Enabling Authentic Transmissions in WSNs – Turning Jamming against the Attacker

Adam Bachorek, Ivan Martinovic and Jens B. Schmitt
disco | Distributed Computer Systems Lab
University of Kaiserslautern, Germany
{bachorek, martinovic, jschmitt}@cs.uni-kl.de

Abstract—**Traditional methods for message authentication are based on the cryptographic verification of received data using some sort of a shared secret. While this task is not critical for traditional networks, Wireless Sensor Networks (WSNs) may pay a high price for the gained protection – sensor nodes are forced to invest their already scarce resources in receiving a message and executing cryptographic computations, only to discard the message afterwards in case of a failed authentication.**

This work introduces a different, crypto-free approach for enabling authenticated communication by leveraging peculiarities of wireless communication, in particular its broadcast nature and the feasibility of channel capacity jamming. Instead of receiving and then verifying transmitted data, sensor nodes are prevented from receiving fake data at all. This is achieved by coupling physical characteristics of signal propagation with legitimate transmissions. Such a coupling enables the detection and invalidation of impersonation attacks by using short jamming pulses emitted by surrounding WSN nodes. We justify this concept by designing a novel communication protocol explicitly integrating the jamming feature, and analyze factors which impact the efficiency of successful jamming, such as the frame length, transmission timing accuracy, and various other issues identified through extensive empirical measurements.

I. Introduction

The current evolution of communication networks towards ubiquitous computing platforms enabling the vision of ambient intelligence becomes manifest in present-day WSNs. These are autonomous networks consisting of microcomputers (called motes) with sensor capabilities allowing for versatile functionality. WSN applications are envisioned to witness an immense growth in popularity for, i.a., environmental monitoring, emergency response, home control and automation [1], [2]. However, the susceptibility of motes to resource impoverishment due to their wireless and miniaturized nature has also revealed many issues and challenges especially in the context of security provisioning [3]. Within the scope of hitherto research endeavors on wireless network security, particularly cryptography-based approaches have been proposed making high demands on hardware resources. Particularly, Sybil attacks constitute a severe security problem which has withstood a non-cryptographic and universally applicable solution as yet. In general, the intention behind an impersonation attack is to use stolen identities from authentic network participants in order to masquerade the hostile objective of injecting malicious data into the network [4]. Some detection and defense strategies have already been proposed against such authentication-based attacks. However, the most promising strategies still rely on cryptographic principles [5]. Furthermore, WSNs are particularly vulnerable to radio channel jamming attacks a categorical review of which along with corresponding detection and defense strategies is provided in [6]. The feasibility and effectiveness of jamming attacks launched using WSN motes have been examined in [7].

The novel approach we propose in this work is to turn jamming against the impersonation attacker in order to enable authentic transmissions in WSNs. In this spirit, central to our contributions is the development of an inherently secure communication protocol which withstands impersonation attacks while fundamentally doing without the need for cryptography. On this note, the remainder of this work is organized as follows. Section II introduces the conceptual nuts and bolts of the novel communication approach in question. Section III provides a concise overview of the methodology applied in empirical measurements and the analysis of results which have been accomplished in the context of a real-world implementation. Concluding, Section IV summarizes the contributions with respect to the findings of this work along with future directions for the considered research topic.

II. Turning jamming against the attacker

Ever since WSNs have emerged suffering from limited computational capabilities, poor energy-conservation methods, and their wireless nature which renders them particularly vulnerable to authentication-based attacks, the need for a novel crypto-free security solution has arisen. In order to substantiate the usefulness of such an approach in a real-world implementation, a concrete WSN application area, which is building automation and control, shall be taken into consideration. WSN-based automation systems for households or manufacturing facilities are typically utilized for, i.a., regulation of the cooling system, adjustment of light intensity or compensation of pressure or oxygen deficiencies. These tasks are based upon the values of environmental phenomena, e.g. temperature, light intensity or pressure, as measured by motes. However, while the exposure of transmitted sensor data for this kind of operations is rather uncritical, their hostile manipulation might lead to disastrous consequences. Obviously, the sore spot of unauthenticated communication is the fact that adversaries are easily able to inject tampered messages on behalf of authentic motes making the controlling entities draw improper conclusions. Likely situations where the injection of impersonated data indicating, e.g., a constant room temperature while actually a fire is about to break out, which would otherwise trigger the system to raise an alarm, makes security-related countermeasures critical to such systems. In this context, our proposal focuses mainly on message authenticity, but, in contrast to previously proposed solutions relying on cryptographic keys to allow for digital signatures, merely takes advantage of peculiarities of wireless communication. Our novel approach of turning jamming against the attacker, henceforth referred to as *Jamming Guardian Concept (JGC)*, involves a set of principles including the employment of a bipartite communication scheme as the cornerstone for a sophisticated yet straightforward guarding mechanism based upon a probabilistic rule for a special mode of operation.

A. Bipartite Communication

The bipartite communication scheme constitutes the initial prerequisite for enabling authentic transmissions in WSNs. The communication pattern is bipartite in that, in each transmission cycle, it includes an additional frame called *Data Follows Notification (DFN)* which is used by a sender to announce a subsequent transmission of a *Data Frame (DATA)* at the destination receiver. Consequently, a single transmission cycle implies a dedicated inter-frame arrival time between the transmission of a DFN frame and the timed transmission of a DATA frame. In this context, the only required mutual basis which both frame types are defined to share, in order to actually be considered a unit, are the address identifiers. That is, a preferably small DFN frame shall merely incorporate the header and footer of the *MAC Protocol Data Unit (MPDU)* for addressing and frame check purposes, respectively.

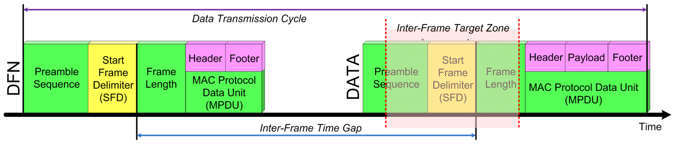


Figure 1. Time separation of DFN and DATA frame in a single data transmission cycle determined by the inter-frame time gap. A DATA frame arriving at the destination receiver is accepted if and only if its SFD is received within the inter-frame target zone and it has previously been announced by a corresponding DFN frame with a similar received signal strength.

As for the time gap parameter defining the duration between the arrival of the *Start Frame Delimiter (SFD)* of a DFN frame and the SFD of the corresponding DATA frame at the receiver, it may be statically set for all subsequent transmissions or dynamically announced in each preceding DFN frame. Either way, both communication participants are supposed to be aware of the point in time the actual DATA frame transmission will be issued. This necessitates a certain level of timing accuracy which, however, cannot be taken for granted on most WSN platforms. Therefore, the introduction of a certain tolerance level becomes necessary. On this note, the tolerance level is defined to be the time difference between the center and the upper or lower bound of the inter-frame target zone which, in turn, constitutes the time window during which a previously announced DATA frame is expected to arrive so as to be accepted by the destination receiver or discarded otherwise (see Figure 1).

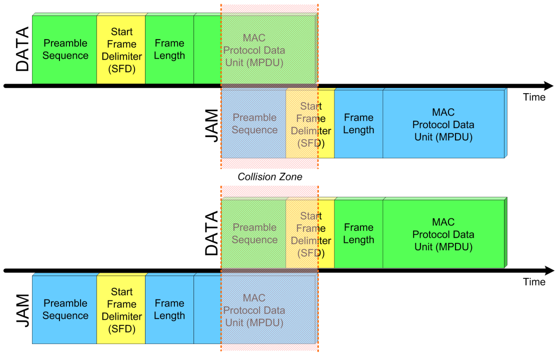

DATA
Preamble Sequence
Start Frame Delimiter (SFD)
Frame Length
MAC Protocol Data Unit (MPDU)
Time
JAM
Preamble Sequence
Start Frame Delimiter (SFD)
Frame Length
MAC Protocol Data Unit (MPDU)
Collision Zone
DATA
Preamble Sequence
Start Frame Delimiter (SFD)
Frame Length
MAC Protocol Data Unit (MPDU)
Time
JAM
Preamble Sequence
Start Frame Delimiter (SFD)
Frame Length
MAC Protocol Data Unit (MPDU)

Figure 2. Frame collision scenarios when synchronization and physical layer header of a DATA frame are completely received before a JAM frame arrives at the receiver (upper) and vice versa (lower). If the difference in received signal strength of both frames is above the *Signal-to-Noise Ratio (SNR)* threshold in favor of the DATA frame, it will be received correctly. Otherwise, the jamming is said to be successful. The lower case depicts the reverse situation where the receiver has already synchronized to the JAM frame resulting in a successful jamming no matter what signal strength the DATA frame is received with.

The rationale behind the bipartite communication pattern is that by means of the customizable inter-frame arrival time, receiving nodes can be provided with enough time to detect an ongoing impersonation attack on the basis of the initially transmitted DFN frame. Also, what is even more important, receivers are able to make arrangements for attack counteraction in advance, since the actual malicious data contents will reach the destination not before the DATA frame arrives. That is to say, the detection of an impersonation attack basically requires the inspection of the source address field of the frame header. To this end, an inspecting entity has to receive the frame completely to check for transmission errors prior to being able to draw any conclusions with respect to attack detection. In fact, this renders any prophylactic attack counteraction difficult if not infeasible as far as traditional single-frame transmission cycles are concerned. This is due to the broadcast nature of wireless communication in that a transmitted frame is more or less simultaneously received as by the attacked mote so by potential guarding motes. Consequently, an impersonated single-cycle DATA frame could not be prevented from being injected into the network once it has been emitted completely.

B. Guarding by Jamming

The *Guarding by Jamming* principle leverages the means provided by the bipartite communication pattern for the actual execution of a countermeasure against impersonation attacks. For this purpose, the main aspect is the controlled utilization of channel jamming by network participants (henceforth called *guardians*) which aim at mutually protecting each other against the malicious injection of impersonated data. Yet, in order to take advantage of jamming in the first place, a guardian has to be aware of two important factors, transmission timing accuracy and signal strength peculiarities.

Algorithm 1 JGC - Receiver

```
INPUT:
inter-frame time gap $t_{IF}$, time gap tolerance $\Delta t_{IF}$,
guardian parameter set $N_{guard}$, signal-to-noise threshold $snr_{thres}$

STEPS: on detecting frame synchronization $F_{SFD}$
store $t_F \leftarrow$ timestamp($F_{SFD}$)
if ( $F_{expected} = DFN$ )
    receive $F_{MPDU}$
    if ( type($F_{MPDU}$) $= DFN$ )
        if ( destID($F_{MPDU}$) $=$ ownID )
            if ( srcID( $F_{MPDU}$) $\in$ authorizedNeighborsList )
                store $t_{DFN} \leftarrow t_F$
                store $srcID_{DFN} \leftarrow$ srcID($F_{MPDU}$)
                store $rssi_{DFN} \leftarrow$rssi($F_{MPDU}$)
                store $F_{expected} \leftarrow DATA$
        else if ( srcID($F_{MPDU}$) $\notin$ jammingExclusionList )
                store $Prob_{attack} \leftarrow$ guardianRule($N_{guard}$)
                send $F_{JAM}$ after $(t_F + t_{IF})$ with $Prob_{attack}$
else if ( $F_{expected} = DATA$ )
        store $\Delta t \leftarrow t_F - t_{DFN}$
        if ( $t_{IF} - \Delta t_{IF} \leq \Delta t \leq t_{IF} + \Delta t_{IF}$ )
            receive $F_{MPDU}$
            if ( type($F_{MPDU}$) $= DATA$
                    $\wedge$ destID($F_{MPDU}$) $=$ ownID
                    $\wedge$ srcID($F_{MPDU}$) $= srcID_{DFN}$
                    $\wedge$ ( rssi($F_{MPDU}$) - $rssi_{DFN}$ ) < $snr_{thres}$)
                accept $F_{MPDU}$
            else discard $F_{MPDU}$
        else if ( $\Delta t > t_{IF} + \Delta t_{IF}$ )
                store $F_{expected} \leftarrow DFN$
```

In this context, there are two fundamental approaches for a guardian to provoke a collision of frames on the wireless medium. The first approach relies on the *Received Signal Strength (RSS)* of transmitted frames at the destination. Central to this approach is the circumstance that the higher the strength of a received signal, the more likely it can be filtered and interpreted correctly or, what is even more important for successful jamming, the more likely it can drown out other concurrently propagating signals rendering them unreadable for potential receivers. Hence, a guardian is supposed to use a sufficiently high output power for a *Jamming Frame (JAM)* to increase the chance of drowning out an impersonated DATA frame. The other approach is based on the default operating mode of common radio receiver hardware – a frame which the receiving entity has already synchronized to is attempted to be completely received before another receipt cycle can be started. Thus, a guardian ought to schedule its JAM frame early enough such that its transmission footprint including the frame header reaches the destination receiver prior to the arrival of the DATA frame and that both frame transmission footprints overlap, at least temporarily. Figure 2 illustrates the considered collision scenarios. Comparing both approaches, the latter is obviously more energy-efficient since a high transmission power is not crucial for a successful jamming. However, it must be considered that a premature arrival of a JAM frame before the inter-frame target zone inevitably results in a premature frame drop in favor of an ensuing and possibly impersonated DATA frame. Therefore, a balanced combination of both approaches appears to be the proper way to go.

C. Guardian Rule

The *Guardian Rule* complements the JGC approach representing the means by which guardians are able to estimate the probability for an impersonation attack and, thus, for the application of jamming as attack counteraction. The general idea behind the Guardian Rule is that the reception of a DFN frame shall always be considered a potential initiation of an impersonation attack. The actual probability is defined to be estimated in advance by utilizing a probabilistic formula based upon measurable and/or adjustable parameters. These parameters constitute the leveraging means by which the probability for jamming can be controlled. For instance, the Guardian Rule formula might consider RSS fluctuations of frames allegedly sent by the same mote and determine the attack probability on the basis of the deviation from a user-defined RSS threshold. For the time being, we abstract from a concrete Guardian Rule formula and parameters to be utilized since this would go beyond the scope of this work. Furthermore, this allows for leaving enough room for adequate proposals with respect to different implementations focusing on the trade-off between energy-efficiency and provided security level.

D. Modus Operandi

Summarizing the basic mode of operation of the JGC, Algorithm 1 describes the receiver side of the communication protocol a mote must implement. Central to the algorithm are the input parameters which all network participants must be endued with prior to being prepared for authenticity-aware communication. This shall be subject to any kind of preceding neighbor discovery and initialization protocol. On each detection of a valid frame synchronization, a mote stores the SFD arrival time for later reference. When expecting a DFN frame, the remainder of the detected frame can be completely received since no timing requirements have to be met. After frame type verification, the destined receiver further checks whether it is originated from an authorized neighbor. If so, all announcement-related information is buffered for verification purposes of the subsequently expected DATA frame. A guardian receiver, on its part, merely inspects the source address and if it identifies a neighbor which is not excluded from being guarded, the DFN frame is considered a potentially impersonated frame sent by an illegitimate network intruder trying to inject malicious data. In this case, a JAM transmission is issued after the defined inter-frame time gap with a probability that results from the Guardian Rule estimation. In contrast, the reception of an already announced DATA frame necessitates the verification of the inter-frame timing constraint. A frame reception beyond the time gap tolerance bounds either indicates a premature frame transmission or the end of the currently valid DFN-DATA transmission cycle, which, either way, results in an immediate termination of the reception process. However, in case the SFD arrives on time as scheduled, the receiver preliminarily receives the frame remainder and verifies if it has been announced correctly according to the addressing and RSS criteria. Only if this test is passed, the DATA frame is accepted or discarded otherwise.

III. Implementation

The major objective behind the JGC is to prevent adversaries from injecting fake data on behalf of authentic network entities by leveraging a bipartite communication scheme in conjunction with a probabilistic jamming rule implemented by all involved WSN nodes. Hence, it is essential to figure out in how far commonly deployed motes, such as MICAz running TinyOS, are capable of meeting the corresponding requirements. A concise overview of the applied empirical methodology along with obtained results is given below.

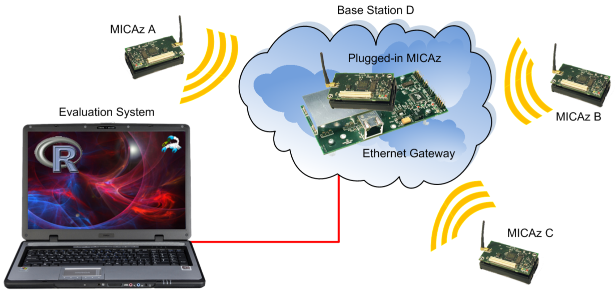


Figure 3. Test bed setup for TinyOS-2.0.1/MICAz platform evaluation in view of JGC compliance. A Linux-based laptop and an Ethernet Gateway module in conjunction with a MICAz mote acting as a packet sniffer serve for network traffic monitoring, measurement control and result evaluation purposes. Considering the impact of signal strength peculiarities, A through C are placed in a random fashion with similar distances to D of up to $1\,m$.

All empirical measurements have been conducted in a stationary in-building environment with typical furnishing not obstructing the line of sight of the involved motes (see Figure 3). For the sake of unambiguous measurement results, no frame acknowledgments have been used and the clear channel assessment mechanism provided by the transceiver hardware through TinyOS has been turned off [8].

A. *Timing Accuracy*

At first, the capabilities of the evaluated platform for accurate timing provisioning had to be revealed when it comes to radio transmissions of bipartite frame sequences. To this end, varying inter-frame time gaps against frame sizes and different operating system settings have been analyzed. TinyOS supports two timer abstractions referred to as Timer (ms precision) and Alarm (µs precision), the operations of which are handled synchronously within task and asynchronously within interrupt context, respectively. Apart from the default parameter configuration for each abstraction, we examined a tuned version of the Alarm configuration being further enhanced by reducing the transmission turnaround time of the radio transceiver along with modifying the *Serial Peripheral Interface (SPI)* chunk size, i.e. number of bytes which are atomically transferred between the microcontroller and radio transceiver [9]. Figure 4 depicts the median timing discrepancy encountered when scheduling an inter-frame time gap of $5\,ms$ while using the different timer abstraction settings. Obviously, the Timer abstraction performs best as far as the nominal time gap overhead of up to $-1251.5\,\mu s$ at a MPDU size of $127\,byte$ is concerned. However, its enormous standard deviation of $\sigma_\mu \approx 260\,\mu s$ averaged over the entire result set points out its inconsistency and thus inapplicability in terms of time-critical communication. Comparably, both Alarm abstraction settings do not produce relief in view of time gap deviation, albeit a mean standard deviation of $\sigma_\mu \approx 31\,\mu s$ for the default and $\sigma_\mu \approx 15\,\mu s$ for the enhanced Alarm setting, respectively, proves their reasonable stability.

In the course of isolating potential factors for the timing overhead, various measurements have been conducted, e.g. Figure 5 (a) depicts the measurement results for different inter-frame time gap values. Apparently, the measured timing overhead highly depends on the MPDU size while being largely independent from the time gap. This is reflected in a maximal standard error of less than $5\,\mu s$ for the entire result set as observed for a $99\,\%$ confidence level. The resulting confidence intervals largely overlap indicating a sufficiently high estimation quality as for the actual population mean. In summary, Figure 5 (b) depicts a breakdown of all major factors which contribute to the timing inaccuracy of the evaluated platform. These factors include the transmission turnaround time of $128\,\mu s$ required for transceiver recalibration, the transmission time required to emit the synchronization header of $5\,byte$ at a data rate of $250\,kbps$ [9] along with an approximately constant delay of about $186\,\mu s$ on average which is considered the in-system processing delay. In fact, the emulation of in-system SPI data transfer, i.e. the copying transaction of data fragments from the microcontroller memory to the transmission buffer of the transceiver via the SPI, has been identified to be the residual MPDU-dependent delay constituting the dominant impact on the encountered timing inaccuracy.

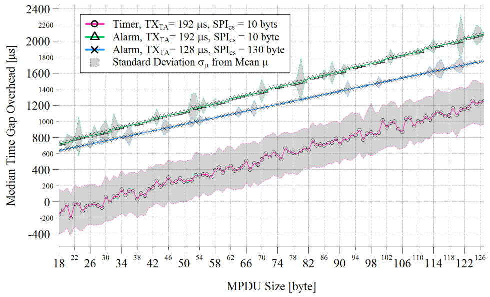
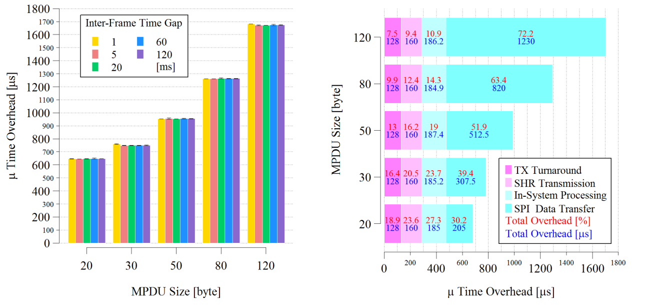


Figure 4. For any TinyOS timer abstraction setting, the median timing accuracy decreases with increasing frame size in an approximately linear fashion whereas its standard deviation from the mean remains rather stable.

In order to countervail the deviation phenomena identified, a straight-forward timing correction mechanism has been developed which adapts the start of radio transmissions on the basis of the scheduled data size [10]. Further empirical results reveal the actual capability of the enhanced evaluation platform to adhere to a preferably small inter-frame target zone defining the tolerance bounds for successful bipartite frame transmissions. Figure 6 depicts the cumulative frequency distribution of the measured differences between the frame arrival times for DFN-DATA and DFN-JAM sequences, respectively. More than $98\,\%$ of the samples gather around a time window bounded by a tolerance value of $\Delta t_{IF} = 79\,\mu s$ with respect to a targeted inter-frame time gap of $t_{IF} = 5\,ms$, whereas more than $50\,\%$ thereof even constitute a perfectly scheduled bipartite transmission as indicated by a zero-deviation.



(a) (b)

Figure 5. (a) Independence of time overhead from the selected time gap value may be considered statistically certain. (b) Breakdown of factors influencing timing inaccuracy reveals the dominant role of in-system data transfer.

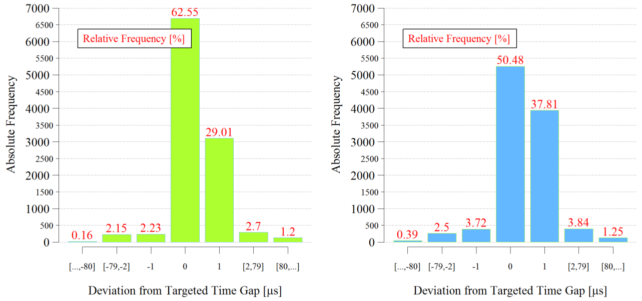
Further results of measurements conducted focusing on signal strength volatility, which cannot be dwelt on in detail due to space limitations, substantiate that a tight time coupling between two consecutively transmitted frames is a vital means to cope with RSS fluctuations [10]. It has been empirically shown that a shorter inter-frame time gap implies a smaller difference in the RSS. Under increased environmental dynamics being artificially created, a time gap of $5\,ms$ has been shown to imply a value correlation for the RSS of $96.6\,\%$ in contrast to, e.g., $77.9\,\%$ for a time gap of $100\,ms$. Therefore, an inter-frame time gap of $5\,ms$ can be considered an adequate trade-off between a sufficiently high robustness against increased dynamics and a low impact on the sending data rate.

Summing up, it can be stated that the employed timing correction technique in conjunction with proper system settings enables the evaluated platform to provide a reliable timing precision for bipartite frame transmissions in the order of μs.

B. Jamming Capability

At last, the actual capabilities of the evaluated platform for implementing the guarding mechanism, i.e. systematic channel jamming, have been examined. Jamming is a common approach used by adversaries to disturb wireless communication. In the context of our novel approach, a guardian mote is envisaged to harness this attacker weapon in order to protect its neighbors against injections of impersonated data by intentionally inducing controlled signal interferences on the wireless medium. Particularly, timing accuracy and signal strength peculiarities have been identified as crucial factors for the applicability of jamming as the means by which authenticated communication is made possible. The results of empirical measurements are summarized in Figure 7 shedding light on the effectiveness of the *guarding by jamming* feature.

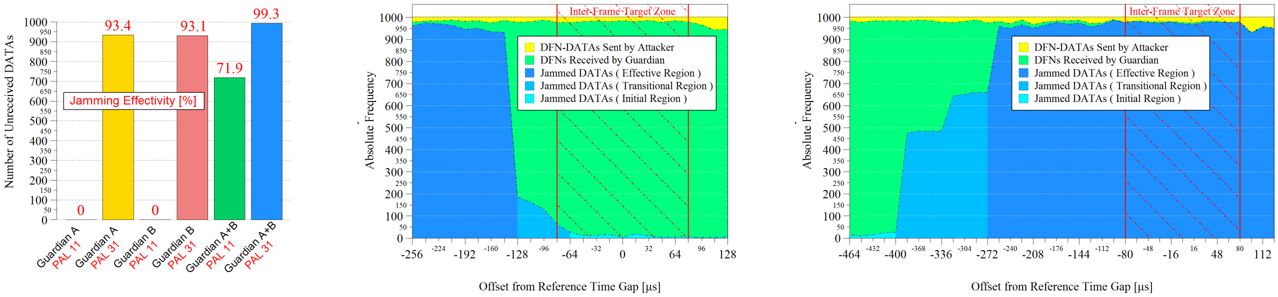
Expectedly, a single MICAz mote is not able to prevent any impersonated DATA frame from being injected as long as the jamming signal strength is significantly lower than the RSS for the DATA frames at the attacked destination node (see Figure 7 (a)). However, as soon as the *Power Amplifier Levels (PALs)* are swapped and the JAM frames completely drown out the DATA frame signals, the injection ratio of the emulated attacker drastically declines. Not surprisingly, an even higher jamming rate of $99.3\,\%$ can be observed when both guardians are involved in the protection process using the maximal PAL 31 simultaneously which is due to the cumulation effect increasing the probability for frame collisions. A rather curious observation is the fact that the cumulated noise as created by two jamming guardians applying PAL 11 already suffice to approximate the RSS of a transmitter which uses PAL 31 with a probability of $71,9\,\%$. However, this is a rather uncommon case induced by obviously strong shadowing effects together with the convenient proximity of the involved motes.



(a) DFN-DATA (b) DFN-JAM

Figure 6. By accumulating the dispersed deviation samples into a coherent number of histogram cells, the high timing precision of the enhanced evaluated platform in terms of bipartite transmissions becomes evident.

Further experiments have been performed providing a more detailed view of the guarding process and emphasizing the importance of timing precision and PAL settings in terms of a trade-off between guarding effectivity and energy efficiency. In this context, the JAM-DATA time gap offset from the default inter-frame time gap of $5\,ms$ is gradually shifted while the DFN-DATA time gap remains unchanged. According to Subsection II-B, Figure 7 (b) depicts the expected jammin effectivity results when a single guardian mote is using a significantly lower output power (PAL 11) than the attacker mote (PAL 31). At first, the jamming effectivity remains well below a maximal rate of $2.7\,\%$ in the ineffective region. This is due to the fact that the DATA transmission footprint already begins at about $80\,\mu s$ before the inter-frame target zone. This circumstance becomes more apparent when considering its further developing which moderately increases to $\mu \approx 29.5\,\%$ on average within the transitional region and then drastically escalates to a value of $93.1\,\%$ reflecting the situation when the SFD of a JAM frame is completely received before the first preamble byte of the DATA frame arrives at the attacked destination. Hereupon, the jamming effectivity levels off at $\mu \approx 95.7\,\%$ as for the value range visualized by the effective region. Figure 7 (c) depicts the jamming effectivity results of the complementary approach for energy saving purposes by minimizing the size of the JAM frame while using PAL 31. In



(a) (b) (c)

Figure 7. (a) Using a maximized JAM/DATA frame size of 133 $byte$, an attack resistance ratio of 93 % for a single guardian and even 99 % can be achieved when two jamming guardians are involved in the protection process. (b) A guardian is able to prevent an attacker from injecting fake DATA frames even if its transmission power is inferior to its adversarial counterpart, provided that the receiver synchronizes to the JAM frame prior to the arrival of the DATA frame synchronization part and that both transmission footprints overlap within or preferably beyond the inter-frame target-zone. (c) Minimizing the JAM frame size to 7 $byte$, an average jamming effectivity of 97 % can still be achieved as long as the jamming signal footprint overlaps with DATA frame transmissions.

line with expectations as per Subsection II-B, the attacker is not able to inject almost any DATA frames within the effective region except for those which are announced by DFN frames not received by the guardian. This holds true as long as the time gap offset is not set below $\Delta t_{ref} = -272\,\mu s$ which constitutes the situation when the footprint of a JAM frame transmission gradually shortens and becomes insufficiently long to interfere with DATA frames by covering a correspondingly wide region within the inter-frame target zone.

IV. Conclusion

Since cryptography-based add-on solutions for security provisioning are not necessarily suitable for WSNs due to resource restrictions of motes, this work has introduced a novel approach for authentic transmissions in WSNs by leveraging peculiarities of wireless communication and the feasibility of channel capacity jamming. The promising capabilities of present-day WSN platforms, such as TinyOS running on MICAz, have been shown to be sufficiently mature for an appropriate implementation of the proposed inherently secure communication approach. Applying proper system settings in conjunction with a straightforward timing correction mechanism enables the evaluated platform to reliably provide a timing precision in the order of microseconds with a receipt accuracy of more than 98 % when considering an inter-frame time gap tolerance of 79 μs. Furthermore, it has been substantiated that time coupling is a vital means by which inter-frame signal strength fluctuations can be coped with, in that a shorter inter-frame time gap of 5 ms renders the novel JGC approach less vulnerable to environmental dynamics. At last, empirical measurements have evidently proven the viability of channel jamming for impersonation resistance purposes. A successful jamming ratio of more than 99 % on average can already be achieved with two guardian motes involved in the protection process. Moreover, a single guardian has been shown to achieve an average jamming effectivity of more than 95 % irrespective of whether it is inferior in terms of the signal strength compared to its adversarial counterpart or when using a minimal 7 $byte$ jamming frame as another energy saving measure. After all, beside the simplicity in terms of implementation and effectivity in terms of impersonation attack resistance, another edge of this novel approach over previous proposals is its flexible energy saving potential due to the probabilistic nature of the *guarding by jamming* mechanism.

Our future work will include a simulative evaluation of JGC performance in adequately realistic scenarios. In the scope of further investigation, jamming efficiency in terms of energy consumption shall be opposed to the aspired security level. In this context, a concrete *Guardian Rule* implementation based upon signal strength measurements and a probabilistic formula for the inference of jamming decisions will be focused on.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 38, pp. 393-422, March 2002.

[2] F. L. Lewis, "Wireless sensor networks," in *Smart Environments: Technologies, Protocols and Applications*, pp. 11-46, John Wiley & Sons, Inc., January 2005.

[3] A. Perrig, J. A. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, pp. 53-57, June 2004.

[4] J. R. Douceur, "The sybil attack," in *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02)*, March 2002.

[5] J. Newsome, E. Shi, D. X. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN '04)*, pp. 259-268, April 2004.

[6] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, vol. 20, pp. 41-47, May 2006.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*, pp. 46-57, May 2005.

[8] P. A. Levis, "Tinyos: An open operating system for wireless sensor networks," in *Proceedings of the 7th International Conference on Mobile Data Management (MDM '06)*, May 2006.

[9] Texas Instruments Incorporated (http://www.ti.com), *Chipcon CC2420 - 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver*, March 2007.

[10] A. Bachorek, "Design and evaluation of a probabilistic approach against impersonation attacks in wireless sensor networks," Diploma thesis, University of Kaiserslautern, December 2007.