Bluetooth-Based Context Modeling

Eric Vance
California State University, Northridge
18111 Nordhoff Street
Northridge, CA 91330-8281
Los Angeles, USA
eric.vance.821@my.csun.edu

Ani Nahapetian
California State University, Northridge
18111 Nordhoff Street
Northridge, CA 91330-8281
Los Angeles, USA
ani@csun.edu

ABSTRACT

In this work, we explore the feasibility of using only the Bluetooth received signal strength of a smart device to infer its user context. Devices that use Bluetooth wireless communication constantly transmit their wireless signal, especially in the case of smart watches that communicate via Bluetooth with their paired smart phones for their most basic functions. Adversaries or non-malicious applications can monitor Bluetooth signal strength to extrapolate the activities in which a user is engaged and the location of certain devices (e.g. cellphone in pocket or on a desk). We experimentally evaluate the accuracy with which a range of activities, including walking, typing, writing, and using a mouse, can be differentiated, simply by using the RSSI of a user-worn smart watch.

CCS Concepts

• Human-centered computing → Ubiquitous and mobile computing → Ubiquitous and mobile computing theory, concepts and paradigms → Mobile computing
• Security and privacy → Security in hardware → Embedded systems security

Keywords

Bluetooth; context-awareness; wearable computing.

1. INTRODUCTION

Bluetooth is a popular short-range wireless communication technology. Its adoption enabled the replacement of physical cables for connecting mice, keyboards, and joysticks to personal computers. In the mobile paradigm, its ubiquity enabled personal area networks (PANs) and body area networks (BANs). For example, Bluetooth is the enabling technology for hands-free smart phone usage in cars, popular wireless audio/music speakers, and smart phone tethering.

Bluetooth is also the predominant communication channel between smart watches and their paired smart phones. Therefore, with the growing adoption of smart watches, large swaths of the consumer population will be continuously emitting at least one Bluetooth signal. This is in addition to any signal from their smart phones and other wearable devices.

Once a user enables Bluetooth on their device, a signal will broadcast continuously. Other devices within range can be programmed to capture these signals. Without pairing devices, we show that a great deal of information can still be gathered by the client device just by analyzing the signal of parent device.

When two or more Bluetooth enabled devices come into proximity, they automatically establish a connection, by adopting a common clock and hopping sequence to form a piconet. After which, the two devices are considered paired, with one device serving as the master, and the other device the slave.

To prevent the pairing of a Bluetooth device with a malicious entity, a comparison of six digit keys can be used or device-level authentication can be carried out. For example, an iPhone's smart phone camera is used to confirm the Apple Watch with which it is being paired. However, such pairing approaches and service-level encryption do not limit the transmission of the Bluetooth signal prior to the pairing attempt.

A Bluetooth device can be placed into 'nondiscoverable mode,' but a brute-force search attack can still discover the device. [8] The only effective solution to prevent signal receipt by a client device is to disable the Bluetooth radio.

This research identifies a user's activity by merely examining the Bluetooth signal strength from a smart device. Common

SMARTOBJECTS'18, June 25, 2018, Los Angeles, CA, USA

ACM 978-1-4503-5857-6/18/06…$15.00
https://doi.org/10.1145/3213299.3213300

activities including walking, typing on a laptop, using a mouse, and using a smart phone are explored in our experimentation. The location of the receiver device, in our case a smart phone, is also varied to include the pocket and on an adjacent desk. Thus enabling the localization of devices, simply using RSSI.

Bluetooth has been used to infer location, especially in retail settings (albeit by explicitly pairing devices as part of a proprietary app). Proximity sensing in a nursing context [6], indoor positioning using Bluetooth [4], and location-aware computing [5] have all been considered in the literature.

This work goes beyond merely determining the person's distance from the receiver, as is the case with the previous work, to classifying fine-grained user activity and the positioning of devices on the body.

We do not require the person being monitored to be aware of or participate in the monitoring. Bluetooth receivers can be placed across retail and public spaces to determine consumers' interaction with the products in the space and to capture user contextual information. A malicious agent can similarly determine this information with a masquerading app that does not interface with the smart watch, at all.

The remainder of this paper is organized as follows. Section 2 outlines the underlying sensing paradigm which uses received signal strength to determine beacon's user activity. In section 3, we describe the approach and how retailors and other agents can exploit this information to their benefit. In section 4, we detail our experimental set-up involving monitoring a smart watch's Bluetooth signal while the person is engaged in a variety of activities. In our experimentation, the Bluetooth signal from a Moto 360 smart watch was captured using an Android smartphone. The Bluetooth's received signal strength indicator is used to classify the user activity. In Section 4.3, we present the results of the various experiments we conducted, encompassing 3 study participants, 7 activities, and 3 different device placements. We conclude the paper in Section 5.

2. RECEIVED SIGNAL STRENGTH INDICATOR (RSSI)

Received signal strength is the relative strength of the beacon's received signal by the client device. RSSI values are read from the input power function register RSSI_VAI which has a dynamic range of 100dB [1]. Depending on the network chip, readings will be given in the range of 0 to -00 or 0 to -127. The larger the value, the closer to 0, the stronger the received signal is and the closer the beaconing device is to the receiver. RSSI is measured in decibel-milliwatts (dBm).

RSSI ranging technology is used to approximate the distance between the device and the beacon, without additional hardware. It infers the distance between nodes by analyzing the received signal strength which is the lowest cost distance measurement for wireless networks [1].

RSSI raw values have an inherent inaccuracy, but are still used as a standard tool for distance measurements in range-based localization [2]. Various filters, such as Gaussian and Kalman, have been commonly used to improve accuracy of readings within sensor networks. We use the Savitzky-Golay filter, which had been shown to perform better than other standard averaging filters [3].

3. APPROACH

In this work, we explore the granularity and accuracy with which user activities can be determined by monitoring only the received signal strength indicator of a worn device. Specifically, we use the Bluetooth RSSI from a worn smart watch as detected by a neighboring device. The approach can easily be applied to a smart phone or other Bluetooth enabled device worn by the user.

3.1 MONITORING IN PUBLIC AND RETAIL SPACES

In public or retail spaces, by simply putting Bluetooth receivers across the space, the actions of the users in those contexts can be determined and monitored.

Consider the following scenario. In a museum, the users walking through the space, talking on the phone, photographing art, and writing in journals can all be determined simply by monitoring the changes in their device's Bluetooth signal strength.

Similar parallels exist in retail spaces. The user can be price-comparing on the smart phone, calling someone, searching for an item online. There is no requirement for the user to download and enable retailor apps, as is required by the currently available Bluetooth-based consumer monitoring systems.

3.2 ATTACKS BY MALICIOUS AGENTS

This approach can also be used by malicious agents trying to determine private user information. Although it is not fine-grained enough to determine passwords, the approach can be used to determine when smart phone usage is taking place to initiate the start of more costly information gathering and data trasmission.

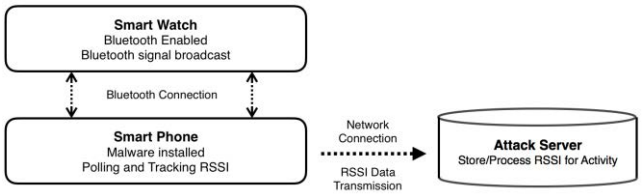

Figure 1. Attack model where malware is located on the user's smartphone with a paired smart watch. The malware polls the RSSI from the smart watch and relays the readings to a server off site for processing and storage.

Proximity is not a requirement for the attack. The adversary can implant malware on the smartphone of the target. No malicious apps are needed on the smart watch. Permissions are required to access the phone's network connection and Bluetooth. Both permission requests are relatively common in apps, as free apps use network connectivity to serve users ads for monetization. Bluetooth permissions can be disguised by the applications purpose. One example is a specialized fitness application that uses sensor readings in the smart watch to track fitness progression and caloric expenditure. Another common functionality is a message service from the phone to watch, which would clearly require Bluetooth permissions.

Note, that Bluetooth connectivity with the smart watch is not a requirement. For example, Bluetooth can be for pairing the smart phone with the car speaker. With this permission in place, the app can monitor the smart watch, without even requiring an app for the wearable device.

It is a safe assumption that the smart watch has Bluetooth enabled, as the value and utility of the smart watch is greatly diminished otherwise.

The adversary can be anywhere. Data can be streamed and stored on a remote server for processing and collection. Since processing is happening on the server, power usage will be dominated by the network data transfer of the minimal RSSI readings. Figure 1 gives a high level diagram of the attack layout.

3.3 DYNAMIC TIME WARPING (DTW)

To carry out the activity classification, we use dynamic time warping (DTW). DTW is an algorithm that determines the optimal stretching and compressing of a signal to match another reference signal, resulting in a distance value between signals.

Using a single reference signal for each activity, we compare test signals against all reference signals to obtain a set of distances. Then, we classify the test signal as the activity whose distance from the test signal is the least.

4. EXPERIMENTATION

4.1 EXPERIMENTAL SET-UP

A series of experiments to evaluate the effectiveness of the approach was carried out on three different users. All the users wore a Moto360 Android smart watch on their right hand and the RSSI values were recorded with a Nexus 6PAndroid smart phone. The smart phone acted as a receiver. The placement of the receiver, i.e. the smart phone, was varied. It was either placed on the table or in the right pocket of the user.

A custom Android application was developed to control and aid in the testing process. The app established a TCP connection to a local server. Each sample was started, stopped, and named from the application interface. The application polled the RSSI values between the smartphone and smart watch every second and sent these values to the server. The data was stored in a CSV format text file on the server

Various activities with variations for receiver locations were tested. Twenty 2-minute samples of each activity were collected, for a single user, resulting in 40 minutes of test data per activity. Additionally, for 3 different study participants 5 2-minute samples for 9 different activity/set-up combinations were collected.

The Savitzky-Golay filter was used to plot and analyze the RSSI data. This filter was chosen as it increases signal-to-noise ratio without greatly distorting the signal [7].

Dynamic time warping was used to identify if each activity's signal shared a similarity with other signals of the same activity. A moving mean, with a window size of 7, were used in the comparison.

4.2 ACTIVITIES

Seven different activities were considered in the testing. They included activities a user may commonly engage in and those that can involve sensitive data. The phone was placed in the pocket or on the table next to the user during tests to replicate typical usage.

4.2.1 Walking

Walking was done at a normal pace and continuous for two minutes. The user was required to not stop during the 2 minutes and use the natural motion of swinging each arm with the motion of the opposite leg. The smartphone was placed in the right pocket with the smart watch on the right wrist.

4.2.2 Typing Pocket/Table

Typing is separated into two tests of twenty samples each using a different setup. The first test was collected with the phone in the right pocket. The second typing dataset with the phone on the table far side of the computer, Figure 2.

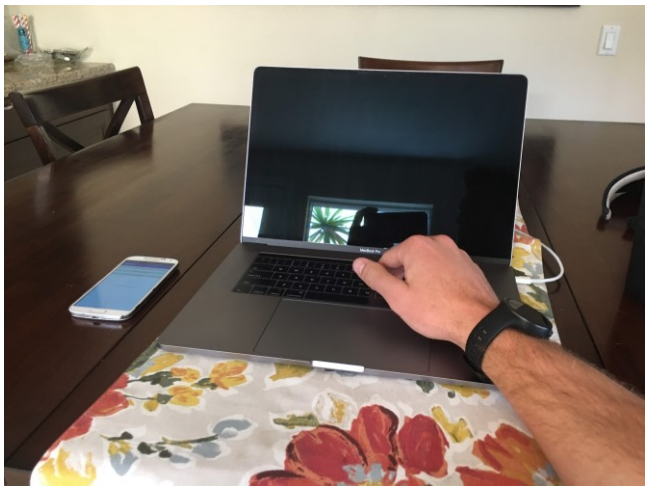

Figure 2. The alternative typing setup consisted of the phone being placed to the left of the computer. This is the same position that the phone was placed during the Bluetooth mouse testing.

4.2.3 Bluetooth Mouse

The smartphone was placed next to the laptop on the left side of the desk as it was in the typing tests, see Figure 2. An Apple Magicmouse 2, connected via Bluetooth to a Macbookpro laptop, was used in the right hand during each testing sample. The smart watch was worn on the right wrist positioned just above the mouse.

4.2.4 Smart Phone

The smartphone held in the right hand closest to the smart watch. The right hand simulated gestures and maneuvered through various screens on the phone.

4.2.5 Using a Tablet on Lap/Desk

During the first test, an iPad 1 was positioned on the users lap. The user performed any activity they chose while they were using the iPad. The only constraint put on the user was to swipe or touch the iPad with the right hand. During the second test, an iPad 1 was positioned on a table where the user sat and in front of the user. The user was not limited to any activities while using the iPad, but was constrained to swipe or touch with their right hand.

4.2.6 Picking up Item

During this test, a user was asked to repeatedly pick up an imaginary item and put it in their pocket. The user would take a brief 2 seconds once the motion of putting the item in the pocket was finished, and repeat the process of picking up the item off the floor. The spot where the imaginary item on the floor was located was directly in front of the user's foot.

4.2.7 Writing on Paper

A user was asked to write anything they would like on a piece of paper using a pencil. The user was not restricted to what they could write or draw. The user was asked to write or draw using their right hand. The smartphone was placed just to the left of the piece of paper, similar to the typing activity.

4.3 RESULTS AND ANALYSIS

The comparison of the RSSI across activities and multiple runs of activities makes evident that the RSSI is distinct across activities, while still fairly consistent across different runs of the same activity.

Figures 3, 4, and 5 graph the RSSI for 5 runs of walking, typing at a desk, using a mouse.

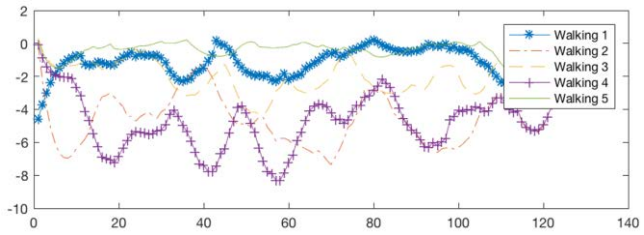

Figure 3. RSSI (dBm) across 2-minute period for a single user walking across 5 different runs.

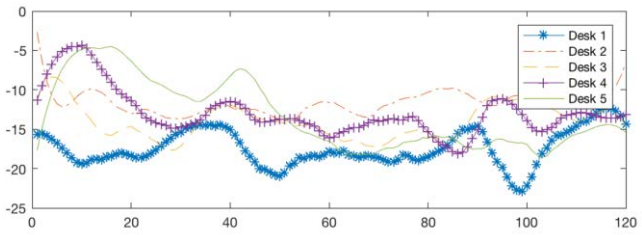

Figure 4. RSSI (dBm) across 2-minute period for a single user typing at a desk across 5 different runs.

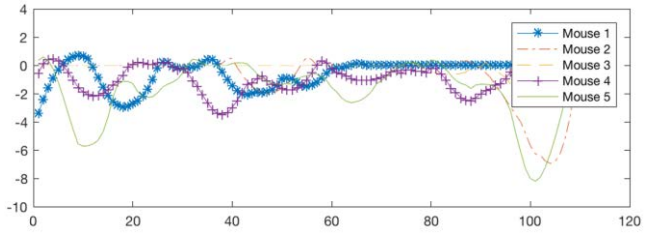

Figure 5. RSSI (dBm) across 2-minute period for a single user using a mouse across 5 different runs.

Figure 6 provide the median tendency of 20 samples of five different activities for a single user across multiple days.

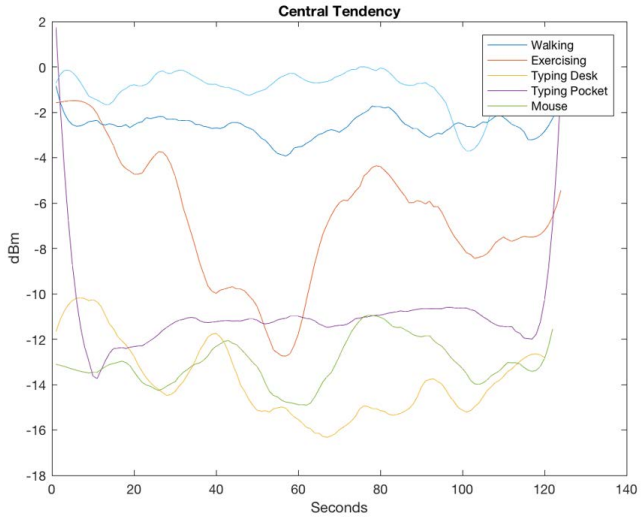

Figure 6. Central tendencies of activity's RSSI. This graph is comprised of the median tendency of the 20 samples for each activity tested. Each sample lasted two minutes totaling 40 minutes of test data per activity. The 20 test samples were collected over multiple days.

Table 1 provides the mean, median, and mode for different sets of experiments on a single user for a set of activities, for 20 samples of data per activity and set-up. As demonstrated, there are clear distinctions among the RSSI across the various activities.

Table 1. The mean, median, and mode RSSI for the various activities are shown across twenty sample for a single user.

Activity	Samples	Mean	Median	Mode
Tablet on table	20	-20.848	-22	-24
Tablet on lap	20	-13.892	-14	-25
Using Mouse	20	-13.536	-13	-15
Walking	20	-6.907	-7	-8
Typing, phone on desk	20	-8.021	-9	-13
Typing, phone in pocket	20	-17.820	-17	-27
Using phone	20	-1.036	0	0
Picking up item	20	-8.315	-8	-7
Writing with a pencil	20	-13.132	-13	-15

In our experimentation, we had three study participants (2 male, 1 female) carry out a series of activities, 5 times per activity, over a period of 2 minutes per activity. We used a 20/80 train/test split.

We took one recording as the reference signal for the DTW implementation, resulting in four test sample per activity. Then we repeated this train/test split two more times, arbitrarily selecting a different reference signal each time.

The prediction matrix for the DTW-based classification is provided in Table 2. The table represents 4 and half hours of collected data.

For the one female participant, activities including walking, picking up an item, talking on the phone, typing with phone in pocket, and using tablet on lap achieved a classification accuracy of 100%. The two male participants had greater error in all of their activity classifications.

For all three participants, the classification of walking and using a tablet on the lap was above 75%, with random chance at 11%. Using a phone, was also over 63% accurate. Some activities with very similar signal profiles were confused for each other, thus affecting the total classification results.

5. CONCLUSION

We demonstrate that Bluetooth RSSI can be used to determine user activity, without requiring additional hardware and without requiring the user to do anything other than have the Bluetooth enabled. Our experimentation using a smart watch as the Bluetooth beacon demonstrates that some activities, including walking, using a tablet on the lap, and using a smart phone, can be classified with high accuracy.

6. REFERENCES

[1] Z. Jie, L. HongLi, and Tanjian, “Research on ranging accuracy based on rssi of wireless sensor network,” in The 2nd International Conference on Information Science and Engineering, Dec 2010, pp. 2338–2341.

[2] H. S. AbdelSalam and S. Olariu, “Towards enhanced rssi-based distance measurements and localization in wsns,” in IEEE INFOCOM Workshops 2009, April 2009, pp. 1–2.

[3] G. Deak, K. Curran, and J. Condell, “Filters for rssi-based measurements in a device-free passive localization scenario,” Image Processing & Communications, vol. 15, no. 1, pp. 23–34, 2010.

[4] G. Anastasi, R. Bandelloni, M. Conti, F. Delmastro, E. Gregori, and G. Mainetto. 2003. Experimenting an Indoor Bluetooth-Based Positioning Service. In *Proceedings of the 23rd International Conference on Distributed Computing Systems* (ICDCSW '03). IEEE Computer Society, Washington, DC, USA, 480-.

[5] A. Huang and L. Rudolph, “A privacy conscious bluetooth infrastructure for location aware computing,” In Proc. of SMA 2005 Symposium, Singapore, January 2005.

[6] H. O. R. Naya F. Noma and K. K, “Bluetooth-based indoor proximity sensing for nursing context awareness,” Ninth IEEE International Symposium on Wearable Computers, vol. ISWC’05, 2005.

[7] J. Y. Jung, D. O. Kang, J. H. Choi and O. G. Min, "Near field distance awareness algorithm using bluetooth for device sociality service," *2016 18th International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, 2016, pp. 140-143.

[8] Cross D., Hoeckle J., Lavine M., Rubin J., Snow K. (2008) Detecting Non-Discoverable Bluetooth Devices. In: Goetz E., Shenoi S. (eds) Critical Infrastructure Protection. ICCIP 2007. IFIP International Federation for Information Processing, vol 253. Springer, Boston, MA.

Table 2. Prediction matrix for all 3 participants using dynamic time warping for 2-minute tests per activity. Three different reference signals were selected from the 5 runs of each activity, resulting in 3 different reference signal and 12 test signals per participant. The table represents a total of 270 minutes of data.

Actual Activity	**Predicted Activity**								
	Walking	*Picking up item*	*Using mouse*	*Typing, phone on desk*	*Typing, phone in pocket*	*Using tablet on table*	*Using tablet on lap*	*Writing*	*Using phone*
Walking	77.8% (28)				8.3% (3)	8.3% (3)			5.6% (2)
Picking up item	36.1% (13)	55.5% (20)				2.8% (1)			5.6% (2)
Using mouse		13.9 (5)	25% (9)	22.2% (8)	2.8% (1)		2.8% (1)	11.1% (4)	22.2% (8)
Typing, phone on desk			66.7% (24)	2.8% (1)	16.7% (6)	8.3% (3)			5.6% (2)
Typing, phone in pocket	16.7% (6)				52.8% (19)	11.1% (4)		8.3% (3)	11.1% (4)
Using tablet on table	19.4% (7)	8.3% (3)	5.6% (2)		13.9 (5)	16.7% (6)	2.8% (1)	33.3% (12)	
Using tablet on lap	13.9 (5)	2.8% (1)				8.3% (3)	75% (27)		
Writing	11.1% (4)	8.3% (3)	19.4% (7)	2.8% (1)	5.6% (2)	8.3% (3)		36.1% (13)	8.3% (3)
Using phone		27.8% (10)				8.3% (3)			63.9% (23)