# A Novel Initial Ranging Algorithm for mobile WiMAX (802.16e)

V V Girish, V K Govindan
National Institute of Technology
Calicut, Kerala
India-673601

Shakeel Baig, Vijaya Yajnanarayana
Nokia Siemens Networks-DC
Bangalore
India-560001

## ABSTRACT
Initial ranging process plays an important role in the mobile worldwide interoperability for microwave access (WiMAX) standard (IEEE 802.16e). Timing offset adjustment, power offset calculation and synchronization between the base station and all the users within a cell are achieved during the initial ranging process. A comparative study of existing and a novel ranging algorithm is proposed in this paper. Most of the current ranging algorithms do not take in to account the interference created by the ranging codes sent by other ranging users in an Orthogonal Frequency Division Multiple Access (OFDMA) setup [2][4][5][7]. The novel ranging method cancels the interference created due to the other raging codes in the ranging area. The simulation results indicate a significant improvement in performance under practical scenarios.

## General Terms
Algorithms, Performance, Design

## Keywords
IEEE 802.16e, Ranging, OFDMA, Ranging Simulations

## 1. INTRODUCTION
WiMAX is a new 3.5G telecommunication standard providing point to point and point to multi-point communication. This emerging technology is defined in IEEE 802.16e specification. IEEE 802.16-2005e defines the wireless communication for the mobile users, moving at a maximum speed of 125 KMPH in the frequency range of 2-6 GHZ [1][2]. The Medium Access Control layer of mobile WiMAX supports different physical layer modes; this offers several organizations to configure their mobile WiMAX deployment depending on their requirements. The most popular physical layer mode for the Mobile WiMAX is OFDMA.

In OFDMA, the subcarriers are divided into different groups called sub channels and are assigned to different users for multiple user access. The subcarriers for each channel are made orthogonal to one another, allowing them to be spaced very close together, this provides good spectral efficiency. The OFDM can be viewed as breaking a high data rate stream in to several parallel low rate streams modulated on the orthogonal carriers described above. Thus the symbol time on each of these carriers are widened there by reducing the Inter Symbol Interference (ISI) [3].

One of the disadvantages of an OFDMA system is requirement for the perfect synchronization in time and frequency. If the mobile subscriber station (MSS) does not synchronize with the Base Station (BS), then the probability of occurrence of Inter Carrier Interference (ICI) and Inter Symbol Interference (ISI) is high, which can cause the entire system to perform worse. To avoid these interferences, the MSS should synchronize with the BS in time and frequency, hence detecting the exact timing offset, frequency offset and power level of the MSS is critical. The process in which these parameters are calculated is called initial ranging process. After perfect synchronization is achieved between the MSS and the BS, User synchronization is maintained by the periodic ranging. In periodic ranging, MSS sends a code division multiple access (CDMA) code allocated for bandwidth requests, similar to initial ranging. In this case it is sufficient to detect the presence of user rather than the exact timing or frequency offset. [2].

On initialization or signal loss, MSS scans for the Downlink (DL) channel and gets coarse synchronization with the BS. After coarse synchronization, MSS acquires the transmit parameters from the Uplink Channel Descriptor (UCD), Uplink (UL)-MAP, and DL-MAP. MSS performs the initial ranging process by transmitting the randomly chosen ranging code from the pool of initial ranging codes allocated by the BS. As defined in the standard IEEE 802.16e, The MSS transmits the ranging codes over two OFDM symbols for initial ranging process at random time during the uplink frame as long as there is a ranging opportunity. The BS, at the receiver side detects the ranging codes being sent by the users and estimates the timing delay and power offset. Then, BS broadcasts the ranging codes with adjustment data [2].

Synchronization between the BS and all MSS's has been discussed in the literature [4][5][7]. Since all initial ranging users are transmitting their randomly chosen codes on the same subcarriers over two OFDM symbols. The BS calculates the timing offset by using different ranging algorithms, but once one user has been detected, then BS does not need any information of that user. The presence of that user will lead to interference to the other user's detection. Earlier research has not focused on the interference, which degrades the performance significantly. The proposed algorithm removes the interference of the detected codes in the received signal to enrich the signal used to detect the subsequent user, a performance and complexity comparison between the proposed algorithm and current algorithms will be discussed.

## 2. SYSTEM MODEL
We design the entire system based on the IEEE 802.16e-2005 standard. The BS defines a group of six sub channels for ranging

process. The subcarriers allocated for each sub channel is done randomly and need not to be adjacent. The ranging sub channels, ranging opportunities and information about ranging code pools will be sent by the BS in the UL-MAP broad cast messages IEEE 802.16e-2005[1] specified the Pseudo random binary sequences (PRBS) generator to generate the ranging codes as binary sequences. We consider UL of an OFDMA with $N$ subcarriers. The $i$th user ranging signal is denoted as $C_i = [C_i[0], C_i[1], ..., C_i[L-1]]$, where $L$ is the length of the ranging code. As per the standard 802.16e-2005, the number of available codes is 256 and each BS uses a subgroup of these codes, where the subgroup is defined by a number S. The first $A$ codes are produced for initial ranging by clocking the PRBS generator 14 * ($S$ mod 256) times to 144 * (($S$+$A$) mod 256) -1 times. The next $B$ codes are produced for periodic ranging by clocking the PRBS generator 144 *(($B$+$S$) mod 256) times to 144* (($A$+$B$+$S$) mod 256)-1 times. The next $C$ codes are generated for bandwidth requests by clocking the PRBS generator 144*(($A$+$B$+$S$) mod 256) times to 144*(($A$+$B$+$C$+$S$) mod256)-1 times. The next $D$ codes are produced for handover ranging process by clocking the PRBS generator 144*(($A$+$B$+$C$+$S$) mod256) times to 144* ($A$+$B$+$C$+$D$+$S$) mod 256)-1 times [1]. The user selects one set of the codes depending on his purpose. The standard specified to use 144 subcarriers for the initial ranging process. Then the ranging signal is applied to the BPSK modulation and defined as

$\mathrm{Re}\{C_i[r]\} = 1- 2\, C_i[r]$,

$\mathrm{Im}\{C_i[r]\} = 0$, where $C_i[r]$ is $r^{th}$ ranging sub carrier of $i^{th}$ user.

The ranging code needs to be mapped on to the OFDMA symbol of $N$ subcarriers. The standard specifies a permutation scheme for mapping and in our simulation we used a random mapping scheme to induce similar effects as shown in the Fig. 1 and each tile of CDMA code consists of four adjacent bits of ranging sequence.

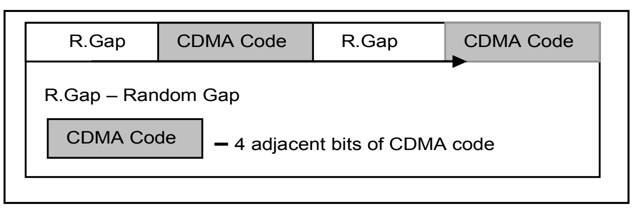


**Figure1. Mapping of CDMA code onto the OFDM Symbol**

The resultant symbol is denoted as $X_i = [X_i[0], X_i[1],..,X_i[N-1]]$ after extending to $N$ sub carriers by inserting $N$-$L$ zeros and this vector is fed to an $N$ point Inverse Discrete Fourier Transform (IDFT). Then the resultant signal is extended over two OFDM symbols by repeating the $X_i$ twice and adding the cyclic prefix (CP) and cyclic post fix to avoid the phase discontinuity over the ranging time slot as shown in the Fig. 2. The resultant signal is denoted by $T_i$ = [$X_i[N\text{-CP}]$,…, $X_i[N\text{-}1]$, $X_i[0]$,…, $X_i[N\text{-}1]$, $X_i[0]$,…, $X_i[N\text{-}1]$, $X_i[0]$,…, $X_i[CP\text{-}1]$].

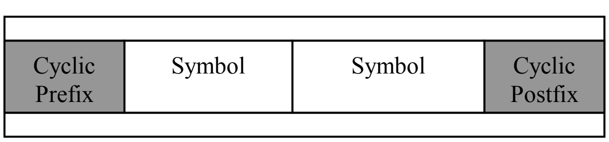


**Figure2. Initial Ranging Transmission over two OFDM symbols**

The transmitted signal $T_i$ goes through an additive white Gaussian noise (AWGN) channel with noise power spectral density $N_0$. The received signal is denoted as

$R_i = T_i + W + D_i$, where $W$ is a vector of complex white Gaussian noise samples with zero mean and $N_0/2$ variance and $D_i$ is the interference created by the $i$th user to the other ranging users. The block diagram of the initial ranging process is shown in the Fig 3.

In real time environments at any instance of time more number of users wants to get synchronized with the BS. As per the standard requirement, initial users will start with the minimum power level possible. Then, if it fails to get the response from the BS, the power is increased incrementally until a response is achieved. In an UL time frame opportunity, different users will be trying to be synchronized with the BS by transmitting the initial ranging requests with different powers. The transmitted requests with higher power levels may create interference to the other ranging users. So the received signal contains both the white Gaussian noise samples and interference. Now received signal $R_i$ is fed to the ranging algorithms to calculate the timing offset and power levels and also to detect the users.

# 3. CURRENT RANGING ALGORITHMS

There exist some simple methods [2][4][5][7] to compute the timing offset during initial ranging process. One of those methods is time domain cross correlation method (TD method). The CDMA code which is used for ranging is assumed such that it has very good auto correlation property. The received signal in time domain is stored and cross-correlation is performed between the received signal and different predefined CDMA codes in time domain. However this method leads to more computational requirements. To avoid heavy computation, auto correlation of received signal can be performed thus exploiting the repetition of ranging code. But this method is more prone to the interference created by the other codes being sent by the other ranging users. Ultimately these methods lead to weaker performance because of interference of the other users.

Another method is frequency domain correlation method (FD Method). The timing offset can also be found by performing the correlation in frequency domain. The advantage of this method is less interference, as we are separating data subcarriers from the subcarriers used for ranging. Finding a time offset in time domain is equivalent to finding phase offset in frequency domain. To find correct phase offset, the received ranging subcarrier data is phase rotated, for all possible values and correlated with CDMA code. For the correct value the phase rotation cancels the phase offset introduced due to timing offset and the following correlation results in peak. This system works well because of reduced interference from the data subcarriers, but the complexity is very high because of the high number of multiplications. Moreover it fails to reduce the interference created by the codes being sent by the other users, which leads to performance degradation with higher number of ranging users.

Another simpler approach is to calculate the average differential phase offset between all adjacent subcarriers by multiplying one subcarrier with adjacent subcarrier conjugate. If some delay occurs in the transmitted signal, then it will manifest as the phase offset in the frequency domain. The mathematical representation of this method is shown in the Eq. 1.

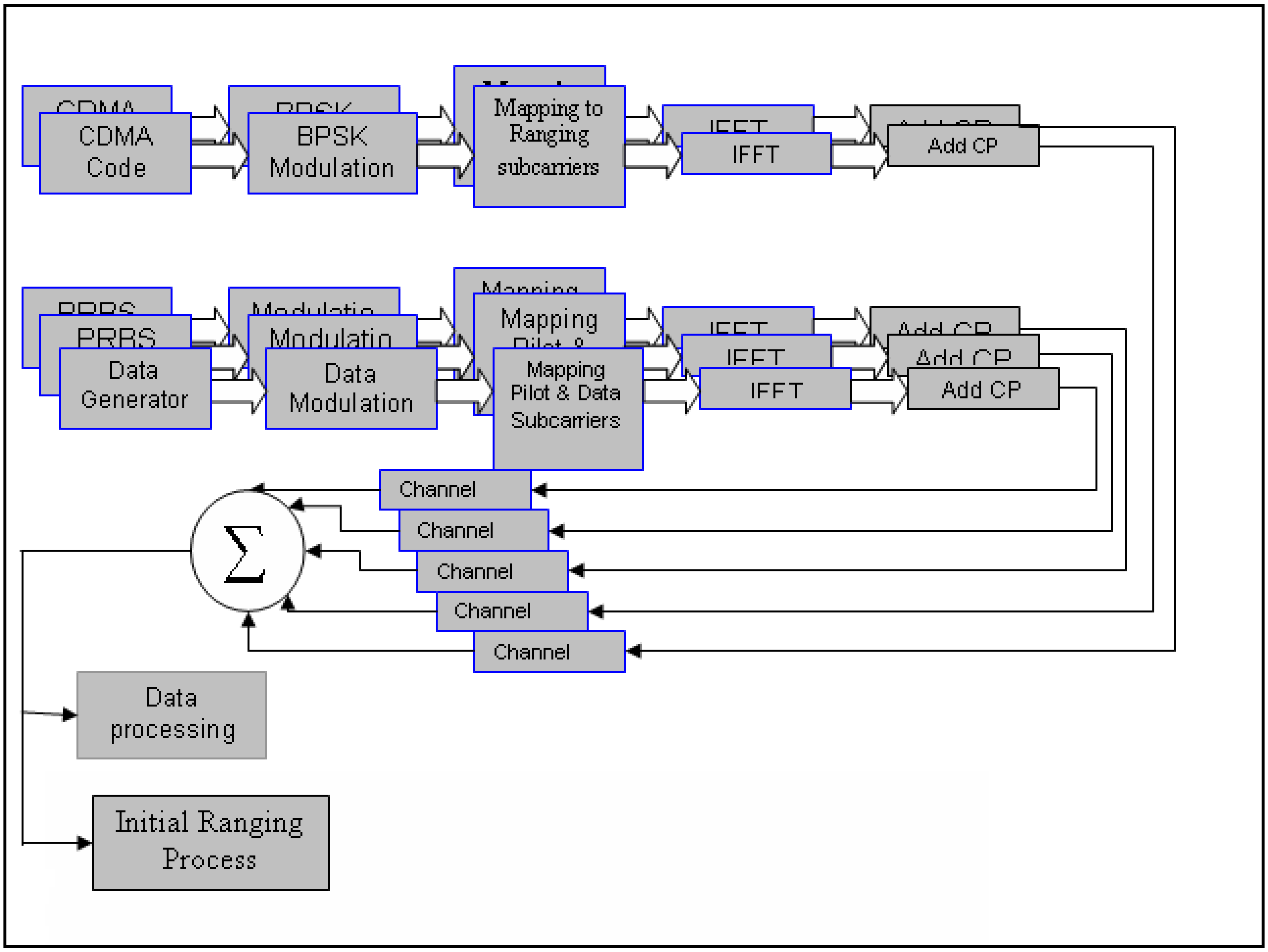


**Figure3. Block diagram of Initial ranging process**

$$sum = \sum_{i=\#tiles} \left[ \sum_{n=1:t-1} R_{i+n} R^{*}_{i+n+1} \right] \qquad \textbf{Eq. 1}$$

This method leads to fewer computations, but still prone to the interference created by the other ranging users which ultimately affects the performance. This method is called differential phase detection method (DPD).

The main disadvantage of the above discussed algorithms is the high computational complexity. As per the wireless standard, IEEE802.16e-2005, the number of ranging codes is 256 and is divided into four categories: initial ranging codes, periodic ranging code bandwidth request and handover ranging codes, but in practice the number of ranging codes is much lower. The ranging signals are more prone to the multi path affect which causes some algorithms to have lot of computations required to do correct estimations. Many of the ranging algorithms are more prone to error due to the interference caused by the high power level signals of the ranging users, which cause interference to the other users, since these algorithms do not deal with the interference reduction aspect. IEEE802.16e-2005 adds mobility to the users to use network while they are moving at a speed of 125KMPH at most. The above algorithms do not deal with the mobility of the users. The proposed algorithm proved that it offers better trade-off between accuracy and complexity of the initial ranging process by dealing with the interference reduction and users mobility.

## 4. PROPOSED ALGORITHM

The proposed algorithm attempts to improve the performance mainly by reducing the interference created by the other users. At the receiver side we choose an observation window of $N+CP$ size and extract the signal and then apply the algorithm in frequency domain. We break the initial ranging process into three main tasks. Our first step is to detect the valid users, by comparing the user's strength with threshold value $n_l$, which will be discussed in Section 4.1. The second step will calculate the timing offset values, by applying the IDFT, which will be discussed in Section 4.2. Section 4.3 discusses the reduction of the interference by subtracting the detected user's ranging data. Using this approach computation complexity is significantly reduced while the performance is still acceptable when compared to the other algorithms, which will be shown in the sections 5 and 6.

## 4.1 User Detection

The BS extracts the signal into *N+CP* samples and removes the *CP*; the resultant signal will be fed to the DFT, which contains the ranging data and noise from the other users. In case of multiple users', if the initial ranging algorithms are not optimal, then the BS may detect an MSS as a ranging user even if it has not sent a ranging code or the BS may detect the actual timing offset incorrectly.

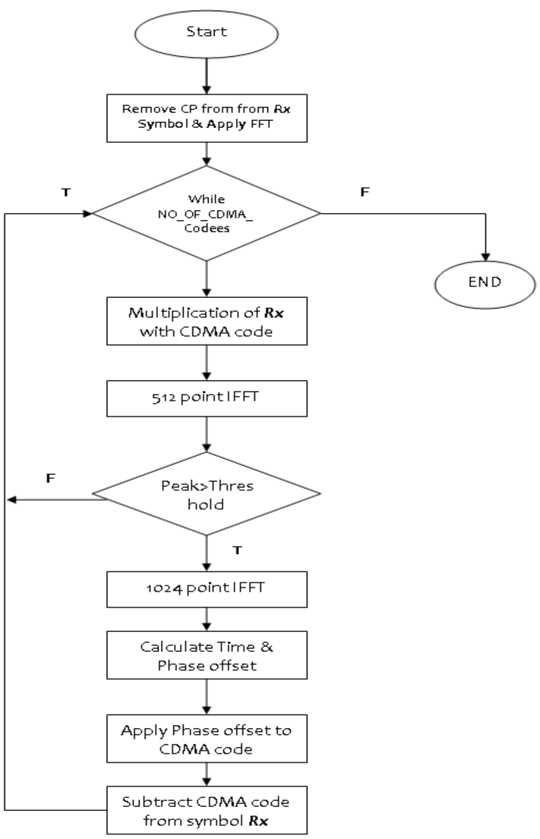


**Fig4. Flow chart of the proposed algorithm**

First part of our ranging algorithms checks the presence of a particular code in $R_x$ data to have certain minimum power level. If the power level is more than the threshold value $n_1$, then we conclude the user is present and proceed to the second part to compute timing offset for the detected user. To check the threshold value, a 512 point IDFT is applied instead of 1024 point IDFT, which reduces the computational complexity. The IDFT peak gives the power level of the signal.

## 4.2 Timing Offset Calculation

In previous step, we detected the ranging users contained in an OFDMA symbol. Now we proceed to estimate the timing offset. By applying 1024 point IDFT to the received signal, the timing offset would be calculated by cross correlating the received signal with all possible codes and with all possible linear phase shifts. By using a threshold we could detect the ranging codes. This method is discussed in the current ranging algorithms section.

## 4.3 Interference Reduction

The main task of the proposed algorithm is to reduce the interference caused by the other users. The timing offset estimation was done in the second phase of our algorithm. The detected user's signal will not be useful for further purposes and hence it will be removed from the $R_x$ signal. To generate the user's transmitted data, we use the estimated timing offset of that particular user. We calculate the linear phase shift using the timing offset and apply the calculated phase shift to the transmitted CDMA code. Now we subtract this data from the Rx signal thus reducing the interference for subsequent detection of other users.

Since all users are transmitting their initial ranging requests using unique CDMA codes on the same sub carriers with different power levels, reducing one users data recursively from the received signal will certainly reduce the over all interference for the sub sequent user detections.

# 5. SIMULATION RESULTS

An OFDMA system model based on the standard [1] is used with the following parameters:

$N$ = 1024, $L$ = 144, $CP$ = 128 samples, $T_{del}$ = 0 t0 512 samples, the total number of ranging codes is 256, i.e. $P$=256. The channel is an additive white Gaussian noise channel and the SNR = 10dB. Ranging users send their ranging requests on two randomly chosen consecutive symbols during the UL frame. For every number of ranging users, k, the performance is obtained after 1000 simulation runs. The threshold value was chosen as $n_1$ = 6dB above the noise floor. Fig 5 shows the comparative performance analysis of the algorithms studied in [4], [5], [7] and proposed algorithm, DIIC (Double IDFT Interference Cancellation).

But in general, the channel conditions may not follow the linear distribution. To achieve the real time scenario, we simulated all the algorithms with Rayleigh distribution with the channel models, recommended by the ITU-R for the vehicular test and pedestrian test. Fig. 6 shows the performance of all algorithms in Rayleigh fading channel for vehicular test-A.

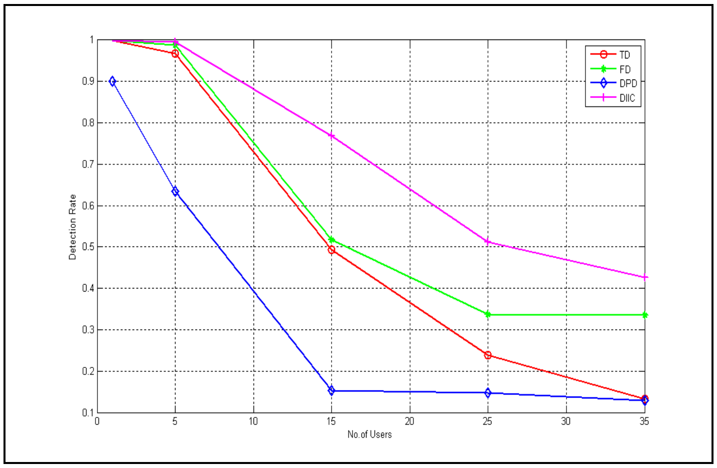


**Fig5. Detection rate versus number of users in AWGN channel**

When the number of users is one, then the proposed algorithm performs equally with the frequency domain algorithm, since there is no need of interference reduction. But in real time scenarios, more number of users will be trying for initial ranging, so the interference reduction in this case will surely increases the detection rate significantly, shown in the Fig 5.

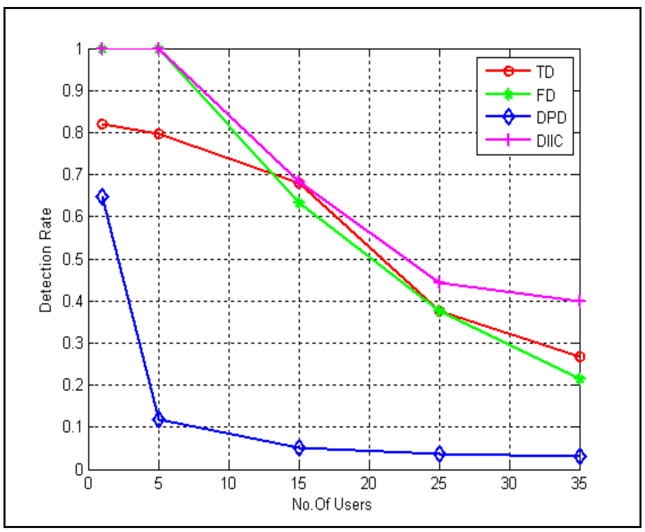


**Fig6. Detection rate versus number of users in Rayleigh fading channel**

As shown in the Fig. 6, the performance of TD (Time domain) correlation algorithm, FD (Frequency domain) algorithms are degrading when the number of users is increasing. The DPD (Differential Phase Detection) Algorithm is performing worse than in the AWGN channel environment. The proposed algorithm, DIIC (Double IDFT interference cancellation) algorithm is performing better than the traditional algorithms discussed in above sections, though the number of users is increasing.

## 6. COMPLEXITY

For the real time environment applications, the computational complexity of an algorithm plays an important role. In this section we evaluate the complexity of the proposed algorithm and we compare with the current/traditional algorithms.

We computed the complexity of all the algorithms in terms of the number of additions and number of multiplications, to avoid the platform dependency, since different processors may take different number of cycles for the basic operations [8].

We compare the proposed algorithm with the other three traditional algorithms discussed in the earlier sections. For time domain algorithm, the received signal is correlated with bank of predefined codes, p. If the delay occurred at max of $T_{del}$, then the number of correlation operations would be $(T_{del}+1)P$ and these are performed for every OFDM symbol. Assuming that the number of OFDM symbols are $Q$, the total number of correlation operations would be $Q(T_{del}+1)P$.

In Frequency domain algorithm, the received signal is cross correlated with the bank of predefined codes P in frequency domain. But this algorithm applies cross correlation by applying quantized linear phase shifts to the bank of P codes,

In differential phase detection algorithm, we simply compute the timing offset by multiplying the ranging sub carrier with the conjugate of neighboring sub carrier. We perform these multiplications for $L$ sub carriers, which leads to significant complexity reduction.

In the proposed algorithm, the received signal is multiplied with all predefined ranging codes in the set P, and then the energy is calculated to check for the valid user. But here we reduced the complexity significantly by using 512 point IDFT instead 1024 point IDFT. To compute timing offset, again we applied 1024 point IDFT and finally the detected user's data with applied linear phase shift would be subtracted from the received signal Rx.

We assume that $Q$= 2 OFDMA symbols, $P$=256 codes, $L$=144 bits, $T_{del}$=512 samples, and $N$=1024.

The following table gives the approximate number of additions and multiplications of all the algorithms.

| Algorithms | No. Of Additions (Approx) | No. Of Multiplications (Approx) |
|---|---|---|
| TD | 150764544 | 151289856 |
| FD | 37822464 | 38117952 |
| DPD | 97424 | 33936 |
| DIIC | 24148992 | 24153256 |

**Table 1. Complexity of Algorithms**

From Table.1, it is evident that the proposed algorithm takes less number of additions and multiplications than TD, FD and DPD regardless of the number of user's $K$.

## 7. CONCLUSION

In this paper, we presented a novel algorithm for initial ranging process based on IEEE802.16e-2005 standard. The proposed algorithm performs multi user detection and timing offset estimation for initial ranging users. The performance analysis demonstrated that the proposed algorithm provides better results than the existing algorithms, when the number of users is high. The complexity comparison between proposed algorithm and current/traditional algorithm indicates a good trade off in terms of computational load and detection accuracy.

## 8. REFERENCES

[1] IEEE standard for local and metropolitan area networks part16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004) Std., 2006.

[2] Girish V V, "*Ranging Algorithms in WiMAX*", Master thesis, Computer Science Engineering Department, National Institute of Technology, Calicut, India, 2009.

[3] M Shakeel Baig, "*Signal Processing Requirements for WiMAX (802.16e) Base station*", Master thesis, Signal Processing Group Department of Signals and Systems Chalmers University of Technology Göteborg, Sweden, 2005.

[4] X. Fu, Y. Li, and H. Minn. "*A new ranging method for OFDMA systems*," IEEE transactions on wireless Communications, vol. 6, no. 2, pp. 659-669, February 2007.

[5] Sanguinetti. L, Morelli. M, H. Vincent Poor, "*An Improved Scheme for Initial Ranging in OFDMA-based Networks*," IEEE transactions on Communications, volume, Issue, 19-23 May 2008.

[6] D. H. Lee, H. W. Je and K. B. Lee, "*Differential Detection Scheme with Combining Multiple FFT Blocks for OFDMA Ranging of IEEE 802.16e*", in Proc. IEEE 10th International OFDM-Workshop, Aug. 2005.

[7] Mahmoud. H. A, Arslan. H, Ozdemir. M. K, "*Initial Ranging for WiMAX (802.16e) OFDMA*", IEEE transactions on Military Communications Conference, 2006, Volume, Issue, 23-25 Oct.2006 Pages(s):1-7.

[8] John G.Proakis, Dimitris G.Manolakias, "Digital Signal Processing", Prentice-Hall, Inc, ISBN: 013394338, 1996.