Geolocation of WiMAX Subscriber Stations Based on the Timing Adjust Ranging Parameter

Don E. Barber, John C. McEachen
Graduate School of Engineering and Applied Sciences
Naval Postgraduate School
Monterey, California

Abstract—This paper examines the geolocation of standard compliant WiMAX subscriber stations based on timing adjust values captured from the air interface during network entry and initial ranging. Field tests were conducted to verify a linear correlation between timing adjust and distance. Repeated observations at fixed distances established the variance within timing adjusts. Results of this field testing were extended to multiple base station networks modeled in computer simulation, ultimately suggesting the possibility for geolocations based on WiMAX initial ranging with ten times greater accuracy then similar methods applied to GSM.

Keywords-802.16; WiMAX; geolocation; timing adjust; ranging

I. INTRODUCTION

A. WiMAX

Just as Wi-Fi was developed as a common subset of the 802.11 standard to insure compatibility between vendors, Worldwide Interoperability for Microwave Access (WiMAX) is an industry consortium that certifies products which must commonly comply with specified aspects of the 802.16d-2004 fixed and 206.16e-2005 mobile standards. The fixed wireless standard provides the capability for leap frog advancement in connectivity without the high costs associated with the need to run cable to every subscriber. The mobile standard offers greater data rates than current 3G cellular technologies and provides greater mobility than 802.11. While WiMAX leaves room for different hardware implementation and special features for vendors to differentiate themselves, it also insures that there is commonality to ensure interoperability between base stations (BS) and subscriber stations (SS). Already, many WiMAX networks have been built out globally, with many more planned.

B. Geolocation

With the potential for wide deployment of WiMAX compliant devices in the near future, one important consideration is how to locate subscribers in both fixed and mobile applications. Emergency response personnel need to be able to quickly locate people and law enforcement may need location data for stolen property recovery. Beyond emergency response, there may be other homeland security necessities to find the location of a threat using wireless or mobile communications.

There are several means of locating wireless devices through both handset based and network based solutions. A GPS chip built into a mobile unit can provide accurate location data, but increases the cost to manufacture and power draw on the mobile device, while requiring the transmission of extra data. An external, passive approach to location trades off some accuracy to overcome the cost, power, and bandwidth penalties of a GPS solution. It also continues to provide a location capability even if the GPS location capability should malfunction or be maliciously disabled, which may be critical in law enforcement or homeland security applications.

In looking to the future, it is best to begin with what has already been done. GSM mobile stations can be located within several hundred meters based on an internal parameter for time of arrival called timing advance. Timing advance is used by the network and handset to align the traffic bursts with the time division multiple access frames of GSM. Using this timing advance and speed of propagation, range rings from base station towers can be approximated, and the intersection of these range rings from multiple towers provides an approximate location for the mobile station as illustrated in Fig. 1 [1]. Further refinement of this approach found averaging multiple timing advance measurements minimized error in random variable sampling, tightening location accuracy [2].
The uplink in the 802.16 MAC is also shared between SS in a time division multiple access fashion, with initial assignment of a timing adjust (TA) generated by the BS after the initial entry and ranging request by a SS [3]. This parallel to GSM creates an opportunity to leverage similar location techniques.

II. WIMAX SIGNAL INTERNALS

Given relative time robustness of WiMAX’s orthogonal frequency division multiplexing physical layer, one may wonder why an accurate timing adjustment mechanism is needed and included in the standard. The answer lies in the media access layer (MAC), between the physical signaling implemented via orthogonal frequency division multiplexing and higher internet protocol functionality. In order to control access to the shared wireless medium, a time division multiplexing scheme is used where the BS first transmits its information during the downlink before SS are allowed to transmit their information during allotted times during the uplink.

In order to keep this process functioning in an orderly manner, it is important for each SS to transmit their data at the correct time for it to arrive at the BS in its designated uplink slot. Timing for the downlink is already established since all stations use the preamble at the beginning of the downlink frame as a timing reference and simply count slots back from the beginning of the frame. Any delay in the downlink arriving at SS is then obviated since the frame clock starts when the frame arrives. However, on the uplink, since the data the SS is sending is still part of this frame, propagation time must be accounted for so that the SS’s information arrives at the BS in the correct slots as assigned in the uplink map. Because of this TA is a critical component of ranging.

A. Network Entry

In order to join a BS a SS must compete in a contention window, be recognized by the BS, and assigned frame slots. When initialized, a SS scans its allowed frequencies (as provided by the service provider’s network) to see if a WiMAX network is available. Once a BS frequency is acquired, the SS listens for the frame preamble to synchronize itself. If the SS finds the BS frequency suitable, it will also be able to find the contention opportunities for initial ranging to send its initial ranging request.

If the BS properly receives the initial ranging request, it responds with a ranging response message during the next downlink which indicates to the SS any adjustments needed to its power, frequency, and timing. This initial response contains the MAC address of the SS for identification purposes. The SS will again transmit a range request during its uplink slot and receive either a ranging response message for further adjustments or a ranging response message indicating the ranging status is complete.

Beyond network entry initial ranging, ranging also occurs periodically to account for changes in channel conditions and mobility, during bandwidth requests, and for handovers. Handover ranging is particularly interesting for geolocation since the message contains ranging from multiple BS [4].

B. Ranging Response Message

The ranging response message is defined in the 802.16d-2004 and 802.16e standards to contain a four byte TA containing a 32 bit signed number; negative to advance the burst transmission time and positive to delay [4],[5]. The standard defines the value to be variable depending on the physical layer, but commonality is expected between the fixed and mobile WiMAX standards based on nearly identical verbiage in the 802.16 standards and the focus on vendor time division duplexing interoperability [6]. The expected consistency indicates that work on geolocation based on fixed WiMAX equipment, which is significantly less expensive and more readily available for laboratory experimentation, will be easily transferable to mobile WiMAX. Vendor timing division duplexing interoperability implies that observations on one vendor’s WiMAX equipment will also be a valid representation of other vendor’s implementations.

C. Timing Adjust

The expected range per unit of TA can be calculated based physical layer specific units which are simply the reciprocal of the sampling frequency. The sample frequency is defined in the standard as

$$F_s = \text{floor}\left(\frac{n \cdot BW}{8000}\right) \times 8000.$$  (1)

The sampling factor, $n$, is dependent on the bandwidth used and also specified in the standard. For example, utilizing a 3.5 MHz bandwidth, the sampling factor is 8/7. Solving for $F_s$ with this sampling factor and bandwidth gives 4 MHz. Using the speed of light, approximately $3 \times 10^8$ m/s, and a TA of $1/F_s$, each unit of TA correlates to a distance of approximately 75 m.

III. FIELD EXPERIMENTS

Field testing was conducted to confirm that the TA captured in the ranging response messages linearly correlated to distance and establish variability in repeated measurements at a fixed distance. This variability in repeated measurements is crucial in determining the accuracy of a location fix based on TA, since a high variance in TA at a fixed location would lead to a rather large area of uncertainty in approximating a SS location.

A. Testing Procedure

In order to conduct testing, Redline WiMAX equipment was used to establish a simple outdoor WiMAX network,
consisting simply of the BS and SS operating at 3.4175 GHz with a 3.5 MHz bandwidth. The testing site was predominately flat terrain with some trees and small single story buildings, providing primarily line of sight conditions during testing. Conditions were clear, with temperatures approaching 35 degrees Celsius at midday.

Configuring the WiMAX network, the AN-100U BS and antenna were mounted on top of a raised observation platform, with the antenna mounted 7 m above the ground. The SU-O SS was attached to a portable wood stand with the SS antenna 2 m above the ground. Network entry was facilitated simply by powering up the SS, which began the network entry process, just as turning on a cell phone negotiates network entry even if the user is not immediately placing a call. Powering down the SS and powering it back up at the same location allowed for repeated captures of the network entry process to capture multiple RNG-RSP messages at the same distance from the BS.

Collection in the field was done from a vehicle, simulating what would realistically be done by emergency response personnel. Using a roof mounted omni-directional antenna, the WiMAX signal was captured from the air interface by a Sanjole WaveJudge 4800. GPS coordinates were also manually entered from the output of a basic consumer Garmin nüvi 200. Fig. 2 diagrams the configuration of test equipment.

B. Results

The SS was set up at six different locations, with trials run until at least five TA were successfully collected. One exception occurred later in the day at the final range of greater than 1 km when only one TA was successfully captured due to equipment difficulties.

The collected data is plotted in Fig. 3. The observed TA were all negative, which from the standards is defined to indicate the SS should be transmitting sooner. For the sake of clarity, only the magnitude of TA is shown so a greater TA reflects greater distance and timing advance, avoiding any possible confusion with larger negatives being smaller.

The results show an average meters per unit of TA is 36.99. A basis offset was taken into account correcting for the TA seen at no distance due to the delay between the BS transmit and receive channels. The offset was based on the measurements in the lab for this particular BS, but the phenomenon has also observed on other vendors WiMAX BS equipment [7].

To establish the overall variance in TA, the results of all tests were combined into a single probability density function by using the median at any given distance as a reference point. Based on this cumulative data, the overall standard deviation of TA was calculated to be 0.673 units.

Each unit of TA resulting in a radial distance increase of 37 m is almost exactly half of the calculated distance of 75 m. The factor of two difference between the calculated and measured TA is likely unique to initial ranging. Initial range occurs after the SS synchronizes to the received BS preamble. However, since the BS does not know how long it took for its downlink to arrive at the SS, the first delay it sees includes the time it took for the downlink to reach the SS plus the propagation time for the SS’s initial ranging request to reach the BS. The total round trip time takes twice as long as the SS normal uplink to the BS, essentially decreasing the meters per unit TA by two during initial range. However, despite the extra resolution this provides during initial ranging, once the SS has an assigned uplink slot, continuing periodic ranging adjustments may return to a range resolution of 75 m.

IV. MONTE CARLO SIMULATION

While field and laboratory testing were limited to the one available BS, to better understand the potential for geolocating a SS in a real world WiMAX network, several multiple BS scenarios were simulated in software. Using the data collected from the BS in the field tests, MATLAB was used to simulate multiple BS with the same mean TA per distance of 37 m and cumulative standard deviation in TA at constant range of 0.673. While this assumes that all BS in the network share the same characteristics as the one AN-100U BS used in testing, it remains a reasonable premise based on the designed interoperability within the standard.

A. Two Base Station Simulation

First, two BS scenarios were simulated to approximate the location of a SS based on two radii. The algorithm to find this location base on two radii is shown in Fig. 4, were first the radii are compared to the distance between the BS and then an estimate center point is determined. If the radii do not intersect, the approximation is where the radii are closest to intersecting. If the radius circles do overlap, the points of intersection can be calculated based on the two radii and distance between the BS.

For example, assuming a basic Cartesian coordinate plane with one BS at the origin and the other at a distance, D, along the X axis, the X coordinate of the intersect is

$$X = \frac{R_1^2 - R_2^2 + D^2}{2D}. \quad (2)$$

Applying the Pythagorean Theorem with this base distance and the first radius as the hypotenuse, the Y coordinate of the intersections is
The simulation created two BSs at varying angles as observed by the SS, each with normally distributed random distance with a mean of 1 km and a standard deviation of 300 m, and TA fluctuations as observed through field measurements. At 180 degrees, the two BSs and SS form a straight line, and SS is location is accurately approximated in the middle. However, as the angle collapses from this ideal geometry, the two intersections of the radii get farther and farther apart, and since there is ambiguity as to which intersection represents the location of the SS, the location approximation of a midpoint between the intersections becomes farther and farther from the true SS location. If other a priori knowledge could distinguish between the two intersections, one of the intersections is always close to the SS, but the algorithm alone cannot differentiate the two intersections. Fig. 5 shows the results of these two BS simulations.

\[ Y = \pm \sqrt{R_1^2 - \left( \frac{R_1^2 - R_2^2 + D^2}{2D} \right)^2}. \]  

(B) Multiple Base Station Simulations

Noting the limitations of a two BS fix, a second set of simulations was conducted in MATLAB using multiple BS. Except in rare cases, introducing a third BS removes the ambiguity in which of the intersections of the two BS solution represented the true location of the SS. The general approach of the multiple BS simulation algorithms is simply to calculate the intersections of each pair of BS radii, and then for each pair's intersections, see which is closest to the nearest intersection of the next pair of BS’s radii. This intersection should represent the intersection nearest the SS.

Using this refinement to the approximation algorithm to remove two BS fix ambiguity, several multiple BS scenarios were tested. First, all BS were placed at random angles from the SS with normally distributed random distances with a mean of 1.2 km and a standard deviation of 400 m. This completely random placement of BS was repeated for 100,000 runs at each number of BS, and the average distance from the estimate to SS at each number of BSs was recorded as in the earlier two BS simulation. Fig. 6 shows sample plots from a run of this simulation with three and four BS.

As previous alluded, an interesting result of the completely random BS placement was that sometimes rare geometries would cause even the three BS scenario to produce an inaccurate result if the algorithm selected to weight a cluster of intersection where the SS was not actually located. Basically, a three BS fix can devolve to the two radii ambiguity problem with unfortunate geometry and nearly collocated BS. Since all of the geometries are averaged in with the other runs, estimates that are hundreds of meters off weigh in with many very accurate estimates from a three BS geolocation, as reflected in the results shown in Fig. 7. Given that the overall average error between the approximated center point and the SS is still only 80 m, there are many more accurate fixes than the outlier cases that pull up the average.

In a real world network, BS locations can be anticipated to be more logically distributed. While actual tower locations in modern cellular networks rarely align exactly to the idealized honeycomb cell layout, they are generally spaced to provide maximum coverage with the least number of towers dependent on subscriber density. As such, two follow-on multiple BS simulations were run that added some structure to the BS placement. First, the angles were fixed to be evenly spaced based on the number of towers while distances were randomly assigned as in the initial multiple BS simulation, and then for even further structure, the same even angle distribution was used but with all BS at a one kilometer range from the SS. Fig. 7 shows these results, which show greater location accuracy than the completely random case. In networks with more structured BS spacing the error estimate, despite TA rounding and variations, is still less than 30 m in all cases.
V. CONCLUSION

Both laboratory and field testing indicate a high linear correlation to distance with low variance in the TA observed in the initial ranging response message. Based on this result, it is possible to establish a range radius from the BS. Using multiple range radii from several BS crossing radii can establish very accurate locations.

The interoperability standards established by the WiMAX forum provide that, taking due diligence, these results should easily extend to other vendor’s equipment and the near verbatim replication of verbiage in the 802.16d-2004 and 802.16e standards suggests easy adaption of this methodology to mobile WiMAX taking into account adjustments to physical layer dependent parameters. Furthermore, WiMAX’s chief competitor for the fourth generation cellular market, Long Term Evolution (LTE), also operates in a very similar manner, featuring time division duplexing profiles which could similarly be used to geolocate just as explored here for WiMAX networks.

Using the measurements from field testing and results of simulation, it is possible to geolocate a WiMAX SS within approximately 50 m during initial ranging, offering potentially 10 times better location accuracy than the GSM methods previously explored in literature, and providing a great capability to be further developed and explored for use both by emergency response and homeland security personnel.

ACKNOWLEDGMENT

Our thanks is extended to all of the Naval Postgraduate School faculty and staff who enabled this research, as well as Dr. Xavier Leleu, Sanjole CTO, for his insights on monitoring and diagnostics in WiMAX networks.

REFERENCES


