Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks

V. Vijayalakshmi and Dr. T.G. Palanivelu ,

Pondicherry Engineering College, Puducherry – 605014, India

Summary

The crucial problem in Wireless Sensor Networks (WSNs) is position estimation or Localization, due to their dynamic method of deployment. There are several methods in determining their physical locations but the greatest challenge imposed is in communicating with their authenticated neighbors, their precise location in a secured manner. The mutual authentication between sensor nodes is of vital importance i.e. node should only accept and forward their own precise location messages from authenticated neighbors. The objective of this paper is to solve this problem of insecurity in sensor networks. Against the popular belief that public key cryptographic schemes are not practical for sensors, an authentication technique which makes use of Elliptic Curve Cryptography (ECC) along with the TOA positioning scheme is implemented. ECC has got excellent enhanced features which include smaller key size, lesser bandwidth, higher computational capability and lesser hardware. This new technique is compared for its performance with Rivest-Shamir-Adelman (RSA) and Mean Power with Rivest-Shamir-Adelman (MPRSA). The simulation results clearly indicate that ECC is well suited for secure localization in sensor networks as it satisfies the constraints of the sensor networks which include minimum bandwidth, power, energy and computational speed.

Key words:
Elliptic Curve Cryptography (ECC), ECC key exchange, Localization, TOA localization scheme, Wireless Sensor Networks (WSNs).

1. Introduction

A sensor network consists of large number of sensor nodes. Each sensor node is capable of only a limited amount of processing. But when coordinated with the information from a large number of other nodes, they have the ability to measure a given physical environment in great detail [1]. Hence precise location and authentication of the sensors in the sensor network is vital. Several localization techniques have been investigated including exploiting the Received Signal Strength Indicators (RSSI) [2], Time of arrival (TOA) [3][4], Time Difference of Arrival (TDOA) [5], or Angle of Arrival (AOA) [6]. Our scheme implements the TOA approach [7] along with ECC for secure localization. After the precise location of the sensors has been determined, the exchange of the precise location of the sensors in their infrastructure and also in communicating with their authenticated neighbors imposes the need for security in sensor networks. The distance estimated for positioning of the sensor nodes is highly vulnerable to both the internal and external attackers. While the internal attackers report false distance information in order to cheat on their positions, the external attackers modify the positions of the other sensor nodes. This necessitates a highly secure positioning scheme for sensor nodes. Elliptic Key Cryptography [8] [9], a public key cryptography scheme for secure localization and authentication between sensor nodes is proposed in this paper. The key exchange between the nodes is done by using ECC key Exchange. A comparison of this technique is also done with the other asymmetric algorithms like RSA and MPRSA [10]. The exchange of the key is also done using Diffie-Hellman and then compared so as to prove that ECC is the best. Thus, the paper proposes an efficient authentication scheme between sensor nodes. The rest of the paper is organized as follows. In section 2, the localization in sensor networks and how important security is, in it, is focused. In section 3, The TOA positioning scheme is discussed. Section 4, focuses on the Elliptic Curve Cryptography algorithm and ECC key exchange. In section 5 TOA positioning technique is simulated so as to determine the precise spatial coordinates of the sensor nodes. The implementation of ECC and its comparison with RSA and MPRSA is done in section 6. The conclusion finalizes that the TOA based ECC localization technique is well suited for WSNs environment.

2. Secure Localization In Sensor Networks

Localization in sensor networks is important because the sensor nodes have to know their physical positions for their communication. Examples include those for target detection and tracking, precision navigation, search and rescue, geographic routing, security surveillance, and so on. In sensor networks, nodes are deployed into an unplanned infrastructure in a dynamic manner without prior knowledge of their location. The problem of finding the positions of all the nodes given a few anchor nodes and relative distance and angle information between the nodes is called the position estimation or localization problem. Determining the physical positions of sensors is a fundamental and crucial problem in wireless sensor network operation for several important reasons. We briefly list two of them: first, in order to use the data collected by sensors, it is often necessary to have their

Manuscript received May 5, 2008
Manuscript revised May 20, 2008

position information stamped. For example, in order to detect and track objects with sensor networks, the physical position of each sensor should be known in advance for identifying the position of the detected objects. In addition, many communication protocols of sensor networks are built on the knowledge of the geographic positions of sensors. In most cases, sensors are deployed without their position information known in advance, and there is no supporting infrastructure available to locate them after deployment. Hence it is necessary to find the position of each sensor in wireless sensor networks after deployment. This is done by using a reference node known as the anchor node whose position is already known through Global Positioning System (GPS) or manual configuration. Once the spatial coordinates of the sensors are determined, the greatest challenge imposed by the sensor nodes is in exchanging these spatial coordinates with authenticated neighbors. Thus secure mutual authentication between neighboring sensor nodes is of vital importance. For example, a node should only accept and/or forward messages of its location from authenticated neighbors. Otherwise, attackers can easily inject bogus messages into the network to interrupt normal network functionalities. Therefore, it is appropriate to employ public keys technique to enable one time neighborhood authentication. Our location based authentication scheme is built on the ID-based cryptography by using ECC and ECC key exchange. The results thus obtained are compared with the other public key cryptography schemes like RSA and MPRSA.

3. TOA based positioning scheme

Many localization schemes have been proposed in recent years, with most assuming the existence of a few anchors that are special nodes knowing their own locations, e.g., via GPS or manual configuration. These proposals can be divided into two categories: range-based and range-free. The former are characterized by using absolute point-to-point distance (range) or angle estimates in location derivations, while the latter depend on messages from neighboring sensors and/or anchors. Range based solutions can provide more accurate locations, but have higher hardware requirements for performing precise range or angle measurements. By contrast, although having lower hardware requirements, range-free approaches only guarantee coarse-grained location accuracy.

It is observed that almost all existing range-based proposals were designed for benign scenarios where nodes cooperate to determine their locations. As a result, they are ill-suited for unattended and often hostile settings such as tactical military operations and homeland security monitoring. Under such circumstances, attackers can easily subvert the normal functionalities of WSNs by exploiting the weakness of localization algorithms. In this paper, it is not intended to provide brand-new localization techniques for sensor networks. Instead, a focus on analyzing and enhancing the security of existing approaches when applied in adversarial settings is made.

The TOA technique [7] is pictured in Fig.1. Node A is unaware of its position. Three position aware nodes are involved; let us say B_1, B_2, and B_3. Each position aware node Bi sends a message to A and the trip time of the signal is measured. The trip time multiplied by the propagation speed of signals (i.e. the speed of light) yields a distance d_i. The distance $d(A,B_i)$ defines a circle around node $d(A,B_i)$. The position of A is on the circumference of this circle. In a two dimensional model, the position of A is unambiguously determined as the intersection of three such circles. Trip time measurement from each node Bi to node A requires synchronized and accurate clocks at both locations.

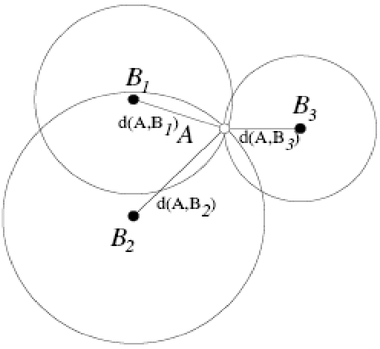

Fig.1 TOA technique

If round-trip time is measured instead (halved to obtain trip time), then this requirement is relaxed.

4. Elliptic Curve Cryptography

Elliptic curve cryptosystems were proposed independently in 1985 by Victor Miller [9] and Neal Koblitz [8]. At the time, both Miller and Koblitz regarded the concept of ECC as mathematically elegant; however felt that its implementation would be impractical. Since 1985, ECC has received intense scrutiny from cryptographers, mathematicians, and computer scientists around the world. On the one hand, the fact that no significant weaknesses have been found has led to high confidence in the security of ECC. On the other hand, great strides have been made in improving the efficiency of the system, to the extent that today ECC is not just practical, but it is the most efficient public-key system known.

The primary reason for the attractiveness of ECC over systems such as RSA and DSA is that the best algorithm known for solving the underlying mathematical problem (namely, the ECDLP) takes *fully exponential* time. In contrast, *sub exponential-time* algorithms are known for underlying mathematical problems on which RSA and DSA are based, namely the integer factorization (IFP) and the discrete logarithm (DLP) problems [11]. This means that the algorithms for solving the ECDLP become infeasible much more rapidly as the problem size increases than those algorithms for the IFP and DLP. For this reason, ECC offers security equivalent to RSA and DSA while using far smaller key sizes.

The attractiveness of ECC will increase relative to other public-key cryptosystems as computing power improvements force a general increase in the key size. The benefits of this higher-strength per-bit include:

- Higher speeds
- Lower power consumption
- Bandwidth savings
- Storage efficiencies and
- Smaller Certificates

A. Elliptic Curve Encryption and Decryption

To encrypt and send a message Pm to B, A chooses a random positive integer k and produces the cipher text Cm as given by equation (1) consisting of the pair of points.

$$Cm= [kG, P_m+kP_B] \qquad (1)$$

Note that A has used B's public key P_B. To decrypt the cipher text, B multiples the first point in the pair by B's private key n_B and subtracts the result from the second point as shown by equation (2)

$$P_m+kP_B-n_B\ (kG) =P_m+k\ (n_BG)-n_B(kG) =P_m \qquad (2)$$

B. ECC key exchange

A key exchange between users A and B can be accomplished as follows:

1. A selects an integer n_A less than n. This is A's private key. A then generates a public key $P_A=n_A*G$; the public key is a point in Eq(a,b).
2. B similarly selects a private key n_B and computes a public key P_B,
3. The public keys are exchanged between the nodes A and B. A generates the secret key $K=n_A*P_B$. B generates the secret key $K=n_B*P_A$.

5. Simulation Results of TOA Positioning Scheme

The proposed TOA positioning method is simulated with Matlab 7. Fig.2. shows the deployment of 25 sensor nodes randomly in an area of size 10×10.

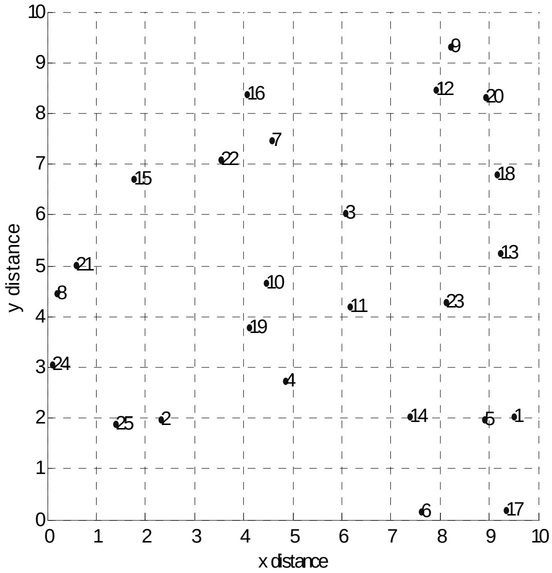

Fig.2 Deployment of nodes

5.1. Transmission of Data between the nodes

The position of the sensor nodes in the network are determined by applying the TOA algorithm. To find the Time of Arrival of signal, a data is sent from the anchor node to sensor node and the time of arrival is calculated by setting a timer. The timer is set ON when the last bit of the binary data is sent from the anchor node and the time is set OFF when the last bit of the data is received from the sensor node. The binary data 00110110 is used for the TOA scheme. The Fig.3 shows the transmission of data by a QPSK transmitter by modulating with a pseudo random bit stream.

A serial to parallel conversion of the pseudo random bit stream is performed with mapping of two bits per symbol (phase). The QPSK based system is used because it gives better performance and bit error rate compared to other system. A cosine and sine carrier is configured and the I and Q symbols modulate these carriers via mixers.

Serial to parallel conversion of a serial bit stream is done by mapping of two bits to a symbol (phase). The binary data is divided into the odd bits and even bits. The even bits are the Q Channel Data at one half the original serial bit stream bit rate. The odd bits are the I Channel Data at one half the original serial bit stream bit rate.

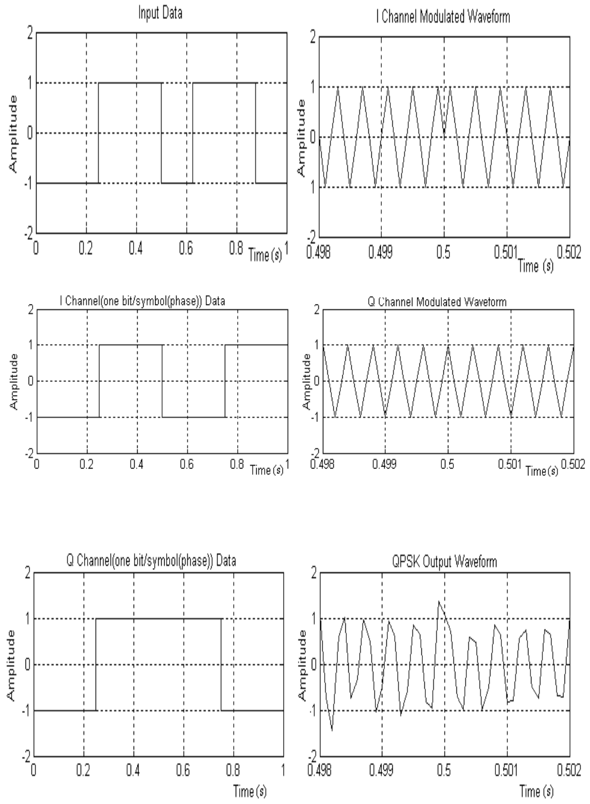

Fig.3 Data Transmission between nodes

5.2. Receiving of Data between the nodes

The Fig.4 shows the receiving of data between the nodes. After receiving the data the time of arrival of the signal is calculated. At the receiver side a parallel to serial of data send by the anchor node is implemented which is in the serial to parallel form. The simulation uses the passband approach. The binary data received is low pass filtered which consists of I Channel output and Q Channel output. For the better BER performance, bandpass filters can be added at both the transmitter and receiver side. When the last bit of the binary data is received, the timer is set OFF and time is noted. From the time of arrival of signals, the distance between the nodes is calculated which is used to find the position of the nodes in the network.

After finding the time of arrival of signals between nodes, the position of the nodes is found. From the time of arrival of the signal, the distance is computed by the formula distance = (speed * time), the speed of light is assumed in computing the distance. After computing the distance, location verification is done for the validation of the distance.

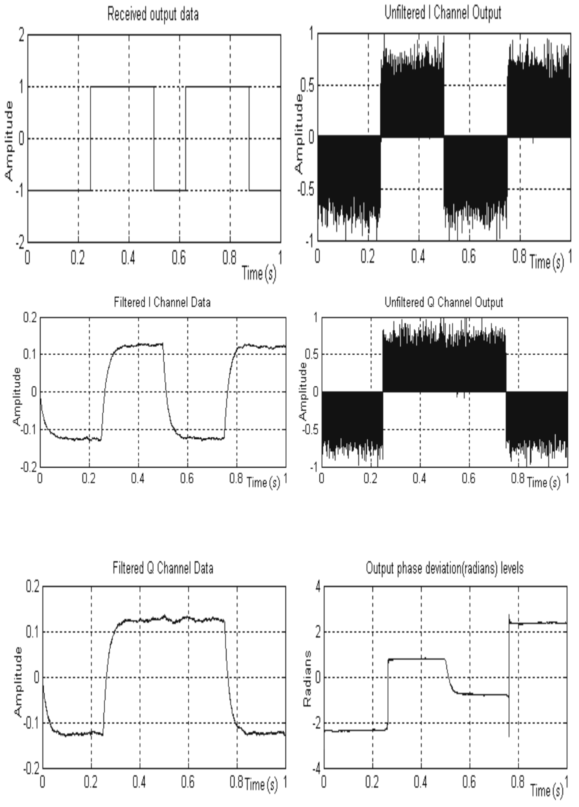

Fig.4 Data Receiving between nodes

6. Results of ECC Implementation

Once the spatial coordinates of the sensor have been determined from the distance computed, the exchanges of the precise location of the sensor were carried out using ECC technique. The authentication between the sensor nodes was done by the ECC key exchange. The encryption of the distance computed and hence the position determined was carried out by the ECC encryption scheme. Comparison of the encryption time and decryption time using RSA, MPRSA and ECC was done and from the simulated results ECC was proven the best since it had the least encryption and decryption time. The comparison of the cryptographic schemes was carried out for both Diffie-Hellmann key exchange and ECC key Exchange.

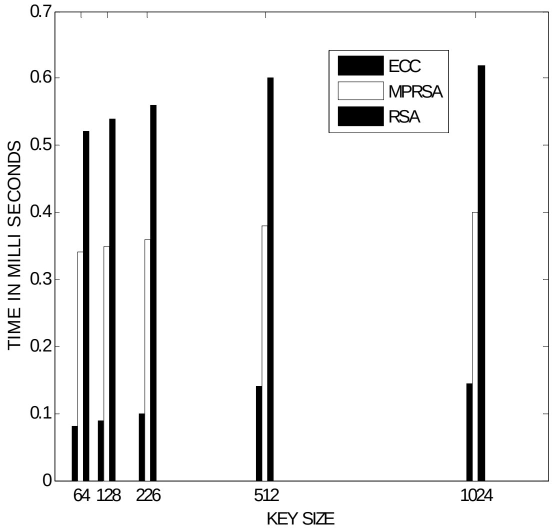

Fig.5 RSA , MPRSA and ECC encryption time for different key sizes.

Fig.5 shows the performance of RSA, MPRSA and ECC encryption time with different key sizes. Fig.6 shows the performance of RSA, MPRSA and ECC decryption time with different Key sizes. From the simulated results ECC shows the best timing performance both in terms of encryption and decryption.

Fig.7 and Fig.8 represents the comparison of encryption and decryption time of the three algorithms namely, RSA, MPRSA and ECC using Diffie-Hellmann key Exchange.

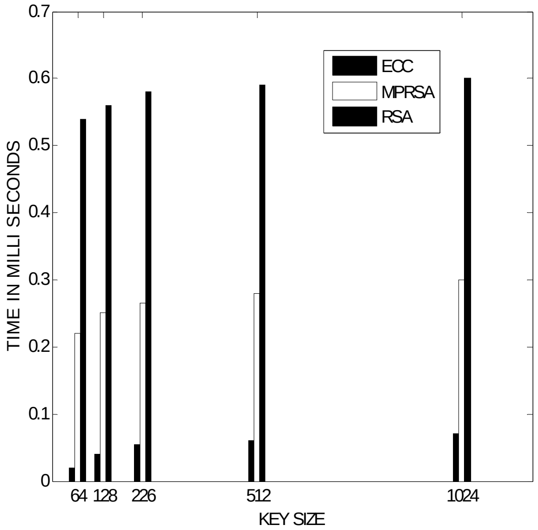

Fig.6 RSA, MPRSA and ECC decryption time for different key sizes.

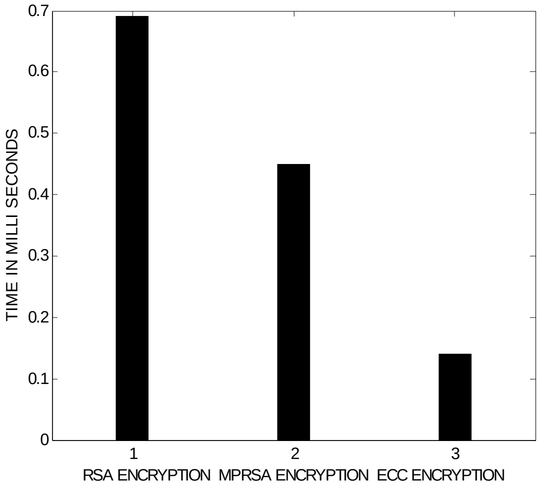

Fig.7 Performance Comparison of RSA, MPRSA and ECC encryption time using Diffie-Hellman key exchange.

Fig.9 and Fig.10 shows the comparison of encryption and decryption time of the three algorithms namely, RSA, MPRSA and ECC using ECC key Exchange. From the simulated graphs it is clearly seen that ECC with ECC key exchange gives better computational speed for lower key sizes.

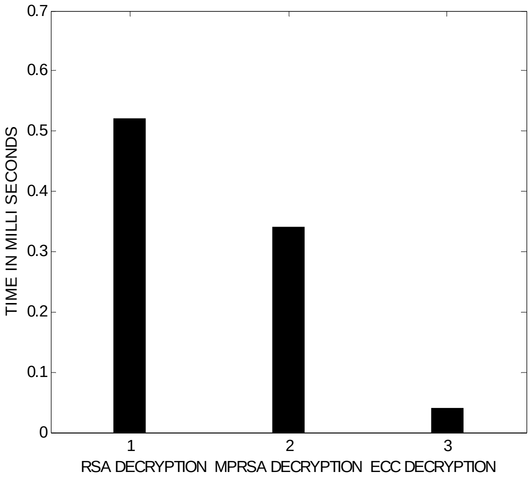

Fig.8 Performance Comparison of RSA, MPRSA and ECC decryption time using Diffie-Hellman key exchange.

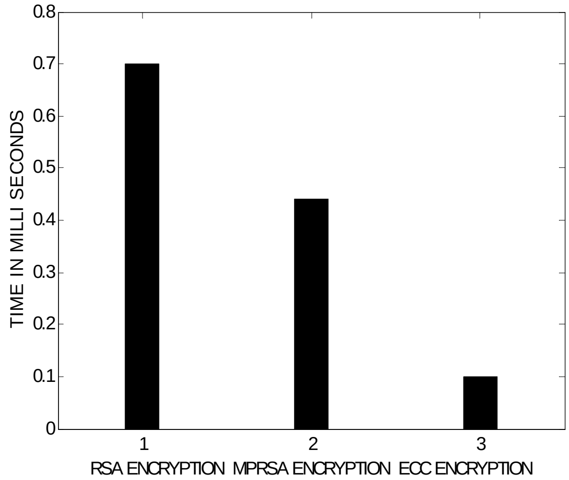

Fig.9 Performance of RSA MPRSA and ECC Encryption time using ECC key exchange.

The simulation was done for 25 sensor nodes and can also be done for any number of nodes. Fig.11 shows the computed positions of the nodes based on time of arrival scheme. The performance of the TOA based ECC scheme is measured with the mean error, which is widely used and it is given by equation

$$error = \frac{\sum_{i=m+1}^{n} \left\| x_{est}^{i} - x_{real}^{i} \right\|^{2}}{(n - m) \times (radio - range)} \qquad (3)$$

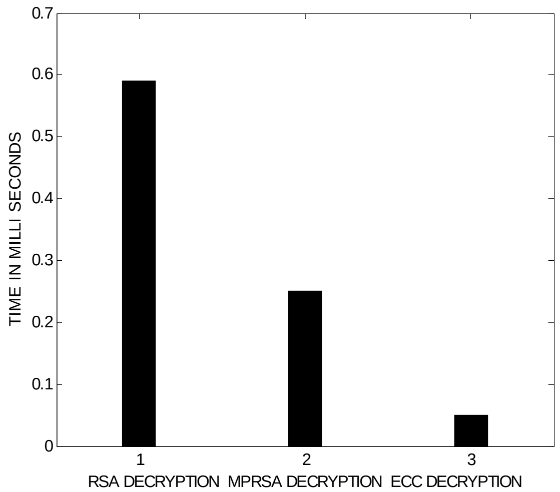

Fig.10 Performance of RSA MPRSA and ECC Decryption time using ECC Key exchange

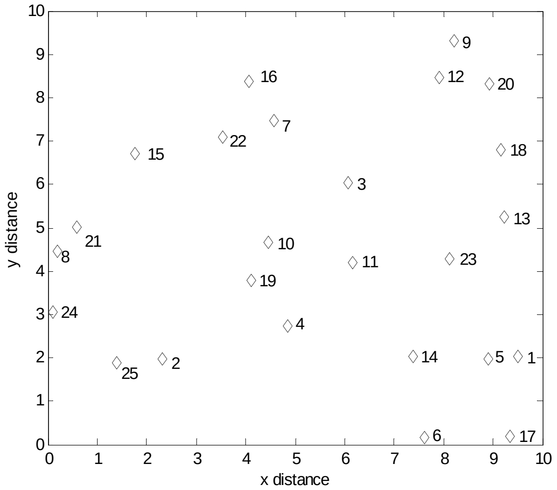

Fig.11 Computed position of the nodes

The position of the nodes is computed from the knowledge of the time of arrival of the signals and then compared with the initial randomly deployed positions. Because of the implementation of the ECC technique, the distance estimation and positioning technique is capable of overcoming attacks and accurate positions were obtained. But, if the time of arrival of signal is itself prone to error, then the computed position of the nodes is to be erroneous only which can be clearly seen from the Figure 12.

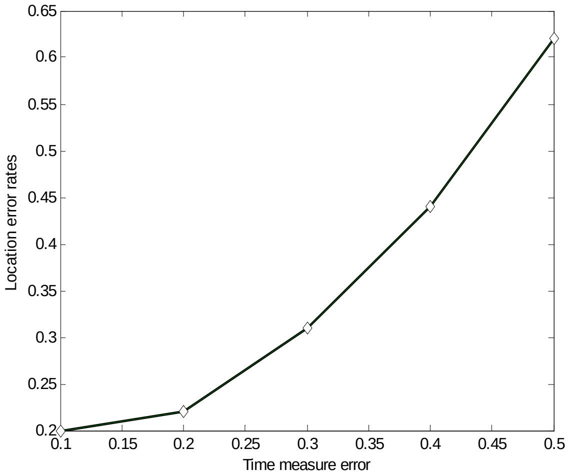

Fig.12 Time measure error Vs Location error rate

7. Conclusion

In this paper, the TOA localization scheme along with ECC for secure localization and authentication was implemented. This TOA-ECC scheme was compared with the other public key cryptographic schemes like RSA and MPRSA. A further comparison was done by implementing both Diffie-Hellmann key exchange and ECC key exchange. Our simulation results clearly indicate that TOA approach of localization along with the implementation of ECC with ECC key exchange is well suited for Wireless Sensor Networks.

References

[1] K. Holger, and A. Willig, “A Short Survey of Wireless Sensor networks”,*TKN Technical Reports Series*, Technical University Berlin, Berlin, pp. 1-19,Oct 2003.

[2] J.G. Castano, M. Svensson, and M. Ekstrom, “Local Positioning for Wireless Sensor Networks Based on Bluetooth,” *IEEE Radio and wireless Conf.*, pp. 195-198, Sep 2004.

[3] W.C. Chung, and D. S. Ha, “An Accurate Ultra Wideband Ranging for precision Asset Location”, *Int. Conf. UWB Systems and Technologies*, Reston, Virginia, pp. 383-393, Nov 2003.

[4] J.Y.Lee, and R.A. Scholtz, “Ranging in a Dense Multipath Environment Using an UWB Radio Link,” *IEEE J. Selected areas in Communication*, vol.20, no. 9, pp.1677-1683, Dec 2002.

[5] K.C. HO, and W. Xu, “ An Accurate algebraic solution for moving source location using TDOA and FDOA measurements’, *IEEE Trans. Signal processing,* vol. 52, Issue 9, Sep 2004

[6] A. Pages-Zamora, J.Vidal, and D.H. Brooks, “Closed-form solution for position based on angle of arrival measurements”, *The 13th IEEE Int. Symposium personal, Indoor and Mobile Radio Communications*, vol. 4, Sep 2002.

[7] Y. Zhang, W. Liu, Y. Fang, “Secure Localization and authentication in Ultra Wideband Sensor Networks,” *in IEEE Journal on Selected Areas and Communication*, Oct 2005.

[8] N. Koblitz, “Elliptic Curve Cryptosystems”, Mathematics of Computation, vol. 48, pp. 203-209. 1987.

[9] V. Miller, “Uses of Elliptic Curves in Cryptography” Advances in Cryptology; proceedings of Cryto’85, pp. 417-426,1986.

[10] A. Menezes, P. Van OOrschot, and S.Vanstone. Handbook of Allied Cryptography. CRC press, 1997

[11] Certicom Research. SEC 2:Recommended Elliptic Curve Domain parameters. Standards or efficient Cryptography Version 1.0, Sep 2000.

Vijayalakshmi V is Senior Lecturer, Department of Electronics and Communication Engineering in Pondicherry Engineering College, Puducherry, India. She teaches courses on Information Security for both under graduate and post graduate engineering students. At present she is pursuing her PhD program in Information Security. She has authored 6 international journals and 15 international and national conferences. Her research areas of interest include Cryptography and Network Security, VLSI and ASIC Design.

Dr. Palanivelu T G is Principal of Pondicherry Engineering College, Puducherry, India. He received his PhD in Electronics and Communication Engineering from Indian Institute of Science, Bangalore .He has authored more than 50 research papers both in international conferences and reputed journals. His research areas of interest include Cryptography, Mobile Communication and Bio-Medical Engineering.