Proceedings of 2010 IEEE International Conference on Ultra-Wideband (ICUWB2010)

The Cicada Attack: Degradation and Denial of Service in IR Ranging

Marcin Poturalski, Manuel Flury, Panos Papadimitratos, Jean-Pierre Hubaux, Jean-Yves Le Boudec
Laboratory for Computer Communications and Applications, EPFL, Switzerland
firstname.lastname@epfl.ch

***Abstract*—We demonstrate that an interferer with *malicious* intentions can significantly degrade the performance of impulse-radio (IR) ranging. The *cicada attack* we have developed can decrease the distance (*degradation of service*) measured by ranging algorithms designed to cope with weak NLOS conditions; it can also jam communication (*denial of service*). The attack is easy to mount and can be effective even against receivers designed to cope with *benign* multi-user interference. We also sketch possible countermeasures.**

I. Introduction

A distinguishing feature of IR-UWB is the ability to perform high-precision ranging in multipath environments and/or under interference. This makes IR-UWB an ideal candidate for implementing services such as indoor localization, tracking, or physical access control. Thanks to the fine timing resolution of IR-UWB, even low-cost energy detectors (EDs) are able to achieve sub-meter ranging precision in weak non-line-of-sight (NLOS) conditions: A receiver can first lock onto the strongest multipath component, and afterwards perform a back-search to find the first arriving path [1], [2]. As recent works [3], [4], [5] show, this can be achieved even under interference from *benign* users (multi-user interference (MUI)). However, many of the envisioned applications of IR-UWB ranging are security sensitive, and we cannot help but ask the question: What could an interferer with *malicious* intentions do?

We identify a simple and destructive attack that we call the *cicada attack*. It unfolds as follows: Consider two IR transceivers, T and R, performing ranging. T transmits a preamble that allows R to acquire the packet and estimate the time of arrival (ToA). The preamble commonly consists of a sequence of pulses created by spreading a predefined preamble code (Fig. 1a). Meanwhile, a malicious device M transmits constantly a sequence of pulses (Fig. 1b), reminiscent of the cicada song. Both signals propagate through the multipath environment and interfere at R (Fig. 1c). If M's signal is stronger than T's, R will lock onto the former, and T's packet will be ignored, resulting in *denial of service*. If M's signal is weaker than T's, R will lock on T's signal, but there is a good chance that the back-search algorithm will incorrectly find the “fist arriving path” in the signal of M (Fig. 1d). The estimated distance is then significantly lower than the actual one, resulting in *degradation of service*.

The cicada attack is very easy to mount. It needs only an unsophisticated IR transmitter that is not much more energy-consuming than a benign IR transmitter, and it does not require the knowledge of the preamble code. In contrast, the consequences of the cicada attack are severe. It can effectively achieve denial of service against ranging and data communication (even when secret spreading codes are used). Degradation of service applies only to ranging, but it is more subtle and harder to detect, which can make it more dangerous in some cases. For example, consider a robot-operated factory, in which robots rely on IR ranging for navigation. A denial of service attack can be detected instantly, and the robots can stop on the spot rather than roam around blindly. Under a degradation of service attack, the robots still obtain distance measurements, but incorrect ones. Acting upon this false input, the robots can run into walls, each other, or other equipment, causing significant property damage.

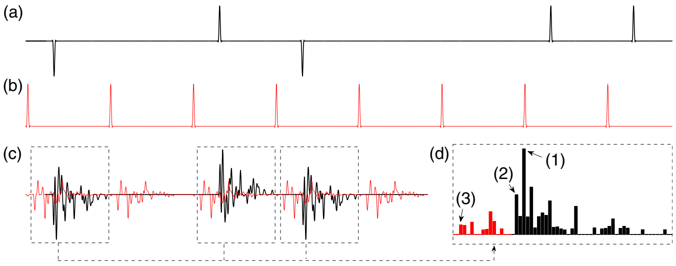

Fig. 1. The cicada attack. (a) Benign transmitter T sends a preamble derived from a preamble code $[-1, 0, 1, -1, 0, 0, 1, 1, \ldots]$. (b) Attacker M transmits a cicada signal. (c) Both signals propagate through the multipath environment before they are received by R. (d) R aggregates the received signal over a number of pulses, and finds the strongest path (1). It then searches back for the first path (2), but instead finds the bogus path introduced by M (3).

In the rest of the paper, we demonstrate the feasibility of the cicada attack. We do this for the IEEE 802.15.4a PHY [6], but the attack applies to a large class of IR-UWB systems. We evaluate a basic ED, and two EDs implementing state-of-the-art MUI-mitigation techniques for synchronization: the min filter [3], [4] and PICNIC [5], as such techniques could potentially thwart malicious interference created by our attack. We show that for all three receivers, the attack can reach close to 100% degradation, as well as virtually 100% denial with moderate energy costs. We then outline possible countermeasures and directions for future work.

II. System Model

A. Packet Format

We consider the mandatory low pulse repetition frequency (LPRF) mode of the IEEE 802.15.4a PHY [6]. Packets consist

978-1-4244-5306-1/10/$26.00 ©2010 IEEE

of a synchronization preamble (*SYNC*), followed by a start frame delimiter (*SFD*) and payload. The latter two are of lesser importance to our investigation; we refer the reader to [6] for details. The SYNC is constructed from N_{psym} *preamble symbols* of duration T_{psym}. A preamble symbol consists of N_{pcode} *code symbols* of duration T_{pcode}. A code symbol contains a single pulse of polarity, determined by a ternary *preamble code* C_k, $k = 1, \ldots, N_{\text{pcode}}$. The transmitted signal is:

$$s(t) = \sum_{j=1}^{N_{\text{psym}}} \sum_{k=1}^{N_{\text{pcode}}} C_k p(t - kT_{\text{pcode}} - jT_{\text{psym}}) \qquad (1)$$

where $p(t)$ is the pulse shape of a single pulse. In the mandatory LPRF IEEE 802.15.4a mode $N_{\text{psym}} = 64$, $N_{\text{pcode}} = 31$ and $T_{\text{pcode}} = 128\text{ns}$. We use preamble code 5.

B. Receivers

We consider EDs composed of an antenna, a 500MHz bandpass filter, followed by a squaring device and an integrator. The integrator outputs a discrete time sample y_m every $T_{\text{int}} = 2\text{ns}$.

We evaluate three receivers: a classical ED (termed *Vanilla*), and two EDs robust to MUI: *MINF* and *PICNIC*. All receivers operate in stages: *a) coarse synchronization* to acquire the packet and determine the strongest multipath component, *b) fine synchronization* to determine the ToA by finding the first multipath component, *c) channel estimation*, *d) SFD detection*, and *e) data demodulation*. The last 3 stages use standard algorithms, or (in case of MINF and PICNIC) versions robust to MUI [7].

a) Coarse Synchronization: For Vanilla and MINF, coarse synchronization follows the baseline method from [5]. Essentially, the incoming y_m samples are correlated with a binary template formed from $N_G = 16$ preamble symbols for processing gain. The maximum correlator output sample corresponds to the strongest path.

In the PICNIC coarse synchronization [5], a *PID* (power independent decision) filter is applied to the y_m samples before correlation. Samples below (above) a noise-based threshold are set to 0 (1), to limit the effect of high-power interferers. Further, the signal is inspected for presence of a benign interferer using an alternative preamble code (e.g., code 6 [6]), and if detected, *interference cancelation (IC)* is applied.

b) Fine Synchronization: All receivers perform a *back-search* [1], [2] in a window of duration $T_{\text{BS}} = 64\text{ns}$ preceding the sample containing the strongest path. The ToA is identified as the first sample i in this window that is 1) above a threshold and 2) greater than sample $i + \frac{T_{\text{pcode}}}{T_{\text{int}}}$ (one code symbol later). The second test mitigates "self-interference": With non-coherent reception, autocorrelation of the preamble code is always strictly positive [5], which creates secondary peaks in the correlator output (repeating every code symbol). The *self-interference test (SIT)* proposed in 2) relies on these peaks being strictly smaller than the main correlation peak.

Vanilla and PICNIC perform the back-search on the correlator output, with appropriate noise-based thresholds. MINF [3], [4] uses an average of an equivalent number of code symbols, filtered with a moving min filter before averaging (min-window length $W_{\min} = 8$). The min filter removes interference based on the assumption that the interference is present in at most $W_{\min} - 1$ consecutive code symbols (typical for MUI).

III. Attack

A. Threat Model

We assume that an attacker deploys a *cicada device*, M, in an area where benign devices perform ranging. The cicada device constantly transmits a *cicada signal* of the following structure:

$$m(t) = \sum_{j=-\infty}^{\infty} \sum_{k=1}^{N_{\text{p}} \cdot N_{\text{pcode}}} A_j p(t - \frac{k}{N_{\text{p}}} T_{\text{pcode}} - jT_{\text{psym}}) \qquad (2)$$

where N_{p} is the number of (uniformly spaced) pulses transmitted per code symbol, and A_j is a periodic binary sequence that determines when the cicada device remains silent. Note that the start time and duration of silent periods are multiples of the preamble symbol duration T_{psym}, rather than T_{pcode} – this mitigates the min filter. We use the abbreviation *i-attack* to denote an attack with $N_{\text{p}} = i$. We call the attack *continuous* if $A_j = 1$ and *intermittent* if $A_j = 1$ for j a multiple of 3, and 0 otherwise. A more general signal structure can be envisioned, but this format is sufficient for our purposes.

The attacker can adjust N_a and A_j, as well as the transmission power, and the location of the cicada device. We will mostly focus on an attacker interested in degradation, rather than denial of service.

B. Performance Evaluation

Setup. We assume that a receiver R is exposed to the cicada signal at signal-to-noise ratio SNR_{M}. R receives, at random times, ranging packets transmitted by a benign transmitter T with SNR_{T}. (In both cases, the SNR is defined as $\frac{E_p}{N_0}$, where E_p is the energy of a single pulse.) We simulate the entire packet reception process (from synchronization to demodulation). We use the residential (weak) NLOS channel model [8].

Metrics. We consider that *denial* occurs if a packet is not received correctly (failure of coarse synchronization, SFD detection, or data demodulation). If the packet is received correctly, *degradation* occurs if the estimated ToA is at least $2T_{\text{int}} = 4\text{ns}$ below the actual ToA. We measure the percentage of packets subject to degradation or denial.

Attack performance. The main factor determining the attack performance is SNR_{M}. This can be seen in Fig. 2a, which shows the continuous 1-attack performance against the Vanilla receiver at $\text{SNR}_{\text{T}} = 20\text{dB}$. From $\text{SNR}_{\text{M}} \approx -2\text{dB}$ degradation begins, and it reaches its maximum of around 70% for $\text{SNR}_{\text{M}} \approx 15\text{dB}$. 100% is not reached: With $N_{\text{p}} = 1$, the cicada signal, even though spread by the channel (Fig. 1c), is not always present in the search-back window. Beyond the maximum point, denial starts to take over, and

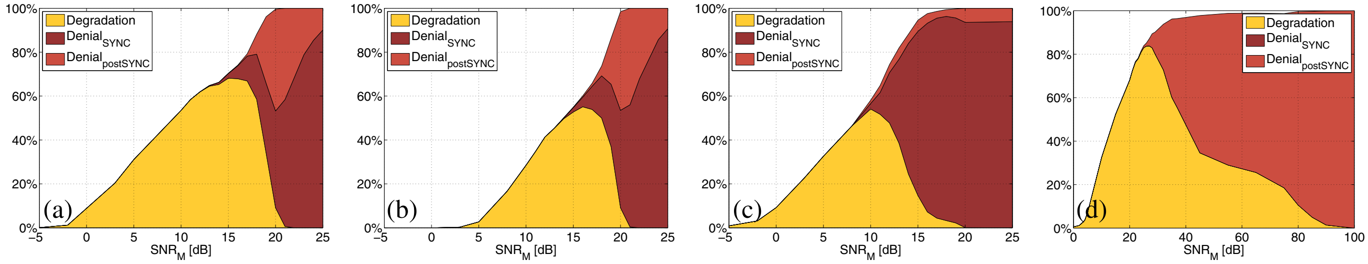

Fig. 2. Cicada attack performance at $\mathrm{SNR_T} = 20$. Denial$_{\mathsf{SYNC}}$ represents failure in coarse synchronization, Denial$_{\mathsf{postSYNC}}$ – failure in subsequence reception stages. (a) Vanilla (b) MINF and (c) PICNIC under continuous 1-attack, (d) PICNIC under intermittent 1-attack.

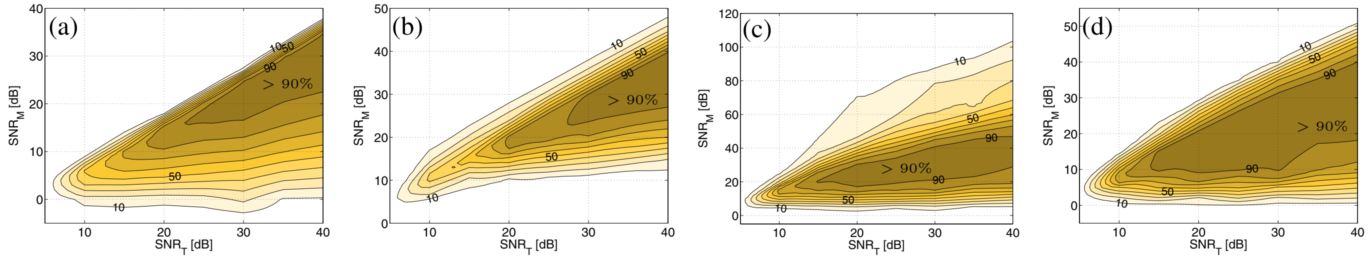

Fig. 3. Cicada attack performance: degradation. (a) Vanilla under continuous 1-attack, (b) MINF (c) PICNIC under intermittent 2-attack, (d) PICNIC under intermittent 8-attack.

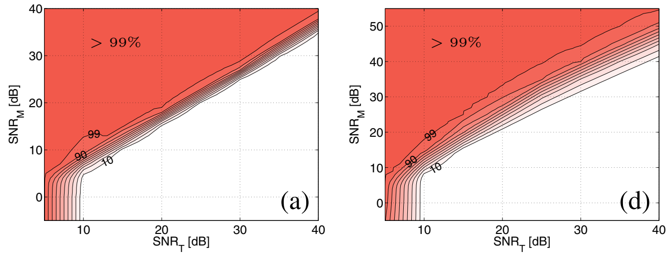

Fig. 4. Cicada attack performance: denial. (a), (d) as in figure Fig. 3.

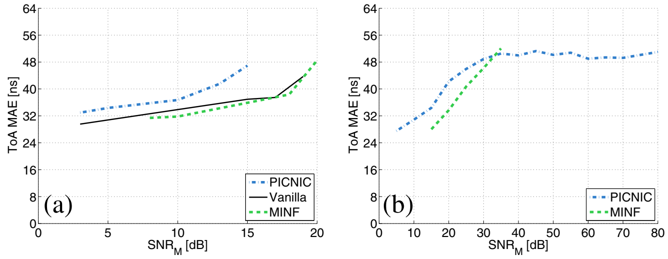

Fig. 5. ToA error under degradation. (a) continuous 1-attack at $\mathrm{SNR_T} = 20\mathrm{dB}$ (b) intermittent 2-attack at $\mathrm{SNR_T} = 30\mathrm{dB}$.

for $\mathrm{SNR_M} \approx 22\mathrm{dB}$, it reaches 100% – partially due to coarse synchronization failure (Denial$_{\mathsf{SYNC}}$), and partially due to failure of subsequent reception stages (Denial$_{\mathsf{postSYNC}}$).

We observe a similar attack performance for the MINF and PICNIC receivers (Fig. 2b,c). Both methods were designed with benign interference in mind but, as expected, neither can prevent the attack. In case of the MINF receiver, this is because the min filter cannot remove the cicada signal present in *every* code symbol. Degradation is less pronounced than for Vanilla, but only because of a more conservative back-search threshold (inherent to MINF). In the case of the PICNIC receiver, the attack persists because the cicada signal rarely triggers interference cancelation (the cicada signal does not match the triggering pattern). Denial sets in about 5dB sooner than for Vanilla, and is due mostly to coarse synchronization failure. The reason is PID: As soon as $\mathrm{SNR_M}$ is high enough, samples containing cicada signal peaks rise above the threshold, and are converted to 1. After correlation with the binary template, the output sequence contains a large number (at least N_{pcode}) spurious maxima. These maxima are equal to the maximum corresponding to T's signal. The latter is hence unlikely to be found, and coarse synchronization fails.

This suggests that switching to the intermittent attack can be more effective in achieving degradation against PICNIC. Indeed, under the intermittent attack the correlator output for cicada signal peaks is roughly $\frac{1}{3}$ of the maximum, because the cicada signal is present only in $\frac{1}{3}$ of the preamble symbols. This is too low to interfere with coarse synchronization, but it is sufficient to mislead the back-search algorithm. Fig. 2d confirms this: Degradation prevails over a much wider range of $\mathrm{SNR_M}$. This demonstrates that the attacker can abuse techniques designed for benign interference mitigation to his own ends.

We now show the attack performance as a function of both $\mathrm{SNR_M}$ and $\mathrm{SNR_T}$. For all receivers and attack variants, the pattern is similar (Fig. 3): degradation occurs in the triangle between the lines $\mathrm{SNR_M} = \alpha\mathrm{dB}$ and $\mathrm{SNR_M} = \mathrm{SNR_T} + \beta\mathrm{dB}$ (where α and β depend on the attack type and receiver). Denial occurs above the degradation triangle (Fig. 4), and for low $\mathrm{SNR_T}$ (where the system does not work irrespectively of attacks).

Increasing N_{p} multiplies the number of cicada signal peaks in the back-search window, and hence improves degradation performance: For example, at $\mathrm{SNR_T} = 20dB$ the 2-attack against Vanilla reaches 80% versus 70% reached by the 1-attack. Larger values of N_{p} present a trade-off, best visible for the PICNIC receiver: degradation with a success ratio $> 25\%$ spans wider (in terms of $\mathrm{SNR}_{\mathrm{M}}$) for the 2-attack (Fig. 3c) but the $> 90\%$ degradation spans wider for the 8-attack (Fig. 3d).

Interestingly, in contrast to the other two receivers, PICNIC degradation does not exceed 98%. This is because interference cancelation is triggered occasionally, and when it is, it effectively removes the cicada interference.

Ranging error under degradation. Fig. 5a shows the mean absolute error (MAE) of the ToA under the continuous 1-attack (degraded packets only). All receivers exhibit the same trend: the MAE grows with $\mathrm{SNR}_{\mathrm{M}}$. This is expected, as more cicada signal peaks rise above the back-search threshold. Fig. 5b shows the ToA for the intermittent 2-attack for $\mathrm{SNR}_{\mathrm{T}} = 30\mathrm{dB}$. For PICNIC the MAE levels out around $\mathrm{SNR}_{\mathrm{M}} \approx 35\mathrm{dB}$, whereas for MINF, denial takes over before leveling out can be observed.

All attacks and receivers exhibit similar behavior, with the ToA MAE spanning from 24 to 56ns (ranging error of 7 to 17 meters). This error is lower than could be expected – e.g., with a heavily polluted back-search window, such as under the 8-attack, one could anticipate MAE close to $T_{\mathrm{BS}} = 64\mathrm{ns}$. MAE is low because of the self-interference test, which neutralizes a significant number of cicada peaks.

Clock drift. We verify that clock drift below 40ppm (the largest allowed by IEEE 802.15.4a) does not degrade the attack performance.

C. Transmission Power and Location

Due to the denial effect of the attack, the closer a victim receiver is to the cicada device, the shorter its communication (and ranging) range becomes. Thus, an attacker interested in degradation of service can place the cicada device in a location that victim receivers do not visit, and can transmit with relatively high power. This way, the "pure denial" area close to the cicada device does not affect victim devices. At the same time, a relatively large area is covered with a low-power cicada signal. This increases the number of devices experiencing degradation, while it retains a decent communication range. A more costly alternative is to cover an area with a large number of cicada devices transmitting at low power.

IV. Countermeasures

The simplest way to prevent the degradation attack is to discard fine synchronization and perform ToA estimation based on the strongest multipath component only. This, however, degrades the benign case (no attack) performance in weak NLOS conditions. Furthermore, an alternative *reactive* attack could degrade the ranging performance of even such receivers, both decreasing and increasing the distance. In the reactive attack, the interfering signal is simply the preamble. The attacker begins transmitting after it detects the presence of a benign preamble on the channel. He adjusts the start of transmission such that his preamble arrives tens of nanoseconds before (or after) the benign preamble and tunes the power to overshadow the benign preamble. Although this attack is more sophisticated (it requires a receiver synchronized with a transmitter, and the knowledge of the preamble code), it is still feasible.

Another potential countermeasure is a time-hopping preamble, which avoids the periodicity of the IEEE 802.15.4a-like preambles, exploited by the cicada attack. For this to be effective, the greatest common factor of the time-hopping intervals should be as low as possible. We might also detect and filter out a periodic cicada signal using a Fourier transform.

Finally, in Section III we identified two mechanisms that limit the effectiveness of the attack – modifying them might prevent the attack more effectively. The self-interference test (SIT) could check $y_i > y_{i+\frac{T_{\mathrm{pcode}}}{T_{\mathrm{int}}}} + C$, where C is a noise-based security margin. PICNIC could apply interference cancelation (IC) unconditionally (without detection). A preliminary evaluation reveals that the SIT countermeasure can reduce degradation to below 10%, but not without a noticeable loss in benign case ranging performance; whereas unconditional IC completely prevents degradation and has minor effect on single-user benign case ranging performance. However, such countermeasures might be circumventable by a more sophisticated cicada signal structure. Also, the unconditional IC countermeasure is likely to degrade performance under MUI.

V. Conclusion and Future Work

We have identified a novel attack against IR-UWB that can significantly degrade the ranging service: the cicada attack. We have demonstrated it is effective against energy-detection receivers, even those implementing state-of-the-art MUI mitigation techniques. The attack's applicability is likely much broader, as it exploits a fundamental difficulty in distinguishing the signal of interest from interference. Other receiver architectures are assumably vulnerable, but additional investigations are required to confirm this. Other directions for future work include the development and evaluation of countermeasures, in parallel with an investigation of variants of the attack.

References

[1] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M.Z. Win. Ranging with ultrawide bandwidth signals in multipath environments. *Proceedings of the IEEE*, 97(2), 2009.

[2] I. Guvenc, Z. Sahinoglu, P. Orlik, and H. Arslan. Searchback algorithms for toa estimation in non-coherent low-rate ir-uwb systems. *Wirel. Pers. Commun.*, 48(4), 2009.

[3] Z. Sahinoglu and I. Guvenc. Multiuser interference mitigation in noncoherent uwb ranging via nonlinear filtering. *EURASIP J. Wirel. Commun. Netw.*, 2006.

[4] D. Dardari, A. Giorgetti, and M.Z. Win. Time-of-arrival estimation of uwb signals in the presence of narrowband and wideband interference. In *ICUWB*, 2007.

[5] M. Flury, R. Merz, and J.-Y. Le Boudec. Robust non-coherent timing acquisition in IEEE 802.15.4a IR-UWB networks. In *PIMRC*, 2009.

[6] *IEEE Std 802.15.4a-2007 (Amd. to IEEE Std 802.15.4-2006).*

[7] M. Flury, R. Merz, and J.-Y. Le Boudec. An energy detection receiver robust to multi-user interference for IEEE 802.15.4a networks. In *ICUWB*, 2008.

[8] A.-F. Molisch, K. Balakrishnan, C.-C. Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak. IEEE 802.15.4a channel model - final report, document 04/662r1, 2004.