IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Secure Localization and Key Distribution in Wireless Sensor Network

K.Karthika Keshav[1], R.Arthi[2], Dr.K.Murugan[3]

[1]Electical and Electronics Engineering, Anna University, College of Engineering, Chennai, Tamil Nadu, India

[2, 3]RCC, Anna University, College of Engineering, Chennai, Tamil Nadu, India

Abstract

Secure localization of unknown nodes in a Wireless Sensor Network (WSN) is an important task for many applications. The crucial problem in Wireless Sensor Networks (WSNs) is position estimation due to their dynamic method of deployment. There are several methods in determining their physical locations but the greatest challenge imposed is communicating with authenticated neighbors in a secured manner. The mutual authentication between sensor nodes is of great importance i.e. node should only accept and forward their own precise location messages from authenticated neighbors. When WSNs are deployed in hostile environments, many attacks happen, e.g., wormhole, sinkhole, Sybil etc,. The attackers may disguise as normal node and attack the unknown nodes to interfere with localization process. They may forge, modify or replay localization information to make the estimated positions incorrect. The objective of this paper is to solve the problem of insecurity in localization of sensor nodes. Hence to provide security to localized coordinates during coordinate exchange security has been provided through Elliptic curve cryptography (ECC) to solve this issue. In this paper common attacks against localization and their security measures for secure transmission of localized coordinates.

Keywords: *Elliptic Curve Cryptography (ECC), ECC key exchange, Localization, Wireless Sensor Networks (WSNs).*

1. Introduction

Localization is one of the most important topics in Wireless Sensor Networks (WSNs),e.g., location-based Key distribution, requirement of positions of unknown nodes play a critical role in many WSNs applications, such as monitoring applications include environmental monitoring, health monitoring and tracking applications include tracking objects, animals, humans, and vehicles. When a WSN is deployed in hostile environments, it is vulnerable to threats and risks. Many attacks exist, e.g., wormhole, sinkhole, Sybil etc, to make the estimated positions incorrect. Specifically for some applications, e.g., military applications like battlefield surveillance or environmental applications like forest fire detection [5], incorrect positions may lead to severe consequences, e.g., wrong military decisions on the battlefield and false alarms to people [6]. Hence, the issues of secure localization must be addressed in WSNs.

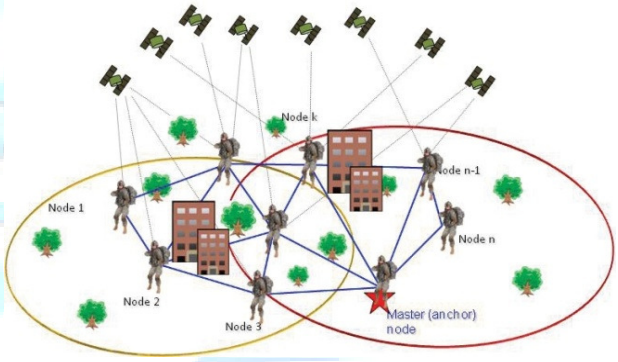

Fig1: Wireless Sensor Network (WSN)

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 the given physical environment in great detail [1]. Hence precise location and authentication of the sensors is vital. After the precise location of sensor nodes has been determined, exchange of locations to individual sensor nodes and communication with authenticated neighbors imposes the need for security in sensor networks. The distance estimated for positioning of sensor nodes is highly vulnerable to both internal and external attackers. While internal attackers report false distance information in order to cheat their positions, external attackers modify the positions of other sensor nodes. This necessitates a highly secure positioning scheme for sensor nodes. Elliptic Curve 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 in the presence

of attackers. Thus, the paper proposes an efficient authentication scheme between sensor nodes.
The rest of the paper is organized as follows. In section 2, localization in sensor networks and the importance of security is focused. Section3 focuses on Elliptic Curve Cryptography algorithm and ECC key exchange. In section4 normal distribution of localized coordinates in the presence of malicious node is analyzed. In section5 implementation of ECC in the presence of malicious nodes is simulated so as to determine how secure the coordinates are distributed to the sensor nodes in the presence and absence of malicious nodes. The conclusion finalizes that secure localization using ECC technique is well suited for WSNs under hostile environment.

2. Secure Localization In Sensor Networks

Secure location involves location verification, location privacy and secure coordinate distribution. Secure localization algorithms can be classified into two main categories according to their objective. The first category aims to verify location of nodes. This is important because, usually, nodes are granted more services and privileges when they are closer to other nodes. So, an adversary node probably would claim to be in a closer location to an anchor node than it actually is. The second class of algorithms (location estimation) aims to assure that nodes can estimate their own precise locations with the help of other nodes, even when some of the nodes are malicious. Several secure localization systems have been proposed in the last few years to provide the secure positioning of nodes in hostile and military applications of WSNs. 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.

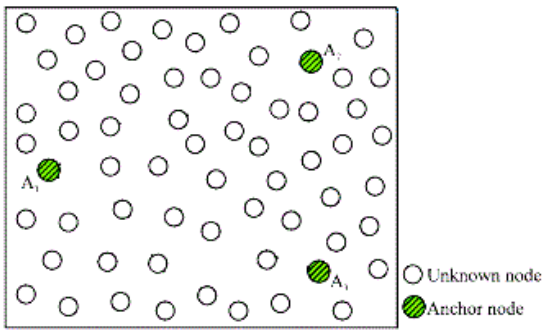

Fig 2: Anchor nodes and Non-Anchor nodes

Determining the physical positions of sensors is a crucial problem in wireless sensor network for several important reasons. First, in order to use the data collected by sensors, it is necessary to have their position information stamped. 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 has been 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. 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 neighborhood authentication. Our location based authentication scheme is built on the ID-based cryptography by using ECC. The results thus obtained are analyzed by introducing Sybil attack.

3. Proposed Work

The assumptions made is an attack-free base station located behind the deployment field, where it is secure to perform any necessary pre-deployment operation, such as downloading program code and distributing an initial key to each sensor node[13]. The sensor nodes are close to the anchor node when they are deployed and therefore, it is the anchor node that makes all the localization and key distribution decisions. During deployment, the anchor node remains turned on. Sensor nodes are in the proximity of the anchor node and turned on and deployed.

Algorithm1: Secure Transmission of Localized Coordinates

Begin

1. $S_i \rightarrow A_c$:$NID(S_i) \| \{req\_deployment\}$ Ecc
2. $A_c \rightarrow S_i$:$NID(A_c) \| \{location\} K_i^d \| \{K^C_{i,1}, K^C_{i,2}, \ldots\ldots K^C_{i,m}\}$ Ecc
3. $S_i \rightarrow A_c$: $NID(S_i)\{ack\}$ Ecc

End

When requested by the sensor nodes anchor node transmits individual node id and localized coordinates to individual sensor node. To distribute the localized coordinates of

individual sensor nodes secure distribution of coordinates is essential which is done using ECC. Attacks are launched and improved performance measures are obtained using ECC.

3.1 Attacks in Localization

Localization process can be attacked in a number of different ways. When an attacker attacks on victim, the original connection is broken down and the new connection is established between the sensor node and the victim. All information exchanged between two different sensor nodes passes through the attacker. Localization process can be attacked in a number of different ways researchers have addressed a set of known attacks. They can be divided into two categories: external and internal attacks. The adversary is external if it is outside the WSN and implements malicious behaviors without right cryptographic key. Otherwise, the adversary is internal, and the adversary controls over one or more fraudulent nodes.

3.2 Elliptic Curve Cryptography

The main concept of secure Localization and key distribution is to provide the location and keys of each sensor nodes securely through Elliptic curve cryptography. Elliptic Curve Cryptography is a proven technology that is used many in different commercial products such as mobile phones, smart cards, email systems and many others. The difficulty of these problems directly impacts the performance, since it dictates the size of the domain and key parameters. These values are very important in a security system as the performance of arithmetic operations relays heavily on them. One of the main operations in elliptic curve cryptography is the calculation of a scalar point multiplication $Q = sP$, where Q and P are two points on a certain elliptic curve. For public key systems that are based on integer factorization and discrete logarithm problems fast algorithms are known that have a sub exponential expected running time. This feature allows Elliptic Curve Cryptography based systems to provide the same level of security as traditional schemes but with smaller parameters. Table 1 compares the key sizes in symmetric, RSA and Elliptic Curve Cryptography Systems for achieving different security levels. This shows that much smaller key sizes can be used in the elliptic curve system than with RSA at a given security level. The difference in key sizes between Elliptic Curve Cryptography and RSA is especially visible for higher security levels. At 256 bits of security Elliptic Curve Cryptography uses only a 512-bit key which is 97% smaller than the corresponding RSA key. The advantages that can be gained from smaller keys include not only faster computations and smaller memory requirements, but also energy savings for sensor devices, as fewer bits are required to be transmitted by the radio.

Security Bits	*Symmetric Encryption algorithm*	*Minimum Size (bits) of Public Keys*		
		DSA/DH	*RSA*	*ECC*
112	3DES	2048	2048	224
128	AES-128	3072	3072	256
192	AES-192	7680	7680	384
256	AES-256	15360	15360	512

Table 1: Key Comparison Table

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

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

3.2.1 Elliptic Curve Encryption and Decryption

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

$$C_m = [k\,G,\ P_m + k\,P_B] \qquad (1)$$

$$P_m + kP_B - n_B(k\,G) = P_m + k(n_B\,G) - n_B(kG) = P_m$$

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 from equation (2)

3.2.2 ECC key exchange

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 $P_A = n_A * G$.
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 $K = n_B * P_A$.

4. Results of ECC Implementation

Once the spatial coordinates of the sensor nodes have been determined, the exchanges of the precise location of the sensor were carried out using ECC technique. The authentication between the sensor nodes was done by ECC key exchange. The encryption of position was carried out by the ECC encryption scheme. Comparison of performance was carried out in three different scenarios such as in the presence and absence of attack and providing security during distribution. Performance measures are taken under different types of attacks for both grid and random network. From the simulated results ECC was proven to be attack resistant with improved performance.

The comparison of the cryptographic schemes was carried out for Sybil attack using ECC key Exchange. Fig 3and 5 shows three cases, location distribution in the presence of Sybil attack, absence of attack and security implementation using ECC. The performance gets decreased when an attack is launched. This is compensated when security is implemented, in the presence of attack which shows a performance increase in Throughput when compared with launch of attack. Similarly Fig 4 and 6 shows location distribution in the presence of Sybil attack, absence of attack and security implementation using ECC. The overhead gets increased when an attack is launched. This is compensated when security is implemented in the presence of attack, which shows a performance increase by reducing the overhead when compared with launch of attack. Comparison is made for multiple nodes (20, 40, 60, 80 and 100) for both grid and random network.

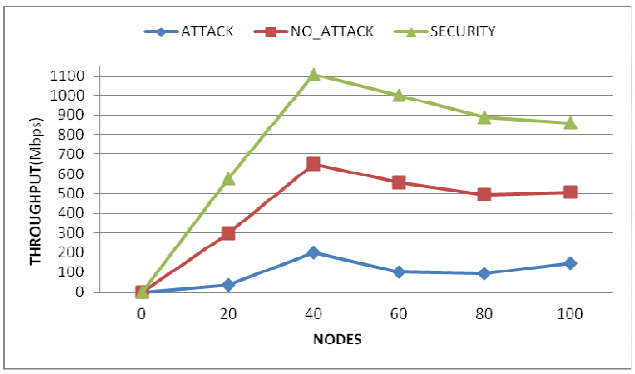

Fig3: Performance of Throughput under Random network using Sybil attack

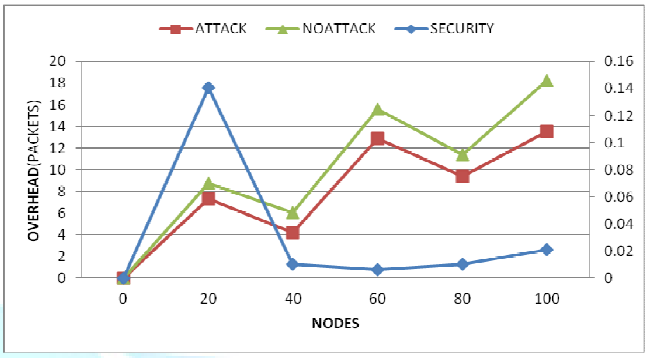

Fig4: Performance of Overhead under Random network using Sybil attack

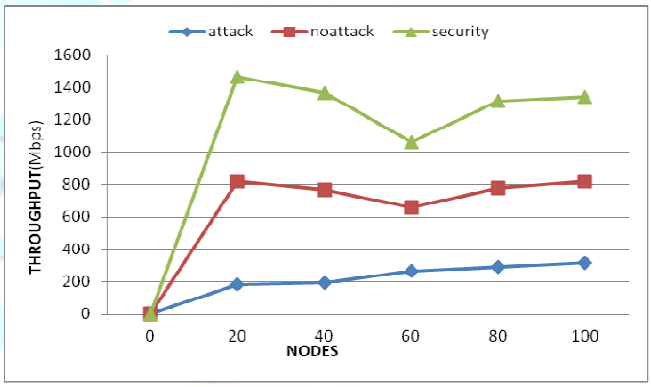

Fig5: Performance of Throughput under Grid network using Sybil attack

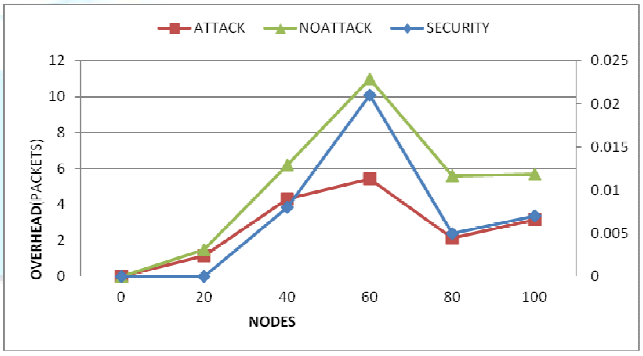

Fig6: Performance of Overhead under Grid network using Sybil attack

5. Conclusion

In this paper, secure localization and authentication using ECC was implemented. The performance of ECC was

compared with different types of attacks. A further comparison was done by implementing it in both under grid and random network using ECC key exchange which requires less computation time when compared with other types of cryptographic schemes. Our simulation results justify that the implementation of ECC with ECC key exchange is well suited for Wireless Sensor Networks since the communication overhead is reduced and improved throughput and packet delivery ratio for various scenarios.

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

[12] Implementing Data Security in Wireless Sensor Network's through Location Aware Multifunctional Key Management Framework Prof. D. Durga Bhavani, International Journal of Computer app (0975 – 8887) Volume 13– No.1, January 2011.

[13] Practical and secure localization and key distribution for wireless sensor networks, Qi Mi, John A. Stankovic, and Radu Stoleru. Ad Hoc Networks 10(6):946-961 (2012)

[14] Secure Localization Algorithms for Wireless Sensor Networks, Azzedine Boukerche, University of Ottawa, January 12, 2009 from IEEE Xplore.

[15] Secure Localization in Wireless Sensor Networks: A Survey Waleed Ammar, Ahmed ElDawy, and Moustafa Youssef fammar.w, aseldawy, Computer and Systems Engineering Department, Alexandria University Egypt July 7, 2009.

[16] A. Srinivasan, J. Wu, A Survey on Secure Localization in Wireless Sensor Networks, CRC Press, Taylor and Francis Group, 2008.

[17] Secure probabilistic location verification in randomly deployed wireless sensor networks. E. Ekici , S. Vural , J. McNair , D. Al-Abri ,E. Ekici et al. / Ad Hoc Networks (2007).

[18] S. Capkun, M. Cagalj, and M. Srivastava, \Secure Localization With Hidden and Mobile Base Statioins", in IEEE INFOCOM, 2006.

[19] S. Capkun, and J. Hubaux, Secure Positioning of Wireless Devices with Application to Sensor networks", in IEEE INFOCOM, 2005.

[20] L. Lazos, R. Poovendran, Serloc: secure range-independent localization for wireless sensor networks, in: Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe), 2004, pp. 21–30.