A Discussion on Noise Addition for Relay Attack Detection

Ensel, Timon Ole
Technical University of Munich
Munich, Germany
timon.ensel@tum.de

***Abstract*—Relay Attacks, a special form of man-in-the-middle attacks, are a significant threat to the communication between two parties. This attack can be used on, but is not limited to NFC cards, which often have close to zero computational power, making it hard to introduce counter measures. There are multiple approaches dealing with this attack, to either detect or even prevent it. The most common are based on distance bounding protocols, which often are a feasible solution, but come with their own set of disadvantages. Especially the precise time measurements needed pose a big problem. A different approach, clearly taking a step away from these distance measuring protocols, was suggested by Omar Choudary and Frank Stajano. It introduces a completely new solution for Relay Attack detection based on introducing artificial noise and thereby intentional transmitting errors, which can be measured and evaluated by both communicating parties. While being an interesting concept this paper lacks acknowledgment in other scientific papers and has not been analyzed properly yet. This paper aims to provide a thorough discussion on this new "Make noise and whisper" approach and shows advantages, disadvantages, as well as the possible fields of application and compares it with other common solutions. Lastly we will introduce a new concept for relay attack detection based on noise addition for wireless applications, coming to the result, that noise based relay attack detection can, with further research, be a feasible solution.**

***Index Terms*—security evaluation, digital relays, relay algorithms**

I. Introduction

Man-in-the-middle attacks can be (maliciously) used in many ways, such as intercepting, reading, modifying, or simply transmitting messages using other paths between the communicating parties as originally intended in the concept. While the last point might seem harmless, it can be used to amplify signals to overcome physical distance limitations set in a system and connect two endpoints to overcome the systems security measures. This specific attack is known as the Relay Attack and is a comparatively easy way to get access to a verification process between sender and receiver. Common examples for attack areas are the Near Field Communication (NFC), or passive keyless entry and start (PKES) systems found in modern cars. The NFC protocol is used in many modern smart phones and (banking-)cards for contactless payment and their widely spread usage makes it a lucrative goal for malicious attackers.

It is important to note that relay attacks like the DFSCoerce attack on the Windows Distributed File System (DFS) Namespace Management Protocol, where hashed passwords can be relayed to gain access to the file system [1] are not relevant in this paper.

In 1993 David Chaum and Stefan Brands introduced distance bounding protocols [2] to propose the first applicable solution to relay attacks. Many variations followed, from which the most important developments can be found summarized in [3]. Due to their simple design this solution is the most researched so far. Still it is not perfect and comes with its own set of disadvantages, which are pointed out in (III-A3).

Next to distance bounding protocols, a lot of different approaches got introduced over the past years, trying to deal with the downsides of this timing based idea. One of them is a scientific paper called "Make noise and whisper" [4], where O. Chourdary and F. Stajano introduce the general idea of detecting relay attacks using artificial noise addition on the shared communication channel and provide two specific implementation ideas. The concept itself will be referred to as MNAW in this paper. Rarely mentioned in other papers, this solution provides an efficient alternative to D. Chaums and S. Brands approach. It solves the main disadvantage of the common distance bounding protocols, avoiding the need for precise time measurements for the distance calculation.

Due to the lack of fair evaluation and thorough analysis of noise addition for relay attack detection, the goal of this paper is to analyze MNAW (IV) and provide a detailed discussion of this approach. We will analyze advantages and disadvantages (IV-C) and compare it to existing approaches (III-A3), especially to distance bounding protocols.

While MNAW solves the precise timing needed in distance bounding protocols (III-A3), as well as the timing manipulation, new problems get introduced in this idea. Especially the need for very specialized hardware in O. Chourdarys and F. Stajanos proposed methods seem to lead to the conclusion, that noise based protocols are not feasible for most real-world applications. In this paper we will discover, that although only very specialized applications could be relevant for the methods introduced in [4] and the possibility of implementing it in real-world scenarios is very limited (IV-E), it does not rule out the possibility of implementing other noise based protocols to protect a system against relay attacks.

We will do so by proposing a new concept for the wireless environment in (V), compare it to O. Chourdary and F. Stajanos methods and evaluate its future in real world applications. This concept will demonstrate, how noise based solutions are a implementable approach, which with further research can reach the same, if not a greater level of security than other common protocols.

II. Related work

A. Relay Attack Description and Example Attacks

The concept of relay attacks was first introduced by J. Conway [5] in 1976 as a theoretical concept, described in more detail in (III-A1). Relay attacks today are a much used technique and a common security threat.

Papers like [6]–[9] showcase practical relay attacks. In [6] 10 automobiles from 8 different manufacturers were tested for this attack, coming to the conclusion that the keyless entry and start system could be be exploited by relaying the signals between key and car. [7] and [8] focus on contactless smartcards and [9] on performing the relay attack on the NFC payment system integrated in many modern smartphones. All of these attacks were able to overcome any security measures in the according implementations, using a relay attack to successfully penetrate the security of the system.

B. Solutions to Relay Attacks

Concrete solutions for this problem in computer science only were proposed much later than J. Conways first introduction to the concept. Distance bounding protocols, introduced by D. Chaum and S. Brands [2], are currently the most researched solution to avoid such an attack. In [3] a simple overview of related papers can be found, in which various ideas get introduced to make these kind of protocols more secure.

Later ideas work on the basis of channel based protocols. One of them is O. Chourdary and F. Stajanos “Make noise and whisper“ [4], which serves as the main reference used in this paper. In it a new idea is being proposed, that works by artificially adding noise to the channel and using the channels attributes to detect any man-in-the-middle. This solution, including its basic idea and the two specific implementation methods will be discussed in this paper. [4] has been referenced in other papers related to solutions to relay attacks, but lacks a clear discussion in those: In [10], a paper proposing an other channel-based relay attack detection protocol, the use of noise related detection methods, such as proposed in [4], is denied completely. [10] mentions the full-duplex channel, needed in this approach, which is “not feasible for wireless communications“ [3], excluding the wireless application field. Other one-sentence evaluations can be found among different papers, including [10], [11]. A further problem mentioned in the second paper is the high complexity and the “possibility for an attacker with higher computing capabilities than those of legitimate entities to compromise the security of the system“ [11]. Other papers, such as [3] only refer to noise addition as a general idea and do not evaluate it.

C. This paper

This lack of discussion of this idea is the main motivation for this paper. We will take a look at O. Chourdarys and F. Stajanos proposed methods for how such an implementation could look like and compare them with common distance bounding protocols. The above mentioned problems and more, as well as fields of application, will be discussed in (IV-C) and (IV-E). To add to the pool of concepts in this area and to showcase that MNAW is also relevant for the wireless field we will also introduce a new basic concept in (V), trying to solve the main disadvantage of O. Chourdarys and F. Stajanos approach.

III. Background

A. The Relay Attack

1) Problem Description: The term Relay Attack refers to a special form of a man-in-the-middle attack. It was first brought up in [5], where J. Conway described the problem using a specific example: A little girl plays against two chess masters with opposite colors. In order to fool both into seemingly playing at their level, the girl simply reproduces the moves from both masters, *relaying* them between both. This way the girl wins at least one game, or draws against both masters.

The generalized concept of a modern relay attack is very similar: Two communicating parties, usually named Alice and Bob, can identify themselves by accessing the same channel and therefor establishing a connection. This is often used for proximity authentication with NFC, RFID or similar protocols for application fields like mobile payment, or access keys. A third party, Eve, now is able to relay the physical signal to overcome a larger distance between the two authentication parties, than originally intended, connecting both even though they should not be. Because this attack can be performed only on the physical layer, by simply forwarding the message there is no cryptographic solution to it. The attacker does not need to identify, modify, or decrypt the message.

2) Attacking Example: A common example for this attack is based on the passive keyless entry (PKE) system of cars. Modern cars often do not require the driver to unlock the car manually, as the car detects the key being in proximity via a wireless connection. The problem with this comfortable solution is, that any attacker could relay the signal between the car and the according key. This would result in them being able to communicate just like they were next to each other. The attacker is now able to open the door, even though both communicating parties are virtually out of reach. This attack is often not shielded against and still possible on many car models [6]. In a similar way this attack vector also applies, but is not limited to other door access systems with key-cards any two party exchange systems.

3) Common Solutions: The most common solutions against relay attacks are distance bounding protocols. Due to the simple design of these protocols they can be implemented in many fields. They work by using a precise measurement of the round trip time of transmitted messages to calculate the distance between Alice and Bob. This value is then being compared with a preset maximum value, which limits the physical distance. What provides the security is the intuitive assumption, that an attacker cannot extend the range without an increase in the round trip time. This would render a relay attack near impossible, since the attacker cannot overcome this physical boundary.

The first proposed example was introduced by Brands and Chaum in [2] and uses three phases: A build-up phase, to exchange initial parameters for the communication, a distance-bounding phase to create a quick pace information exchange (Bob sending responses to Alice without delay) and a verification phase, evaluating the exchange. This approach is often combined with challenge-response ideas to try to overcome the biggest disadvantage of these protocols: The precise timing constraints set by the fast physical speed of signal transfer, which in the worst case can get very close to the speed of light (about 3×10^8m/s) when using fiber optic cables. This leaves measuring margins of less than 4ns for 1m accuracy. Many more modern papers try to deal with this downside in different ways, including combinations with modulation and secret sharing [3], but imprecise measurements remain a big problem.

In the wireless environment this problem is even more significant. The slower propagation speed of radio waves compared to light makes it hard to set a physical distance boundary. The attacker is not limited to this constraint and can use a cable to overcome the distance between both communicating parties illustrated by the following figure 1, where the dashed lines represent the intended wireless communication and the normal lines represent the attackers cable-transmission with a quicker propagation speed. The timing is limited, so that a maximum distance is defined. By shortening the wireless communication distance only by a small amount the attacker can extend the signal by a significantly longer distance, when using a cable. In figure (1) the “limited time t“ is always the same, but the physical distance can be stretched by using a cable (compared to using a wireless transmission).

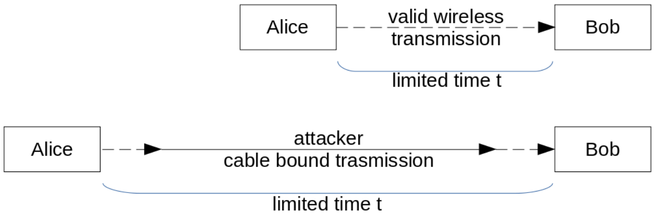

Fig. 1. Distance enlargement with shortened (slow) wireless distance and faster cable based signal transfer in a relay attack

Based on round trip timing there is also specialized hardware and new concepts like ultra wide band (UWB) [12], which the industry tries to implement for commercial usage (e.g. in PKEs) [13], but they follow a completely different idea and will not be discussed in this paper.

There is a second class of protocols worth mentioning: The Channel Based Protocols. The general idea behind them is to use the channels attributes on both endpoints to detect relay attacks. They slowly gain in popularity as many papers try to create new alternatives to overcome the distance bounding problems. Those ideas include using ambient conditions, posture recognition and more [14]. Specific propositions worth mentioning are multi-channel protocols in [14], a “Channel Based Relay Attack Detection Protocol“ [10] and most importantly [4], proposing the noise addition.

B. Noise Addition

An essential concept for MNAW is the signal layer noise addition. There are multiple forms of noise, such as additive (also referred to as white) noise, multiplicative and logarithmic-multiplicative noise. In [4] the only mentioned form is the first one, being performed on a signal layer. The ratio between the signal and added noise, the Signal to Noise Ratio (SNR), is used for measuring the noise intensity:

$$SNR = \frac{SignalVariance}{NoiseVariance} \tag{1}$$

Noise addition in general describes the addition or multiplication of randomized noise to mask or transform data being sent on a channel [15]. One important use case for noise is data privacy, where artificial noise is being added to a message on the application layer to encrypt a message using mathematical constructs [16].

In contrast to this use case MNAW makes use of a physical layer noise addition, using the channels attributes to detect possible middle-men. This form of noise addition will therefore be the relevant one for this paper, especially for the approach from [4]. It offers the possibility to add noise on a channel without knowing anything about the transmitted message. This transforms the channels properties and therefore intentionally manipulates the message.

1) Cable bound transmissions: In a physical cable, artificial noise can be added by either sending additional pulses through the medium, or by grounding the cable at certain points of time. Both approaches mask the message by forcing other values on the cable (1 for additional pulses, 0 when the cable is grounded). Both ideas will be relevant for the two methods proposed in [4], which completely rely on a cable bound transmission. They will be described in (IV).

2) Wireless transmissions: In a wireless environment physical layer noise addition is very different to the one in cables. It can only be achieved by transmitting extra signals through the medium, adding ”false” values. Noise addition for wireless communication was extensively discussed in [17]. The key difference of this paper to the needed noise addition for MNAW is the field of application: In [17] the encryption of messages is the focus, meaning it again covers the topic data privacy. For this application the noise is not being added on a physical level, but rather on the application layer based on mathematical encryption off the message. The form of noise addition that would be relevant to this paper would be to add false bits on the wireless channel, separate from sending the message.

Another method for introducing noise is to abuse the wireless communication as a full duplex channel. While this form of communication in the wireless environment is not a widely spread idea, there are many papers dealing with it, including [18] and [19]. Still all of the papers agree, that using a full duplex communication in the wireless environment is not possible without the loss of information. There are papers that propose solutions by using passive and active noise suppression [20] but the problem cannot be solved entirely [21]. This means we always have a certain amount of lost information which we can interpret as irreversible noise. This last noise addition approach will be needed for our own concept proposed in (V).

IV. O. Choudary and F. Stajanos Approach

A. Introducing Noise

In this section we will take a closer look at the MNAW idea, as well as the two proposed practical methods in [4] and discuss the future of this of noise based relay attack detection concept.

1) Make noise and whisper: [4] describes a new possibility for relay attack detection, clearly differentiating itself from other common solutions (III-A3), like distance bounding. It relies on the concept of signal layer noise addition (III-B) to be able to calculate the amount of hops between the original sender and receiver. This enables the detection of men-in-the-middle, as they increase the hop-count when forwarding the signal.

The concept itself works as follows: Before starting the transmission the receiver, Bob, introduces a certain amount of artificial noise on the communication channel, which can be measured by the sender, Alice. Should there be no added noise Alice detects an error and interrupts the communication. Otherwise Alice continues the protocol by starting to send a bit sequence, which will be repeated by Bob later on. This results in a full duplex channel requirement, meaning that both parties are able to send and receive at the same time. Here Alice must be able to send bits while listening to the noise on the channel. Bob receives the sequence with a certain amount of information loss, due to the generated noise. In the next phase Bob stops the noise addition and repeats the exact message received including the errors, meaning we stay at the physical layer and no upper layer error recognition is made. Alice, knowing what the original message was, now is able to detect some of the errors and determines with a probabilistic approach, if the amount of false bits is within a certain predefined range. Should there be less or more than expected, a man-in-the-middle is detected, as this attacker would unavoidably modify the channels properties by adding, not introducing or modifying the noise or other logical properties.

2) Difference to Distance Bounding: The key differences to distance bounding protocols are now clear: MNAW does not need a precise timing method, taking advantage of the limited transmission speed of physical signals, like it is is in distance bounding protocols. Instead it uses a method using noise, similar to a hop-count metric, that is able to determine if there are 0 or greater than 0 hops between both communicating parties. It detects a man-in-the-middle by being able to determine a forwarded signal using the modified channels attributes instead of trying to set a distance boundary between the two legitimate communication parties.

B. Two proposed implementations

Following the general concept of MNAW, we can take brief look at the two concrete methods proposed by O. Chourdary and F. Stajanos. Both ideas take advantage of a full-duplex capable trusted entity for transporting the signal.

1) Method 1: The first method consists of three phases, which we will call the *noise exchange phase*, the *echo phase* and the *evaluation phase*. For this method O. Chourdary and F. Stajano suggest a simple hardware implementation for the physical channel, which must be able to perform a logical AND function on every signal. This is reached by every party grounding the wire every time a 0 is being sent.

In the first phase Bob is masking a bit-sequence sent by Alice by adding noise in the form of sending ones and zeros with a probability of 0.5, while the channel performs the logical AND on every bit. This approach results in Bob receiving every bit where he sends 1, while disregarding every bit where a 0 is sent. The full duplex channel enables Alice to check if Bob is really masking the bits by listening to the channel and comparing the bit with the own sent one (a 0 by Bob forces a 0 on the whole channel, independent of what Alice sends).

In the second phase Bob stops the noise addition and replies with the whole previously received message, which is received by Alice, including all the previous errors. Alice now evaluates the received bits in the last phase and determines the amount of errors previously introduced.

2) Method 2: The second method requires a communication build up, which we will call the *build-up phase*, before entering the now significantly different *noise exchange phase* and the *evaluation phase*. Also the channel properties have changed compared to the first method, as now Alice and Bob must be able to switch it into 3 different states: Grounding the wire, listen to the signal and sending a one. It is important to note that this approach relies on detecting attackers with short circuits and the system must be capable of dealing with those. For the build-up phase both parties agree on a sequence of bits, which alternatively can be represented by a shared secret. This sequence must be unknown to the attacker. The actual man-in-the-middle detection starts again with the *noise exchange phase*, where both parties simultaneously send the previously agreed bit sequence through the channel, by grounding the wire for every 0, and sending a 1 for every 1. With a probability of 0.5 each communicating party may decide to listen to, or send each bit. When listening each party can compare the signal with their own. If both parties send non-matching bits, it results in a short circuit. therefore non-matching bit sequences always result in an attack detection.

This method comes with a very intuitive problem: The bit sequence generation itself, which is not discussed in [4]. This is a cryptographic problem and therefore always comes with its own weaknesses and solutions and will not be further discussed here. Other significant disadvantages will be listed in the next chapter.

C. Problems and Advantages

In this section we will now analyze, which problems are solved by MNAW and which stay, or are even newly created.

1) Advantages: Both approaches solve the biggest disadvantage of distance bounding protocols: They solve the relay attack issue without the need of precise time measurement, overcoming the need for hardware that can measure timings of only a few nanoseconds. They implement an idea, which leads to a hop-count based system that detects if there is a man-in-the-middle, fully independent of the physical distance between the communicating parties. This represents a significant advantage over distance bounding protocols, which can be easily exploited in close range applications.

Another advantage is the hardware requirement needed in the two methods proposed in [4]. Even thought the hardware is very specialized, both approaches only require few electrical components and the ability to simply store and repeat a bit sequence on Bobs side. Adding some form of key exchange afterwards would allow a very minimalist implementation for the confirming party (Bob). how to tie together?

2) Problems: The main problem with the current idea of MNAW are four newly introduced major disadvantages, which can be found in both methods:

1) Both communicating parties are required to be synchronized with an ideal clock. The communication has to be limited in a way, that each communicating party can only send exactly one bit in the exact same time slot as the second party. The same limitations must hold for any attacker.
2) They require specialized hardware to be able to implement the full duplex exchange. The second approach even requires this hardware to be able to handle short circuits.
3) Often relay attacks are relevant in the wireless field, in form of NFC, RFID, or other keyless entry/payment systems. At first glance MNAW does not seem to be applicable in this important area.
4) The first method only verifies a certain hop count between two parties. The parties themselves are not verified in any way.

1) The first problem is also addressed in [4]. The problem is the idealized scenario used in both methods, where timings are perfect and the synchronized participants as well as the attacker are limited to send and read one bit per time slot. This leads to obvious problems, where the attacker can overcome the protocol by being able to send and receive quicker than the synchronized participants and modify bits (like grounding the wire) during one time slot. When used in the right way the attacker can reconstruct information from the messages while keeping up the illusion that irreversable noise is added on the channel.

2) The specialized hardware problem is difficult to solve without heavily changing the concept of both proposed methods. Both implementation ideas rely on a channel reserved completely for the communication between both parties. While good hardware for the time measurement falls away, the new solution again is based on a very specific hardware implementation. This heavily affects the possible fields of application , which will be discussed in (IV-E).

3) The third problem is the most addressed in other papers. The argument that the need for a full-duplex communication excludes MNAWs use in wireless environment, as stated in [10], is not strictly right, as there has been thorough research on this topic which we mentioned in (III-B), with promising future ideas [20]. Still there is a big problem related to the second one: Without the possibility of changing the hardware requirements for both proposed methods it is not possible to apply the idea in a wireless environment. This problem will be discussed in the next chapter (IV-D) in more detail.

4) The last and probably most critical issue when looking at the protocol usage is relevant when looking at the first method proposed in [4]. The problem is that there is no actual verification of the two parties in the proposed processes. It seems like [4] relies on the idea, that some kind of a key exchange can be executed after verifying, that both participants are within their range limitation. In the current stage any participant could be able to answer Alice and establish a connection with Bob. A man-in-the-middle (Eve) could use this to their advantage, as they could establish separate connections Alice-Eve and Eve-Bob. Both parties now think their partner is within the required distance, making the rest of the exchange (the follow-up verification) attack-able with the basic man-in-the-middle attack. GOOD!

This last problem could be solved by sharing a secret, like pre-calculated keys, between the two legitimate parties and making Alice send an encrypted version of this key. Bob would receive this key with the noise, but still could compare the message to his key, using a probabilistic approach accounting for the errors. This would at least add some sort of security.

Excellent

D. MNAW in wireless communication

As mentioned, one of the biggest disadvantages of MNAW currently is the lack of possible implementation in wireless communication (Issue 3). In this section we will therefore look deeper into the possibility of a future implementation of MNAW in this environment. We will have to make use of noise addition in the wireless environment, making a specialized hardware harder to implement. Especially approaches that rely on grounding the signal are obsolete (Issue 2). The second hurdle to overcome is the timing issue, which gets worse when moving from a cable to a wireless field. This rules out both methods proposed in [4], since they rely on both parties being able to send bits in precise time slots (Issue 1).

The first step is to analyze the possibility of integrating the key concept, the noise addition, into the new environment. The most important boundary set in [4] is the channel. Both ideas rely on it being full-duplex capable in the sense, that both communicating parties receive the same signal over the channel, combined of both outputs. In method 1 this was used for the logical AND function between the sent bit sequence and the receivers added noise, in method 2 for the grounding of the cable to mask any input by the other party. For wireless environments this is a clear problem:

1) There is no possibility to ground the signal
2) bit-wise functions (such as a logical AND, as is necessary for both approaches in [4], performed by the channel are only possible in ideal environments
3) Noise / interference is caused by overlapping waves, not changing the channel properties (like grounding a wire)

Based on all these issues we can conclude that an implementation similar to O. Chourdarys and F. Stajanos idea is impossible for wireless applications. Still other implementation ideas that are noise based might still be possible for the wireless environment. We will look into a new concept in (V).

E. Fields of Application

As discussed in the section above, MNAW is not applicable in the wireless communication area. Therefore in this section we will discuss other possible fields of application. Even though the relay attack is by far most performed in wireless applications (NFC, RFID, PKES,...) there are niche areas where a physical relay attack is possible and must be prevented.
A common use case are contact based identification cards, like banking cards or building access cards relying on the insertion of a card into a slot. This ensures a direct communication over a reserved, specially designed direct contact between card and reader. While in the example of banking cards this shielding against relay attacks is not that necessary, as all readers require the according PIN when paying with the insertion method, other systems like door entry systems using any contact based identification could be a relevant use case. Even thought the hardware requirement is very specialized there are not many other requirements for Bob, except him repeating the message. This would result in a good implementation for simple hardware keys. Here the contactless payment would be the important method that needs protection. When talking about access cards there are a lot of forms of them, although most modern cards moving to a contactless approach as well. As the shift in the modern world moves to wireless systems we can see that the above mentioned methods would only fit into very specific niche areas. We need a new method proposal to fulfill the requirements for this.

V. Concept for wireless applications

In the following we propose a general idea of how a new noise based alternative could look like. Note, that this will be a rough concept for further development, as there will remain open problems, which we will look at in (V-D). This goal is to show that transitioning the idea of noise addition for relay attack detection into wireless applications is possible and offers a secure alternative to existing protocols.
This idea will use the existing noise level, as well as the artificially added noise to compare them and identify a man-in-the-middle through guessing the amount of channels the signal traveled through. Similar to O. Choudarys and F. Stajanos approach this is achieved with a probabilistic approach, comparing the error rate in the transmitted messages.
Additionally it will be necessary for both to share a common secret, which can be used to generate new identical keys. This will not only be important for the exchange, but also to solve the fourth issue mentioned in (IV-C) by creating a possibility of verification during the noise-exchange.
In (V-C) we will introduce a more specific research direction, in which we try to show that the combination of the noise addition concept with another field of research, namely the wireless full-duplex communication, can make a wireless application possible, not only in a theoretical area.

A. The Protocol

Our introduced concept consists of 4 major steps in the threat detection between Alice and Bob: The 1) *noise measurement phase*, the 2) *noise addition phase*, the 3) *second noise measurement phase* and the final *evaluation*. The exchange is illustrated in figure 2:

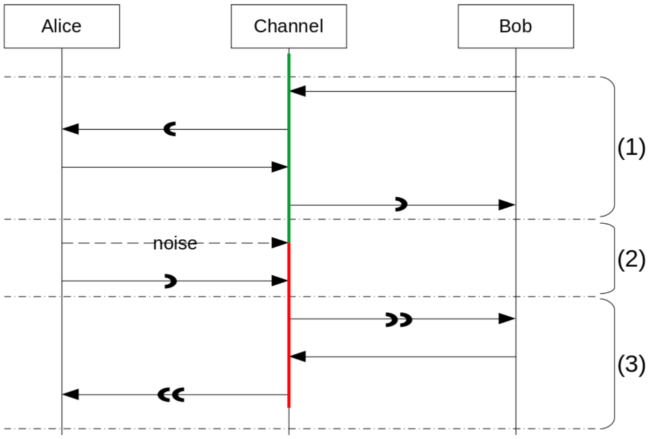

Fig. 2. Flow chart of the exchange without an attacker. *Bows symbolize the highly simplified amount of noise / errors in the message, green / red indicates the amount of noise on the channel(without/with artificial noise)*

1) In the first phase both parties measure the already existing noise on their channel. This is achieved by Bob sending a bit-sequence of length n to Alice that is previously known by Alice. Alice can therefore measure the amount of false-bits $f_{1,1}$ in the received message and calculate the SNR $s_{1,1}$ (see (III-B)) on the commonly used channel. This step will be repeated into the other direction as well, so that both parties now have a estimated noise level ($s_{1,1}$ and $s_{1,2}$) before the artificial noise addition starts.
2) In the *noise addition phase* Alice now introduces a certain amount of noise to the channel, which is being kept throughout the rest of the protocol. Following the noise addition a second generated bit-sequence will be sent from Alice to Bob.
3) The most important phase is the *second noise measurement phase*. Here Bob receives the new bit-sequence from Alice and

calculates the SNR, just like Alice did for the first message. He now has a reference to what the noise level with Alices noise addition looks like ($s_{2,1}$). Should there be no added noise on the channel ($s_{1,1}$ and $s_{2,1}$ have no significant difference) it is assumed that a man-in-the-middle attack is being performed. On the other hand, if noise is being added but the noise value drops rapidly in the time until the protocol has ended a manipulation will be detected as well. Keeping that in mind, Bob will now send a final bit-sequence of length n back to Alice, who can now re-calculate the noise level with the new amount of errors $f_{2,2}$.

why?

Now Alice is able to evaluate if the increased amount of errors $f_{2,2} - f_{1,1}$ matches with the expected increase due to the artificially added noise. In case there is no middle-man the error-increase will roughly match up with the noise-increase.

B. Middle-Man Detection

The detection of a potential middle-man (Eve) using a relay attack will be explained in the following. For this we must first understand what the sequence of transmissions looks like in the case of a relay attack. When simply relaying any signal it is important to note, that Eve is forced to forward the complete communication on the channel. This means that the noise will be forwarded just like the message. We will define the two channels as *channel*$_{AE}$ (between Alice and Eve) and *channel*$_{BE}$ (between Bob and Eve). The exchange can be seen in figure 3:

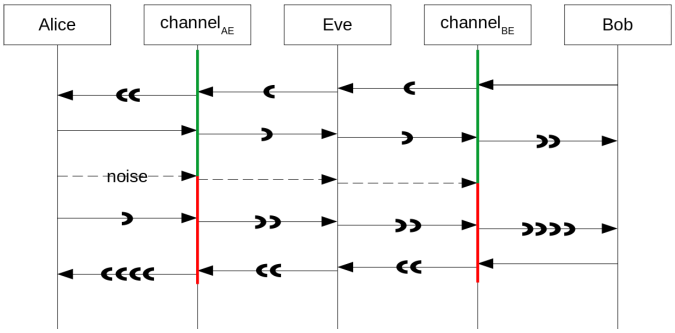

Fig. 3. Flow chart of the exchange without a middle-man. *Bows symbolize the highly simplified amount of noise / errors in the message, green / red indicates the amount of noise on the channel(without/with artificial noise)*

The first *noise measurement phase* nearly stays the same as without the attacker. All Eve has to do is forward the first message from channel$_{BE}$ to channel$_{AE}$. Alice therefore calculates the SNR of both channels combined. The second phase still does not allow any relay detection, as Eve again simply forwards Alices noise and signal from channel$_{AE}$ to channel$_{BE}$.

The third phase now leads to the attack detection: When Bob sends the last sequence, the signal will be disturbed not only by the added noise on the channel$_{AE}$, but also on the channel-BE, because Eve forwards the noise between the two. This is why it is important for Bob to listen to the channels noise during his own transmission. Eve is forced to keep the noise transmission up, otherwise Bob will detect an attacker. This leads to the noise being added twice to the signal from Bob to Alice. Alice can detect a unusual increase in the SNR (more than expected with a single noise addition) and detect, that Alice and Bob must communicate over at least two channels. A man-in-the-middle is detected.

wow

C. Using full duplex communication noise

We will now look at a field of research, which allows a more specific concept using the idea introduced in (V). Even though many papers commenting on [4] agree, that noise related protocols like the one proposed by O. Chourdary and F. Stajano require an in-band full duplex communication, which is impossible in the wireless environment, we will use the results of the previously mentioned papers (in (III-B)) to propose a new concept. This concept will not be composed to a full protocol, but should rather show, how the combination between two research fields can be used to make this noise-addition approach possible for real-world scenarios.

In (III-B) we mentioned the forced information loss in in this form of communication, which we will now use instead of the previous artificial noise introduction. This results from the self interference caused by the own sending signal colliding with the receiving signal as soon as one device must do so at the same time. This results in information loss and therefore can only be used in short range systems. While being a disadvantage for the proper usage of wireless full duplex communication as a quicker way for information exchange, we can interpret this resulting information loss as a form of noise and use this physical limitation of the channel to our advantage.

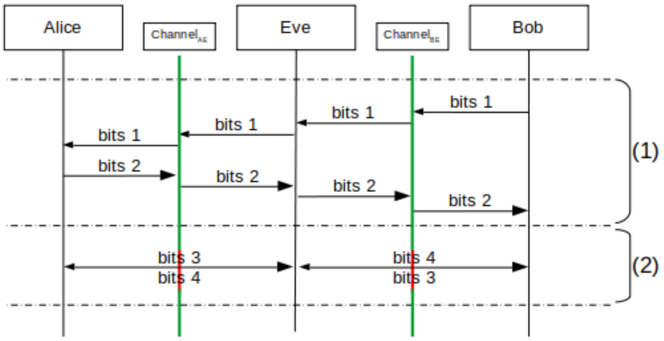

Fig. 4. Flow chart of the exchange with a middle-man. *Green / red indicates the amount of noise on the channel(without/with artificial noise)*

In the *noise addition phase* and the *second noise measurement phase* Alice would not need to introduce noise by adding it artificially to the channel. Instead it would be enough to send a bit-sequence to Bob while receiving his at the same time. The first step would stay the same. This would have the advantage that Bob could again compare the signal received by Alice to a pre-calculated bit sequence, ensuring that the ”noise” received at Bob is the same as introduced by Alice. This would lead to a similar idea, that the attacker is forced to add noise “twice“

to the signal, by communicating over two separate wireless full duplex channels. This new exchange sequence (including a man in the middle) can be seen in (4), where in step (2) we can see both full-duplex communications the attacker needs to establish a connection.

D. Evaluation and Discussion

1) Advantages: The proposed ideas solve the main problems of the previously summarized methods. We eliminated the requirement of a specialized channel, which can perform bit-wise operations, by taking advantage of the attributes in a wireless channel. There is no need for grounding a cable, as was in method 2 in [4].

Secondly, there is no need for precise timing methods, similar to the ones above. Due to the nature of wireless signals and because Alice and Bob do not need to know which bits were flipped during transmission the noise introduced does not have to be synchronized with the transmitted message. All the steps are defined by the start and end of a transmission.

Further more this new idea kept the advantage, that no distance bounding is necessary and therefore the disadvantages, like the distance enlargement, that come with it are eliminated.

Another important advantage are the hardware requirements needed for this wireless full-duplex solution. Regular antennas can be enough to be used for this form of exchange, eliminating the need for any special hardware implementation.

2) Problems: Still there are some new unsolved questions for this new method that we did not discuss in this paper. The main problem is our simplified behavior of noise. We assumed:

- a simplified possibility to add noise.
- that noise-levels during the protocol execution are stable.
- that additive noise always leads to more information loss on the channel.
- and that any information lost through noise cannot be recovered in any way.

With the second point we assume, that the protocol either works quick enough, so that major noise level changes are unlikely, or that it is generally stable enough. Both assumptions are fully dependent on the environment, the protocol itself has no influence over it.

Additionally for a practical application we would need to analyze the physical layer interference in more detail. Papers like [22] provide a thorough analysis of this phenomena, including upper bounds for noise errors.

Using random noise for the artificial noise addition also leads to a second problem, where Eve is not forced to insert the same noise into the channel$_{BE}$ as provided by Alice on channel$_{AE}$ after the third message is sent. If Eve can somehow add noise onto channel$_{BE}$ with a similar noise level as Alices noise, so that Bob cannot detect it, she could possibly later filter the noise from the last message Bob-to-Alice. She therefore could avoid the ”duplicate noise addition”. A similar problem arises if Eve is able to recover any information that was ”lost” through the noise.

These problems, the ”fake”-noise insertion and the information recovery, can be solved with the enhancement mentioned in (V-C). In this version Eve is forced to enter a full-duplex exchange with both legitimate participants and, due to the nature of the in-band full duplex channel (III-B), is forced to ”lose” information. You could say the man-in-the-middle is again forced to forward the ”noise” on both channels. A problem with this approach is the needed computing power of Bob. While in O. Chourdarys and F. Stajanos methods Bob only needs simple (but specialized) hardware which is able to return the received bit sequence (IV) in the proposed enhanced wireless approach Bob needs to be able to compare the noise-bit-sequence by Alice, while evaluating the amount of errors in that sequence and sending one in parallel. This creates difficulties for a passive device approach like for many NFC chips.

It is important to note, that we will not look at problems from the shared key generation. This process is widely researched and considered secure enough to be used in many application fields, like for example with modern car keys. There are a lot of traditional approaches and some modern approaches, like key generation based on the channels properties. One of those approaches specialized for wireless networks gets introduced in [23].

We can summarize, that for our introduced concept further research must be done in the field of signal theory to combine noise addition and the proposed concept into an applicable implementation, as we only used a simplified concept. For the enhancement with the wireless in bound full duplex channel we would need to combine a fairly new field of research with our proposed method.

VI. Conclusions

This paper discussed the new concept of using noise for relay attack detection. We analyzed O. Chourdary and F. Stajanos paper “Make noise and whisper“ [4], where this idea got introduced and summarized both specific implementation methods proposed. After a thorough analysis of both we could determine MNAWs biggest advantages and disadvantages. We concluded that while this concept is not dependent on precise time measurements and therefor saves precise hardware and cannot be overcome by distance-enlarging attacks. But while it solves the main problem of distance bounding protocols, it introduced many new ones:

We came to the conclusion that MNAW is a very new idea and current proposals for an implementation are hard to translate into real world scenarios due to the specific requirements for the communication channel. This includes it being completely reserved for this exchange and it being able to perform logical bit-operations, while providing full-duplex capabilities. We only found few scenarios where an implementation similar to the proposed methods would be possible, those being specialized cable bound exchange protocols with a specific hardware implementation, maybe used in contact based key-cards.

For the field, where relay attacks are the most common threat, the wireless communication (including popular protocols as NFC, RFID and systems like PKES) O. Chourdarys and

F. Stajanos methods are not implementable. But coming to the conclusion that other concept based on this noise addition approach could still be possible, we introduced a new ”third” idea, keeping the advantages of the noise based relay attack detection. Using the wireless channels attributes we took advantage of the information loss in the noise (or the full-duplex connection, as suggested in (V-D)) to create a protocol that would fit the new environment. While this new method still has many areas that need more specific inspection and research, especially a more detailed physical layer noise addition analysis in wireless communication, further research on this topic can lead to finalized real world implementations. MNAW therefore creates a base for a new class of relay attack detection protocols.

All in all the noise addition concept is a promising new approach. Due to its lack of research there are no implementations yet, that could be implemented in real-world scenarios, but this paper showed that after overcoming these first hurdles it has potential to be an efficient alternative to the distance bounding scheme, not only in a niche market, but in common wireless protocols as well.

References

[1] D. Naim, “How microsoft defender for identity protects against dfscoerce,” 2022. [Online]. Available: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/how-microsoft-defender-for-identity-protects-against-dfscoerce/ba-p/3562912

[2] S. Brands and D. Chaum, “Distance-bounding protocols,” in *Advances in Cryptology — EUROCRYPT ’93*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 344–359.

[3] G. Avoine, M. A. Bingöl, I. Boureanu, S. čapkun, G. Hancke, S. Kardaş, C. H. Kim, C. Lauradoux, B. Martin, J. Munilla, A. Peinado, K. B. Rasmussen, D. Singelée, A. Tchamkerten, R. Trujillo-Rasua, and S. Vaudenay, “Security of distance-bounding: A survey,” *ACM Comput. Surv.*, vol. 51, no. 5, sep 2018. [Online]. Available: https://doi.org/10.1145/3264628

[4] O. Choudary and F. Stajano, “Make noise and whisper: A solution to relay attacks,” in *Security Protocols XIX*, B. Christianson, B. Crispo, J. Malcolm, and F. Stajano, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 271–283.

[5] J. H. Conway, “On numbers and games,” 1976.

[6] A. Francillon, B. Danev, and S. Capkun, “Relay attacks on passive keyless entry and start systems in modern cars.” *IACR Cryptology ePrint Archive*, vol. 2010, p. 332, 01 2010.

[7] G. P. Hancke, “A practical relay attack on iso 14443 proximity cards,” *Technical report, University of Cambridge Computer Laboratory*, vol. 59, pp. 382–385, 2005.

[8] Z. Kfir and A. Wool, “Picking virtual pockets using relay attacks on contactless smartcard,” in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM’05)*, 2005, pp. 47–58.

[9] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, “Practical relay attack on contactless transactions by using nfc mobile phones,” Cryptology ePrint Archive, Paper 2011/618, 2011, https://eprint.iacr.org/2011/618. [Online]. Available: https://eprint.iacr.org/2011/618

[10] Abubaker, Radi, “Channel based relay attack detection protocol,” Master’s thesis, 2019. [Online]. Available: http://hdl.handle.net/10012/14691

[11] C. Camara, P. Peris-Lopez, J. M. de Fuentes, and S. Marchal, “Access control for implantable medical devices,” *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1126–1138, 2021.

[12] M. Singh, P. Leu, and S. Capkun, “Uwb with pulse reordering: Securing ranging against relay and physical-layer attacks,” Cryptology ePrint Archive, Paper 2017/1240, 2017, https://eprint.iacr.org/2017/1240. [Online]. Available: https://eprint.iacr.org/2017/1240

[13] V. AG, “Realtime safety with uwb,” 2019. [Online]. Available: https://www.volkswagen-newsroom.com/en/stories/realtime-safety-with-uwb-5438

[14] Y. Tu and S. Piramuthu, “Lightweight non-distance-bounding means to address rfid relay attacks,” *Decision Support Systems*, vol. 102, pp. 12–21, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923617301215

[15] J. Domingo-Ferrer, *Noise Addition*, L. LIU and M. T. O. ZSU, Eds. Boston, MA: Springer US, 2009.

[16] K. Mivule, “Utilizing noise addition for data privacy, an overview,” 2013. [Online]. Available: https://arxiv.org/abs/1309.3958

[17] R. Brand, *Microdata Protection through Noise Addition*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 97–116. [Online]. Available: https://doi.org/10.1007/3-540-47804-38

[18] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, “In-band full-duplex wireless: Challenges and opportunities,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, 2014.

[19] D. Kim, H. Lee, and D. Hong, “A survey of in-band full-duplex transmission: From the perspective of phy and mac layers,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2017–2046, 2015.

[20] A. Sahai, G. Patel, C. Dick, and A. Sabharwal, “On the impact of phase noise on active cancelation in wireless full-duplex,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, pp. 4494–4510, 2013.

[21] M. Duarte, “Full-duplex wireless: Design, implementation and characterization,” 2012.

[22] I. Shomorony and A. S. Avestimehr, “Worst-case additive noise in wireless networks,” *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3833–3847, 2013.

[23] Q. Wang, H. Su, K. Ren, and K. Kim, “Fast and scalable secret key generation exploiting channel phase randomness in wireless networks,” in *2011 Proceedings IEEE INFOCOM*, 2011, pp. 1422–1430.