Poster: Come Closer - Proximity-based Authentication for the Internet of Things

Hossein Shafagh
Department of Computer Science
ETH Zurich, Switzerland
shafagh@inf.ethz.ch

Anwar Hithnawi
Department of Computer Science
ETH Zurich, Switzerland
hithnawi@inf.ethz.ch

ABSTRACT

This paper presents a proximity-based authentication approach for the *Internet of Things* (IoT) that works in-band by solely utilizing the wireless communication interface. The novelty of this approach lies in its reliance on ambient radio signals to infer proximity within about one second, and in its ability to expose imposters located several meters away. We identify relevant features sensed from the RF channel to establish a notion of proximity across co-located low-power devices. We introduce our proximity-based authentication protocol and show the feasibility of our approach with an early prototype using off-the-shelf 802.15.4 sensors and an evaluation conducted in a real-world environment.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General – Security and protection

Keywords

Wireless Communication; Security; Internet of Things

1. INTRODUCTION

With the advent of the IoT, there is a rise in the number of smart devices that are empowered with sensing, actuating and communication capabilities to enhance and create unique forms of interaction with our immediate surroundings. As these devices are integrated in our proximate living space, they deal with sensitive and private data that can be misused to infer information about our daily habits. This consequently raises unique security and privacy challenges that drive the need for security to be an integral part of any IoT system. Due to cost, size and energy efficiency requirements, commodity IoT devices are designed with minimalistic physical interfaces. Among these interfaces, the radio transceiver is the common physical interface, which makes it a natural candidate to be utilized for security services.

MobiCom'14, Sep 07-11 2014, Maui, HI, USA
ACM 978-1-4503-2783-1/14/09.
http://dx.doi.org/10.1145/2639108.2642904.

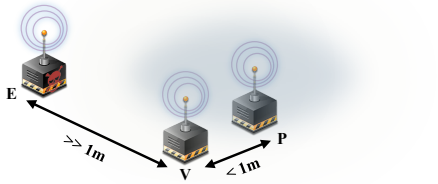


Figure 1: Proximity-based authentication of two co-located devices P and V, in the presence of an adversary E.

The ubiquity of the wireless medium, has given a raise to the number of RF communication technologies and devices being used, particularly in the ISM bands. This implies that there is a form of continuous energy fluctuations in the wireless channel, generated by a diverse set of communication technologies. RF signals constitute a source of electromagnetic energy that radiates in the channel. As the RF signals traverse the medium they undergo many propagation effects that can cause large or small scale energy losses. This energy is absorbed and scattered in different directions as it propagates in the space, thus inducing different levels of observed energy spatially and temporally. At the same time, the perceived RF signals appear to be highly correlated in two co-located points. The correlation drastically decreases as the distance between the two points increases. Quantifying these variations of energy in the channel by sampling the cumulative RF signal strength at a high rate provides us with a unique time-variant metric that we source for our proximity-based authentication approach.

In order to protect the communication of two smart devices, traditionally pre-shared keys are used, and recently *Public-Key Cryptography* (PKC) has been advocated. The former does not scale for the IoT, and the latter is not affordable by highly resource-constrained devices. Specifically, the mere use of PKC-based key agreement protocols, such as *Diffie-Hellman* (DH) without authentication, for instance by means of certificates, leaves the communication vulnerable to man-in-the-middle attacks.

In this work, we propose a proximity-based authentication approach for low-power IoT devices. This approach is based on correlating fine-grained samples of channel information in form of *Energy Levels* (EL). In order to compensate for the narrow-band of low-power transceivers, i.e., 2 MHz, we collect the channel information over several frequencies. In contrast to existing approaches, we do not require the exchange of huge amounts of packets, which increases the energy efficiency of our protocol in favor of less radio pollution. We utilize the broadcast nature of the wireless medium and

how electromagnetic signals from uncontrolled transmitters are propagating and affecting the level of energy perceived by nodes. The results of our experiments show the feasibility of our protocol even for underutilized networks.

2. RELATED WORK

The temporal and spatial variations in the radio channel have been exploited by researchers in RF-based localization, secure key extraction, and proximity estimation. In RF-based localization [7, 6], the range between a device and the reference points is estimated by means of RSSI. Afterwards, techniques such as triangulation can be used to estimate the relative location. Key extraction approaches [4, 8, 10] use the reciprocal behavior of communication links to generate a secure key between two end-points. These approaches are complementary to our work, since they aim at securing the communication between two nodes without prior knowledge, whereas we provide proximity-based authentication.

Prominent RF-based proximity estimation approaches are: Amigo [3], Ensemble [2], and ProxiMate [9]. Amigo relies on observing the channel in promiscuous mode for 802.11 frames. The observed packets and their corresponding RSSI readings are fed to a classifier which determines proximity. In order to reach low false positive rates, more than 5 s are needed. Ensemble relies on RSSI readings of packets generated by a network of trusted devices. It requires at least 3 trusted devices in communication range, each sending 40 packets per second for 70 s. ProxiMate relies similar to our approach on ambient RF signal. However, they focus on TV signals and require software-defined radios to extract the required features (amplitude and phase) from the signal.

Proximity estimation can as well be achieved by other means such as *Time-of-Arrival* (TOA). Rasmussen et al. [5] introduce an RF distance bounding technique based on TOA, which requires high processing time in the range of nanoseconds, since an error of 3 ns results into an estimation error of approx. 1 m. They achieve this high precision with a custom designed radio-chip.

In this work, we present a proximity-based authentication, which is based on captured energy level variations. These variations exist due to propagation effects on ambient RF signals from inter/cross-technology devices emitting in the same frequency bands. Considering the resource-constraints of smart devices, we limit the number of packet transmissions to a few packets that are required to indicate the next channel rendez-vous, i.e., frequency, and to achieve loose synchronization for signal acquisition. During the inter-packet times, we collect EL readings. The signal acquisition time is a protocol parameter which is related to the level of experienced entropy.

3. ATTACKER MODEL

In our attacker model, as depicted in Figure 1, we distinguish between passive and active attackers, who are not in the proximity of the genuine device. By design, we are immune against a passive attacker, who eavesdrops on the medium aiming at observing a similar physical channel. This is due to the fact that we rely on the continuous stochastic channel properties that are uncorrelated in the time and spatial domains. An active attacker who makes use of jamming by means of emitting energy with certain patterns, aims at deceiving two not co-located nodes to falsely decide they are

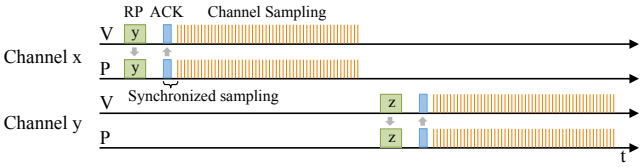


Figure 2: Signal acquisition stage of our protocol for two rounds at channels x and y. The *Rendez-vous Packet* (RP) indicates the next channel for sampling. The ACK is used for a synchronized sampling at a rate of 7.69 kHz, which lasts for 234 ms.

in close range. Due to radio wave characteristics such as fading, reflection, diffraction and scattering, such an attack is complex. Additionally, by taking the level of induced energy which disperses by distance [1] into our algorithm, we make such an attack more difficult. In future work, we quantify the effectiveness of an active attacker.

4. SYSTEM ARCHITECTURE

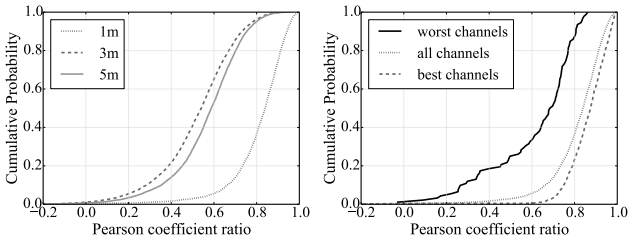
In this section, we describe our authentication protocol.

Signal acquisition and quantization. *Proofer* (P) initiates the handshake with a request packet. Upon reception of such a packet, *Verifier* (V) sends a *Rendez-vous Packet* (RP) indicating the next communication channel. As the low-power transceivers typically communicate over narrow-band channels, i.e., 2 MHz, certain channels may be exposed to less variations. Hence, in order to increase the chances of capturing enough channel variations, we rely on several channels. Possible rendez-vous channels are the 16 available channels of 802.15.4. To optimize the channel selection, V maintains a profile of good channels that exhibit high variations based on previous observations. After receiving the RP, P sends a MAC-layer *Acknowledgment* (ACK) to V. We use the ACK for a loose synchronization required for an aligned signal acquisition. This is achieved with a sampling routine starting immediately after reception of the ACK. P and V sample the EL at a frequency rate of 7.69 kHZ for the time unit t_{el} (in our experiments t_{el}=234 ms corresponding to 1800 readings). After t_{el}, V sends the next RP on the previously announced rendez-vous channel, where the same procedure of EL sampling repeats. This procedure, as depicted in Figure 2, continues n times, until V requests the proof of proximity from P. Currently, we consider $n \in \{3, 4, 5\}$ which depends on the quality of the signal acquired by V. The end-points divide the $i \in \{1..n\}$ collected signal traces, h_v^i and h_p^i, into $j \in \{1..45\}$ blocks $b_v^{i,j}$, each consisting of 40 channel readings. The block size corresponds to 5.2 ms. This achieves a downsampling from 1800 to 45 values. For each block $b_v^{i,j}$ and respectively $b_p^{i,j}$, we compute the maximum induced power level which we rely on for the correlation algorithm. At the same time, we validate if all blocks $b_d^{i,j}$ from the two devices $d \in \{v, p\}$ have experienced enough entropy, i.e., randomness:

$$R(d,i,j,k) = \begin{cases} 1 & \text{if } b_d^{i,j}[k] > (mean(b_d^{i,j}) + \alpha) \\ 1 & \text{if } b_d^{i,j}[k] < (mean(b_d^{i,j}) - \alpha) \\ 0 & \text{otherwise} \end{cases}$$

$$\forall\ i \in [1..n],\ j \in [1..45], \quad R\_ratio_d^{i,j} = \frac{\sum_{k=1}^{40} R(d,i,j,k)}{40} > 0.1 \tag{1}$$

To this end, we require that in each block at least 10% of the readings deviate by about α=2 dBm from its average readings. At a higher level, we require that again 10% of all



(a) Three Distances (b) Channels at 1 m

Figure 3: CDF of Pearson correlation coefficient computed over 38400 traces, collected with 802.15.4 motes, at several distances, and over all frequencies.

blocks fulfill the entropy condition:

$$\forall\ i \in [1..n], \quad R\_ratio\_total_d^i = \frac{\sum_{j=1}^{45} R\_ratio_d^{i,j}}{45} > 0.1 \qquad (2)$$

Traces not fulfilling this requirement are discarded, due to low entropy. V observes the quality of traces during the handshake and if required increases n, the number of rounds.

Reconciliation. The alignment of traces is achieved by a synchronized sampling. As illustrated in Figure 2, after the ACK transmission, P waits t_s μs, which is the time required for V to receive and process the ACK, and enter the sampling routine. This way, both end-points start to sample the channel at the same time. We decided against exchange of the channel hopping sequence at the beginning of the handshake, to avoid possible inaccuracies due to channel switching and clock drifts. Hence, the channel rendez-vous packets serve as a measure for a synchronized signal acquisition.

Correlation. For each pair of traces h_v^i and h_p^i, we compute the degree of correlation by means of the Pearson correlation coefficient r. We use the induced power levels for the calculation of the Pearson correlation coefficient. If the majority of the traces have a high correlation, then physical proximity can be assumed. We detail our decision for a majority vote in the next section based on our empirical observations.

5. EXPERIMENTS

In order to validate our assumptions about the correlation of channel variations at co-located devices, we perform experiments within our offices using TelosB motes, a low-power sensor node with an 802.15.4 compatible radio transceiver, and a built-in omnidirectional antenna.

We use Contiki OS for our implementation and collect approx. 800 traces in each of the 16 channels. The two nodes are placed in line-of-sight, at distances of 1, 3, and 5 m. Our measurements are conducted mainly at night, and accumulate to more than 38400 traces. We compute the Pearson correlation coefficient averaged over all channels for these distances. As depicted in Figure 3(a), for co-located devices at distance 1 m, 80% of the runs exhibit a correlation coefficient ratio higher than 0.7. For distances 3 and 5 m, only 15% to 20% of the runs have a higher ratio than 0.7. Setting the threshold for proximity to a correlation ratio of 0.7 results into 15% false negatives (rejected co-located nodes) and 15% to 20% false positives (falsely accepted far nodes). With a simple majority vote over at least 3 runs, we reduce the amount of false negatives and false positives. More importantly, the randomness of the channel varies over time and frequency. As depicted in Figure 3(b), the two best channels exhibit high correlation coefficients, whereas the worse two

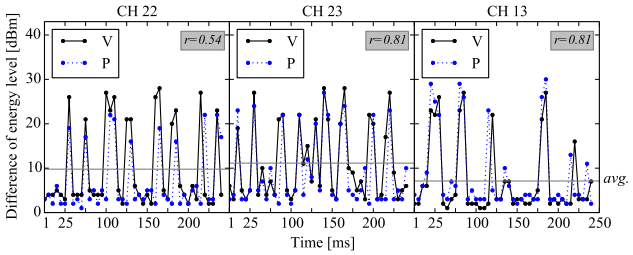


Figure 4: Three selected traces from co-located devices. All traces, experience enough randomness, measured in form of deviations from the average value (depicted as a gray line). Traces from channels 23 and 13 have a good correlation coefficient r.

channels behave similarly to distanced nodes. To explain our majority-vote-based proximity decision, as illustrated in Figure 4, we selected three traces from co-located devices at three different channels. The traces exhibit enough randomness. However, only the middle and right traces show a high correlation coefficient. The first trace has a low correlation coefficient, though we observe a similar trend on the readings. This is due to different energy levels, which implies different distances, explaining the low correlation coefficient.

6. FUTURE WORK

In this paper, we introduced our proximity-based authentication scheme, tailored for resource-constrained devices. We presented the results of our prototype implementation on TelosB motes. Currently, we are improving our correlation algorithm, and extending our implementation. We plan to conduct extensive measurements to assess the impact of cross-technology interference, static environments with low entropy, mobility and human motion on our protocol.

7. REFERENCES

[1] A. Hithnawi et al. Low-Power Wireless Channel Quality Estimation in the Presence of RF Smog. DCOSS'14.

[2] A. Kalamandeen et al. Ensemble: Cooperative Proximity-based Authentication. MobiSys'10.

[3] A. Varshavsky et al. Amigo: Proximity-based Authentication of Mobile Devices. UbiComp'07.

[4] J. Croft et al. Robust Uncorrelated Bit Extraction Methodologies for Wireless Sensors. IPSN'10.

[5] K.B. Rasmussen et al. Realization of RF Distance Bounding. USENIX Security'10.

[6] M. Youssef et al. Challenges: device-free passive localization for wireless environments. Mobicom'07.

[7] N. Patwari et al. Relative Location Estimation in Wireless Sensor Networks. *Transactions on Signal Processing*, 51(8), 2003.

[8] S. Jana et al. On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments. MobiCom'09.

[9] S. Mathur et al. ProxiMate: Proximity-based Secure Pairing Using Ambient Wireless Signals. MobiSys'11.

[10] S. Mathur et al. Radio-Telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. MobiCom'08.