Extended Abstract: SecNav: Secure Broadcast Localization and Time Synchronization in Wireless Networks

Kasper B. Rasmussen
Dep. of Computer Science
ETH Zurich
8092 Zurich, Switzerland
kasperr@inf.ethz.ch

Srdjan Čapkun
Dep. of Computer Science
ETH Zurich
8092 Zurich, Switzerland
capkuns@inf.ethz.ch

Mario Čagalj
FESB
University of Split
21000 Split, Croatia
mario.cagalj@fesb.hr

ABSTRACT

We propose SecNav, a new protocol for securing wireless navigation systems. This protocol secures localization and timesynchronization in wireless networks by relying on devices' *awareness of presence* in the power-range (coverage area) of navigation stations. We perform a detailed security analysis of SecNav and show that, compared to existing secure navigation approaches, it prevents the widest range of attacks on navigation. Our implementation of SecNav, using 802.11b devices, shows that this scheme can be efficiently implemented with existing technologies.

ACM Categories & Subject Descriptors

C.2.1 Wireless communication, J.7 Real time, K.4.4 Security

General Terms

Design, Experimentation, Security.

Keywords

Secure Localization, Secure Time Synchronization.

1. INTRODUCTION

Recently, a number of secure localization systems were proposed. Among them are Kuhn [1] Lazos [2, 3] and Capkun [5, 7], however, these either require bi-directional communication or they do not prevent replays of aggregated signals[1].

In this work, we propose SecNav, a novel secure navigation protocol, based on navigation signal broadcasts, which does not require bidirectional communication between the infrastructure and navigation devices. We show that this protocol prevents a wide range of attacks on localization and time synchronization, including location spoofing attacks using aggregated signal replays. SecNav relies on integrity coding [4] of navigation signals and on devices' awareness of their presence in the coverage area of navigation stations (e.g., within a building, university campus, or a city). We show how this coding prevents message manipulation attacks and protects the integrity and the authenticity of transmitted navigation messages. We further show how the requirement of devices' and/or users' awareness of presence in the (wider) coverage area of the infrastructure can be efficiently ensured in a number of applications. To the best of our knowledge, SecNav is also the first secure broadcast-based time synchronization system for local-area and sensor networks.

We propose two instances of SecNav: SecNav-R, which secures range-based navigation, and SecNav-F, which secures range-free navigation. Our implementation of SecNav-F using 802.11b illustrates the range and detectability of SecNav signals. Compared to SecNav-R and to distance-bounding-based secure localization approaches, SecNav-F is light-weight and does not require any high-speed processing hardware. However, given that SecNav-F is a range-free navigation scheme, it generally has a lower accuracy than range-based schemes.

SecNav can be effectively used for secure in-door and outdoor localization and synchronization of wireless devices, whose communication is supported by an infrastructure, but equally for localization and synchronization in multi-hop sensor and ad-hoc networks. Although intended primarily for smaller local environments (e.g., company buildings, university campuses), with appropriate technology and legislation in place, SecNav can be equally used in larger areas.

2. SECNAV

SecNav consists of a set of stations forming a navigation infrastructure which provides radio signals that enable devices to determine their location and to obtain an accurate time reference. We assume that the stations are strategically located such that they *cover* a given physical space (e.g., a university campus). Here, we consider that a point in space is covered by the infrastructure if it is within the communication range of at least four infrastructure stations. We further assume that the navigation infrastructure is under the control of an authority and that the stations are protected such that they cannot be compromised by an adversary. Each navigation device is aware that there is at least one honest navigation infrastructure that covers the space in which it resides; otherwise, little can be done to enable secure navigation. This awareness is achieved through public authenticated knowledge (e.g., owners of devices are made aware of the presence of the infrastructure by local civil authorities). We note that the adversary *is not* prevented from setting-up her own navigation infrastructure covering the same space covered by the legitimate infrastructure.

We observe two types of broadcast navigation systems: range-based and range-free localization systems.

2.1 SecNav-R: Secure Range-based Broadcast Navigation

Here, we consider navigation systems that have the same or similar mode of operation as the Global Positioning System (GPS).

[1] A more thorough review of related work can be found in [6]

MobiCom'07, September 9–14, 2007, Montréal, Québec, Canada.
ACM 978-1-59593-681-3/07/0009.

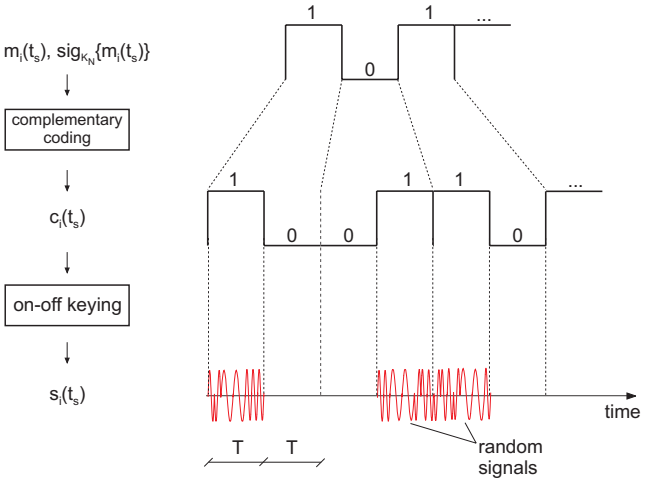

Figure 1: SecNav navigation message encoding. The navigation message is first encoded using unidirectional (Manchester) coding resulting in message $c(t_s)$, which is then transmitted on the wireless channel using on-off keying (signal $s(t_s)$). On-off keying is implemented such that for each "1" of $c_i(t_s)$, the station emits a random waveform during the *symbol period* T (a fresh random waveform is generated for each symbol), and for each symbol "0" of $c_i(t_s)$, the sender is silent (does not emit any signals) during the period T.

However, what makes SecNav significantly different from other localization schemes is the fact that the navigation signals are encoded using *integrity-codes* [4] which eliminate navigation message replay and modification attacks. Figure 1 shows the process of navigation message encoding using I-codes.

Like in GPS, we assume that navigation stations are tightly synchronized and emit navigation signals simultaneously (up to a measurable drift). Each navigation signal s_i, contains a timestamp t_s of the time at which it was sent and a location L_i of the base station BS_i that sent it. Upon receiving at least four signals and registering their reception times, the navigation device calculates the distances to the stations, and determines the location p and time reference of the device by multilateration. The cumulative signal observed at the navigation device at time t is given by the following expression:

$$r(p,t) = \sum_i A_i(p,t) \cdot s_i(t_s + \frac{|L_i - p|}{c} + \delta) + n(p,t) \quad (1)$$

where $A_i(p,t)$ and $n(p,t)$ are the strength of the signal s_i and the noise at location p and time t, respectively; δ is the synchronization error between the device and the navigation stations, and c is the speed of light in vacuum. Upon the reception of a navigation signal from station BS_i, the device registered its reception time t_r^i, from which it computes a pseudo range $\hat{d}_i$ to BS_i as

$$\hat{d}_i = (t_r^i - t_s) \cdot c \quad (2)$$

Each pseudo-range contains (the same) error $c \cdot \delta$ introduced by the offset δ between the device's and stations' clocks. By measuring pseudo-ranges to (at least) four stations, the device can determine it's location p and the synchronization offset δ and therefore synchronize to the stations. This is done by solving (for p and δ) the following system of (at least four) equations

$$\hat{d}_i = |L_i - p| + c \cdot \delta \quad (3)$$

where each equation corresponds to one pseudo-range $\hat{d}_i$ measured by B to station BS_i. This is illustrated in Figure 2(a).

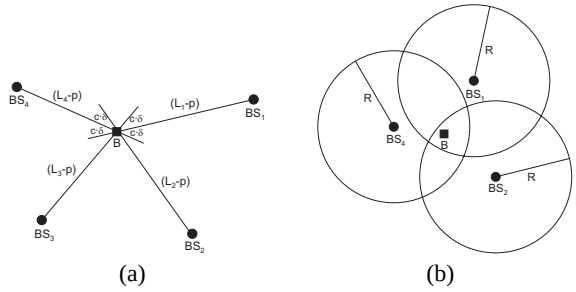

Figure 2: (a) Range-based navigation: B determines its locations and time reference by measuring pseudo-ranges, which consist of true ranges $|L_i - p|$ between B and BS_i and of a ranging error $c \cdot \delta$ caused by an offset between B's clock and clocks of navigation stations. (b) Range-free navigation: B estimates its location within the intersection of power ranges (R) of navigation stations, whose beacons it hears. B synchronizes to the infrastructure by observing the timestamps contained in navigation messages.

To see the benefits of I-codes for navigation signals we give a short description of how I-codes work. For a more detailed description, refer to [4].

Sending a navigation message using I-codes is a two step process. The first step is to encode the message using Manchester coding, this ensures that the message will contain an equal number of ones and zeros. In the rest of this paper we call the ones and zeros of the message *bits*, and the ones and zeros of the Manchester encoded message *symbols*. Step two is to transmit the message symbols using on-off keying with random signals (see Figure 1). This ensures that the attacker can not turn a "1" symbol into a "0" since the attacker can not remove the random signal from the channel.

On-off keying along with a fixed signal strength threshold at the receiver also ensures that the attacker can not jam, overshadow or alter the message in flight without being detected, i.e., any transmission from the attacker would add "1" symbols with no way to remove them to restore the ratio of ones and zeros.

In SecNav-R the navigation device collects messages from stations for a predefined time period of duration Δt. Upon receiving verified messages from at least three (four in the case of 3D localization) navigation stations, the device starts the computation of its location. The duration of Δt is set by the wireless device and it depends on device's speed of displacement.

The device first demodulates navigation messages and verifies their integrity and authenticity by performing four message verification steps: (i) verify that it resides in the infrastructure coverage area, (ii) verify that the channel on which it received the signal $s_i(t_s)$ is the channel used by the infrastructure, (iii) verify that the demodulated message $c_i(t_s)$ is valid, i.e., it contains an equal number of symbols "1" and "0" symbols and (iv) verify that the demodulated signature $sig_{K_N}\{m_i(t_s)\}$ correspond to the demodulated message $m_i(t_s)$.

Thus far, we have observed that each station BS_i transmits a single navigation signal $s_i(t_s)$ at time t_s. However, in our system, the absence of legitimate navigation signals in the infrastructure coverage area would enable an attacker to insert messages and provide false reference to navigation devices in that area. To prevent this, in our scheme, each navigation station is required to keep the channel busy by either transmitting valid navigation messages in uninterrupted sequence or by transmitting I-coded sequences that will prevent the attacker from forging any meaningful messages on that channel.

Note, however, that in this case there has to be a way for the navigation station BS_i to inform the receiver B about the beginning and the end of any message $c_i(t_s)$ emitted over the channel. In SecNav this is achieved by means of the *incongruous-delimiter* (*I-delimiter*). In the following paragraphs, we show how navigation stations (BS_i) and navigation devices (B) can use I-delimiters in order to synchronize securely with respect to the beginning and the end of the transmission of the given message $c_i(t_s)$.

We introduce message delimiters through the following example. Let us assume that the station wants to transmit the following two codewords consecutively $c_i(t_s) = 1010011001$ and $c_i(t_s+\Delta t) = 1010010101$ which, under Manchester coding, correspond to navigation messages $m_i(t_s) = 11010$ and $m_i(t_s + \Delta t) = 11000$, respectively. The station BS_i emits the following sequence using on-off keying:

$$\underbrace{111000}_{\text{delimiter}}\ \underbrace{1010011001}_{c_i(t_s)}\ \underbrace{111000}_{\text{delimiter}}\ \underbrace{1010010101}_{c_i(t_s+\Delta t)}\ \underbrace{111000}_{\text{delimiter}}$$

Here, the delimiter "111000" is a specially constructed symbol-string such that no delimiter can be changed into part of a message and no message can be changed into a delimiter. This is true as the delimiter sequence 111000 cannot be forged by an adversary, given that the adversary cannot convert "1" symbols to "0" [4]. This effectively prevents the adversary from "shifting" delimiters in time and thus forging transmitted navigation messages without being detected.

2.2 SecNav-F: Secure Range-Free Broadcast Navigation

We further consider range-free broadcast navigation systems. These systems are similar to range-based localization in that a device determines its location and synchronizes to the infrastructure based on the messages that it receives from the navigation stations. The main difference is that, instead of measuring distances to the stations, the device simply registers from which stations it received the messages and then estimates its location within the area defined by the intersection of the power ranges of navigation stations. This is illustrated in Figure 2(b). The device synchronizes to the infrastructure by simply adjusting its clock to the timestamp contained in the received beacons.

In SecNav-F, every navigation station BS_i transmit navigation messages $m_i(t_s) = BS_i||t_s||L_i$ containing an identifier BS_i, message sending time t_s and its location L_i to navigation devices in its vicinity. This message is appended with the message signature $sig_{K_N}\{m_i(t_s)\}$, generated with the infrastructure private key K_N. Before emitting $m_i(t_s)$, $sig_{K_N}\{m_i(t_s)\}$ over a radio channel, BS_i transforms this message using integrity coding [4].

The navigation device performs the same four verification steps as in SecNav-R. If these verifications are successful the navigation device computes its location (x_B, y_B) within the area defined by the stations' ranges. This is illustrated in Figure 2(b). One example of such computation is the Minimum Mean Square Estimate (MMSE), which computes the devices location as follows:

$$\text{Let } f_i(x'_B, y'_B) = R - \sqrt{(x_i - x'_B)^2 + (y_i - y'_B)^2}$$

The location (x_B, y_B) is then obtained by minimizing $F(x'_B, y'_B) = \sum_{BS_i \in \mathcal{S}} f_i^2(x'_B, y'_B)$ over all estimates (x'_B, y'_B)

where $L_i = (x_i, y_i)$ is the location of station BS_i, R is the power range of stations and S is the set of stations whose messages B received within Δt.

Note that for localization purposes, in SecNav-F, navigation stations do not need to be mutually synchronized and that navigation messages do not need to be sent simultaneously. Stations, however, do send navigation messages continuously.

In SecNav-F, for a navigation device to synchronizes to the infrastructure it is sufficient that it receives messages from at least one of the navigation stations. It then adjusts its local clock Cl_B as follows: $Cl_B = t_s - t_{Pr} - t_{Tr}$ where t_s is the timestamp contained in the navigation message, t_{Tr} is the message transmission time (which depends on the message length and on the transmission speed) and t_{Pr} is the message propagation time (which depends on the distance between the station and the device); t_{Pr} is typically few nanoseconds, and it can therefore be neglected in most applications.

3. SECURITY ANALYSIS

In SecNav, attacks on localization are prevented by the encoding scheme used for navigation signals and by devices' awareness of presence in the coverage area of the infrastructure. In the following security analysis, we will assume that devices and/or users are aware of their presence in the infrastructure coverage area. We will first describe the attacker model.

3.1 Attacker Model

We adopt the following attacker model. We assume that the attacker Mallory (M) controls the communication channel in a sense that she can eavesdrop on messages, insert messages, modify and schedule transmitted messages. More specifically, we assume that the attacker can relay and delay transmitted messages. We do assume that the attacker cannot disable the communication channel between infrastructure nodes and navigation devices (e.g., by using a Faraday cage to block the propagation of radio signals). However, the attacker can jam all transmissions and in that way prevent the transmission of the information contained in the message; the receiver will still receive the signal from the sender, superimposed on the attacker's signal. Our attacker model is similar to the the Dolev-Yao model in that the attacker controls the communication channel, but it differs in that the attacker cannot trivially remove the energy of emitted signals from the channel.

3.2 Message Manipulation

Message **forgery**, manipulation and **replay** is prevented through permanent transmissions of navigation signals on the communication channel. By permanent presence of legitimate navigation messages on all four communication channels and over the entire infrastructure coverage area, the attacker is prevented from inserting false navigation messages, without being detected. If the attacker inserts its (false) navigation message, this message will interleave with navigation messages sent by the infrastructure. The receivers will therefore reject the received superposition of two messages because the ratio of the number of symbols 1 and 0 in that message will be different from the one expected at the receivers. Essentially, any message forged by the attacker, replayed, or simply modified in transmission will be equally rejected at the receiver as it will change the ratio of the number of 1s and 0s in the received message. Following the same reasoning, **replay of aggregated navigation signals** will be equally prevented. These aggregated navigation signals will interleave with legitimate navigation signals sent by the infrastructure and will cause the receivers to reject the received signals. If the device is unknowingly displaced from the infrastructure coverage area, message forgery is still prevented by the use of digital signatures.

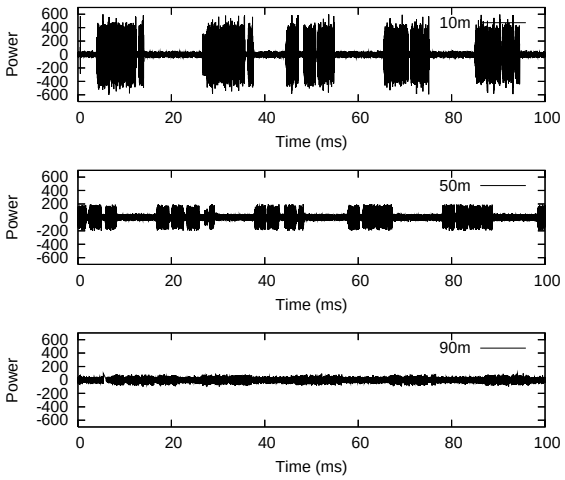

Figure 3: Signal strength at 10, 50 and 90 meters. Note that the "symbol width" is much wider ($\sim 10ms$) than it needs to be to make the bits easy to identify.

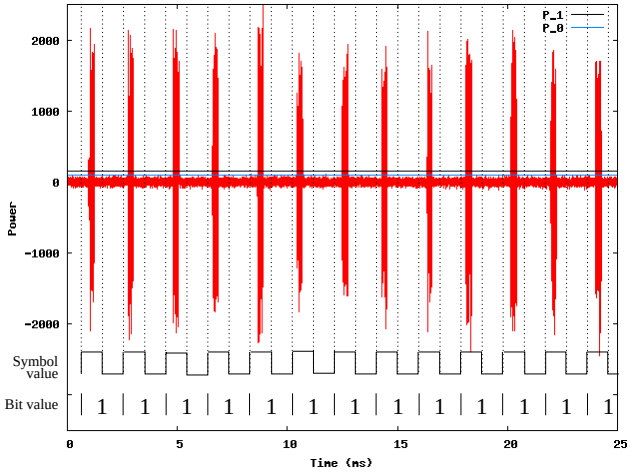

Figure 4: SecNav signal with $2\ ms$ bit duration, resulting in SecNav signal transmission rate of $500\ bits/s$. The signal is shown with the corresponding symbol- and bit-values.

Since message replay and forgery are prevented in SecNav, attacks on localization and time-synchronization by pulse-delays are equally prevented. E.g., if a pulse-delay attack is attempted by **jam-and replay**, this will be detected at the receivers as the messages replayed by the attacker (and the jamming) will be superimposed on the legitimate messages sent by the infrastructure. Given that to detect symbols 0 and 1 on the channel, receivers measure strengths of the received signals (as opposed to their signal-to-noise ratio), attacks by message **overshadowing** will be equally detected.

4. IMPLEMENTATION ISSUES

In this section, we show results of our SecNav implementation feasibility study. Our study focused on the range and detectability of SecNav signals and the feasibility of a future full-scale robust implementation.

To receive SecNav signals, the receiver must be able to reliably detect the presence and absence of signal on the channel. A symbol "1" is decoded at the receiver if the average received signal strength at the receiver during the symbol duration period T is above a threshold P_1. Equally, if the average power during T is below a threshold P_0, the receiver detects symbol "0". Figure 3 displays the results of measurements of SecNav navigational signals at the receiver whose distance from the sender was changed from 10 to 90 meters (LoS). In this experiment, the signals were sent using a standard built-in Atheros 5212 wireless network card and received by a software radio. Both the transmitter and the receiver were equipped with built-in omnidirectional antennas, whose gains were not enhanced. The transmission power at the sender was set to $100mW$. These results show that the receiver can clearly distinguish symbol "1" from environmental noise (i.e., symbol "0") up to almost $100m$. Note that these results can be further enhanced if higher transmission powers and antenna gains are used at the stations.

Besides the range of navigation signals, our experiments also included the estimation of the maximal rate of SecNav navigation signals, using 802.11b devices. Using available MadWifi drivers we were successful in transmitting SecNav signals with bit durations of approx. $2\ ms$ (i.e., symbol durations of approx. $1\ ms$). The results of this experiment are illustrated in Figure 4. This experiment showed that with off-the-shelf cards and drivers, the data rate of SecNav signals can be $500\ bits/s$, which is sufficient to transmit at least one navigation message/second. This means that the devices will be able to synchronize to the infrastructure each second, and determine their location in the worst case every few seconds (accounting for possible clock drift between navigation stations). Appropriate modifications of the wireless card drivers of the sender (and receiver) will allow the rate of the SecNav signals to be further increased; this is part of our ongoing work.

5. CONCLUSION

In this work, we proposed SecNav, a novel secure navigation protocol based on navigation signal broadcasts. We showed SecNav prevents a wide range of attacks on localization and time synchronization, including message forgery and replay; SecNav is the first navigation system that effectively prevents location spoofing attacks using aggregated signal replays.

We proposed two instances of SecNav: SecNav-R, which secures range-based navigation, and SecNav-F, which secures range-free navigation. Our implementation of SecNav-F using 802.11b shows that SecNav signals can be successfully detected upto ranges of ~100m with off the shelf hardware. We also show that the data rate is high enough, even with unmodified WiFi cards, to send the needed navigation messages.

6. REFERENCES

[1] M. G. Kuhn. An Asymmetric Security Mechanism for Navigation Signals. In *Proceedings of the Information Hiding Workshop*, 2004.

[2] L. Lazos and R. Poovendran. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. In *Proceedings of WiSe*.

[3] L. Lazos, S. Čapkun, and R. Poovendran. ROPE: Robust Position Estimation in Wireless Sensor Networks. In *Proceedings of IPSN*.

[4] M. Čagalj, S. Čapkun, RamKumar Rengaswamy, Ilias Tsigkogiannis, M. Srivastava, and Jean-Pierre Hubaux. Integrity (I) codes: Message Integrity Protection and Authentication Over Insecure Channels. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, California, USA, 2006.

[5] S. Čapkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of InfoCom*, 2005.

[6] S. Čapkun, K. Rasmussen, and M. Čagalj. SecNav: Secure broadcast localization and time synchronization in wireless networks. Technical Report 546, ETH Zurich, 2007.

[7] S. Čapkun, M. Čagalj, and M. Srivastava. Secure Localization with Hidden and Mobile Base Stations. In *Proceedings of InfoCom*, 2006.