no WSS but 1 US
     <inWaterColumn    type=BIT[1] value2="1" /> % 0 no (Gateway), 1 yes
    </AppDataBlock>
   <CRC type=BIT[8] />
 </Baseline>
 <Cargo></Cargo>
</JANUS>
```

Beschreibung 3: Mark-Snap-INRES-Interaktion zur Bestimmung der Laufzeit zwischen den beiden nutzenden Teilnehmern.

Damit hat Alice die Möglichkeit, die Laufzeit $\Delta = (t_2^A - t_1^A - \mu^B)/2$ durch Kenntnis der Bearbeitungszeit $\mu^B = t_2^B - t_1^B$ zu schätzen. Wenn Alice nun ebenfalls kooperativ ist, kann nach Aussendung einer ,,Let's talk"-Nachricht (Nummer 53) mit der eigenen Bearbeitszeit $\mu^A = t_3^A - t_2^A$ auch Bob die Laufzeit schätzen: $\Delta = (t_3^B - t_2^B - \mu^A)/2$. Jedoch auch jeder andere, z.B. Mallory mittels: $\Delta = (t_3^M - t_1^M - \mu^B - \mu^A)/2$. Das wäre nicht sinnvoll. Auch ein Offset zwischen zwei getrennten Mark-Snap-Interaktionen ist nicht hilfreich, da ebenfalls Mallory mittel $\Delta = (t_4^M - t_3^M + t_2^M - t_1^M - \mu^B - \mu^A)/2$ schätzen kann. Daher ist μ_A dekodiert zu übertragen. Dazu kann man nun das Wissen von Alice nutzen, die anders alsMellory die Empfangszeiten bei Bob bestimmen kann. Alice kann zudem zur Stärkung des Vertrauens auf das 4-bit-Watchword zurückgreifen, das von Bob vorab abgesprochen richtig gewählt werden muss.

Diese Individual-Link-Encryption erlaubt Alice und Bob die Laufzeit zu schätzen, die aufgrund der Kommutativität der Schallausbreitung gleich ist - bis auf kleine Variationen, also $\Delta^A \approx \Delta^B$. Analog haben beide beim Empfang der Nachrichten den Doppler-Versatz festgestellt, $\omega^A \approx \omega^B$. Wichtig ist, dass Eve und Mallory nicht die Empfangszeitpunkte schätzen können, um so die Laufzeit zu bestimmen.

Diese beiden Parameter können beide kooperativen Teilnehmer durch den Meßvorgang getrennt voneinander messen und bewerten, es wird daher die Schlüsselregel erfüllt. Die beiden Parameter (Δ, ω) sind damit Hydroschlüssel. Anders ist es mit den Patentanspüchen 3 und 5 aus [4], die aus der Impulsantwort hervorgehen. Die akustische Impulsantwort unter Wasser ist jedoch kein

Hydroschlüssel, da sich abhängig vom Eigengeräusch und der geographischen Position bei den Teilnehmern die Rauschgrenzen und die Echostrukturen unterscheiden. Ein Schlüssel muss jedoch getrennt voneinander von beiden gleich gemessen werden, [5] erfüllt daher diese Forderung nicht.

Das Ausführungsbeispiel zur Individual Link Encryption bei unsynchronisiertem Ablauf bedarf nun der Hydroschlüssel (Δ, ω). Gegeben sei ein Klartext bestehend aus fünf Zeichen basierend auf der Murray-Kodierung (5-bit CCITT-2-code). Zudem muss auf den Link, also die Kommunikation von Alice und Bob, Bezug genommen werden. Das wird hier durch die Übermittlung der CRC-Prüfzahl realisiert. Der Klartext ,,PASTO" und die CRC führen zum Block ,,cccc cccc 10110 00011 00101 10000 11000 0". Ein vorgegebener Pseudozufallszahlengenerator liefert basierend auf den beiden Hydroschlüsseln als Saatwerte eine 34-bit-Zahl (modulo 17179869183). In diesem Beispiel sei als Ergebnis des Zufallsgenerators die folgende Bitfolge ,,0010 1100 00001 10110 01010 00001 10101 1" erzeugt, und führt mittels EXOR auf die Block-Nachricht ,,rrrr rrrr 10111 10101 01011 10001 01101" (QYJZF). Diese Eingaben werden in der Nachricht Nummer 54 durch Alice oder Bob formuliert:

```
<JANUS UserClass="FirstContact" Application="encryptedProword">
 <Wakeup  type=BIT[1]  choice={enable,disable}/>
 <Baseline>
  <Version     type=BIT[4]  value=0011 />
  <MobilityFlag type=BIT[1] choice={0=static} />
  <Schedule    type=BIT[1]  choice={0=off} />
  <TxRxFlag    type=BIT[1]  choice={1=Tx/Rx} />
  <Forwarding  type=BIT[1]  choice={0=No} />
  <ClassUserID type=BIT[8]  value10=12 />
  <Application type=BIT[6]  value10=54 />
   <AppDataBlock type=BIT[34]>
    <CRC-Link  type=BIT[8] value2=CRC("Hello, I am not compatible!") /> % Block chain Example
    <Char0  type=BIT[5] value2="10111" /> %  5-bit CCITT-2-code (Murray) %             Q P
    <Char1  type=BIT[5] value2="10101" /> %  5-bit CCITT-2-code          %             Y A
    <Char2  type=BIT[5] value2="01011" /> %  5-bit CCITT-2-code          %             J S
    <Char3  type=BIT[5] value2="10001" /> %  5-bit CCITT-2-code          %             Z T
    <Char4  type=BIT[5] value2="01101" /> % 5-bit CCITT-2-code           %             F O
    <switch type=BIT[1] value2="1" />   % CCITT-2-code-switch of Chars 0=char / 1=numbers
   </AppDataBlock>
  <CRC type=BIT[8] />
 </Baseline>
 <Cargo></Cargo>
</JANUS>
```

Beschreibung 4: Basierend auf dem Austausch der beiden Mark-Snap-Nachrichten an unterschiedlichen Positionen und Zeitpunkten kann dann eine individuelle Blockchiffre formuliert werden.

Durch die in dem Prozess definierten Hydroschlüssel kann nun auf der anderen Seite durch Bob respektive Alice mit den gleichen Sequenzen mittels EXOR die gleiche Klartext-Nachricht zurückerzeugt werden.

```
    rrrr rrrr 10111 10101 01011 10001 01101 1 (QYJZF)
xor 0010 1100 00001 10110 01010 00001 10101 1, 34 bit key
    cccc cccc 10110 00011 00101 10000 11000 0 (PASTO)
```

Damit kann durch Messung eine Verschlüsselung erzeugt werden, nicht durch Übertragung. Sofern man nicht die beiden Mark-Snap- Interaktionen koppelt, um eine Nachrichtenübermittlung zu sparen, ist es für Eve und Malleroy ohne Zusatzwissen nicht möglich, die Laufzeit und den Doppler-Versatz zu schätzen.

II: Spezialfall: Alice ist Mallory. Ohne fremde Hilfe ist dieser ,,Enkel-Trick" nicht aufzudecken. Mit Voraussetzung E wird davon ausgegangen, dass sich die ,,wahre" Alice ebenfalls meldet, wenn eine Adressdoppelnutzung vorliegt.

III: Standardform: Bob ist Mallory. Alice kann anhand der in der Nachricht angegebenen Losung prüfen und Vertrauen aufbauen. Wenn Mallory hier Bob's Identität annimmt, wird Mallory in Vorleistung gehen müssen, seine Existenz preisgeben. Mallory muss zwei Mal die Nachricht 53 ausstrahlen.

IV: Alternativen: Welche Gegenmaßnahmen kann Mallory einsetzen? Das ist derzeit noch nicht gesichert, diese Veröffentlichung soll zu mehr Klarheit führen.

Authentifizierungsexperiment

Mit diesem hier vorgestellten Ansatz wird ein Skimming, also die Fälschung einer rechtmäßigen Authentisierung oder Signatur erschwert. Es gibt daher drei wissenschaftliche Fragestellungen:

- Wie groß sind die Laufzeit- und Doppler-Shift-Unterschiede zwischen Alice und Bob?
- Welche Funktion bietet sich an, um den Saatwert zu bestimmen?
- Was sind mögliche Gegenmaßnahmen von Eve und Mallory?

In dem EXPERIMENT 2 bei REPMUS21 (Robotic Experimentation Prototyping augmented by Maritime Unmanned Systems) soll diese Individual-Link-Encryption mit Alice, Bob und Eve durch Sammeln von Nachrichten-Messungen auf See beantwortet werden.

References

[1] Fatih Bülbül, Thies Petersen, Michael Recker, Fabian Sell, Kim Wachlin, Ivor Nissen. (2017). Fehlertoleranz bei Prozessabläufen - mit Anwendungen bei akustischen Unterwassernetzwerken. 10.13140/RG.2 .2 .34205 .51682.

[2] R. L. Rivest, A. Shamir, L. Adleman. (1978). A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb. 1978), 120-126. DOI:https://doi.org/10.1145/359340.359342

[3] Iwona Kochanska, Ivor Nissen, Jacek Marszal. (2018). A method for testing the wide-sense stationary uncorrelated scattering assumption fulfillment for an underwater acoustic channel. The Journal of the Acoustical Society of America. 143. EL116-EL120. 10.1121/1.5023834.

[4] Helmut Logemann, Patent: Verfahren zum Erzeugen einer nicht abhörbaren Schlüsselregel in einem Fernmelde-, insbesondere Funknetz, Philips Kommunikations Industrie AG, DE000003401562A1, 18. 01.1984

[5] Konstantinos Pelekanakis, Camila MG Gussen, Roberto Petroccia, João Alves. (2019). Towards Physical Layer Cryptography for Underwater Acoustic Networking. In Proc. of the 5th International Underwater Acoustics Conference and Exhibition.