Scalability of Passive and Active Solutions for Time-Based Ranging in IEEE 802.11 Networks

Israel Martin-Escalona, Marta Malpartida, Enrica Zola, Francisco Barcelo-Arroyo

Scalability of passive and active solutions for time-based ranging in IEEE 802.11 networks

Israel Martin-Escalona, Marta Malpartida, Enrica Zola, Francisco Barcelo-Arroyo

Universitat Politècnica de Catalunya (UPC)
Barcelona, Spain
{imartin,enrica,francisco}@entel.upc.edu
Barcelona, Spain

Abstract Wireless positioning systems have become popular in recent years. Outdoor positioning has been addressed successfully, but location indoors still presents some open issues. One of them is related with the scalability of time-based ranging algorithms. The aim of this study is to develop a simulation framework in order to evaluate the scalability and stability of two time-based ranging positioning algorithms in IEEE 802.11 networks: 2-Way Time of Flight (TOF) and passive TDOA. Details about this simulation model are provided and both algorithms are compared in a proof-of-concept scenario. Results show that Passive TDOA provides a better scalability and more stable measurements than the solutions based on pure 2-Way TOF algorithms.

Keywords: Positioning, ranging, scalability, IEEE 802.11

1 Introduction and goals

The knowledge of their own position is perceived by users as essential information that mobile devices need to provide. This information, which was initially used to enrich already developed services and applications, such as geotagging the pictures users take, has become the core of the new set of services and applications that are to come in the next years, such as augmented reality [1], location-based social networks [2] or smart cities [3].

The widespread inclusion of GPS receivers in mobile phones has boosted the use of location-based services. This technology provides a world-wide coverage and excellent accuracy outdoors. However, the same does not apply to indoor scenarios, where GPS provide low accuracy or simply stops working.

Currently, there is no a counterpart of GPS to be used indoors. The industry and the research community are actively looking for a global technology that allows mobile devices to be globally positioned indoors. Several approaches have been proposed in the last years. Most of them try to take advantage of communication networks already deployed to position the network users as well. This approach simplifies the deployment of location systems and extends their availability. One example of this approach

consists of using public land mobile networks (PLMN) to support positioning. Techniques, such as the Observed Time Difference Of Arrival (OTDOA) can be used in LTE networks to get the user's location [4]. Although the accuracy of these solutions are suitable for most of location-based services, those of them designed to run specifically indoors tend to be much more restrictive in terms of accuracy, demanding often a precision around 1 meter. Such requirements are hardly satisfied by location systems based on PLMN, since signals used for positioning are often impacted by several radio artifacts: attenuation, blocking, mutipath, delay-spread, etc.

Networks local to the user's location are then preferred for positioning purposes. Bluetooth and 802.11 are the technologies that concentrate most of the research on indoor positioning. Bluetooth low energy networks are being used by companies such as Apple [5] and Paypal [6] to provide location systems working indoors. Although Bluetooth-based solutions are promising, they have the drawback of the coverage, requiring usually specific network upgrades to fully support location-based services. On the other hand, communication networks based on IEEE 802.11 are known to be widely deployed, mainly indoors. This fact makes this technology really appealing for location systems. However, location systems using IEEE 802.11 technologies must cope with several issues related with the position accuracy, the latency, the scalability and the integrity of the location system. Solutions based on received signal strength (RSS) are known to be easily implemented in IEEE 802.11 devices, thus providing excellent coverage, but they tend to provide poor accuracy figures [7]. Fingerprinting is a technique usually related with IEEE 802.11 location systems [8]. It consists of a database that stores data vectors related with specific positions. Those vectors typically contain the RSS (sometimes other data) of the set of access points at sight in a given place (x,y,z). When users want to get their own position or a third party request such information, the mobile device computes the vector in real time and delivers that vector to the location server where the database is. Then the reported vector is compared with the data stored in the database and the most likely position according to all these data is returned. Fingerprinting tends to provide excellent accuracy, delay and scalability, but requires setting up the location database before the system is deployed. Furthermore, changes in the environment have a severe impact on the quality of the position, so the database needs to be updated often. Depending on the scenario, this database maintenance may involve a noticeable effort.

Time-based location techniques use the time-of-flight (TOF) to estimate distances to well-known references (i.e. landmarks). Those references are perfectly located so that the only unknown is the position of the mobile user. There are several proposals using this approach, most of them based on the round-trip-time [9] to skip the need for synchronizing all the network devices. This approach is extended in [10] to provide a software-based solution that at the same time improves the accuracy of the regular 2-way time-of-arrival solutions.

Collaborative solutions have been proposed in order to improve the accuracy of time-based solutions [11]. Although the accuracy has been improved, time-based solutions still have an open issue: the scalability. Most of the time-based location systems inject traffic in the network to perform the measurements, which directly impacts the network performance after the traffic increase. The more measurements required, the

more likely frames collide and the longer the time to reach a valid computation of the position. Passive solutions were presented to overcome this issue and boost the scalability of time-based location systems, without a severe degradation of the accuracy of the computed positions.

This work is focused on one of these passive algorithms: the passive TDOA. In [12], the authors presented the benefits of this algorithm and provided a short study on the expected accuracy, showing figures better than those achieved by its active-solution counterpart. However, the scalability benefits, though claimed based on the fact that no extra traffic is injected, were never studied in detail or numerically evaluated. This work is aimed at studying the scalability benefits of the passive TDOA over a regular 2-way TOF solution, both systems working in IEEE 802.11 networks.

The rest of the paper is structured as follows. Section 2 presents the algorithms that are going to be assessed. The simulation tool and the simulated scenario are presented in Section 3. The results achieved are shown in Section 4, while the main conclusion and the planned future work are drawn in Section 5.

2 Passive vs active ranging

Time-based positioning in IEEE 802.11 networks is based on ranging, i.e. it infers the distance between the mobile device that needs to be positioned and several well-located network entities (landmarks or anchors). Those distances feed a multilateration algorithm, which finally fixes the position. Ranging models, i.e. the procedures followed to turn time measurements into distances, tend to require several measurements for a single distance estimation [9]. Only after processing a set of measurements the channel artifacts can be properly filtered and hence their impact on the position accuracy reduced. This approach can be followed as long as only few nodes are being positioning in the network. If there are a large number of nodes requiring their position, positioning traffic tends to flood the radio channel, which yields frames colliding frequently. This increase in the collision rate has a twofold effect. On one hand, the response time of the location system (i.e. the time spent by the system until the requested position is fixed) becomes longer. This fact impacts on the quality-of-service perceived by the user and might have a negative effect on the position accuracy as well, especially when the user is moving. On the other hand, the heavier the location traffic, the lower the available throughput for remaining communications.

Passive ranging solutions try to compute positions by only listening to the radio medium. Thus, they try to take benefit of the regular traffic in the network to infer the position of the user. This kind of solutions are known to favor the scalability, since increasing the amount of nodes requiring their own position does not involve a noticeable increase in the location traffic.

2.1 Assisted passive TDOA

The Passive TDOA [12] is one of these time-based passive ranging algorithms. This algorithm was designed to complement regular active 2-way TOF systems and enhance

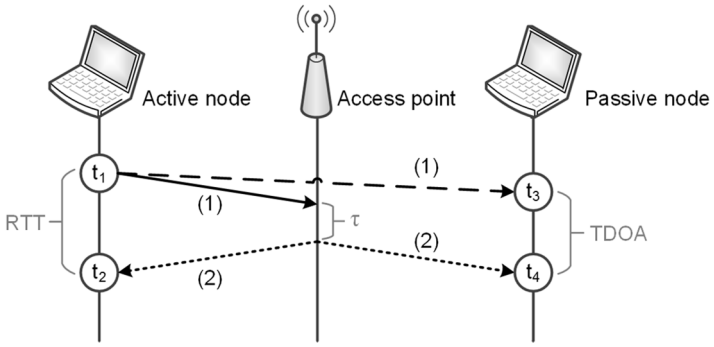

Figure 1: Estimation of a single TDOA in the passive node

their scalability. Accordingly, the passive TDOA algorithm assumes the presence of few nodes in the network running 2-way TOF positioning solutions. The point of the passive TDOA is locating a node using only the information of its active neighbor nodes. The basic procedure followed by Passive TDOA to allow the passive positioning is described in Fig. 1. In the figure, two nodes are represented, one running a 2-way TOF algorithm (i.e. active node) and one running the passive TDOA algorithm (i.e. passive node).

The location process starts when the active node obtains its position by using the 2-Way TOA technique. Meanwhile, the passive node is listening to the radio medium and receiving the messages that the active node exchanges with the access point. Fig. 1 illustrates the performance of the algorithm. Whenever the active node wants to estimate the distance to an access point, it sends a message (1) to the access point. This message, because of the diffusion network, is also received in the passive node, which marks the time of arrival before discarding the frame. After a known time τ, the access point sends back a message (2) to the active node, as response to message (1). When this message is received in the active node, the distance between the active node and the passive node can be computed (with an indeterminate error). The message (2), because of the diffusion network is also received in the passive node. Then, a time difference of arrival (TDOA) can be computed in the passive node as $t_4 - t_3$ in Fig. 1.

Repeating this procedure with enough access points (e.g. three in the case of 2D positioning) let the active node to compute its own position using a multilateration algorithm. Finally, this position has to be sent so that the passive node can compute its own position according to the TDOA measurements previously computed.

2.2 Autonomous passive TDOA

The passive TDOA algorithm is able to estimate both active and passive nodes positions if the measurements are grouped in couples. Accordingly, the measurement procedure is extended to include two procedures like the one depicted in Fig. 1.

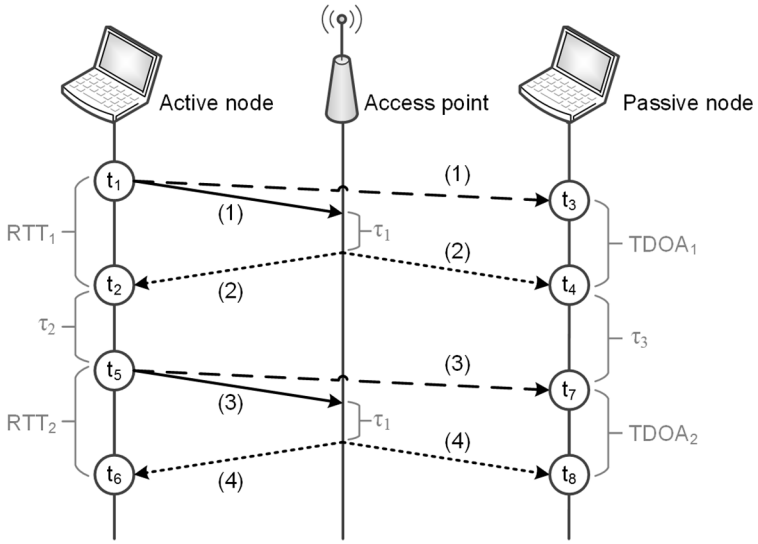

Figure 2: Joint estimation of TOF and TDOA in the passive node

Fig. 2 illustrates how the measurements are taken. As shown, the active node is able to compute two RTTs (i.e. RTT_1 and RTT_2) and consequently the passive node collects two TDOAs (i.e. $TDOA_1$ and $TDOA_2$). These TDOAs are observations of the time-distance between two different paths as

$$TDOA = (T_a + T_p) - (T_{ap}) \tag{1}$$

where T_a and T_p is the TOF from active and passive nodes to the access point, respectively, and T_{ap} is the TOF between active and passive nodes.

The point of grouping the measurements in couples is that relating these two TDOAs allows the distance from the active node to the access point to be inferred as

$$RTDOA = \tau_3 = t_7 - t_4 = T_a + \tau_2 + T_{ap} - T_p \tag{2}$$

Accordingly, under the assumption of the measurement-to-measurement delay (τ_2) is known and measurements to enough access points are available (at least 3 for 2D positioning), the passive node is able to compute both the active and the passive node positions, providing a twofold benefit. First, it involves a fully passive solution, minimizing the location traffic in the network (i.e. there is no need for the active node to send its own position). Second, it provides redundancy for active node positions, which can be statistically combined to improve their accuracy.

3 Simulation tool and scenarios

Simulation has been used to provide a rich and realistic scenario where to assess the scalability of the algorithm and compare the results with what is expected using regular

active 2-way TOF solutions. To achieve this goal, a simulation tool implementing the 802.11 b/g protocol stack and the 2-Way TOF and Passive TDOA algorithms is required. In this simulation, messages showed in Fig 1 and 2 are implemented over IEEE 802.11 as data frames, while the answers are built using ACK frames.

3.1 Simulation tool

OMNET++ [13] is the network simulator used to evaluate the scalability of 2-Way TOF and Passive TDOA over IEEE 802.11 networks. The INET framework [14] has been used to provide a full implementation of the IEEE 802.11 protocol stack, including a rich set of radio models and mobility patterns.

Several parts of the code of the INET framework have been modified in order to implement the 2-Way TOF and the Passive TDOA algorithms. In the case of the 2-Way TOF algorithm, two measurements are provided for a single RTT, depending on when the transmission time-marks are taken: 1) in the IEEE 802.11 management layer (RTT-MNGT), i.e. just before the CSMA/CA delay chain begins; and 2) just before sending the data frame to the physical layer (RTT-MAC). The reason to include these two figures for each RTT measurement procedure is to provide thresholds that can match software-based (i.e. only the first measurement is likely to be available) and hardware-based (i.e. the second measurement is likely to be available) implementations. Fig. 3 shows the basic flow of the implementation followed to take the time measurements. Whenever a data frame is received in the access point, the location timestamps included in it (if applies) are copied to the ACK frame built as response, as shown in Fig. 4. Finally, the timestamps applied to the received frames are taken once the frame enters in the reception function of the MAC layer, whenever the transmission time is taken, as shown in Fig. 5. As it can be seen, all those figures include the name of the INET files and the methods in these files that have been upgraded to support the 2-way TOF

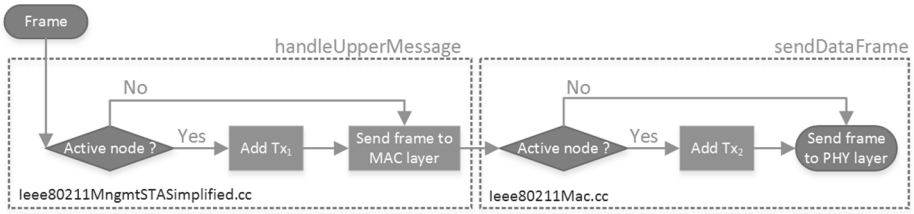

Figure 3: Flow of the 2-way TOF algorithm (data frames in active nodes)

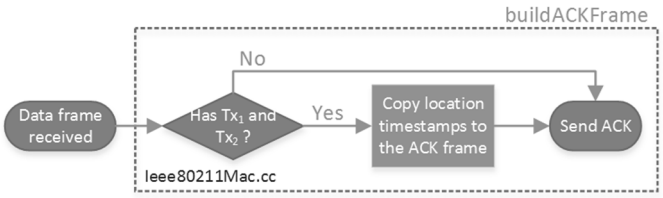

Figure 4: Flow of the 2-way TOF algorithm (ACK frames in access points)

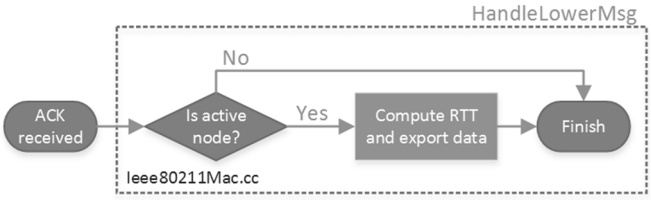

Figure 5: Flow of the 2-way TOF algorithm (ACK frames in active nodes)

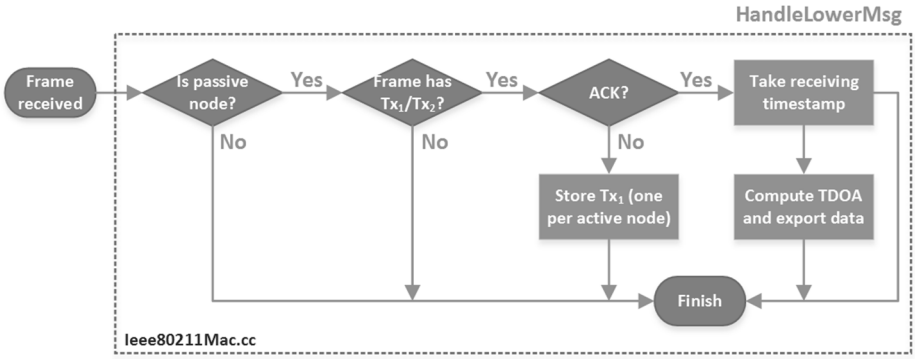

Figure 6: Flow of the passive TDOA algorithm (passive nodes)

algorithm. In the case of the passive nodes only received frames have to be inspected. Fig. 6 shows the basic flow followed in that case.

3.2 Simulated scenario

A basic scenario has been built to provide a preliminary assessment on the scalability of the passive TDOA. It consists of one access point, which is placed at the top-left corner of a square-shaped simulation area, and twenty-six nodes. The nodes form a grid in the simulation area, as shown in Fig. 7. These nodes are static, i.e. they are settled in a position of the square-shaped simulated grid and keep the same position along the whole simulation. Different simulations are run considering from one single active node (i.e. 24 passive nodes) up to 25 active nodes (i.e. no passive nodes). Active nodes take always the first positions, i.e. from 1 up to *N* in Fig. 7, whilst passive nodes take the remaining positions (i.e. from *N+1* up to 25).

The IEEE 802.11b standard is used in simulations, although the results can be easily extended to other standards such as 802.11g or n. The lognormal shadowing model [15] has been used to model the radio propagation conditions indoors:

$$PL\,(dB) = PL\,(d_0) + 10\alpha log\left(\frac{d}{d_0}\right) + X_\sigma \tag{3}$$

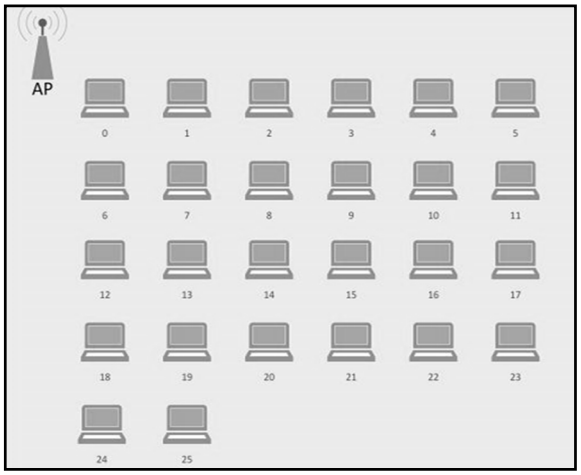

Figure 7: Layout of the simulated scenario

where *PL* is the average path loss, $PL(d_0)$ is the path loss at the reference distance d_0 (typically 1 m.), α is the path loss exponent and X_σ is a zero-mean Gaussian distributed random variable with standard distribution σ. The parameters α and σ are fixed to 4.02 and 7.36 dB respectively, as reported in [15] for indoor conditions. The transmission power and the sensitivity are set to 3 dBm and 85 dBm respectively and apply to all the nodes in the network, including the access point. The coverage radio of the base station is fixed to 10 m, which yields a 7.07 x 7.07 m square-shaped simulation area. This coverage and density conditions are similar to those present in a Wireless Sensor Network environment, which is one of the target applications of location algorithms. Accordingly, the reduced simulation area was maintained and no other radio parameter was modified.

3.3 Observed metrics

In order to study and evaluate the performance of 2-way-TOA and Passive TDOA the following metrics are defined:

- Delay. It is the time that active and passive nodes require to obtain a RTT and a TDOA sample, respectively. This time accounts for the delays introduced by the medium access control (MAC) layer, but it does not include other delays such as those associated with the operating system (e.g. multiple-process management).
- Number of collisions. It is the amount of collisions that each node is aware of, once the simulation finishes.

The simulation is run until 2,500 samples for all observed metrics are collected. The simulation time will thus depend on the specific scenario being simulated (e.g. according to the amount of collisions).

4 Performance assessment

The average amount of collisions are shown in Fig. 8, as an illustration of how loaded is the radio medium. As it is shown and indeed expected, the higher the active nodes, the higher the collision number. The time until a RTT sample is taken (i.e. the RTT delay) depends on the number of times a single frame needs to be transmitted until it is properly received at the access point. Accordingly, the RTT delay is expected to grow with the collision rate (i.e. with the amount of nodes in the network).

Fig. 9 illustrates the average delay until the node is able to estimate the RTT-related metrics (i.e. RTT-MNGT and RTT-MAC). As expected, the RTT-MNGT delay grows

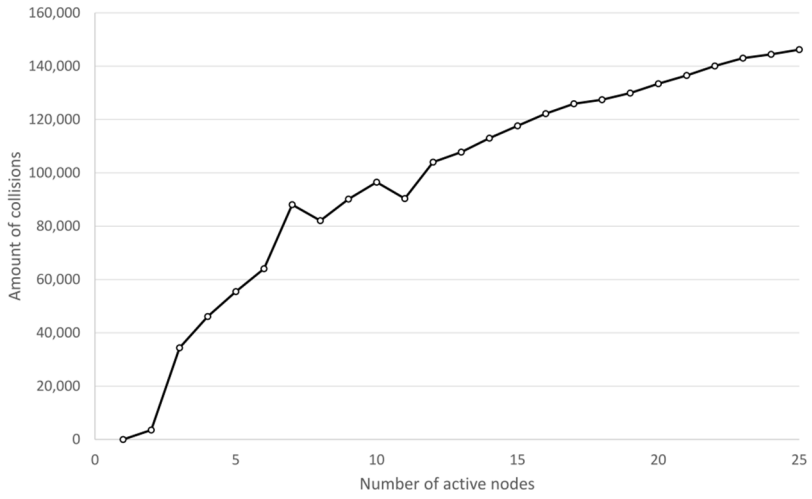

Figure 8: Average amount of collisions

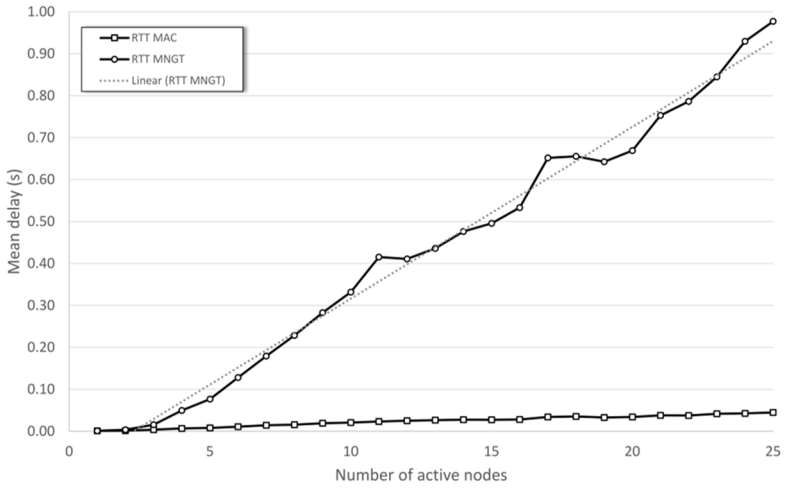

Figure 9: Mean delay until a new RTT sample is taken

together with the amount of active nodes in the network. The more positioning traffic in the network the more likely the location frames collide. The delay increment can be fitted by means of a linear regression, with a coefficient of determination of 98.96%. The resulting expression indicates that each active node in the network involves an increment of about 41 ms in the mean delay until an RTT-MNGT sample can be finally taken.

The RTT-MAC delay is not impacted by most of the delays introduced by the CSMA/CA chain, so the delays for this metric are much shorter. In this latter case, each active node involves an increment of less than 2 ms to the RTT-MAC estimation process. It must be noted that the actual RTT delay is expected to be in between of these two set of measurements. Furthermore, the more active nodes, the more error in the time until a new RTT sample is taken, as shown in Fig. 10. Data in this figure shows that, in the densest scenario (i.e. 25 active nodes), this error can reach up to 50% of the time required to collect a new RTT sample.

Fig. 11 shows the mean time elapsed until TDOA is estimated, using the average and the median estimators. This latter is included to filter some artifacts produced by the way in which active and passive nodes are settled along the simulated scenario. Results demonstrate that passive TDOA technique is much more insensitive to the amount of active nodes in the network, if it is compared with the average delay required by the 2-Way TOA algorithm. Interquartile range (i.e. the difference between the percentiles at 75% and 25%) is about $5 \cdot 10^{-14}$. This is because Passive TDOA nodes are able to estimate TDOAs from several active nodes at the same time and hence they can get enough samples before a single active node is able to estimate its own range to the access point.

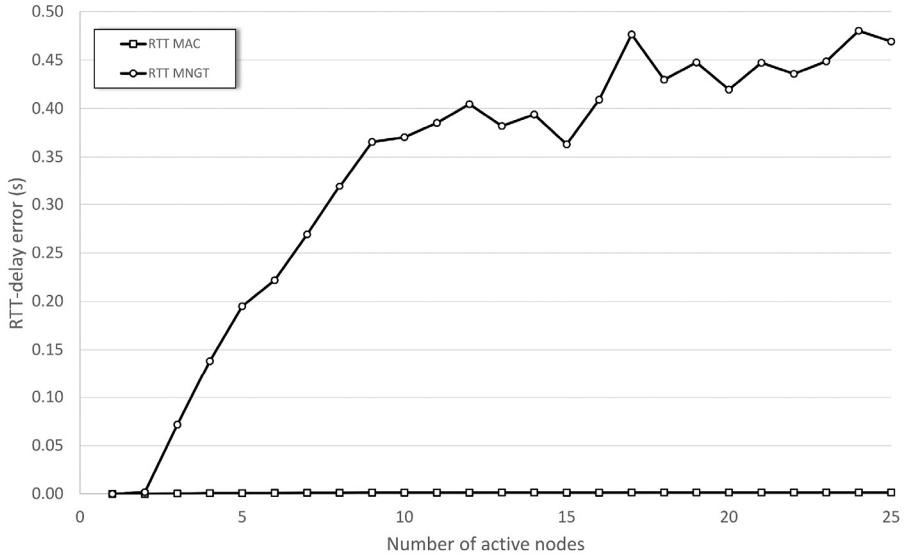

Figure 10: Confidence interval at 95% for the mean delay (RTT) estimation

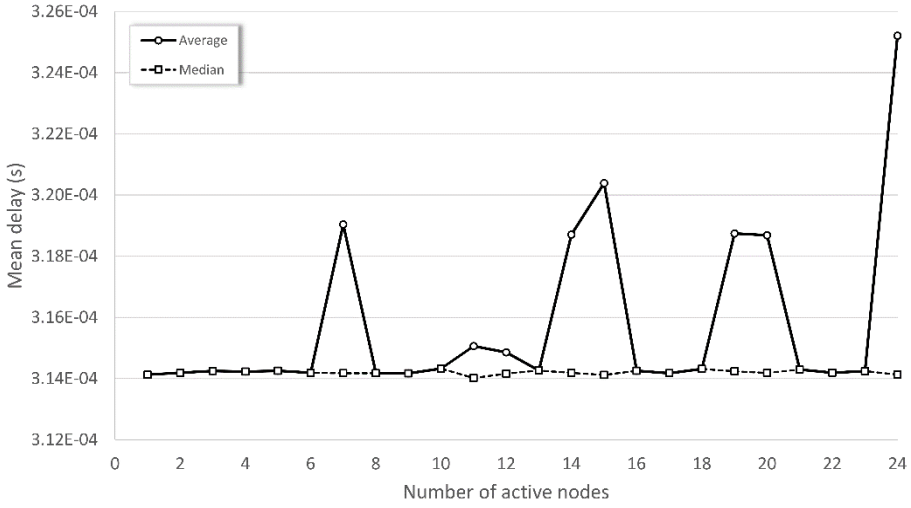

Figure 11: Mean delay until a new TDOA sample is taken

5 Conclusion and future work

This paper presents a preliminary assessment on the scalability of two range time-based solutions for positioning: 2-way TOF and passive TDOA. The INET framework of the OMNeT++ even-driven network simulator has been enhanced to implement those techniques, which have been assessed in a basic scenario implementing a single IEEE 802.11 network with several static nodes. Results indicate that the use of the passive TDOA algorithm can boost the scalability of the active ranging algorithms, providing at the same observation much more stable than those achieved by means of the traditional ranging.

Future work involves a more complete analysis of the scalability under non-static conditions and larger simulation areas and eventually contrasting the results with real measurements achieved by means of an already planned implementation of these techniques on small portable devices such as Raspberry Pi.

Acknowledgments

This work has been partially funded by the ERDF and the Spanish Government through the project TEC2013-48099-C2-1-P.

References

1. Shi, D., Liu, F., Yutian Q., Ji, Y.: A WLAN-based positioning system for indoor augmented reality services. International Conference on Information Science, Electronics and Electrical Engineering, 420-424 (2014).
2. Kunhui L., Jingjin W., Zhongnan Z., Yating C. and Zhentuan X.: Adaptive location recommendation algorithm based on location-based social networks. International Conference on Computer Science & Education, 137-142 (2015).
3. M-Governance: Smartphone Applications for Smarter Cities—Tapping GPS and NFC Technologies. E-Governance for Smart Cities, Part of the series Advances in 21st Century Human Settlements, Springer, 245-306 (2014).
4. 3GPP: LTE Positioning Protocol. ETSI TS 136.355 V13.0.0 (2016).
5. Apple: iOS: Understanding iBeacon. http://support.apple.com/kb/HT6048 (February 2015).
6. GSMA: A Guide to Bluetooth Beacons. A white paper by the GSMA (2014).
7. Stella, M., Russo M., Begusic, D.: Location Determination in Indoor Environment based on RSS Fingerprinting and Artificial Neural Network. International Conference on Telecommunications, 301-306 (2007).
8. Namiot, D., Sneps-Sneppe, M.: Geofence and Network Proximity. 13th International Conference on Internet of Things, Smart Spaces, and Next Generation Networking, 127-137 (2013).
9. Ciurana, M., Barcelo-Arroyo F., Izquierdo, F.: A Ranging Method with IEEE 802.11 Data Frames for Indoor Localization. Wireless Communications and Networking Conference, 2092-2096 (2007).
10. Hoene, C., Willmann, J.: Four-way TOA and software-based trilateration of IEEE 802.11 devices. International Symposium on Personal, Indoor and Mobile Radio Communications, 1-6 (2008).
11. Golden, S.A., Bateman, S.S.: Sensor Measurements for Wi-Fi Location with Emphasis on Time-of-Arrival Ranging. IEEE Transactions on Mobile Computing, 6(10), 1185-1198, (2007).
12. Martin, I., Malpartida, M., Barcelo-Arroyo, F.: Performance evaluation of the passive TDOA algorithm in dark areas. Ubiquitous Positioning, Indoor Navigation, and Location Based Service, 1-8 (2012).
13. Vargas A., et al.: OMNeT++. Discrete event Simulator. https://omnetpp.org (March 2016).
14. OMNeT++ community: INET Framework for OMNeT++". https://inet.omnetpp.org (March 2016).
15. Faria, D.B.: Modeling Signal Attenuation in IEEE 802.11 Wireless LANs, vol. 1. Standford University (2005).