Firewalling Wireless Sensor Networks: Security by Wireless

Ivan Martinovic*, Nicos Gollan, and Jens B. Schmitt

disco — distributed computer systems lab
University of Kaiserslautern, Germany
{martinovic,gollan,jschmitt}@informatik.uni-kl.de

***Abstract*—Networked sensors and actuators for purposes from production monitoring and control to home automation are in increasing demand. Until recently, the main focus laid on wired systems, although their deployment requires careful planning and expensive infrastructure that may be difficult to install or modify. Hence, solutions based on wireless sensor networks (WSNs) are gaining popularity to reduce cost and simplify installation. Clearly, one of the key issues rising from the switch to wireless communication lies in security; while an air gap is among the most effective security measures in wired networks, wireless communication is not as easy to isolate from attack.**

In this paper, we propose a system leveraging the peculiarities of the wireless medium, such as the broadcast nature of wireless communication and the unpredictability of indoor signal propagation to achieve effective protection against attacks based on the injection of fake data. Using a real-world WSN deployment and a realistic implementation of an attacker, we analyze this protection scheme and demonstrate that neither position change, transmission power manipulation, nor complete knowledge of wireless parameters can help an attacker to successfully attack the network. As a result, this work demonstrates how the chaotic nature of radio communication, which is often considered a disadvantage in regard to security objectives, can be used to enhance protection and support implementation of lightweight security mechanisms.

***Index Terms*—Wireless Sensor Networks, Security, Authentication, Implementation, Measurements**

I. Introduction

Consisting of sensors for measuring temperature, pressure, air humidity and other environmental conditions, wireless sensor networks (WSN) provide means for various applications to increase comfort and security within private and public residences. By accumulating data of many sensors, a sophisticated system capable of triggering complex application-specific tasks can promptly react to environmental changes, for example, fire, water or gas leakage, and other origins of catastrophes can be detected and countermeasures promptly initiated (e.g., the room airing if gas leakage is detected, closing the water valve to prevent further flooding, or calling emergency services in case of human injuries). Hence, residential monitoring is among the most important emerging applications for WSN.

However, shifting such critical decisions to an automated system increases the importance of its security. By abusing the broadcast nature of wireless communication, an attacker could easily impersonate sensor nodes and inject fake sensor data into a WSN without even being physically present inside the residence. Continuous aggregation of fake data may lead the system to wrong decisions and provide vectors for more sophisticated attacks, e.g., sending fake packets to emulate gas leakage and initiate room airing may be exploited for physical intrusion.

Traditionally, security in computer networks has multiple objectives and attempts to equally satisfy authentication, confidentiality, and integrity goals of transmitted data. When following such "one size fits all" approaches, the cost of key exchange, identity verification, and data encryption puts high demands on protocol complexity, its implementation, and computational power. While such requirements can usually be met by the relatively high-performance devices in common computer networks, in a WSN the security costs become more tangible through decreased battery life and various vulnerabilities from depletion of computation or memory resources. Another important factor influencing the design of security concepts for WSNs is the paradigm of *data-centric networking*. Rather than ensuring on the identity of a data provider, a WSN is more focused on data itself, meaning that information describing environmental conditions is more important than the device which reports it. Hence, instead of paying a high price for identity authentication, the security objective within a WSN should be to guarantee that the decisions made by the system are based on data aggregated from a legitimate WSN, corresponding to real environmental conditions.

II. Security by Wireless – Using Wireless Properties to Increase Security

A. Wireless Propagation: Confusion and Diffusion

Every cryptographic design is based on the principles of *confusion* and *diffusion*, as identified in Shannon's landmark paper "Communication Theory of Secrecy Systems"[1]. Confusion refers to a relationship between a secret key and a ciphertext; such a relationship should be kept as complex and as possible. Diffusion aims to reduce any statistical relationship between the plaintext and the ciphertext as far as possible. To be able to implement both principles in practice, a source of randomized and chaotic properties is

*Corresponding author.

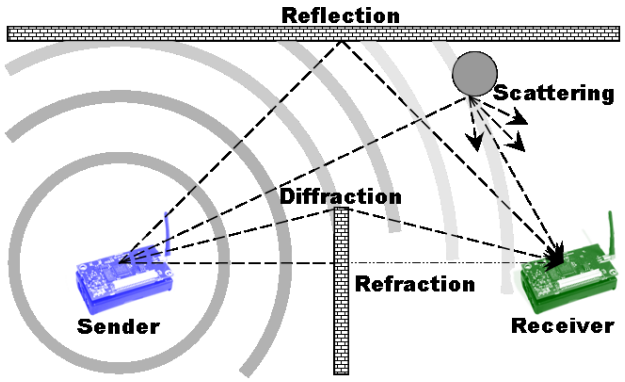


Fig. 1. Indoor radio propagation and different propagation phenomena: reflection, diffraction and scattering result in unpredictability of signal propagation within real-world environments.

highly desired. So for example, traditional symmetric ciphers use complex substitutions and transpositions of a plaintext to produce ciphertext that is irreversible without knowledge of the key. Ciphers with good diffusion properties aim for a strong avalanche effect, so that even minimal changes of the plaintext affect large parts of, if not the whole, ciphertext.

Interestingly, such a diffuse relationship between input and output may also be found in wireless communication. It is well investigated that even a small change in physical position, antenna orientation or subtle changes of the physical environment strongly affect the signal strength measured at a receiver, especially in transmissions lacking Line-Of-Sight (LOS)[2]. Rather than using substitution and transposition to induce chaotic properties, physical phenomena of wave propagation such as reflection, diffraction, scattering and fading account for properties similar to confusion and diffusion. In a security context, this means that determining the exact physical configuration that produces a specific set of signal properties at the receiver may equal an exhaustive brute-force attack on a search space defined by the available physical positions, frequencies, transmission power levels, etc.

In the following, we briefly discuss the major effects inherent to every realistic radio communication as shown in Figure 1 to demonstrate their unpredictable impact on the resulting signal and dependency on the physical environment.

The most common effect is signal *reflection*. It occurs when radio waves hit a flat surface that is relatively large compared to a signal wavelength (in case of $2.4\,GHz$ transmissions the wavelength is $\approx 12.5cm$). Moreover, different properties of the surface and the angle of incidence determine the intensity and the resulting reflected wavefront. For example, if the ray hits an obstacle at an almost perpendicular angle, then a large portion of it penetrates the obstacle (called refraction) and only a small portion is reflected.

Another phenomenon which occurs when a signal interacts with objects along its propagation path is *diffraction*. Diffraction usually takes place when a wave hits the edge of an obstacle. The edge will then act as a transmitter, effectively "bending" the signal around the obstacle.

Similarly, a radio wave encounters *scattering* if it hits a rough surfaces or small objects relative to the wavelength (usually a surface of $1/10$ of a wavelength results in scattering). As a result, the wave is split up into many weaker waves, which are reflected at different angles and phases.

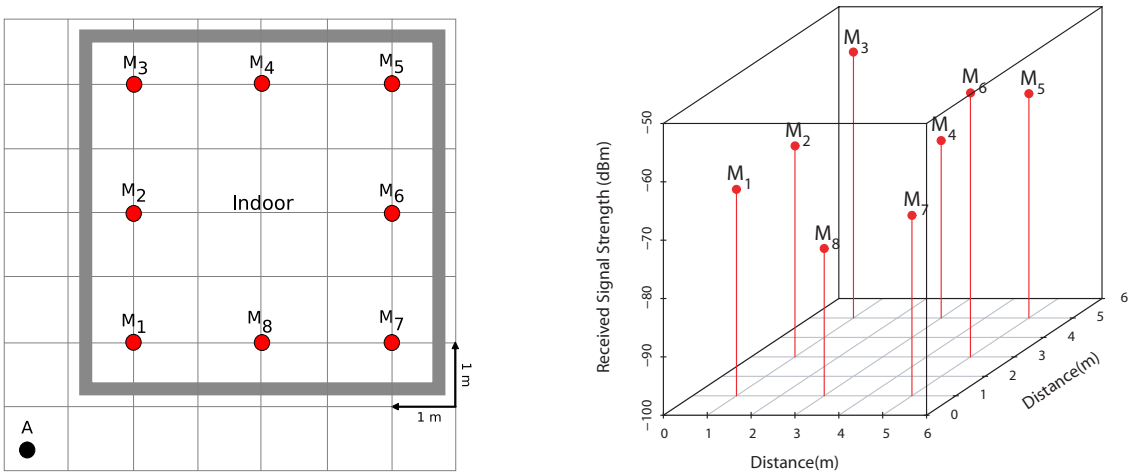
A real-world radio propagation will be subject to any combination of the aforementioned phenomena, resulting in a transfer function depending on many variables. By traveling along several paths, over different distances and consequently arriving with different phases, a signal exhibits *multipath propagation* properties, resulting in constructive or destructive interferences; the received signal strength may be weakened or amplified compared to LOS propagation.

In addition to the propagation models, penetration through different materials also leaves a mark on a signal propagation. For example, an aluminum siding may account for a loss of $20.4\,dB$, a concrete wall for $13-20\,dB$, or light textile for $3-5\,dB$ [3]. Considering that in our case, an attacker is placed outside, his transmission might pass through different walls containing various electrical conductors, pipes, and other obstacles. Since these obstacles are distributed according to a particular physical environment and the penetration effect depends on the distance and angle of signal arrival, the resulting signal is highly randomized and may significantly change among different scenarios.

B. Empirical Analysis

In this subsection we describe results from evaluating the diversity of signal propagation within a real-world indoor WSN network, and analyze the ability of an attacker to inject frames. Our testbed is a network installed in our university lab using 8 wireless sensor nodes and an attacker placed outside the room, as shown in Figure 2(a). The wireless senors are Crossbow MicaZ motes with CC2420 [4] radios, allowing for 32 different transmission power settings and 8-bit resolution of received signal strength. The power measurements are reported in RSSI (Received Signal Strength Indicator), which can easily be converted to dBm by $P_{dBm} = RSSI_{VAL} + RSSI_{OFFSET}$, where $RSSI_{OFFSET} \approx -45$.

The experiment started by measuring the RSS of the outdoor transmission on indoor motes. An ideal free-space model would provide the strongest RSS for the mote which is in the attacker's closest proximity (M_1), while the most distant mote (M_5) would measure the weakest RSS from the attacker's transmission. However, when looking at real-world measurements, the results are significantly different. Figure 2 (b) shows measured RSS on every mote using the topology from Figure 2 (a) . The mote with the strongest RSS is M_3 and the one with the weakest RSS is M_8. In a free-space model, this mote would have measured the second strongest RSS. Furthermore, this RSS relationship between motes and the attacker is changed only by alteration of placement. If it merely manipulates the transmission by increasing or decreasing sending power, the RSS relationship at indoor motes is conserved (i.e., it is scaled, but not changed). To be able for example, to enforce a relationship where the attacker's RSS at M_1 is higher than RSS



(a) (b)

Fig. 2. RSS unpredictability: (a) deployed WSN within an indoor scenario, (b) signal strength from an outdoor transmission measured at indoor sensors.

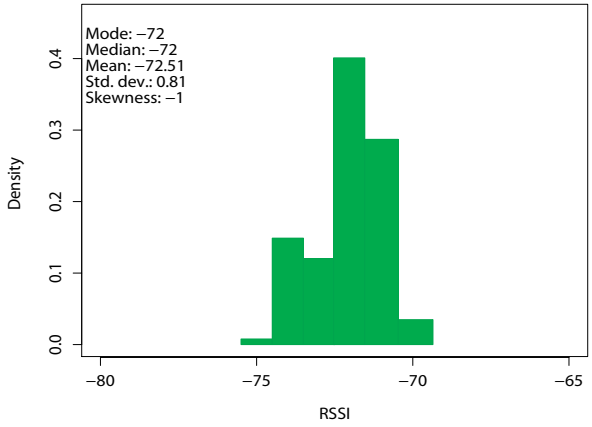


Fig. 3. Low RSS sample dispersion: measurement conducted over a 48 hours period in an indoor, short-distance environment with a sampling interval of 2 minutes. . Motes were positioned at the celling of the university lab maintaining the LOS during measurements.

measured at M_3, the attacker is forced to search for another configuration of physical position and antenna orientation without being able to predict an outcome.

Another property measured is the RSS variability of legitimate transmissions. Various research papers focused on measurements of RSS over long distances, especially with IEEE 802.11 devices, and identified strong time-varying properties of RSS data. These findings were influenced by weather condition which impact long distance outdoor wireless transmissions and introduce periodic trends in measured data (e.g., day/night changes) [5]. However, short distance transmissions, such as those within an indoor environment of a residence monitoring scenario, are more robust and less sensitive to weather trends. Such less varying RSS is already successfully used in many location systems, e.g, [6], or for a comparative study see [7]. Moreover, the RSS sample dispersion may further be limited if the wireless sensors are place on the celling of a room where fewer interruptions of the LOS between sensors occur. To justify this statement, we sampled 48 hours of indoor short distance transmissions at a sampling interval of 2 minutes. The sensors were positioned at the celling of the university lab maintaining LOS. The results of this measurements are given in Figure 3, which shows that the data is scatted over a narrow interval of -75 dBm and -70 dBm with a mean of -72 dBm. Similar results measured in an indoor environment using IEEE 802.11 technology have also been reported in [8].

III. Firewalling WSN

Operating in an indoor environment, a WSN may take advantage of access control offered by the "physical world", where walls, locked doors or other barriers for preventing physical intrusion establish the border between an outdoor attacker and the legitimate WSN sensors. Although radio signals are able to pass such barriers, a signal received from outside is strongly biased by various propagation effects as discussed in previous section.

The idea behind *firewalling* WSNs is to use a concept similar to a traditional network firewalling scenario, i.e., to identify and block messages not complying to predefined rules. However, in this case the rules are defined over properties of indoor wireless communication.

A. Protection Concept

The main objective in security design of the described scenario is data authentication, i.e., a WSN should be able to verify whether sensor data originated from legitimate sensors. To fulfill this objective, our protection concept is based on two mechanisms composed from different elements provided by the wireless "toolbox":

- *acceptance intervals*, which allow to identify fake frames, and

- *dynamic configuration*, used to prevent an attacker from finding an appropriate attack configuration.

Acceptance intervals are statistics based on legitimate transmissions gathered during the network deployment phase. They are used to verify that frames transmitted to a base station comply with wireless properties of authentic sensors deployed within a certain environment. To successfully inject fake frames into the network, an attacker must find an appropriate *configuration* of wireless parameters, such as physical position, antenna orientation, and transmission power level to produce the RSS as requested by the acceptance intervals at each sensor. Only if the transmitted frame complies with acceptance intervals, the frame will be included in further processing and data aggregation. To succeed in this attack, the attacker must produce the correct RSS relationships among indoor motes as discussed in Section II-B. For this reason, the *dynamic configuration* mechanism is concerned with permanently changing the network configuration of legitimate motes. Even if a configuration for successful injection is found, every alteration of the network parameters changes acceptance intervals and invalidates the attacker's configuration.

In the following subsections we provide details of implementation of both mechanisms within a real-world WSN deployment. First, we discuss the results without the presence of an attacker, and analyze the impact of the mechanisms on false positives, i.e., rejection of legitimate frames. Then, we implement an attacker which shares complete knowledge of the network and attempts to inject fake sensor data.

B. Acceptance Intervals

The controlled deployment of a residential WSN allows for careful planning of the nodes' physical positions and configuration of transmission power. Once deployed, the positions of nodes do not frequently change and the properties of legitimate transmissions can be quantified before starting a monitoring scenario, during the so-called initial phase. To allow a certain variance in the signal strength of legitimate transmissions, a rule for accepting frames is defined over the *acceptance interval* $[\mu - k\sigma, \mu + k\sigma]$, where μ is a sample median, σ a standard deviation of a sample, and k (with $k > 1$) is an environment-dependent constant defining the width of the interval, i.e., it describes within how many standard deviations the RSS is still considered legitimate.

Due to the sample's unknown population the interval width can be estimated by Chebyshev's inequality which is valid for any arbitrary distributions (1):

$$Pr(|X - \mu| \geq k\sigma) \leq \frac{1}{k^2} \tag{1}$$

which says that the probability of the random variable differing from its mean by at least k standard deviations is less or equal $\frac{1}{k^2}$. For example, by measuring $\sigma = 1\,dBm$, and assuring that no more than 4% of all legitimate frames miss the selected interval, the required acceptance interval width is $10\,dBm$ ($\mu \pm 5$). Still, this is a very crudely estimated value as it also represents a bound valid for arbitrary underlying distributions.

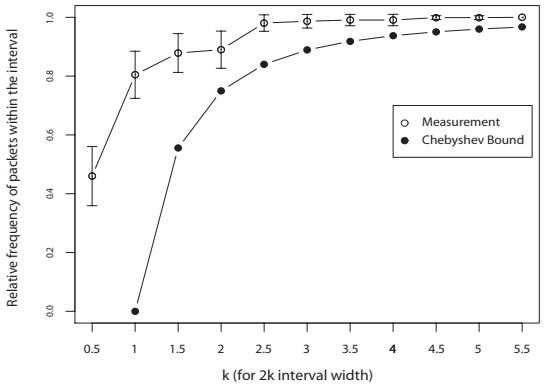


Fig. 4. Acceptance Intervals: estimating width using initial measurements.

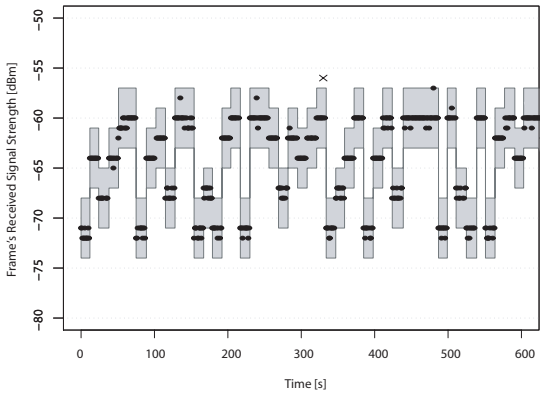


Fig. 5. Dynamic Configuration: dynamically changing acceptance intervals (at one mote).

While this inequality relates the interval width to the magnitude of the standard deviation (which we estimate by using sample standard deviation), the parameter k can also be estimated by empirically measuring the proportion of accepted and rejected legitimate frames within a given scenario. In this case, a binomial distribution can be assumed allowing us to compute the interval width and confidence intervals without paying the price for generalized statement given by (1).

In Figure 4, the results of both methods for interval estimation are shown. Using binomial proportions, we could achieve more narrow intervals, e.g., at $k = 3$ and with a confidence level of 0.95, more than 98% of all legitimate frames are contained within the interval.

C. Dynamic Configuration

To successfully inject fake frames into a WSN, an attacker must find a transmission power level matching the acceptance intervals of the legitimate nodes. Whether such a signal strength exists given a specific physical position can only be tested by brute force, i.e., by trying different power levels and antenna orientations. If no such power is found, the attacker is forced to change its physical position and start again. Unfortunately, to provide a general statement

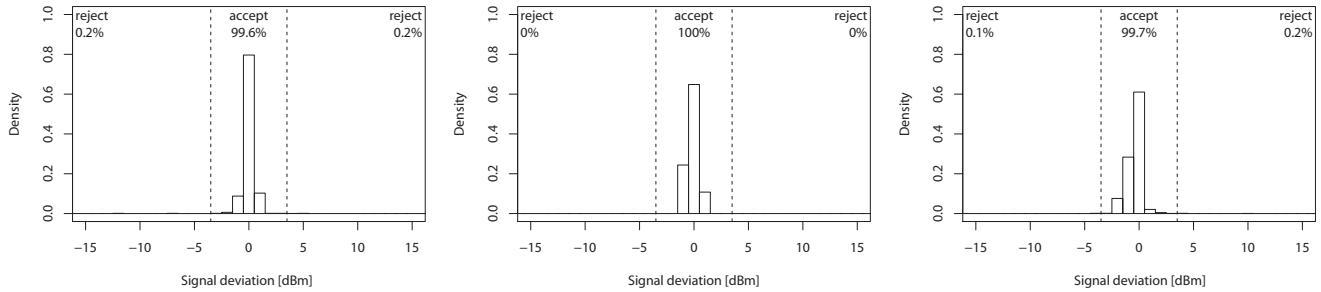


Fig. 6. Analyzing false positives: 18h measurement at three motes implementing acceptance intervals and dynamic configuration.

on the occurrence of such "breakable" configurations, every physical position must be tested, and even then the results can only be valid for a particular scenario. While such testing seems impractical and extremely time-consuming, the same problem can be directed against the attacker. As mentioned, the attacker's success depends directly on the acceptance interval of the legitimate motes. Hence, if the interval changes, the attacker must also change its transmission power, which consequently results in losing the appropriate configuration and forces the attacker to start from scratch.

To allow such dynamic changes of intervals, nodes use the same PRNG seed and randomly choose different power levels for their initial transmissions. Synchronization of their configuration changes can either be assured by a base station or by other means for providing synchronization in WSN (in this work we used a base station which periodically broadcasts synchronization beacons).

The results of such dynamic changes are given in Figure 5 which shows a time series of a single node's perspective and its randomly chosen intervals. In this case the nodes used five different power levels which resulted in five acceptance intervals. The number of acceptance intervals can obviously be preconfigured and the disjoint property enforced, however we leave this as part of our future work.

The black dots present frames accepted within different intervals, while the crosses stand for those rejected due to the signal strength variations of the legitimate transmission. As can be seen, an interval change does not present a problem for the WSN, and the indoor motes have no difficulties changing their transmission power and reaching the acceptance intervals.

For example, three WSN nodes were used to verify the transmitted frames, and the resulting statistics are depicted in Figure 6. It shows the relative frequency of accepted/rejected frames and their RSS as deviation from acceptance interval mean measured over an 18 hour period and a throughput rate of 1 frame per second (the dashed vertical lines depicts interval width). The number of false positives at legitimate transmission detected by three nodes over 18 hours is at a low 0.7%.

D. Reacting to Injection Attacks

The concept of firewalling is a *proactive* mechanism which allows the detection of injection attacks. The reaction to such an attack can be seen as a separate task and its design should

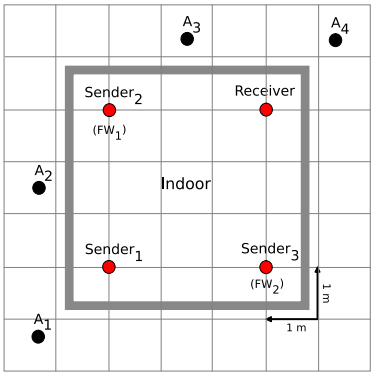


Fig. 7. Real-world WSN scenario under an injection attack from various physical positions (A_1, A_2, A_3, A_4).

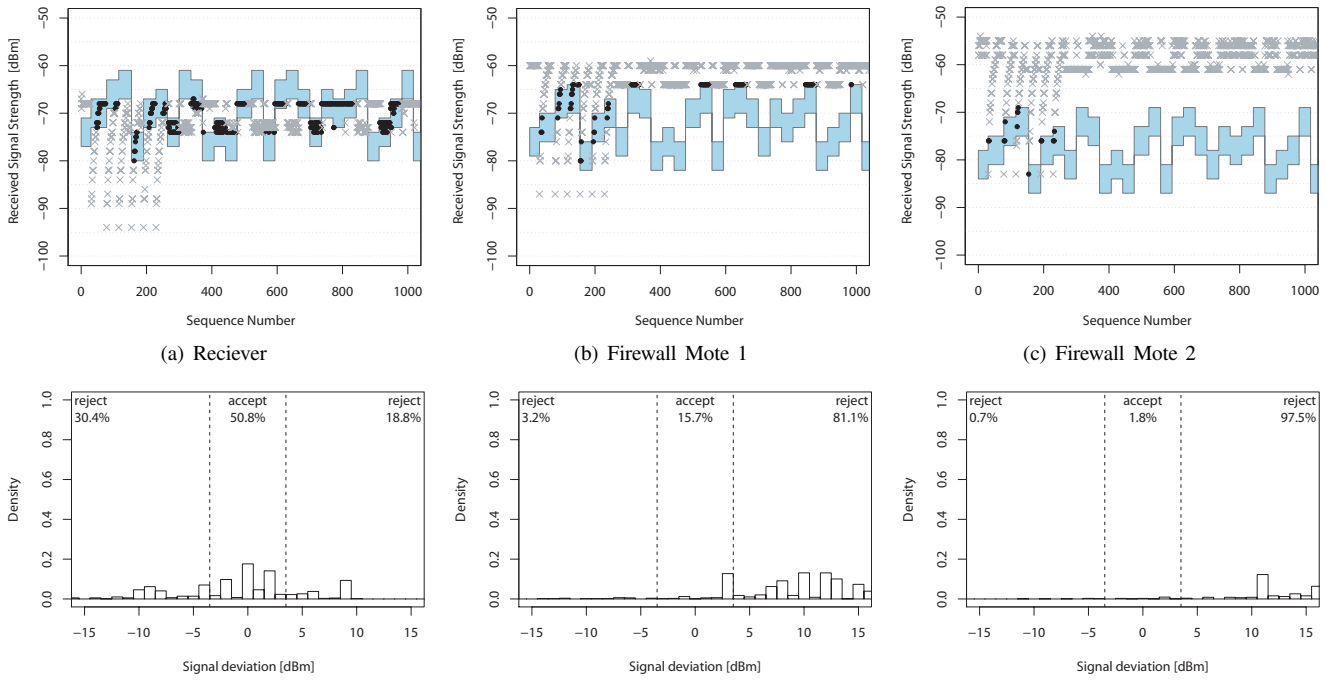
comply with the objectives of a particular scenario to minimize the impact on the overall system. There are various techniques to fulfill that task; some may be based on cryptography and applied only for the duration of an attack, while other, more lightweight reactions can be based on exposing the injected frames to the WSN, making it possible to exclude those frames from aggregation. So for example, sensors which detect injection can notify the WSN segment and the base station by broadcasting the identifier of the fake frame.

While designing a sophisticated reaction mechanism is out of the scope of this work, we implemented a method similar to the aforementioned notification-based reaction to offer a comprehensive analysis of implemented WSN protection. If any of the verifying sensors detects a frame outside its acceptance interval, it broadcasts a warning frame with the sequence number of the injected frame, which is then discarded from further in-network processing. Using this response method, the following section provides an overall analysis of the implemented WSN scenario under a real-world injection attack.

IV. WSN UNDER ATTACK: REAL-WORLD ANALYSIS

As is the previous measurements, the legitimate motes were deployed on the celling of our university lab and the experiment was performed in two phases:

1) *Deployment phase:* Installation of sensors and configuration of transmission parameters, including initial



(a) Reciever (b) Firewall Mote 1 (c) Firewall Mote 2

(d) Receiver (e) Firewalling Mote 1 (f) Firewalling Mote 2

Fig. 8. Attacking a WSN (analyzing false negatives): the attacker probes for intervals and attempts frame injections (compare to Figure 6).

measurements using different power levels and frequencies for defining the width and number of acceptance intervals.

2) *Monitoring phase:* The network is in regular operation while being subject to an injection attack executed from various physical positions outside the deployment area.

A deployed WSN is shown in Figure 7. It consists of three senders and one base station (receiver). Senders 2 and 3 are, parallel to their sensing tasks, extended with firewalling functionalists (FW_1, FW_2). They monitor transmissions and react with a warning frame if an injection attack is detected. For a successful injection, a frame must be received within the acceptance intervals of the receiver *and* the two firewalling motes.

A. Attacker Model

The attacker is modeled with complete knowledge of the network which allows it to observe the progress of its attack by knowing exactly which power levels resulted in the acceptance or the rejection of injected frames. Additionally, before attacking the network, the attacker sends probe frames to discover how many acceptance intervals have been defined and to determine the power levels which resulted in successful injection for each interval. The notification of an interval change is broadcast in clear and the attacker is able to promptly adapt its transmission power. It also attempts to take advantage of frame loss produced by low power-transmissions to sneak away from the firewalling motes in order to avoid detection.

As a result of this attacker model, there is *no secret information* among legitimate motes. Even randomly selected intervals are known to the attacker.

B. Impact of an Injection Attack

The results of the attack are given in Fig. 8. The Subfigures (a),(b), and (c) show the time-line of the attack at three legitimate nodes and their random interval selection, respectively, while Subfigures (d), (e), and (f) provide the relative frequencies of accepted and rejected frames and their RSS deviation from the mean of the acceptance intervals.

During the first $\approx 250s$ the attacker iterated over all power levels and selected those for which a frame was successfully injected at the receiver (missing the receiver's intervals would result in rejecting the frame). For every interval change, the attacker promptly reacted by adapting its transmission. While some intervals were easier to "break in" than the others, the overall attack success at the receiver was $\approx 50.8\%$ of all transmitted fake frames. However, by transmitting with the power suitable for the receiver, the attacker could not keep its frames within intervals of both other firewalling motes (FW_1, FW_2). For every frame that missed the acceptance interval of at least one firewall, the receiver was notified by a warning frame disclosing the sequence number of the injected frame. The attack resulted in 81.1% rejections at FW_1 and even 97.5% rejections at FW_2. Actually, the attacker's signal received at FW_2 exceeded the expected RSS by $\approx 20\,dBm$, which means that the sending power (in mW) should be decreased by at least *100 times* to be accepted by FW_2. Such a decrease in power would consequently result in missing the acceptance intervals of both the receiver and FW_1. Hence, the only possibility for the attacker to continue its attack is to

Attack Position	FWs Detected	Receiver Rejected	Attack Succ.	FWs Loss
1	50.4%	53.15%	0.0%	7.25%
2	82.5%	79,64%	0.0%	2.86%
3	66.1%	63.15%	0.0%	2.95%
4	75.0%	70.12%	0.0%	4.88%

Fig. 9. Results from attacking indoor WSN from different outdoor positions.

retry the complete procedure from another position, without any possibility of predicting the outcome.

We tested various other positions as depicted in Figure 7, the results are given in Table 9 which provides statistics of the attacker's success but also the reasons for failure – frequency of detected injections by the firewalls, and missed intervals at the receiver. It also shows frame losses encountered at both firewalls during low-power injections. The detection of fake packets is distributed over three verifying motes, and the attacker could not succeed in injecting a packet accepted by all three motes. The reason is that the motes in the indoor environment are in close proximity to each other. As a result, it is highly unlikely that the RSS measured at the receiver is strong enough to match the acceptance intervals (e.g.,$-75\,dBm \leq RSS \leq -70\,dBm$), while at the same time being below the sensitivity threshold of the other sensors (e.g., $RSS \leq -95\,dBm$). Even the highest frame loss rate of 7.25% at both firewalls did not result in any successful injection.

V. Related Work

Impersonation attacks constitute a fundamental security problem inherent to the broadcast nature of every wireless communication. A variety of research contributions is based on designing cryptographic solutions to offer both, authentication and confidentiality for WSN communication. Such designs commonly use symmetric ciphers. For example, IEEE 802.15.4 [9] uses AES in CBC-MAC mode of operation and supports 128-bit message authentication codes (MACs). Similarly, TinySec [10] uses a fast Skipjack algorithm, also in CBC-MAC mode and supports 32-bit MAC with 64-bit secret key. However, in CBC-MAC mode of operation, only frames of predetermined length can be securely authenticated, which introduces further constraints on protocol design. MiniSec [11], while utilizing the same underlying cipher as TinySec, extends the secret key to 80-bit and offers more efficient MAC computation using Offset Codebook Mode (OCM). There are also security frameworks using public-key cryptography such as TinyECC [12] which is based on Elliptic Curve Digital Signature Algorithm (ECDSA) enabling even 160-bit for both, secret key and a MAC computation, although with high computational costs on the magnitude of seconds.

However, such cryptography-based solutions simply transfer the concept of protection used in wired networks to significantly different wireless networks. To authenticate a frame, a device must first compute the MAC, and then decide whether to accept or to reject it. Since a wireless network can not provide physical control over the traffic, and devices depend on battery power, arbitrary initiation of frame authentication or the key exchange often results in new resource-depletion vulnerabilities.

For this reason, the peculiarities of wireless communication have been the focus of many wireless security research papers which attempt to include them in the security design. For example, in [13], Čagalj et al., propose integrity codes (I-codes) to support message integrity checks. Using only the properties of the wireless channel and radio transmissions, I-codes enable a broadcast message authentication and the concept of "authentication through presence". In contrast to this work, I-codes are based on wireless message coding. To transmit a codeword over a given radio channel, the sender uses on-off keying modulation at the physical layer. For example, symbol "1" is transmitted as a particular signal during the pre-defined time period. For each symbol "0" the sender remains silent. As a result, the presence or absence of energy in a given time slot carries information used for authentication.

In [14], Chen et al., design protection against spoofing attacks also based solely on physical properties of wireless communication. Using statistics based on cluster analysis, the authors demonstrate that both spoofing and attack location can be identified. Similar to our work, and to [8] they use signal thresholds to estimate legitimate transmissions. Moreover, the authors provide an effective localization mechanism to disclose the approximate position of the attacker. However, in contrast to their work, this paper considers that an attacker is able to successfully inject fake frames into the network, and therefore we extend the protection mechanism to dynamically change its configuration. In our opinion, this is an important issue, since the unpredictable nature of wireless communication may not always play fair.

Various other research papers are concerned with physical properties of the radio environment to enhance security, e.g., [15], [16], [17]. However, the contribution of the work introduced in this paper significantly differs from the aforementioned research. Our solution neither requires specialized hardware, nor introduces complex message exchange. The closest research to our work is probably given by Demirbas et al. in [18]. The authors also take advantage of signal strengths to detect injections attacks and demonstrate their solution using Mica2 wireless sensors. While in their work, the authors attempt to minimize the randomness of signal strength by comparing the ratios of RSSI values, in this work we take the opposite approach and show that protection can be based on the randomness directed against an attacker. Furthermore, our protection concept incurs no additional cost to the legitimate

propagation, while [18] requires sending additional traffic even when the network is not being attacked.

The similar paradigm of *security by wireless* is demonstrated in [19], which tackles the problem of cryptographic (client) puzzles and adapts it to comply with properties of wireless networks, especially IEEE 802.11 technology. In this work, however, we consider WSN technology and provide more general protection not only against DoS attack (e.g. memory-depletion as it is the case in [19]), but also against fake data injections which present a serious threat for deployment of low-cost WSN applications.

VI. Conclusion and Future Work

In a security context, wireless communication has often been considered an Achilles' heel. Its broadcast nature does not allow for traffic to be physically separated, and the performance-limited clients are constrained in using cryptographic mechanisms. Moreover, implementing complex key exchanges and computationally expensive message authentication frequently creates new vulnerabilities. Therefore, security mechanisms should consider the peculiarities of such environments and include them into their design.

This work followed the idea of *security by wireless*, i.e, to use wireless properties offered by the communication itself to design lightweight security mechanisms. Since the concept of firewalling WSNs allows for *proactive* protection, it can easily be incorporated within cryptography-based protocols whose usage should be scarce and adapted to peculiarities of wireless environment, e.g., by limiting the initiation of expensive computations and early rejection of frames that differ significantly from legitimate transmissions.

We implemented our concept within a realistic indoor WSN scenario. Extensive measurements indicate that utilizing acceptance intervals and dynamic configuration mechanisms does not lead to a high number of false positive at the legitimate nodes. Different tests using an implemented "omniscient" attacker confirm that such a protection concept indeed presents a hard challenge. However, there are still issues left for further analysis. For example, we intend to extend the concept of acceptance intervals to include more wireless properties. Also, acceptance intervals should be disjoint to decrease the chance of using the same configuration to successfully attack at different intervals. Furthermore, a WSN may define more sophisticated protection rules, e.g., to only change the configuration if "breakage" at the current interval is detected e.g. by taking advantage of a traffic model. This would prevent an attacker from using the same configuration for periodic attacks in case the number of acceptance intervals is small and their recurrence frequent.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 2, pp. 656–715, 1949.

[2] D. Lymberopoulos, Q. Lindsey, and A. Savvides, "An Empirical Characterization of Radio Signal Strength Variability in 3-D IEEE 802.15.4 Networks Using Monopole Antennas," in *Third European Workshop on Wireless Sensor Networks (EWSN 2006)*, 2006, pp. 326–341.

[3] T. Rappaport, *Wireless Communications: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[4] T. Instruments, "CC2420 Radio Datasheet," http://focus.ti.com/lit/ds/symlink/cc2420.pdf.

[5] A. Howard, S. Siddiqi, and G. Sukhatme, "An experimental study of localization using wireless ethernet," in *Proceedings of the International Conference on Field and Service Robotics*, July 2003.

[6] A. M. Ladd, K. E. Berkis, A. Rudys, L. E. Kavraki, and D. S. Wallach, "Robotics-based location sensing using wireless ethernet," *Wireless Networks*, vol. 11, no. 1-2, pp. 189–204, 2005.

[7] E. Elnahrawy, X. Li, and R. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," in *Proceedings of the Fourth Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks*, 2004, pp. 406–414.

[8] D. B. Faria and D. R. Cheriton, "Detecting Identity-based Attacks in Wireless Networks using Signalprints," in *WiSe '06: Proceedings of the 5th ACM workshop on Wireless Security*, Sep. 2006, pp. 43–52.

[9] I. 802.15.4-2006, "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," IEEE Standard, Jun. 2006.

[10] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a Link Layer Security Architecture for Wireless Sensor Networks," in *SenSys '04: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, Nov. 2004, pp. 162–175.

[11] L. M, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A Secure Sensor Network Communication Architecture," in *IPSN '07: Proceedings of the 6th International Conference on Information Processing in Sensor Networks*, Apr. 2007, pp. 479–488.

[12] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," in *Proceedings of the 7th International Conference on Information Processing in Sensor Networks, IPSN 2008*, Apr. 2008, pp. 245–256.

[13] M. Čagalj, S. Čapkun, R. Rengaswamy, I. Tsigkogiannis, M. Srivastava, and J.-P. Hubaux, "Integrity (I) Codes: Message Integrity Protection and Authentication Over Insecure Channels," in *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06)*, May 2006, pp. 280–294.

[14] Y. Chen, W. Trappe, and R. Martin, "Detecting and localizing wireless spoofing attacks," in *Proceedings of the Fourth Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks*, 2007, pp. 193–202.

[15] S. Čapkun, R. Rengaswamy, I. Tsigkogiannis, and M. Srivastava, "Implications of Radio Fingerprinting on the Security of Sensor Networks," in *Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks*, Sep. 2007.

[16] C. Castelluccia and P. Mutaf, "Shake them up!: A Movement-based Pairing Protocol for CPU-constrained Devices," in *MobiSys '05: Proceedings of the 3rd International Conference on Mobile systems, Applications, and Services*, Jun. 2005, pp. 51–64.

[17] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H.-W. Gellersen, "Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts," in *UbiComp '01: Proceedings of the 3rd international conference on Ubiquitous Computing*, Sep. 2001, pp. 116–122.

[18] M. Demirbas and Y. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," in *WOWMOM '06: Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks*, Jun. 2006, pp. 564–570.

[19] I. Martinovic, F. Zdarsky, M. Wilhelm, C. Wegmann, and J. Schmitt, "Wireless Client Puzzles in IEEE 802.11 Networks: Security by Wireless," in *Proc. ACM Conference on Wireless Network Security (WiSec 2008)*, Alexandria, VA, USA, Mar. 2008, pp. 43–52.