I J C T A, 9(2) 2016, pp. 951-958

Elliptical Curve Cryptography based Secure Location Verification in clustered WSN

S. Velmurugan*, and E. Logashanmugam**

Abstract: Wireless Sensor Networks (WSNs) play an essential role in today's real world applications. Localization is one of the most significant technologies in wireless sensor networks. Secure distance based localization in the presence of unreliable beacon node identification is a challenging task in WSN. In this paper, we propose Elliptical Curve Cryptography based Secure Location Verification (ECC-SLV) in clustered WSN. This paper goal is to detect the unreliable node and obtain the secure localization information from beacon nodes. The random pair wise shared key between beacon node and Base Station (BS) this key detect the malicious beacon node. We using the Elliptical Curve Cryptography (ECC) algorithm also provide the security for beacon node send the message to sensor node. Hence, the malicious beacon nodes cannot access the location information. The simulation results demonstrate that the proposed system achieve high throughput rate and less energy consumption in the network.

Keywords: Localization, Elliptical Curve Cryptography, Random pair wise Key, Clustering, WSN.

1. INTRODUCTION

Wireless sensor networks (WSNs) have increasingly drawn attentions of researchers in the areas of wireless communication, distributed systems, embedded computing and sensor technology. These sensor networks consist of a large number of least cost, little power, and multi-functional sensor nodes that transmit through wireless media. Different WSN applications have been proposed, e.g., environment monitoring, military operations, emergency rescue, medical treatment, and smart home.

A localization system among sensor nodes is a fundamental issue for many applications of wireless sensor. The node localization technology is required in WSN application, especially when location information is necessary WSN nodes localization is determining coordinates of nodes in result the coordinate or normal nodes location is unknown. Anchor nodes can obtain their location via global positioning system (GPS) modules or manually. In many typical localization algorithms assumed that information of anchor nodes location are quite without any interference by adverse factors, so normal nodes can use anchor information safely. However, in real hostile situations, some malicious nodes may enter into the sensor network without authorization in order to sabotage. They are trying to introduce themselves as benign anchor nodes or attack other anchor nodes to force them declare a wrong location. Erroneous distance estimation or erroneous coordinate causes irreplaceable fault in normal sensor nodes localization. In this case, some methods should be applied to eliminate or reduce harness effects, which created by malicious anchor nodes and ensure secure wireless sensor network localization.

In this paper, we propose detect unreliable beacon nodes and remove that node supplies misleading location information to the regular sensor node objective to provide the secure localization in WSN. In this article, Elliptical Curve Cryptography encryption and decryption algorithm used to protect secure location information from unreliable beacon nodes and improve security as well as reliable data transmission in WSN.

* Research Scholar, Department of Electronics and Communication Engineering, St. Peter's University, Chennai, India

** Professor, and Head, Department of Electronics and Communication Engineering, Sathyabama University, Chennai, India

2. RELATED WORKS

A Novel Secure Localization Approach [1] investigates attack resistant localization scheme called Temporal Spatial Consistent based detection (TSCD secure localization) to overcome the distance consistent spoofing attack in WSN. Multi hop range free localization in anisotropic wireless sensor networks offered a secure locating mechanism that detects the anchor malicious nodes under their fake location claims. This method uses the anchor superfluous nodes instead of regular nodes in infected area to deal with malicious anchors. This detection method relies on a centralized base station. Secure Localization Approach [3] proposed robust and secure localization algorithm in order to solve the problem of malicious anchor nodes existence in localization. In this method, each anchor node asks other anchors their locations and deicide about other anchor nodes that are benign or malicious. The sink is informed with anchor node decision to judge about anchors. It consists of two steps. In first step, the correctness investigation has been designed on the base of making a table with valid nodes in the base station. In second step, the mean square of Taylor series is used for estimation the sensor node places.

Robust Position Estimation (ROPE) [4] that provides a location verification mechanism to verify the location claims of the sensors before data collection. However, the requirement of the counter with nanoseconds precision makes it unsuitable in low cost sensor networks. Distributed Reputation-based Beacon Trust Security protocol (DRBTS) [5] aimed at providing secure localization in sensor networks. Based on a quorum voting approach, DRBTS drives beacons to monitor each other and decide which should be trusted. However, it requires extra memory to store the message of Neighbor Reputation Table (NRT) and Trusted Beacon Neighbor (TBN). In [6], a secure localization scheme is presented to make the location estimation of the sensor secure, by transmission of nonce at different power levels from the beacon nodes. As all the computation is implemented on the base station, it will cause a significant bottleneck.

Secure Localization Scheme (SLS) [7] is a novel mobility-assisted secure localization algorithm that can furnish sensor nodes with secure, accurate locations despite the presence of attacks. However, the process of SLS is more complex and it consumes higher energy. An Enhanced Secure Localization Scheme (ESLS) [8] offers strong defense against distance reduction attacks and distance enlargement attacks. In [9], present a two-way “Greet, Meet and Locate” (GML) mechanism for secure location estimation based on geographical sectorization. A double-averaging mechanism uses a Time of Arrival (TOA) technique to help minimize the location estimation errors. Hence, the overall process consumes the least possible power and is lightweight regarding the processing overhead. Detecting Phantom Nodes approach [10] authenticates the locations of truthful nodes as well as detects the existence of the phantom nodes without relying on trusted agents. Localized construction results detect phantom nodes efficiently however it create overhead.

Collaborative Localization and Location Verification scheme [11] introduces the virtual force model to determine the location by incremental refinement. This scheme solved the drifting problem and malicious anchor problem. Location verification algorithm has high accuracy and transmission overhead is low. Threshold and Vote Security Localization (TVSL) [12] algorithm improves the safety performance of positioning process of nodes in WSN by using the threshold idea and vote with sensor nodes. The vote security method is used to reduce the location area. The credibility threshold method is used to position calculation and protects the performance of malicious attack.

3. PROBLEM STATEMENT

Probabilistic Location Verification (PLV) [13] technique introduced to verify the location of sensor nodes. The sensors initially send their position and its id to all the nodes using flooding and when the verifiers gets the message there takes place collaboration between the verifiers to decide whether the location sent by the sensor node is valid or not. If more number of verifier nodes is used then higher is the probability to detect the malicious node. However, this technique contains more problems such as flooding will create some

unwanted traffic in the network, any malicious node compromises the verifier then all adversary nodes gets access the whole network information and this technique is unreliable because packet loss rate is high.

4. PROPOSED SYSTEM

Wireless Sensor Network consists of number of homogeneous and static sensor nodes and Beacon nodes are deployed randomly in a particular area. The Base Station (BS) is located at corner position. ECC-SLV is a Proactive routing protocols that aims to maintain an ongoing routing protocol. Beacon message is exchanged among adjacent nodes to construct and maintain a routing table. Upon receiving a beacon message, a routing table is updated based on sensor location. The sensor node sends data packet to the base station after constructing the routing table. Sensor nodes are initially having same amount of energy and limited communication range. Figure 1 shows that the ECC-SLV structure. The clusters are formed based on the distance. The Cluster Head (CH) is elected based on the residual energy. The energy consumption of sensor includes the power for transmitting, receiving and sensing operation. The energy consumption sensing is negligible compare with transmission and received energy thus sensing energy calculation is ignored. The transmission and received energy is calculated by following formula.

$$E_{tx}(K,d) = E_{elec}(K) + E_{amp}(K,d) \quad (1)$$

$$E_{Rx}(K,d) = E_{elec}(K) \quad (2)$$

Where

$E_{tx}(K, d) \rightarrow$ The transmitter energy consumption for transmitting a k-bit message over a distance d.

$E_{elec}(K) \rightarrow$ The electronics energy consumption for k-bit

$E_{amp}(K, d) \rightarrow$ The amplifier energy consumption to transmit acceptable BER (bit error rate) for signals transmitted to a receiver.

$E_{Rx}(K, d) \rightarrow$ The receiver energy consumption for receiving a k-bit message over a distance *d*

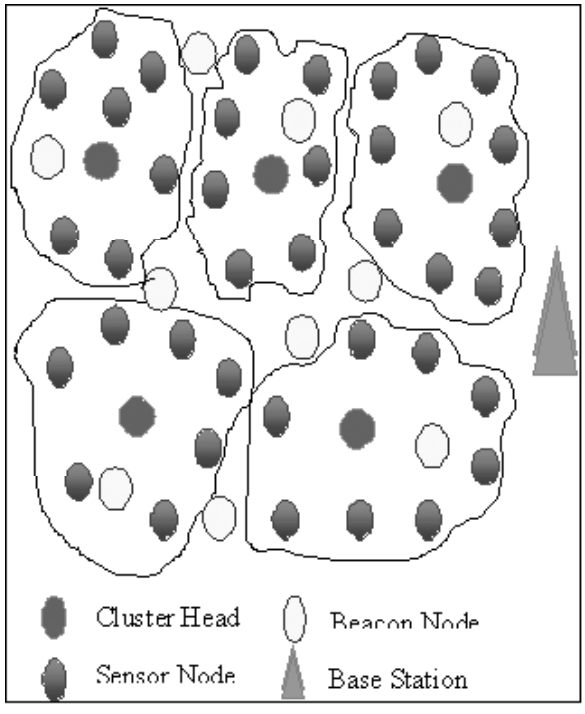

Figure 1: ECC-SLV Structure

In Wireless Sensor Network, a compromised beacon node or unreliable beacon node that has access beacon message and send out the fake beacon message that include wrong location information. Therefore, the sensor node verifies the beacon message send the location information. The shared random pair wise key between the BS and beacon node and this key is used to detect the unreliable beacon node. The Random pair wise key computation is given below.

$$PK = \sum_{i=1}^{n} (y_i)(x_i - x_j) \tag{3}$$

Where

$n \rightarrow$ Number of BN

$x_i \rightarrow x$ Location of BN

$y_i \rightarrow y$ Location of BN

$x_j \rightarrow$ Location of BS

Therefore, the sensor node cannot obtain the beacon message from unreliable beacon nodes. However, the unreliable beacon nodes access the location information from authenticated beacon nodes. To avoid this problem we using Elliptical Curve Cryptography encryption decryption algorithm to provide the security to beacon node send the location information. Therefore, the unreliable beacon node cannot read or hear the beacon message. The beacon node sends the Elliptical Curve Cryptography encryption decryption computation is given below.

Step 1: The location information is encoded the message m as a point on Elliptic Curve P_m.

Step 2: Select suitable curve point G and an elliptic Group E_q (a, b) as parameters.

Step 3: The beacon node selects the private key n_B and computes the public key

$$P_B = n_B * G \tag{4}$$

Step 4: Beacon node chooses a random key K is a positive integer

Step 5: The beacon node encrypts P_m

$$C_m = kG, P_m + kP_B \tag{5}$$

Step 6: Sensor node receives the message and decrypt

$$\begin{aligned} & P_m + KP_S - n_S(kG) \\ & = P_m + k(n_S G) - n_S(kG) \\ & = P_m \end{aligned} \tag{6}$$

Where $n_s \rightarrow$ Sensor Public Key

Finally, sensor node decrypts the message and collects the verified location information. The authenticated beacon node send the secure location information to the sensor node then the sensors node send the message to the BS through the CH.

The figure 2 shows that the working strategy of ECC-SLV. Initially the BS detects and isolates the unreliable beacon node using random pair wise key. The BN encrypt the location information based on ECC and send to the sensor node. The Sensor node received this encrypted message and decrypted. Clusters

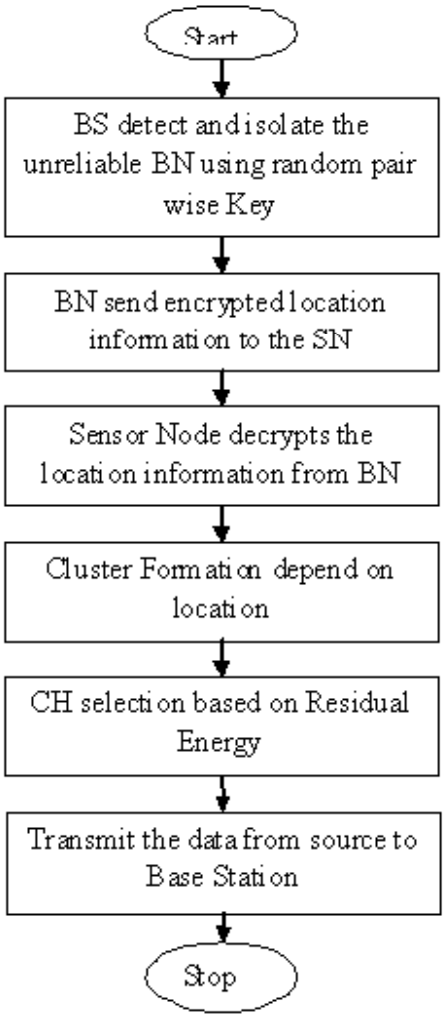

Figure2: Flowchart of ECC-SLV

are formed based on Sensor node location and highest residual energy node is chooses the CH. Finally, the source sends the data through the CH.

5. PERFORMANCE EVALUATION

The performance of the proposed scheme is analyzed by using the Network simulator (NS2). The NS2 is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language). NS2 is a discrete event time driven simulator, which is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The parameters used for the simulation of the proposed scheme are tabulated in Table 1. The simulation of the proposed scheme has 61 nodes deployed in the simulation area 1000×1500. The nodes are moved randomly within the simulation area by using the mobility model Random waypoint. The nodes are communicated with each other by using the communication protocol User Datagram Protocol (UDP). The traffic is handled using the traffic model CBR. The radio waves are propagated by using the propagation model two-ray ground. All the nodes receive the signal from all direction by using the Omni directional antenna. The performance of the proposed scheme is evaluated by the parameters packet delivery ratio, packet loss ratio, average delay, throughput and residual energy.

5.1. Packet Delivery Rate

Packet Delivery Rate (PDR) is the ratio of the total number of packets successfully delivered to the total packets sent. It is obtained from the equation (7) below.

Table 1
Simulation Parameters of ECC-SLV

Parameter	*Value*
Number of nodes	61
Routing scheme	PLV and ECC-SLV
Traffic model	CBR
Simulation Area	1000x1500
Channel	Wireless Channel
Transmission range	250m
Traffic Model	CBR
Communication Protocol	UDP
Antenna	Omni Antenna

$$PDR = \frac{Total\ Packets\ Received}{Total\ Packets\ Send} \tag{7}$$

The Figure 3 shows the PDR of the proposed scheme ECC-SLV is higher than the PDR of the existing method PLV. The greater value of PDR means better performance of the protocol.

5.2. Packet Loss Rate

Packet Loss Rate (PLR) is the ratio of the packets lost to the total packets sent, estimated by the equation (8) below.

$$PLR = \frac{Total\ Packets\ Dropped}{Total\ Packets\ Send} \tag{8}$$

The PLR of the proposed scheme ECC-SLV is lower than the existing scheme in figure 4. Lower the PLR indicates the higher performance of the network.

5.3. Average Delay

Delay is defined as the time difference between the current packets received and the previous packet received. Where n is the number of nodes.

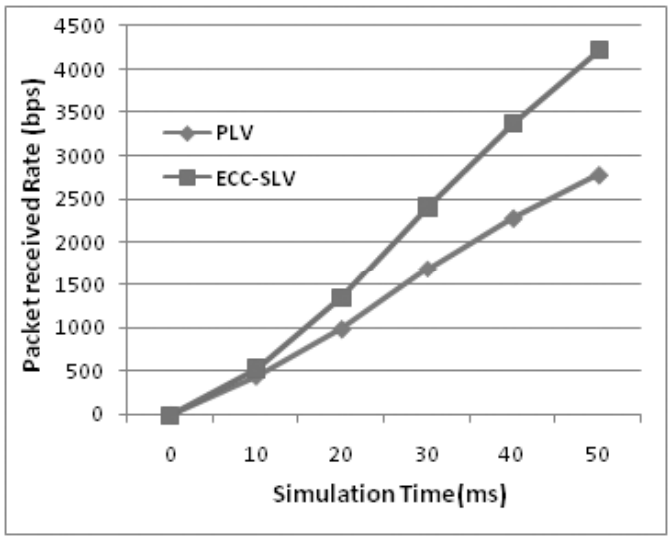

Figure 3: Packet Received Rate

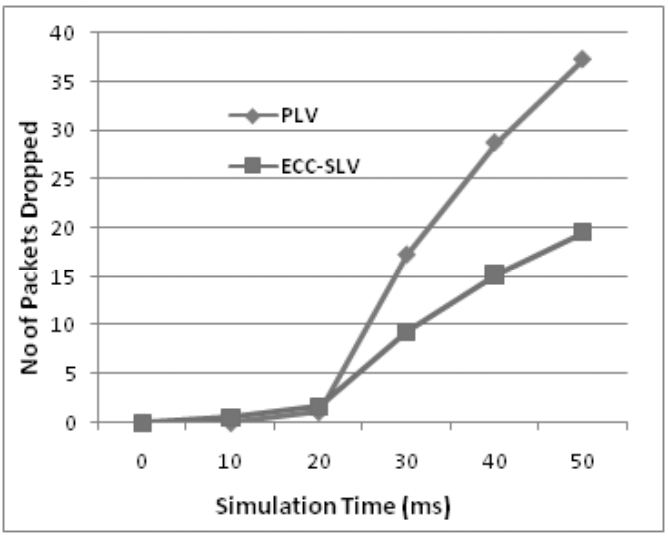

Figure 4: Packet Loss Rate

$$Delay = \frac{\sum_{0}^{n} Pkt\,\mathrm{Re}\,cvd\,Time - Pkt\,Send\,Time}{n} \tag{9}$$

Figure 5 shows that the delay value is low for the proposed scheme ECC-SLV than the existing scheme PLV. The minimum value of delay means that higher value of the throughput of the network.

5.4. Throughput

Throughput is defined as the rate at data is successfully transmitted for every packet sent.

$$Throughput = \frac{\sum_{0}^{n} Pkts\,Received\,(n) * Pkt\,Size}{1000} \tag{10}$$

Figure 6 shows that the proposed scheme ECC-SLV has greater average throughput when compared to the existing scheme PLV.

5.5. Residual Energy

The amount of energy remaining in a node at the current instance of time is called as residual energy. A measure of the residual energy gives the rate at which energy is consumed by the network operations.

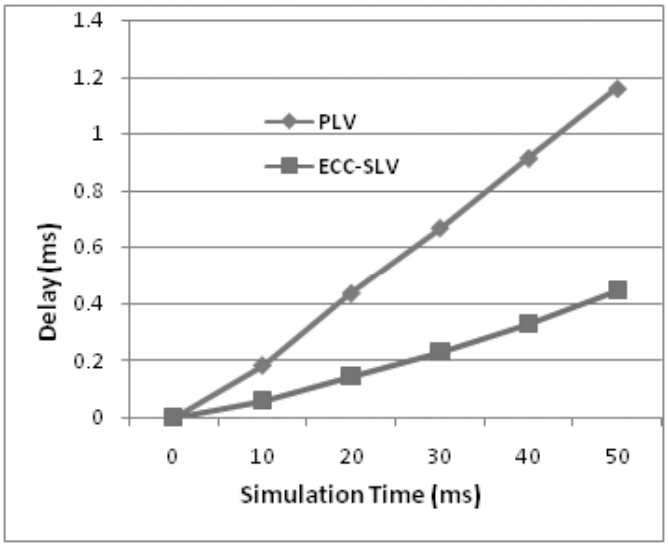

Figure 5: Average Delay

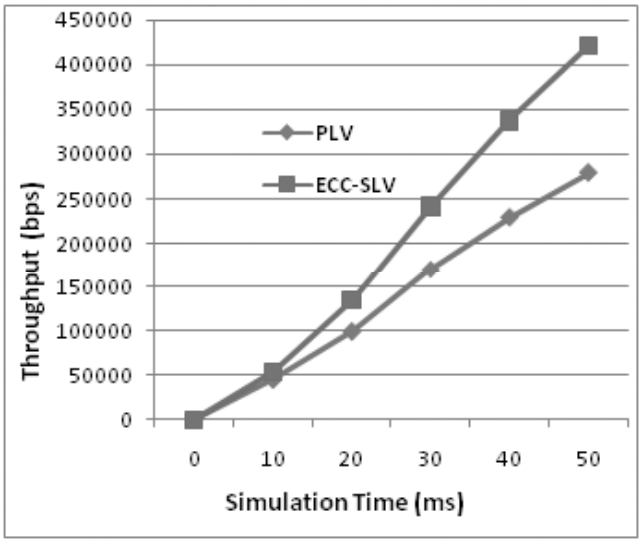

Figure 6: Throughput

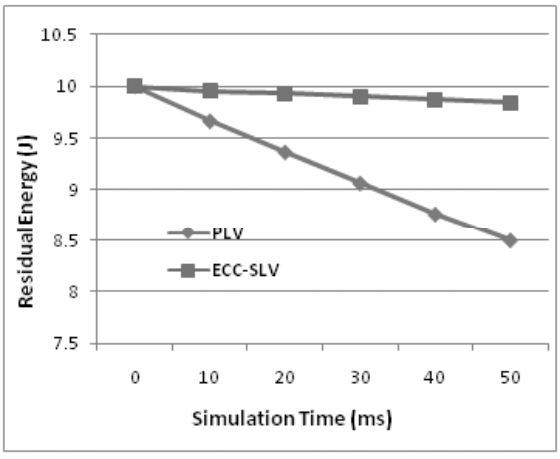

Figure 7: Residual Energy

Figure 7 shows that the residual energy of the network is better for the proposed scheme ECC-SLV when compared with the existing scheme PLV.

6. CONCLUSION

The research on securing localization services presented in this paper targets a very specific type of localization technique referred to as the beacon-based techniques. In this paper new security localization (ECC-SLV) is proposed, the algorithm first to use the random pair wise shared key between beacon node and base station and this key detect the malicious beacon nodes. Then uses ECC algorithm to provide the security to beacon message, therefore the unreliable beacon node cannot read or modify the beacon node send the message to sensor node. The simulation result shows that the ECC-SLV performs better throughput and both lower energy consumption and delay.

REFERENCES

[1] Honglong Chen; Wei Lou; Junchao Ma; Zhi Wang, "TSCD: A Novel Secure Localization Approach for Wireless Sensor Networks," *Second International Conference on Sensor Technologies and Applications*, vol., no., pp. 661-666, 25-31 Aug. 2008.

[2] Q.J. Xiao, B. Xiao, J. N. Cao, and J. P. Wang, "Multihop range free localization in anisotropic wireless sensor networks: A pattern-driven scheme,"IEEE Transactions on Mobile Computing, vol. 9, no. 11, pp. 1592–1607, 2010.

[3] Mazinani, S. M., & Safari, M. (2015). Secure Localization Approach in Wireless Sensor Network. *International Journal of Machine Learning and Computing*, *5*(6), 458.

[4] L. Lazos, R. Poovendran, and S. Capkun. ROPE: Robust Position Estimation in Wireless Sensor Networks. InProc. of IEEE IPSN, pages 324–331, 2005.

[5] A. Srinivasan, J. Teitelbaum, and J. Wu. DRBTS: Dis-tributed Reputation-based Beacon Trust System. InProc. Of the 2nd IEEE Int'l Symposium on Dependable, Autonomic and Secure Computing, pages 277–283, 2006.

[6] F. Anjum, S. Pandey, and P. Agrawal, "Secure localization in sensor networks using transmission range variation," in Proceedings of the 2nd IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, November 2005, pp. 203–211.

[7] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," in IEEE Journal on Selected Areas in Communication, vol. 24, no. 4, 2006, pp. 829–835.

[8] D. He, L. Cui, and H. Huang, "Design and verification of enhanced secure localization scheme in wireless sensor networks," in IEEE transactions on Parallel and Dis-tributed Systems, vol. 20, no. 7, July 2009.

[9] S. Arisar and A. Kemp, "Secure location estimation in large scale wireless sensor networks," in Proceedings of the 3rd International Conference on Next Generation Mobile Applications, Services and Technologies, 2009, pp. 472– 476.

[10] J. Hwang, T. He, and Y. Kim, "Detecting phantom nodes in wireless sensor networks," inProc. the 26th IEEE International Conference on Computer Communications (INFOCOM'07), May 2007, pp. 2391–2395.

[11] Chunyu Miao, Guoyong Dai, Kezhen Ying and Qingzhang Chen, Collaborative Localization and Location Verification in WSNs, sensors, 15, 10631-10649,2015.

[12] Peng Bao, Ma Liang, A Security Localization method based on Threshold and Vote for wireless sensor networks, Procedia Engineering 15 (2011) 2783 – 2787.

[13] Ekici, E., McNair, J., & Al-Abri, D. (2006, June). A probabilistic approach to location verification in wireless sensor networks. In *Communications, 2006. ICC'06. IEEE International Conference on* (Vol. 8, pp. 3485-3490). IEEE.