On the Security of Ultrasound as Out-of-band Channel

Rene Mayrhofer and Hans Gellersen
Computing Department, Lancaster University
{rene,hwg}@comp.lancs.ac.uk

Abstract

Ultrasound has been proposed as out-of-band channel for authentication of peer devices in wireless ad hoc networks. Ultrasound can implicitly contribute to secure communication based on inherent limitations in signal propagation, and can additionally be used explicitly by peers to measure and verify their relative positions. In this paper we analyse potential attacks on an ultrasonic communication channel and peer-to-peer ultrasonic sensing, and investigate how potential attacks translate to application-level threats for peers seeking to establish a secure wireless link. Based on our analysis we propose a novel method for authentic communication of short messages over an ultrasonic channel.

1. Introduction

Spontaneous interaction in wireless ad hoc networks is especially vulnerable to attacks on the wireless communication channels. Such attacks include eavesdropping, injecting and modifying packets, replay, or denial of service. We generally have to assume that attackers are able to mount 'man-in-the-middle' (MITM) attacks, where they agree to two different keys with the communicating devices and which subsumes the other attack types. The major problem of purely wireless communication is therefore key management: to securely exchange keys with the intended communication partner. Using (supposedly) computationally secure key agreement protocols such as Diffie-Hellman [4], this problem is further shifted to that of authentication: to securely verify that a key belongs to the intended communication partner. In pervasive computing, and more generally in peer-to-peer networking, we can not currently assume the availability of a globally trusted third party. For spontaneous interaction, the only option is therefore ad hoc verification of keys, which requires some extra channel with additional security properties. This is a channel other than the main wireless channel and often called 'out-of-band' channel.

Balfanz et al. introduced the notion of *location-limited channels* for out-of-band communication channels that require devices to be in a certain, user-verifiable spatial relationship in order to establish communication [1]. Kindberg et al. discussed *constrained channels* along similar lines [11]. A variety of communication technologies have been considered for implementation of out-of-band channels with the desired characteristic of limiting communication to a user-controlled context. This includes ultrasound, on which we focus our analysis in this paper.

Ultrasound (US) is an interesting candidate technology for out-of-band communication alongside wireless radio (RF), for two reasons. First, ultrasound has inherent limitations in signal propagation (unlike RF, US signals are contained in rooms). Secondly, ultrasonic communication can be used by peer devices to estimate their relative positions (from US time-flight measurements, with RF communication for synchronisation [9]), and thus to obtain information that can be useful for verification of device authenticity. Ultrasound has been noted as a possible technology for authentication of peers within a room, exploiting its broadcast and propagation characteristics [1]. A concrete protocol design with ultrasound as out-of-band channel for authentication of spontaneous device associations has been discussed in [10]. In this protocol, ultrasound is proposed for out-of-band communication of nonces, and for verification of the spatial direction from which a transmission has been received. However, the protocol has not been implemented, and assumptions made concerning the use of ultrasound have neither been tested nor analysed in more depth.

In this paper we contribute an analysis of ultrasound as out-of-band channel for secure authentication of devices in wireless ad hoc networks. We assume a device A seeking to establish a secure wireless link to a device B without prior knowledge of B, or access to a shared trusted third party. The principal threat in this scenario is that a man-in-the-middle E can establish itself between A and B. A and B may be mobile devices, but they are assumed to be static in relation to each other during the initial establishment of the link (but may move freely after successful channel establishment). The protocol proposed earlier [10] has the

1-4244-0910-1/07/$20.00 ©2007 IEEE

disadvantage that users are expected to move deliberately to different locations and verify spatial measurements during the authentication phase, which can be cumbersome for ad hoc interaction. We do not assume any explicit actions by users solely for authentication purposes, but analyse the security properties of an ultrasonic channel by itself.

In the following sections we first look into properties of ultrasonic systems that can be exploited for peer authentication. We then analyse attack scenarios on the ultrasonic communication channel, and further analyse how these translate to threats at application level. We conclude the paper describing a novel method for authentic communication of short messages over an ultrasonic channel.

2. Properties of Ultrasonic Systems

Devices that use ultrasound as out-of-band channel can exploit properties of the medium both implicitly and explicitly. Ultrasound has propagation characteristics that implicitly contribute toward location-limited communication, in particular by containing signals in rooms which provides users with a distinct level of control. Devices can use ultrasound also explicitly, to estimate their spatial relationship for purposes of verifying that the device they are talking to is indeed in the assumed position, for instance 'in front of the user'.

Ultrasound signals are, due to the large differences in acoustic impedances between air and solid materials, (almost) completely reflected or absorbed by walls, doors and windows. Bending around doors or other openings causes chaotic influences on signal propagation and is practically unpredictable from an attacker's point of view. Consequently, we can assume signals or messages transmitted over an ultrasonic channel not to leave a room, and we can also assume that it is not possible to inject ultrasonic messages into a room from the outside.

Ultrasound signals travel at comparatively low speed which makes it possible for a pair of devices to measure time-of-flight of a pulse or message transmitted over an ultrasonic channel, provided they have access to an RF channel for synchronisation. Time-of-flight measurements allow for very accurate ranging (i.e. distance estimation) between peers, with errors reported well below 10cm [13, 9]. Even better accuracy can be achieved if either multiple emitters or receivers are used to take measurements from different angles (as in ultrasonic positioning infrastructures, e.g. [7, 14]). However, for our target use, verification of A and B's authenticity in a spontaneous encounter, we assume that devices will not trust other sensors but their own.

Estimation of the direction from which an ultrasound signal has arrived is possible if a device has multiple receivers on board. If these receivers are placed sufficiently far apart then it can be possible to estimate angle-of-arrival from differences in time-of-flight (this method was suggested though not tried in Kindberg & Zhang's peer authentication protocol [10]). Another possibility, better suited for devices of small dimension as typical in mobile scenarios, is to use an arrangement of receivers facing in different directions and to derive angle-of-arrival from analysis of peak signal values (an incoming pulse or message will register the highest peak with the receiver oriented most closely to the emitting device). This method has been used for instance in the RELATE system with 3 transceivers covering 180 degrees, with reported raw measurement error of 33 degrees [9].

3. Threat analysis for ultrasonic communication and sensing

For our threat analysis we assume devices A and B seeking to secure communication over a wireless radio network. We further assume possible use of ultrasound as out-of-band channel over which messages can be exchanged, and use of ultrasound synchronised over RF for estimation of distance and possible relative orientation. Note that transmitting messages over US as part of an authentication protocol is different from using US for distance-bounding protocols, introduced as a method for determining the maximum distance between devices [2]. As shown recently [3], direct use of US for distance bounding is open to relaying attacks and thus not considered secure for authentication of peer devices. For our analysis, we do not assume US to provide a *secure* upper bound on the distance.

As for attacker capabilities, we make two principal assumptions:

1. An attacker can stage attacks on the RF channel from anywhere within the range of the wireless network, to eavesdrop, to cause Denial-of-Service (DoS), or to impose itself as man-in-the-middle (MITM) between A and B (to the effect that A and B believe to be talking to each other, while actually talking to E).

2. Attacker capabilities on the US channel depend on how the attacker is located relative to the attacked devices[1]; in other words, we assume that an attacker is not able to 'virtualize' their position by using groups or whole arrays of coordinated ultrasound emitters. Note that speaker arrays can be used for spatialised audio [5] but due to the shorter wavelength of ultrasound and its more complex propagation characteristics, it would appear prohibitively difficult to achieve accurate ultrasound spatialisation.

[1] With location or position of an attacker we actually refer to the position of the communication device used to mount the attack.

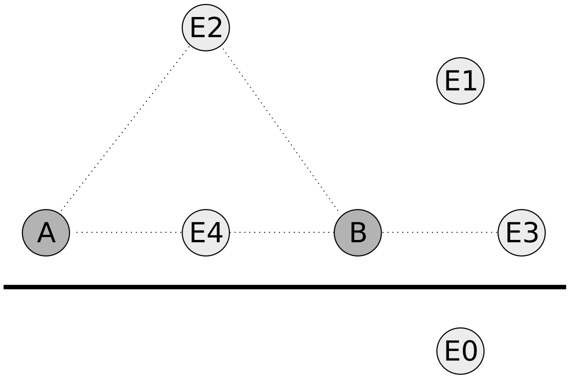


Figure 1. The capability of E to stage an attack on ultrasonic communication and sensing between A and B depends on how E is positioned with respect to A and B.

Figure 1 illustrates our scenario with devices A and B, and an attacker E that can be in different positions (E0, E1, etc.) with respect to A and B. In the following we analyse potential threats to ultrasonic communication and sensing between A and B for each of these positions:

1. *E0 – outside room*: It is an inherent property of ultrasound that signals are blocked by walls, doors and windows. Therefore we can assume that it is not possible to eavesdrop on ultrasound communication from outside a room, and that it is also not possible to interfere with the ultrasound channel from the outside, i.e to insert or modify messages that would compromise ultrasonic communication between A and B. While US signals can bend around doors or corners, this subjects them to distortions that in practice also exclude meaningful attacks. In such situations, accurate location information for both attacker and victim would be needed to produce proper time-delay-of-arrival at the receiver; creating an arbitrary angle-of-arrival is prohibitively difficult [8].

   However, an attacker E would still be able to mount an attack on the RF channel, for general denial of service, targeted prevention of devices from discovery on the network, or tampering with messages that may be used for synchronisation of ultrasonic sensing. The concrete threats with respect to ultrasonic communication and sensing are: a) to *prevent a device from participation in ultrasonic communication*, for example to the effect that a target device B selected by a user with device A becomes barred from authenticating itself; b) to *cause erroneous distance estimates*, i.e. having A estimate B to be closer or further away then they actually are and thus compromising any distance- or position-based verification procedure; and c) to *modify any distance, orientation, or position estimates exchanged over RF* (note it is common in ultrasonic positioning system to exchange measurements over RF, but it is not required and can be avoided). Threat b) also invalidates any assumptions that may be made for distance-bounding methods, even without more complex relay attacks as described earlier [3].

2. *E1 – in room*: If E is in the same room with A and B, or more precisely in the same propagation range, then E will have the additional capability to listen to all ultrasound communication, and to insert pulses or messages on the ultrasound channel, at any time with arbitrary signal strength. However, E will not generally be able modify or replace other messages exchanged over the channel, e.g. between A and B, unless E is positioned ”more strategically” in cases we discuss further below. Concrete threats arising are thus: d) to *eavesdrop on the ultrasound channel*; e) to *insert ultrasonic pulses or messages* with a potential of confusing or compromising ultrasonic sensing between other devices, and to present itself at a certain distance (cf. case E2); and f) to *block ultrasound transmission*, which, depending on the specific implementation of ultrasonic sensing and the sophistication of the attack, may or may not be distinguishable from signal noise. The distinction between blocking of transmission, i.e. denial of service, and selectively removing messages sent by other devices is blurred.

3. *E2 – equidistant positions*: If E is positioned at the same distance from a receiving device (e.g. A) as the intended target device (e.g. B) then E might achieve to be verified as B, if verification were based on distance only. Obviously if E is positioned equidistant from both devices, it may achieve positive verification by both and A and B as a man-in-the middle. Note that E can easily make itself appear at a particular distance from a single receiver, from anywhere in its ultrasonic range, by emitting an ultrasonic pulse or message ahead of the synchronisation schedule (to appear nearer) or delayed after a synchronisation point (to be appear farther). The threat in either case is: g) to *appear at the same distance as the target device*, and it highlights the value of angle-of-arrival estimates in addition to range measurements for device verification purposes.

4. *E3 – in line*: When E manages to position itself in line with A and B, its US messages will be received at an angle-of-arrival that corresponds with the angle at which the device ’in the middle’ is positioned from the perspective of the receiving device. For example,

in the scenario shown in Fig. 1, E will appear to be B from A's point of view, but not to be A from B's point of view. The threat is thus: h) to *appear from the same angle to a single device*. Note that peer-to-peer angle-of-arrival estimates tend not to be very accurate in practice and thus it may suffice for E to approximate a position in line with A and B, in order to produce this threat.

5. *E4 – in between*: A position at some point on the line directly in between A and B offers E most capabilities for an attack on US communication and sensing between A and B. US messages produced by E will be received from the same angle at which A and B are positioned respectively, creating threat i) to *appear from the same angle to both devices*. Additionally, by being directly in the line of US signalling between A and B, the attacker E may be able j) to *cancel or modify specific US messages in transit*, by means of generating anti-ultrasound (similar to noise-cancellation in audio).

Table 1 summarises threats to ultrasonic communication and sensing:

Case	Threats	Safeguards
E0	Attack on RF	US safe as out-of-band channel for authentication
E1, E2	Attack on US ranging	Check for duplicate pulses, verify angle of arrival
E3	Attack from direction of target	Mutual verification of positions
E4	Attack from direction of peer	Requires additional measures

Table 1. Summary of threats and safeguards

The main conclusions from this analysis are:

- Ultrasound can be effective as out-of-band channel for authentication of peer devices if the presence of an attacker in the same room can be ruled out by other means.
- If an attacker has access to the same room as the peer devices, then US ranging as such is not safe for further limiting the communication channel.
- Angle-of-arrival can be used to further constrain the communication channel, and to limit the possibility of an attack to attacker positions approximately in line with the peer devices; only cases E3 and E4 remain to be addressed. Verifying angle-of-arrival also prevents attacks from outside the room that may be relying on reflections e.g. at half-open doors.

4. Application-level threats

In this section we extend our analysis to review application-level threats for devices that use RF in combination with ultrasonic communication and sensing for authentication of peers. For our discussion we assume A to be a device operated by a user, and B to be a target device selected by the user for association with their device. B may be a device in the environment, or the device of another user.

1. *Replacement*: The first threat on application-level is for the attacker E to virtually replace the intended target device (say B), to the effect that A authenticates E instead of the actual target. For E to achieve this attack, they need to first 'silence' B so that B does not emit ultrasound and remains undetected by A (see threats a and f as discussed in the previous section). E further needs to pass potential verification of its position, which it can achieve by manipulating the distance at which it would be sensed by A (threats b and e, or g), and by positioning itself in line with A and B (cases E3 and E4, threat h). In this attack, interaction occurs only between A and E, and no interaction occurs with B. This scenario is limited to situations where the user does not expect a human-verifiable response from B in the process of interaction.

2. *Asynchronous MITM*: An asynchronous MITM attack occurs when the attacker E first achieves authentication with A (replacing B as described above), and in a second step with B (without the need to pretend to be A, and thus without positional constraint). E can then intercept messages from A, and forward them to B, to ensure a response of B as expected by the user. An example for such a situation would be printing: A, when sending a document to a printer B, expects it to print shortly afterwards. In this scenario, the attacker avoids detection by forwarding intercepted messages. However, the scenario requires that B does not verify the sender of the messages (only A authenticates B, but not the other way around).

3. *Synchronous MITM*: For a synchronous MITM attack E must achieve to establish itself between A and B on both the RF and the US channel, to appear to A as B and vice versa. If A and B use angle-of-arrival in the authentication process, E will only be able to achieve this attack if positioned literally in the middle between A and B (case E4).

Spontaneous interactions commonly occur in unknown and open environments, and generally it will not be possible to rule out the presence of an attacker in close enough proximity, and not blocked by walls, in order to threaten peer authentication. For peers to guard further against attacks, sensing of angle-of-arrival can be used to significantly constrain the positions from which attacks remain possible (leaving cases E3 and E4).

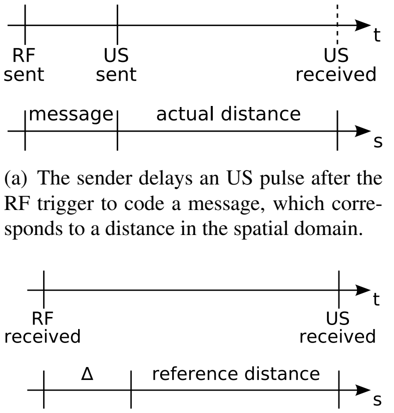
If we assume A as a user's device to be mobile but B to be a stationary device, such as a printer, then it might be plausible that an attacker positions itself strategically, to be in line between the stationary device and a likely user position. A scenario E3 might be excluded when B is mounted to a wall, or placed against wall. However, if B is also a mobile device, carried by another user, then it will generally be more difficult and less likely that an attacker achieves to position themselves between A and B. It could be argued that a user would naturally detect any device positioned between its own device A, and a target device, but it has to be noted that attacks would be possible with very small wireless sensor nodes.

If we accept the possibility of a malicious sensor node E directly between A and B then we need to consider more closely the node's attacking capability, in particular for cancellation and replacement of US messages in transit (threat j). If A sends a US message triggered over RF, E will need to cancel the message with anti-ultrasound, and generate its own US message directed at B. The smaller E is, the less time E has to replace a message to reach B within the expected time-of-flight, because of the time it takes the US messages to pass by E. For example, if E measures only a few centimetres so not to conspicuous, then it will only have a few hundred microseconds for the computations required for modifying the pulse, which, in current wireless sensor hardware, will not be sufficient. Moreover, given the propagation characteristics of ultrasound, it would not seem plausible that pulses can be cancelled without noise effects that would allow to uncover the attack.

5. Authentic communication of short messages over an ultrasonic channel

In this section we introduce a method for communication of short messages over ultrasound, effectively coding bits as distance quantities, in a way that ensures decoding only to be possible by a receiver who is positioned at an expected distance from the sender. This method is designed to overcome the problem that ultrasonic ranging as such is open to attack, and allows effective use of distance estimates to constrain ultrasonic communication. As for the application-level threat discussed, it can be used in conjunction with angle-of-arrival verification, in order to safeguard against attack in cases E3 and E4 (providing the 'additional measure' referred to in table 1, under the assumption that the attacker is not able to modify messages in transit).

Our method requires in a first step, that the authenticating devices take a reference measurement of their distance,



(a) The sender delays an US pulse after the RF trigger to code a message, which corresponds to a distance in the spatial domain.

(b) The receiver measures time from trigger to pulse arrival, and subtracts a stored reference from the corresponding distance to retrieve the message.

Figure 2. Message transmission embedded with ultrasonic ranging.

and that this measurement is verified by a user. This can be elegantly achieved if all devices discovered in ultrasonic sensing range are displayed in a map corresponding with their real-world placement, as proposed in [9] for seamless interaction with across devices.

As illustrated in Figure 2(a), a sender transmits information by delaying an ultrasonic pulse in relation to an RF synchronisation message. By delaying the US pulse, the time-of-flight and thus distance will appear larger than it is, and the virtually added distance represents the transmitted information. A receiver retrieves the virtually added distance and thus the message by subtracting the reference measurement from their actual measurement, see Figure 2(b). The receiver will only be able to retrieve the message content, if the sender's distance matches the stored reference. By retrieving the random nonce this way, it can be used in higher-level protocols as an authentic message from the remote host. Note that the transmitted information is not private; any receiver in the same room will see the same virtually added distance, in comparison to previous measurements.

The authenticity of the proposed channel is created by delaying US pulses, but only provided E does not know the transmitted information beforehand. We propose that the channel can be used for transmitting nonces as part of an authentication protocol such as the MANA I protocol [6]. For authenticity of messages, both the distance and the angle must match the expectations of the receiver. We have already argued that the attacker will not be able to manipulate angle-of-arrival measurements, but E could still be positioned in between A and B (case E4). E could also create US pulses so to appear to come from A's or B's position, but only if it knows when the pulse would be sent. This though depends on the message content, and in the case of nonces would be random. When E introduces its own pulses, the received message will be different from the nonce that the sender transmitted, and authentication protocols can be constructed to detect this. The random element and distance-based coding make the US channel authentic. We have implemented a concrete authentication protocol using this property in conjunction with an interlock protocol and based on an existing peer-to-peer US sensing platform [12].

6. Conclusions

In this paper we have analysed and discussed security properties of ultrasound as out-of-band channel in the context of peer device authentication. We identified potential threats to ultrasonic communication and sensing in dependence of attacker position, and analysed how these translate to application-level threats. A particular observation is the vulnerability of ultrasonic ranging to manipulation. To address this problem, and to provide an authentic out-of-band channel, we proposed a new method for distance-coded communication over ultrasound.

Our proposed method of piggy-backing information on single ultrasound pulses makes the US channel authentic, and thus protects against synchronous MITM attacks even when assuming far-reaching attacker capabilities. Protecting against asynchronous MITM attacks requires changes to the application, e.g. to light an LED when the infrastructure device is engaged in an interaction. Then a user could notice the delay between the two interactions and abort the transaction.

7. Acknowledgements

This work is partly supported by the EC under contract 013790 ”RELATE”, and by EPSRC under grant GR/S77097/01. We thank Mike Hazas for discussions on details of ultrasound propagation characteristics.

References

[1] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *Proc. of the 2002 Network and Distributed Systems Security Symposium (NDSS'02)*. The Internet Society, Feb. 2002.

[2] S. Brands and D. Chaum. Distance-bounding protocols (extended abstract). In *Theory and Application of Cryptographic Techniques*, pages 344–359, 1993.

[3] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In *Proc. ESAS 2006: 3rd European Workshop on Security and Privacy in Ad hoc and Sensor Networks*, pages 83–97. Springer, 2006.

[4] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[5] T. Funkhouser, N. Tsingos, and J.-M. Jot. Survey of methods for modeling sound propagation in interactive virtual environment systems. *Presense and Teleoperation*, 2003.

[6] C. Gehrmann, C. J. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes*, 7(1):29–37, 2004.

[7] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster. The anatomy of a context-aware application. In *Proc. ACM/IEEE MobiCom '99*, pages 59–68, New York, NY, USA, 1999. ACM Press.

[8] M. Hazas. Personal communication, 2006.

[9] M. Hazas, C. Kray, H. Gellersen, H. Agbota, G. Kortuem, and A. Krohn. A relative positioning system for co-located mobile devices. In *Proc. ACM MobiSys 2005*, pages 177–190, New York, NY, USA, June 2005. ACM Press.

[10] T. Kindberg and K. Zhang. Validating and securing spontaneous associations between wireless devices. In *Proc. 6th Information Security Conference (ISC'03)*, pages 44–53. Springer, October 2003.

[11] T. Kindberg, K. Zhang, and N. Shankar. Context authentication using constrained channels. In *Proc. IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pages 14–21. IEEE Computer Society, June 2002.

[12] R. Mayrhofer, H. Gellersen, and M. Hazas. An authentication protocol using ultrasonic ranging. Technical Report COMP-002-2006, Lancaster University, October 2006.

[13] M. Minami, Y. Fukuju, K. Hirasawa, S. Yokoyama, M. Mizumachi, H. Morikawa, and T. Aoyama. DOLPHIN: a practical approach for implementing a fully distributed indoor ultrasonic positioning system. In *Proc. of Ubicomp 2004*, pages 347–365, Nottingham, UK, Sept. 2004. Springer.

[14] N. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *Proc. ACM MobiCom '00*, August 2000.