ResearchGate

See discussions, stats, and author profiles for this publication at: http://www.researchgate.net/publication/261206542

Efficiency analysis of jamming-based countermeasures against malicious timing channel in tactical communications

CONFERENCE PAPER · JANUARY 2013

DOI: 10.1109/ICC.2013.6655188

CITATIONS
2

DOWNLOAD
1

VIEWS
32

4 AUTHORS:

Salvatore d'oro
University of Catania
9 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Laura Galluccio
University of Catania
80 PUBLICATIONS **378** CITATIONS
SEE PROFILE

Giacomo Morabito
University of Catania
150 PUBLICATIONS **2,306** CITATIONS
SEE PROFILE

Sergio Palazzo
University of Catania
149 PUBLICATIONS **977** CITATIONS
SEE PROFILE

Available from: Salvatore d'oro
Retrieved on: 03 August 2015

Efficiency Analysis of Jamming-based Countermeasures against Malicious Timing Channel in Tactical Communications

Salvatore D'Oro, Laura Galluccio, Giacomo Morabito, Sergio Palazzo
Dipartimento di Ingegneria Elettrica, Elettronica e Informatica - University of Catania (Italy)
Email: {name.surname}@dieei.unict.it

***Abstract*—A covert channel is a communication channel that creates a capability to transfer information between entities that are not supposed to communicate. A relevant instance of covert channels is represented by timing channels, where information is encoded in timing between events. Timing channels may result very critical in tactical scenarios where even malicious nodes can communicate in an undisclosed way. Jamming is commonly used to disrupt this kind of threatening wireless covert communications. However jamming, to be effective, should guarantee limited energy consumption. In this paper, an analysis of energy-constrained jamming systems used to attack malicious timing channels is presented. Continuous and reactive jamming systems are discussed in terms of their effect on the achievable covert channel capacity and jammer energy consumption. Also, a simple experimental set up is illustrated and used to identify proper operating points where jamming against malicious timing channels is effective while achieving limited energy consumption.**

I. Introduction

Security and privacy issues are a serious concern in tactical systems. To this purpose one of the most critical communication scenarios to cope with is represented by covert channels communications. A covert channel is defined as "*a communication channel that exists, contrary to design, in a computer system*" [1]. Timing channels are a possible instance of covert channels. In a timing channel the output alphabet is made up of different time values, and coding consists in defining the inter-arrival time between an event and the following one.

Timing channels have been proposed for both wired and wireless scenarios due to the wide range of advantages they offer such as increased transmission capacity (e.g., [2]), reduced energy consumption (e.g., [3],[4]), and ability to hide communications (e.g., [1]). As regards the latter the issue of how to make timing channels robust to malicious attacks has been recently investigated in the literature. For example, Liu et al. [5] explain how to set up a covert timing channel undetectable to common detection systems, such as shape and regularity tests, by properly changing the timing channel transmission pattern. In [6] it has also be shown that the timing channel can still be exploited to transfer the intended information even when a jamming attack is carried out. More in detail, in [6] the authors have proposed an implementation of a timing channel using MICA2 motes and a link-layer overlay which increases security by providing user authentication, error detection/correction and framing. A study on achievable transmission rates of a timing channel under jamming attack in multi-hop networks is presented by Giles et al. [7], showing how jamming reduces the timing channel capacity by introducing random delay on packets delivery times. Although the timing channel is typically used to enhance the network security, it can also be used by malicious users. In fact, as malicious timing channels can be exploited to transmit data covertly without being detected, they represent a real threat, especially in tactical applications. Furthermore, timing channel can be used to send covertly a detonating sequence to activate a *Radio Controlled Improvised Explosive Device* (RCIED), and thus, proper countermeasures need to be found. To this purpose, not surprisingly, jamming can be exploited. In particular, *continuous jamming* can be profitably used to counteract malicious timing channel.

However, continuous jamming requires that nodes are able to jam on all frequencies expected to be used by timing channel, whilst this is feasible only when the energy consumption of the jammer is not a concern and/or the jammer resides on a vehicle. On the contrary, *reactive jamming* can be used when jammers are battery-powered and portable, but does not exhibit the same performance of continuous jamming. In this paper we discuss the impact of different jamming policies on malicious communications over the timing channel. An experimental study on the resilience of timing channels to jamming attacks is presented, which takes the energy consumption of the jammer into account. This study also allows us to identify appropriate operating points where the jamming action on malicious timing channels can be effective while achieving a limited energy consumption.

The paper is organized as follows. In Section II the proposed timing channel framework is illustrated. In Section III an energy efficiency analysis of the jamming applied to timing channel is introduced and then, in Section IV this is used to obtain a numerical estimation of the effectiveness of the jamming-based countermeasures. In Section V the experimental set up is illustrated. Finally, in Section VI conclusions are drawn.

Copyright (c) 2013 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.
The final published paper is available at DOI: 10.1109/ICC.2013.6655188.

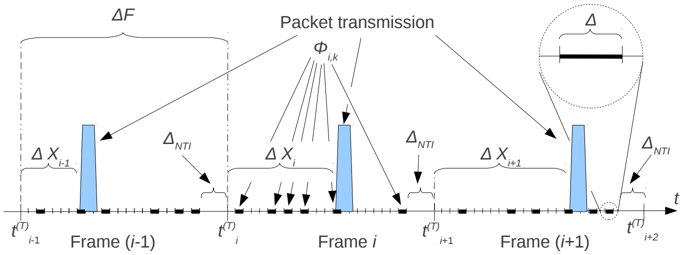

Fig. 1. Communication scheme.

II. System overview

In this section we describe our reference scenario, that is, a communication scheme which employs the timing channel to transfer information.

We assume that the transmitter T and the corresponding receiver R are synchronized, as traditionally assumed in the literature [8]. The communication scheme they use assumes that time is organized into frames of duration ΔF as shown in Figure 1. We call $t_i^{(T)}$ the instant when the i-th time frame begins. In each frame a certain number, say N, of intervals can be distinguished. The set of these N intervals is denoted as $\Phi = [1 \ldots N]$. The duration of each interval is equal to Δ. The parameter Δ characterizes the communication scheme and is assumed to be known by both the transmitter T and the receiver R, and larger than twice the maximum error introduced by the timers. In each frame we denote as *non transmission interval* (NTI) the remaining time interval before the end of a frame. We call Δ_{NTI} the duration of this interval. During the NTI no transmissions can be performed. This is required to avoid that a transmission in the i-th frame can continue in the successive $(i+1)$-th frame. In each frame the transmitter T sends only one packet and starts the transmission in one of the above N intervals, so that the transmitted packet begins and ends within the chosen interval. Furthermore, in order to protect the communication in the timing channel, a simple encryption is provided. To this purpose, the transmitter T and the receiver R share a secret key k. Such a key is utilized to encrypt the communication and filter out transmissions executed by unauthorized transmitters, i.e., potential jammers. In fact, the key k is used at each frame i to identify a subset, $\Phi_{i,k}$, of the intervals within the frame, which depends on both the values of i and k. The transmitter T performs the transmission of the packet only in one of the intervals belonging to $\Phi_{i,k}$. This implies that part of the information sent by the transmitter T can be automatically encoded through the choice of the specific interval belonging to $\Phi_{i,k}$. In order to transfer the packet m_i to the receiver, the transmitter T generates a value ξ_i as follows:

$$\xi_i = f(m_i, i) \mod |\Phi_{i,k}| \tag{1}$$

where $f(\cdot)$ is an appropriate function which returns a value uniformly distributed in the interval $[1, \xi^{(\max)}]$, with $\xi^{(\max)} >> N$. Then the transmitter sets the value X_i equal to the ξ-th element of the set $\Phi_{i,k}$, that is $X_i = [\Phi_{i,k}]_\xi$.

Finally, the transmitter T schedules the beginning of the transmission of the packet during the X_i-th interval of the i-th time frame, whose distance from the beginning of the frame is defined as ΔX_i. The capacity of the transmission scheme employed by T and R is, thus, upper-bounded by $C = \frac{\log_2(|\Phi_{i,k}|)}{\Delta F}$.

III. Efficiency analysis of jamming policies

Jamming is typically used to disrupt data communications between two or more nodes. Jamming consists in transmitting an interfering signal, thus leading to errors and packet corruption. In this section we describe different alternatives for jamming the timing channel. For each of such jamming techniques, we will evaluate the capacity of the timing channel actually established between the transmitter T and the receiver R as a function of the power consumption of the jammer J.

A. Continuous jamming

The simplest way to jam a timing channel is using continuous transmission at a high power level on the entire frequency spectrum in which the communication between T and R is expected. If the transmission power of the jammer J, which we denote as P_J, is sufficiently high, then the RF front-end of the receiver is saturated and it is not possible for R to reconstruct the timing information between the transmissions performed by T. Continuous jamming has been profitably used for military and tactical applications in the context of counteracting radio commanded improvised explosive devices (RCIED). Once the receiver front-end is saturated by the continuous jamming signal, the capacity of the timing channel when there is an active attack executed by a continuous jammer is $C_{CJ}^{(TC)} = 0$; in this case, the average transmission power for the jammer J is equal to the peak transmission power, that is $\bar{P}_{CJ}^{(J)} = P_J$. The applicability of continuous jamming is strongly limited from the very high power consumption implied. In fact, the need for continuously jamming the entire frequency spectrum with a high transmission power level has crucial implications on the jammer operational lifetime.

B. Reactive jamming

A more energy efficient, although less effective, type of jamming is the reactive one. In this case, the jammer J is continuously listening over the wireless channel and, as soon as it detects ongoing radio activity, it generates a jamming signal. Duration of such a disturbing signal is random. Supporting reactive jamming requires the definition of a power threshold P_{th} to distinguish between channel noise and ongoing transmission activity. If the received power estimated by the jammer is higher than the threshold, i.e. $P_{RX} \geq P_{th}$, the jamming signal is sent; otherwise jamming is not activated. As an example, in Figure 2 we show a reactive jamming attack, where we call ΔJ_i the duration of the disturbing signal generated to jam the packet transmitted by T during the i-th frame. As compared to continuous jamming, reactive jamming can be less effective. In fact, the reactive jammer J effectively disturbs the timing channel communication only if the jamming signal transmitted

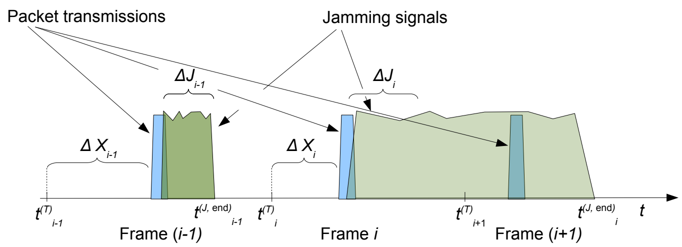

Fig. 2. Reactive jamming attack.

by J as a response to the packet emitted by T compromises the beginning of the subsequent transmission performed by T. More formally, let $j_i(t)$ represent the jamming signal used to disturb the transmission executed by T during the i-th frame; also, let us denote $t_i^{(J,\text{end})}$ as the time instant when the signal $j_i(t)$ ends, i.e.,

$$t_i^{(J,\text{end})} = \min\{t^* : j_i(t) = 0, \ \ \forall t \geq t^*\} \tag{2}$$

In order to have an effective jamming action, the duration of the jamming signal $j_i(t)$ must be such that the following transmission of T during the next $(i+1)$-th frame is compromised. More specifically, the following condition should hold:

$$t_i^{(J,\text{end})} > t_{i+1}^{(T)} + X_{i+1} \cdot \Delta \tag{3}$$

Accordingly, the capacity of the timing channel when reactive jamming is utilized is given by:

$$C_{RJ}^{(TC)} = \frac{1 - p_{RJ}^{(SJ)}}{\Delta F} \log_2(|\Phi_{i,k}|) \tag{4}$$

where $p_{RJ}^{(SJ)}$ represents the probability that a reactive jamming is performed over a timing channel transmission. In calculating $p_{RJ}^{(SJ)}$ we have to consider that the same jamming signal can be extended over different frames. For example, in Figure 2 the signal generated by the jammer J during the i-th frame continues during the $(i+1)$-th frame and fully compromises the reception at R of the packet transmitted during these frames. Accordingly, the information encoded in the timing channel during the $(i+1)$-th frame is lost. It is straightforward to show that the jamming probability $p_{RJ}^{(SJ)}$ can be derived as

$$p_{RJ}^{(SJ)} = \frac{\bar{M}^{(J)}}{1 + \bar{M}^{(J)}} \tag{5}$$

where $\bar{M}^{(J)}$ represents the average number of consecutive transmissions performed by the transmitter T which are disturbed by the same jamming signal. If $M^{(J)}$ is the random variable representing the consecutive transmissions disturbed by the same jamming signal, then the average value $\bar{M}^{(J)}$ is:

$$\begin{aligned} &\bar{M}^{(J)} = \textstyle\sum_{m=1}^{+\infty} m \Pr\{M^{(J)} = m\} = \\ &= \textstyle\sum_{m=1}^{+\infty} m \left(\Pr\{M^{(J)} \geq m\} - \Pr\{M^{(J)} \geq m+1\}\right) \end{aligned} \tag{6}$$

In this expression, the probability $\Pr\{M^{(J)} \geq m\}$ can be calculated as

$$\begin{aligned} &\Pr\{M^{(J)} \geq m\} = \\ &= \tfrac{1}{N^2} \textstyle\sum_{v=1}^{N} \sum_{u=1}^{N} \Pr\left\{\Delta J_i \geq \psi(v,m,u)\right\} \end{aligned} \tag{7}$$

where $\psi(v,m,u) = (N - v + u)\Delta + \Delta_{NTI} + (m-1)\Delta F$ and

- v represents the time interval in which the transmitter T begins its transmission during the i-th frame
- u represents the time interval in which the transmitter T begins its transmission during the $(i+m)$-th frame.

In eq. (7) we assume that T begins its transmission in any time interval, with the same probability. By replacing eq. (7) in eq. (6) and recalling that $\Pr\{\Delta J > \xi\} = [1 - F_{\Delta J}(\xi)]$ where $F_{\Delta J}(\xi)$ is the cumulative distribution function of ΔJ, we obtain

$$\begin{aligned} &\bar{M}^{(J)} = \tfrac{1}{N^2} \textstyle\sum_{m=1}^{+\infty} m \cdot \sum_{v=1}^{N} \sum_{u=1}^{N} F_{\Delta J}\left[(N-v+u)\Delta + \right. \\ &\left. + \Delta_{NTI} + m\Delta F\right] - F_{\Delta J}\left[(N-v+u)\Delta + \Delta_{NTI} + (m-1)\Delta F\right] \end{aligned} \tag{8}$$

In the following we also assume that the duration of the jamming signal ΔJ is distributed exponentially, because this is the distribution that maximizes the jammer unpredictability. Accordingly, by denoting ΔJ^* as the average value of the random variable ΔJ, we obtain

$$\bar{M}^{(J)} = \left[\frac{1 - e^{-\frac{\Delta}{\Delta J^*} N}}{N(1 - e^{-\frac{\Delta}{\Delta J^*}})}\right]^2 \frac{1}{1 - e^{-\frac{\Delta F}{\Delta J^*}}} e^{-\frac{\Delta_{NTI} + \Delta}{\Delta J^*}} \tag{9}$$

The average power consumption for a reactive jammer J can thus be calculated as:

$$\bar{P}_{RJ}^{(J)} = P_J \cdot \frac{\Delta J^*}{\Delta F} \cdot \frac{1}{(1 + \bar{M}^{(J)})} \tag{10}$$

IV. Numerical Results

In this section we present the numerical results obtained by the analysis of the timing channel scenario where a jamming action is performed as discussed above. In particular, both a continuous and a reactive jamming are considered and, in case of reactive jamming, the duration of the jamming signal $\Delta J_i = \Delta J, \ \forall i$ is assumed to be exponentially distributed with an average value ΔJ^*. In both cases we assume that the transmission power is $P_J = 5$ W, which is also the transmission power used by the transmitter T to communicate with the receiver R, and $\Delta F = 100$ ms.

Figure 3 shows $p_{RJ}^{(SJ)}$ calculated in eq. (5) as a function of ΔJ^* for different values of Δ. In case of continuous jamming, which is executed all the time, the jamming probability is 1. It is evident that this technique, as discussed above, is the most effective but it is very costly in terms of energy consumption since the transmitted power is maximum. In case of reactive jamming, $p_{RJ}^{(SJ)}$ obviously increases as we increase the time duration during which jamming is performed. Observe that upon increasing the time duration of the jamming interval we asymptotically converge to the case of continuous jamming. We have also considered the impact of varying the parameter Δ_{NTI} as shown in Figure 4. As Δ_{NTI} increases

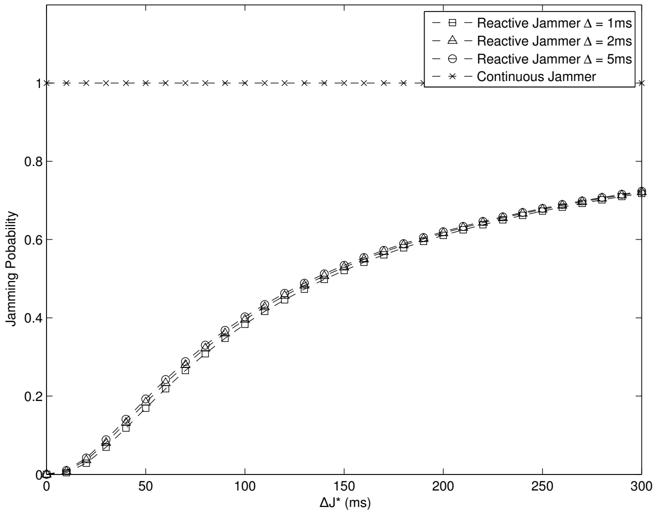

Fig. 3. Jamming probability vs. ΔJ^* for different values of Δ.

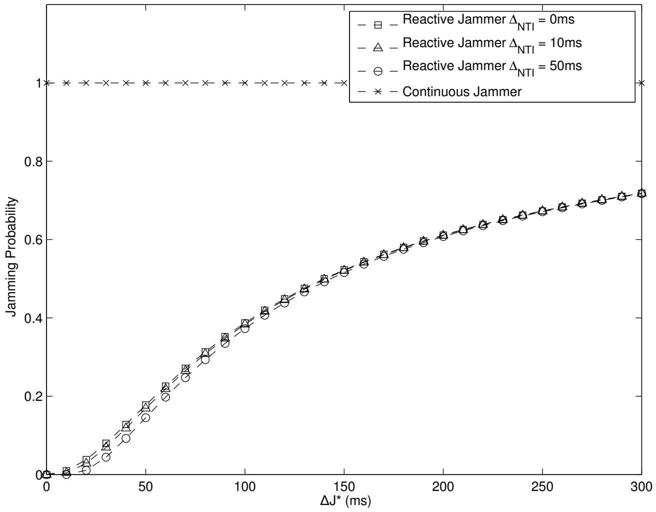

Fig. 4. Jamming probability vs. ΔJ^* for different values of Δ_{NTI}.

and, thus, $\Delta F - \Delta_{NTI}$ decreases, the transmission activity over the timing channel decreases and, consequently, also the jamming probability does. Finally, in Figure 5, the relationship between the jamming probability and the power consumption, normalized to P_J, is presented. As previously discussed, by increasing the jamming probability, the power consumption will increase too. However, considering that in numerous energy-constrained scenarios too costly jamming techniques cannot be utilized, a proper trade-off between power consumption and jamming effectiveness should be achieved. This will be discussed in the next section.

V. Experimental Results

In order to assess the validity of the model proposed in Section III we have set up an experiment which shows how the jamming effectiveness is tightly related to the average power consumption. Our final scope was to verify that the jammer success probability increases when more energy is used, and identify operating regions characterized by a proper trade-off between jamming effectiveness and energy consumption.

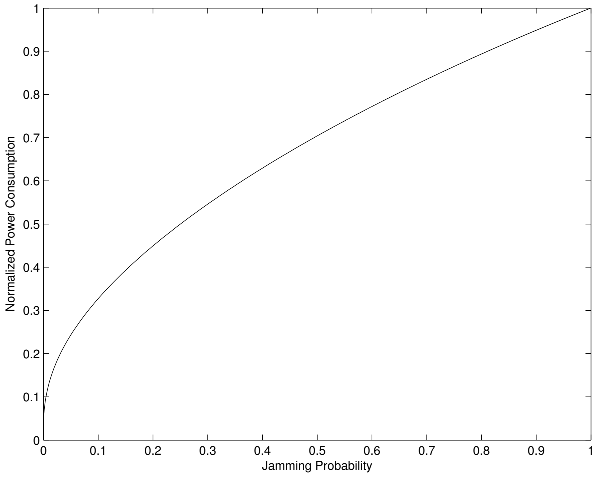

Fig. 5. Jamming probability vs. normalized power consumption.

Symbol	Delay (ms)
00	90
01	140
10	40
11	250

TABLE I
Coding Table

Name	Value	Unit
N	2	N.A.
ΔT	300	ms
ε	20	ms
T_d	600	ms

TABLE II
Parameters

The addressed scenario includes a jammer J, a transmitter T and a receiver R. The transmitter and the receiver communicate through the timing channel. We assume that J, T and R use the same transmission power level P_J. The jammer J aims at disrupting any communication over the timing channel and, to this purpose, is continuously listening on the channel. The jamming is implemented by using a periodic signal $j(t)$ defined as $j(t) = \sum_{n=0}^{\infty} p(t - nT_d)$, where T_d is the repetition period and $p(t)$ is a rectangular pulse of duration ΔJ. We assume that T repeatedly sends the bit sequence $\Psi = \{00011011\}$ to R by exploiting the timing channel. The timing channel employed by both T and R consists in generating packets of duration ΔT and encoding the information of the bit sequence to be transmitted in the inter-arrival time between two following packets, i.e. packet i and packet $i+1$, denoted as Δx_{i+1}.

Figure 6 illustrates the transmission scheme in the experimental set up. The bit sequence Ψ being considered is mapped, using an *N-bits Aggregator*, into symbols of N bits

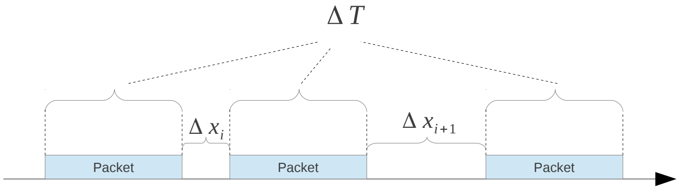

Fig. 6. Experimental set up transmission scheme.

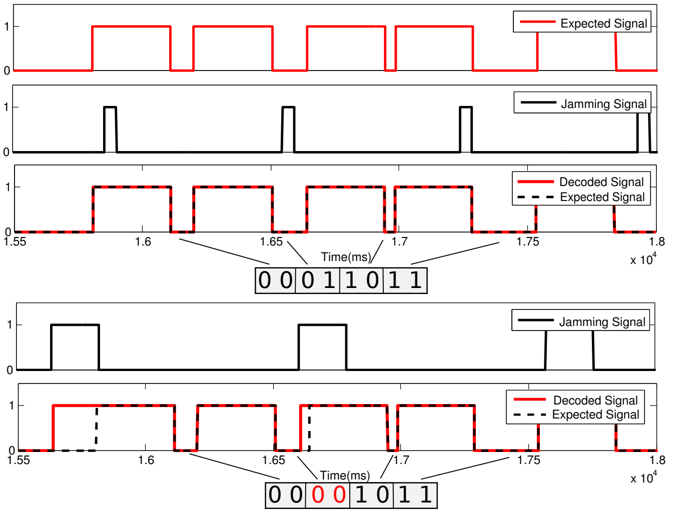

Fig. 7. Jamming performance with ΔJ^*= 40 ms, and 160 ms and packet duration 300 ms.

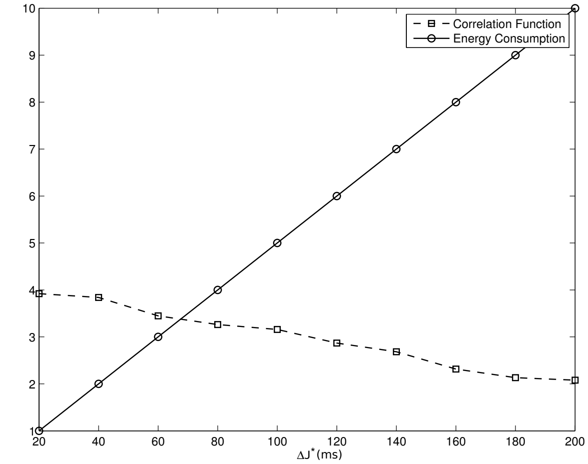

Fig. 8. Correlation between the strings received and expected at the receiver and energy spent by jammer vs. ΔJ^*.

each. Accordingly, $M = 2^N$ is the maximum number of admitted symbols. Each symbol is mapped into the inter-arrival time between two following transmitted packets. This action is performed by the *Delay Encoder*. An example of the adopted coding is shown in Table I. At the reception side, R decodes the received information by using the same coding table employed by T. Considering that both T and J transmit over the same channel, R receives a signal which is given by the superposition of the signals $j(t)$ and $y(t)$ transmitted by J and T, respectively. Accordingly, the signal received by R can be defined as $r(t) = j(t) + y(t) + n(t)$, where $n(t)$ is the white Gaussian noise added by the channel. If we assume that the channel noise is negligible as compared to $j(t) + y(t)$, it follows that $r(t) \approx j(t) + y(t)$. When $r(t)$ is received, R checks if the received power associated to $r(t)$, i.e. $P_{RX} =< |r(t)|^2 >$, is larger than a decision threshold P_{th}; if this condition holds, R sets t_{Start} as the time instant when the condition becomes TRUE, and t_{End} as the time instant when the condition is no longer satisfied. Then R calculates $\Delta T_{RX} = t_{End} - t_{Start}$. To distinguish between jamming pulses transmitted by J and packets transmitted by T, R checks if $\Delta T_{RX} \in [\Delta T - \varepsilon, \Delta T + \varepsilon]$, where ε is a tolerance factor introduced by R to take into account the delay due to the channel. If $\Delta T_{RX} \in [\Delta T - \varepsilon, \Delta T + \varepsilon]$, then R considers that the received signal is a packet transmitted by T, otherwise the signal is assumed to be a jamming signal and R discards it. If neither channel errors occur nor jamming deteriorates the quality of communications, R is able to properly decode the received signal and obtain the sequence Ψ transmitted by T.

The experimental set up has been implemented by using Arduino Uno Rev3 [9] boards, whereas the signal transmission and reception have been performed by employing infrared (IR) interfaces. Table II reports the parameters used in the experimental set up. In Figure 7 we show the effect of jamming on the information transmission when using different values of ΔJ. In particular, the third and fifth plots illustrate how R decodes the bit sequence Ψ when considering the jamming effect for different values of ΔJ^* i.e. $\Delta J^* = 40$ ms (third plot) and $\Delta J^* = 160$ ms (fifth plot). Observe that when ΔJ^* is small, the transmission between T and R is not significantly impacted by the jamming action. On the contrary, as discussed in Section IV, an increase in the jamming pulse duration, leads to the impossibility to support the transmission between T and R, as evident when comparing the signal which is decoded by R and the signal sent by T. As a countereffect, upon increasing ΔJ^*, the jamming effectiveness increases but the power consumption increases as well, so making real applicability of jamming unfeasible. Obviously, if $\Delta J^* \to \infty$ and $T_d \to 0$, then J becomes a continuous jammer and consequently its energy consumption becomes not negligible. Finally, in Figure 8 we show two curves: one is the correlation between the expected bit string and the received string as a function of ΔJ^* and another is the energy spent by the jammer as a function of ΔJ^*. The intersection between the two curves represents the condition in which the jamming mechanism achieves the best performance.

VI. Conclusions

In this paper we have presented a study on the resilience of timing channel malicious communications in case of jamming attacks. In particular, we have analytically estimated the capacity and power consumption for different jamming policies. Also, we have presented an experimental set up aimed at identifying proper operating points where jamming power consumption can be traded-off with timing channel resilience.

References

[1] I. S. Moskowitz and M. H. Kang. Covert Channels — Here to Stay?, *Proc. of COMPASS*, S. Margherita, Italy, Jun.-Jul. 1994.

[2] V. Anantharam and S. Verdú. Bits through queues, *IEEE Trans. on Inf. Theory*, 42(1), Jan. 1996.

[3] G. Morabito. Exploiting the Timing Channel to Increase Energy Efficiency in Wireless Networks, *IEEE Journal on Selected Areas in Communications (JSAC), 29(8)*, Sep. 2011, doi 10.1109/JSAC.2011.110919.

[4] L. Galluccio, G. Morabito, and S. Palazzo. Exploiting timing channel in intra-body sensor networks, *Proc. of IEEE Global Telecommunications Conference (Globecom)*, Dec. 2012.

[5] Y. Liu, et al. Hide and seek in time: robust covert timing channels, *Proc. of ESORICS*, Saint Malo, France, Sep. 2009.

[6] W. Xu, W. Trappe, and Y. Zhang. Anti-jamming Timing Channels for Wireless Networks, *Proc. of ACM WiSec*, Alexandria, VA, Mar.- Apr. 2008.

[7] J. R. Giles and B. Hajek. The Jamming game for Packet Timing Channels, *Proc. of IEEE ISIT*, Sorrento, Italy, Jun. 2000.

[8] S. Cabuk, C. E. Brodley, and C. Shields, IP covert timing channels: design and detection, *Proc. of ACM Comp. and Com. Sec.*, Washington, DC, Oct. 2004.

[9] Arduino, Home Page, http://www.arduino.cc/.