TEA: Transmission Error Approximation for Distance Estimation between Two Zigbee Devices

Weijun Xiao, Yan Sun, Yinan Liu, and Qing Yang
Dept. of Electrical and Computer Engineering
University of Rhode Island, Kingston, RI 02881
{wjxiao,yansun,yinan,qyang}@ele.uri.edu

Abstract

*This paper proposes a simple and cost-effective method named **T**ransmission **E**rror **A**pproximation (TEA) for estimating the distance between two Zigbee devices. The idea is to measure and analyze statistically packet loss rates for approximate distance estimation. We have implemented an experimental prototype for the TEA using Zigbee protocol. The prototype is built on FreeScale's MCF5208 evaluation boards that have a built-in MC13192 ZigBee Transceiver chip. Field experiments have been carried out at the lacrosse field on URI campus. Measurement results show that TEA is a cost-effective way of distance estimation and provides much better resolution than other methods based on signal strength when the distance is greater than 60 feet.*

1. Introduction

Following the technology wave of the Internet, a new emerging network technology, wireless personal area network (WPAN), has gained great momentum. The international standard, IEEE 802.15.4, named ZigBee has emerged with many technology promises. Hardware devices in compliance with the standard are now readily available. For example, a ZigBee wireless transceiver with built-in 8-bit microcontroller is available today in the market for less than $4 dollars. Besides low cost, the distinctive features of ZigBee devices are low power consumption and moderate transmission bandwidth. The ZigBee technologies have opened up many opportunities in real world applications and many products making use of the WPAN are emerging such as home automations, wireless lighting control, wireless security system, wireless utility controls; automotive networks, industrial automations, and interactive toys.

Our focus of this paper is on distance estimation between two ZigBee devices. Although there have been proposals for mobile positioning using sensor networks based on pre-existing infrastructure [1,2], ad hoc mobile network [3], or hybrid of the two [4], most of them need the infrastructure for positioning. Measuring the distance between two communication devices using the existing ZigBee standard and the existing hardware component is technically challenging because of the following reasons:

a) Traditional way of estimating the distance between two communicating devices uses analog devices by measuring the strength of the received signals. This can not be applied directly to digital devices without significant change to the hardware because noise and interference easily affect the measured results.
b) Measuring propagation delay between the two communication devices using sonic transceivers will increase the hardware cost and power consumption losing the advantages of economy of scale.
c) It is possible to estimate the direction of arrival signals using antenna array and examine the phase of the receiving signals. The distance can be determined based on the direction of arrival signals. This will require multiple antennas located far apart increasing the hardware cost significantly.

d) GPS [5] has been well known for positioning but with cost in a different order of magnitude from what we considered here.
e) Another type of positioning services relies on a pre-deployed sensor network. The distance between the device and pre-deployed sensors are estimated first, and the sensor network calculates the location of the device.

Our objective here is to come up with a simple and cost-effective method for estimating the distance between two Zigbee devices using commodity hardware components. With no special hardware needed, our method uses existing network layer protocol (SMAC) between two communication devices [6]. Our method makes use of the power management module on the MCU of a Zigbee device. By configuring and tuning of the power management functions, we transmit a sequence of packets of different sizes at network layer. Statistical analysis is then performed on packet loss rates (PLR). We called the method *Transmission Error Approximation (TEA)*. Based on the analysis, we are able to approximately measure the distance between two Zigbee devices, and trigger desired actions depending on different applications such as pet leash, wireless child safety device, assets tagging, patient monitoring, and so on.

We have implemented an experimental prototype for measuring the approximate distance between two communication nodes using Zigbee protocol. Our prototype was built on FressScale's MCF5208 evaluation boards that have built-in MC13192 ZigBee Transceiver. We have developed a simple application protocol on top of the standard MAC protocol of IEEE 802.15.4. The application protocol measures packet loss ratio for various packet sizes. This packet loss ratio gives a transmission error approximation (TEA). Statistical analysis is then used to estimate the distance between the two communicating devices. Extensive experiments have been carried out on the lacross field on our campus. Measurement results show that TEA is a cost-effective way of distance estimation and provides much better resolution than other methods based on signal strength when the distance is greater than 60 feet.

The rest of the paper is organized as follows. Next section summarizes the related work. The detailed description of the TEA and theoretic analysis are given in section 3. Section 4 presents our implementation and numerical results followed by discussions on security issue in section 5. We conclude our paper in section 6.

2. Related Work

Extensive research has been reported in the literature for distance estimation and positioning of wireless devices. For distance estimation of two wireless devices, existing techniques can be broadly classified into the following three categories: time-of-Arrival (ToA), angle-of-arrival (AoA), and Received Signal Strength Indication (RSSI) [7,8].

ToA is based on the speed of radio wave propagation and the measured time it takes for a radio signal to move between two objects. Signal propagation delay combined with the measured time allows the ToA system to estimate the distance between a sender and a receiver. ToA offers high levels of accuracy, but requires relatively fast processing capabilities to resolve timing differences for fine-grained measurements. This problem is amplified over short distances, making ToA a poor choice for a ranging technique for positioning in wireless, ad-hoc sensing networks.

ToA measurements can be combined with acoustic measurements to achieve accuracy of a few percent of the transmission range. Acoustic signals, however, are temperature dependent and require unobstructed line-of-sight. They are also reliant on directionality. More importantly, using acoustic measurements requires additional hardware, increasing the total cost of devices.

Unlike the ToA, AoA techniques make use of antenna arrays to measure the angle at which a signal arrives. Angles can be combined with distance estimates or other angle measurements to derive positions of devices. A major disadvantage of AoA techniques is the hardware requirement. The antenna arrays are expensive to be implemented and maintained, making AoA a poor choice for cost-conscious applications.

RSSI measures the attenuation in radio signal strength between the sender and the receiver. The power of the radio signal falls off exponentially with distance, and the receiver can measure this attenuation in order to estimate the distance to the sender. Experiments have shown, though, that RSSI yields very inaccurate distances [9]. This is the method assumed to be supplying the range estimates to the positioning algorithms.

As mentioned in the last section, our main objective here is to make use of the commercial off-the-shelf hardware components to implement approximate distance measurements between two nodes. Wide availability of low-cost and low power consumption ZigBee devices provide us with such an opportunity to build and test such distance estimation systems. To the best of our knowledge, packet loss rate has not been used to measure distance between wireless devices. Our experiments show that the TEA can measure the distance using commodity devices and has higher resolution than signal strength. Other benefits are that it does not rely on network infrastructure and is cost-effective.

3. Details of the TEA

3.1 Distance estimation based on signal attenuation (RSSI)

Without extra hardware support, signal attenuation is the only distance measurement method in the current literature. In particular, let d denote the distance between the host device and the remote device, P_t denote the transmission power and P_r denote the received signal power. Then,

$$P_r = \frac{P_t}{d^{\alpha}} \qquad (1)$$

where α is a constant between 2~4, depending on the wireless channel condition. When the transmitter sends pilot signals using a fixed transmission power, the receiver can obtain signal attenuation, defined as P_r / P_t , and therefore estimate the distance d.

Although the RSSI method is simple, it cannot achieve high accuracy for three reasons. First, since P_r can change rapidly due to the variation of wireless channel, mobility and moving obstacles on the transmission path, it is difficult to estimate P_r accurately. Second, the P_r value is affected by noise and interference. When noise and/or interference are not known and not negligible, the received signal power cannot accurately represents the distance. Third, equation (1) indicates that a small estimation error in P_r can result in a large error in distance estimation, especially when the distance is large. This can be verified by the following derivation.

$$P_r = \frac{P_t}{d^{\alpha}};$$

$$\Delta \mathrm{P_r} = -\frac{\alpha P_t}{d^{\alpha+1}} \Delta d;$$

$$\Delta d = -\frac{d^{\alpha+1}}{\alpha P_t} \Delta P_r;$$

where $\Delta \mathrm{d}$ and $\Delta \mathrm{P_r}$ represent distance change and received power change respectively.

3.2 Distance estimation based on the packet transmission statistics

Our approach makes use of the commodity hardware devices that are in compliance with Zigbee standard. To exploit the economy-of-scale, we design and implement the TEA at network layer above the MAC/PHY without any hardware changes. Instead, we try to make use of the existing features of the transmitter/receiver hardware. In particular, we implement a special packet transmission protocol by varying power levels of the MCU. It is a common practice in today's embedded MCUs to have a power management module for the purpose of power savings. Making use of this power management module, we are able to transmit data packets using different power levels. In particular, MCF5208 has 16 different power levels that can be configured at run time. The main ideal of our protocol is to transmit a sequence of data packet using different power levels. The receiver will report to the sender the statistics of successful packet transmission. We then estimate the approximate distance based on this statistics.

Depending on the wireless channel condition in reality, we select an optimal packet size and number of packets for transmission at the calibration stage. During normal operation, we transmit a sequence of packets with predetermined length from the transmitter. The receiver will calculate the packet loss rate based on the packet ID received and the predefined protocol at the calibration stage. The result of the calculation is sent to the transmitter in an acknowledgement packet using the maximum transmission power level. Based on the packet loss rate, the approximate distance between the transmitter and receiver can be estimated. Generally, the TEA method contains the following two steps:

Step 1: the receiver estimates packet loss ratio and feedbacks this information to the transmitter. In particular, the transmitter sends a sequence of data packets to the receiver. Each data packet has a packet ID. For example, the first data packet has ID x, the second data packet has ID x+1, the third data packet has ID x+2, and so on. These data packets are transmitted with different transmission power levels. For the Zigbee implementation by FreeScale, there are 16 transmission power levels, denoted by $P_1, P_2, ..., P_{16}$. Assume that total N packets are transmitted. Among these N packets, q_i percent of packets are transmitted using transmission power P_i . We refer vector $q = [q_1, q_2, ..., q_{16}]$ as *packet distribution*.

The receiver device receives packets. Based on the packet IDs, it knows how many packets are lost and then obtains *packet loss ratio*. The packet loss ratio should be a vector. The receiver sends the PLR back to the transmitter using the maximum transmission power.

Step 2: the transmitter estimates distance based on the PLR. When the transmission power is P_i, the bit error rate is a function of receiving signal-to-interference ratio and is related to the modulation scheme. In ZigBee protocol, modulation scheme is OQPSK [10]. The bit error rate is calculated as:

$$ber_i = erfc\left(\sqrt{\frac{P_i / d^{\alpha}}{I}}\right), \quad \text{and}$$

$$erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-y^2} dy \qquad (2)$$

where I is the noise/interference power, which can be estimated in the calibration stage [11].

The packet drop ratio is determined by bit error rate and the packet size. Let L denote the number of bits in each packet. Then, the packet loss ratio for each transmission power is calculated as

$$PLR_i = 1 - (1 - ber_i)^L \qquad (3)$$

The overall packet loss ratio is

$$PLR = \sum_{i=1}^{16} q_i \cdot PLR_i \qquad (4)$$

From (2)–(4), one can calculate packet loss ratio from the distance d, given q_i, P_i and L.

In Figures 1 and 2, we show how signal attenuation and packet drop ratio change with distance.

Figure 1 shows the received signal power (proportional to signal attenuation) as a function of the distance between the transmitter and the receiver. The upper plot shows the 16 curves, each of which is for a different transmission power. The lower plot shows the average. It can be seen that signal attenuation is not a good indicator of the distance. It can measure short distance. However, when the distance is large, the signal attenuation is not sensitive to distance changes. In other words, if there is a small error in the measurement of signal attenuation, the distance estimation will suffer from a large error.

Figure 2 shows the packet loss ratio as a function of the distance. The upper plot shows the curves for different transmission power and the lower plot is the overall PLR. Compared with signal attenuation, PLR is approximately a linear function with the distance for a large distance range. Obviously, the distance estimation based on PLR will be more accurate.

Figure 1 Received signal amplitude as a function of distance

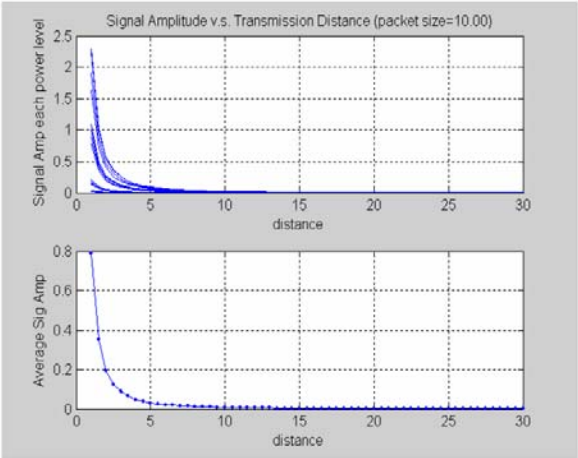
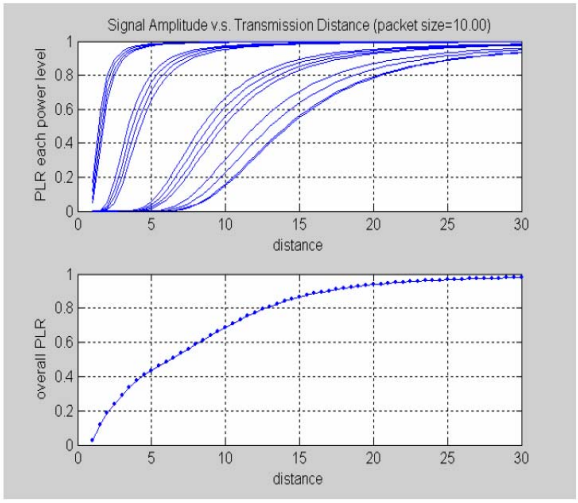


Figure 2 Packet loss ratios as a function of distance



4. Implementation and Experiments

We have implemented our experimental prototype on Freescale's MCF5208EVB with MC13192 transceiver. This implementation includes two wireless communication parities, transmitter and receiver. The embedded MC13192 transceiver is in compliance with ZigBee protocol and communicates with the main board MCF5208EVB through GPIOs [12]. We make use of source code of Zigbee implementation from SBC tools to develop our experimental prototype. The transmitter sends 100 packets for three different packet sizes with different power levels. The receiver side receives packets and sends acknowledgements to the transmitter. In order to compare the TEA with RSSI, the strength of receive signal is carried in acknowledgement packet. Considering the effect of antenna direction and interferences, we fixed the transmitter and measured the data from the transmitter side for every measurement by changing the position of the receiver device.

We have carried out experiments using our prototype implementation. The experiments were performed in a free space at a lacrosse field in a sunny day to minimize the interferences. Figures 3a, b, c, and d show the picture of our field experiments.

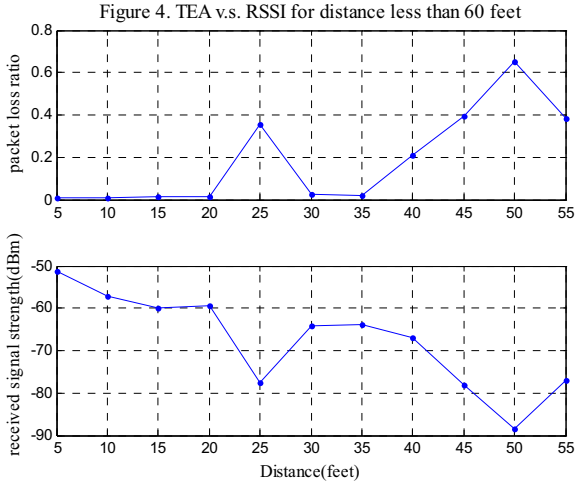
Figure 3a Remote view of the receiver in the lacrosse field of URI

Figure 3b Remote view of the transmitter in the lacrosse field of URI

Figure 3c Close view of the transmitter, MCF5208 EVB with battery power supply

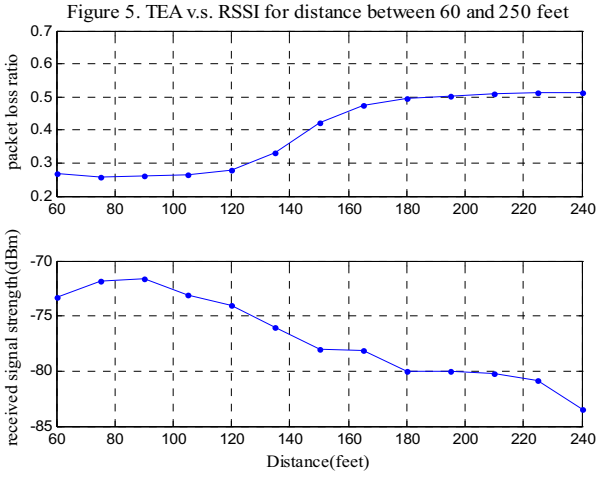
Figure 3d Close view of the receiver: MCF5208EVB with battery power supply

Figure 4. TEA v.s. RSSI for distance less than 60 feet



We measured the PLR and signal amplitude with increment of 15 feet in the range between 60 feet and 390 feet. In the range within 60 feet, we measured the same with the increment of 5 feet. We analyzed our data using three different ranges: less than 60 feet, distance between 60 to 250 feet, and greater than 250 feet. The results for distance less than 60 feet are shown in Figure 4. Both the TEA and RSSI are not effective. This is possibly due to the multi-path effects. The results for distance between 60 and 250 feet are shown in figure 5. The TEA can work for distance estimation. But the estimation is rough and not accurate because the power levels are not linear and are not uniformly distributed. As a result, the contributions of transmissions with different power levels are not equal. Our current design only averages packet loss rate associated with all different power levels to get the overall PLR. We will improve it in the future by weighing packet loss rates with different power levels differently. For the distance greater than 250, the TEA works perfectly and provides much better resolution than RSSI as shown in figure 6. When the distance is greater than 300 feet, the signal strength does not significantly attenuate. This shows the signal is very weak and not sensitive to distance changes. This point is in a good agreement with the theoretic analysis in section 3. But for this case, the TEA is still effective up to 390 feet distance. The function of packet loss ratio with distance is approximately linear.

Figure 5. TEA v.s. RSSI for distance between 60 and 250 feet



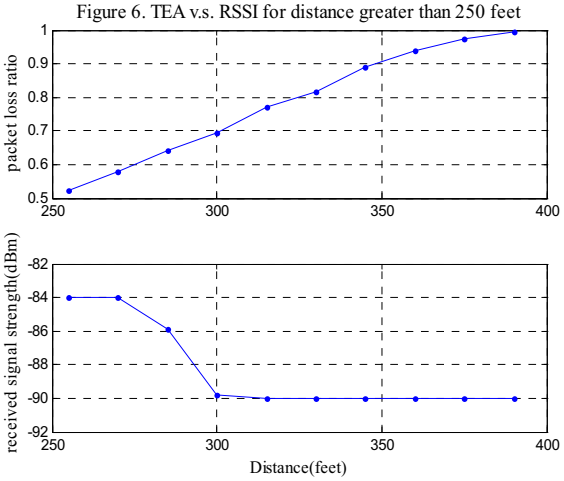
5. Discussions

Theoretic analysis and practical implementation measurements both show TEA can approximately estimate the distance between

two wireless devices in a designed distance range. Compared to RSSI, TEA can provide much better resolution and noise tolerance. In the following we will discuss another benefit of the TEA from the security point of view.

We assume that the attackers are outsiders. That is, they do not compromise the communication devices. What they can do is to interfere with signal and cause estimate error in distance. For the RSSI based methods, attackers can make the distance measurement become larger or smaller. They can reduce the received signal power by placing physical obstacles near the transmitter or receiver to block the direct-line-of-sight. As a consequence, the estimated distance will be larger than the real distance. They can also introduce interference or increase the noise level using a radio transmitter. This will increase the received signal power and the estimated distance can be smaller than the real distance. On the other hand, in out TEA method, attacks can only increase the estimated distance. Introducing physical obstacles and increase interference/noise both result in lower PLR, and therefore larger distance estimation.

Figure 6. TEA v.s. RSSI for distance greater than 250 feet



Many applications use distance measure to detect events that cause the distance between two devices larger than a threshold. For example, when the device carried by a parent and the device carried by the child is larger than a threshold, the parent is notified. When a precious item is taken out of a house, alarm is activated. In this type of applications, the attack that increases the distance measure is far less dangerous than the attack that can reduce the distance measure. In this circumstance, TEA is preferable because attackers only cause false alarm but not miss detection.

6. Conclusions

In this paper, we have presented a cost-effective method of estimating the approximate distance between two wireless communication nodes using ZigBee, referred to as **T**ransmission **E**rror **A**pproximation (TEA). A theoretic analysis has been carried out and an experimental prototype has been implemented using Freescale's MCF5208EVB and SBC tools. All experimental results are in a good agreement with theoretic derivations. Real measurements have demonstrated that the TEA is a cost-effective way of distance measurements providing higher resolution than signal attenuation method when the distance is greater than 60 feet. We will focus on distance range less than 60 feet and interference considerations in the future work.

Acknowledgments

This research is sponsored in part by National Science Foundation under grants CCR-0073377, CCR-0312613, and SGER Grant 0610538. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. The authors would like to thank Michael Smith for his help in our field experiments. The authors are grateful to the anonymous reviewers for their valuable comments that helped in improving the paper.

References

[1] S. A. Zekavat, H. Tong, and J. Tan, " A Novel Wireless Local Positioning System for Airport (Indoor) Security," *In Proc. SPIE'04.*

[2] M. Vossiek, L. Wiebking, P. Gulden, J. Wieghardt, C. Hoffmann, and P. Heide, "Wireless local positioning", *IEEE Microwave Magazine*, Vol. 4, Issue 4, Page(s): 77 - 86, Dec. 2003.

[3] S. Capkun, M. Hamdi, J.P. Hubaux, "GPS-free positioning in mobile ad-hoc networks", In *Proc.*

of Hawaii Int. Conf. on System Sciences, January 2001.

[4] Chris Savarese, Jan M. Rabaey, Jan Beutel, "Locationing in Distributed Ad-Hoc Wireless Sensor Networks," in *Proc. ICASSP'01*, 2001.

[5] M. E. Bernard, "The Global Positioning System," *IEE Review*, Vol. 38, Issue 3, Page(s): 99-102, March 1992.

[6] Intec Automation Inc., "SBC Tools User Manual," http://www.steroidmicros.com/documentation/documentation.aspx.

[7] J Hightower and G Borriello, "A Survey and Taxonomy of Location Systems for Ubiquitous Computing," *IEEE Computer*, Vol.34, Issue 8, Page(s): 57-66, Aug. 2001.

[8] Kaveh Pahlavan, Xinrong Li, and et al, "An Overview of Wireless Indoor Geolocation Techniques and Systems," In *Proc. of International Workshop of Mobile and Wireless Communications Networks*, Paris, May 2000.

[9] J. Hightower, R. Want, and G. Borriello, "SpotON: An Indoor 3D Location Sensing Technology Based on RF Signal Strength," *Technical Report*, UW CSE 00-02-02, University of Washington, Seattle, WA, February 2000.

[10] Freescale Semiconductor, "MC13192/ MC13193 Reference Manual," http://www.freescale.com.

[11] Couch, Leon W. III (1997), *Digital and Analog Communications*, Upper Saddle River, NJ: Prentice-Hall Inc.

[12] Freescale Semiconductor, "MCF5208EVB User Manual," product document, Freescale.