International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-02, May 2018

A Secure Localization Scheme Based on Node Authentication in WSN

Deepak Prashar, Research Scholar, IKGPTU, Punjab, India, deepakprash@gmail.com

Kiran Jyoti, Assistant Professor, GNDEC, Punjab, India, kiranjyotibains@yahoo.com

Dilip Kumar, Associate Professor, SLIET, Punjab, India, dilip.k78@gmail.com

Abstract - Localization is one of the prime area of concern for the applications that having social and economic importance with respect to wireless sensor networks. When WSN is deployed in aggressive environmental areas there is a risk in security breach associated with it. So designing a secure localization scheme is more important in order to maintain the integrity of the position estimations by the localization algorithm in the presence of malicious nodes. The paper focuses on the scheme for node authentication based on digital signature. It also conveys about the possible attacks that are ineffective on the proposed secure localization approach mentioned in the paper.

Keywords — DV Hop, El Gamal , ECC, RSA, SN, WSN.

I. INTRODUCTION

In WSN sensor nodes gets deployed by ad-hoc manner in which the location of the sensor node is not known a priori and then to determine the position of the sensor or to find out co-ordinates of the sensor where it is placed in particular target-area is known as localization [1]. Localization can also be inferred as self-localization that is nodes are able to localize themselves without any human interference. The localization process is subject to various factors like node density, obstacles and irregular deployment area, mobility and security. Localization algorithms further categorize into various dimensions like range based or range free and centralized or distributed one [2]. Different types of attacks are there in WSN such as black-hole, Sybil and sinkhole those can affect the localization in WSN. In some specific application of WSN as Military applications for battlefield surveillance, in forest for fire detection if in these area localizations is not secure then military decisions can be wrong, and false alarms can be there [3]. Security in localization can be considered from 2 aspects [4]. The first is an attack on nodes. The second is an attack on the information. Security is also a major issue in WSN. As when the gathered data is sent by the sensors to the base station, there is possibility that unauthorized entity can read the data or manipulate the data. So when the receiver gets the data, authentication of the data should be there, data should be in encrypted form [4]. Hence designing a secure localization scheme is more important

In order to maintain the integrity of the position estimations by the localization algorithm in the presence of faulty nodes otherwise wrong positions will be computed [5]. This demands the need for integration of security aspects in the localization algorithms before they compute the position so that accuracy is good [6]. This paper proposed a secure approach for localization based on the node authentication through which the possibility of attacks on any localization scheme can be reduced or overruled.

II. RELATED WORK

After conducting a thorough literature review, it has concluded that there are various factors that affect the localization process like the deployment area, mobility of node, security and the algorithmic nature in terms of its basic functionality. Loukas Lazos has proposed [7] a one secure localization algorithm in WSN. In this author narrates the scheme that localizes the unknown-node in the unsecured network. This scheme is decentralized and range, free scheme known as SeRLoc (Secure Range-independent Localization). This secure localized approach is strong for the different types of attacks as worm-hole attacks, Sybil attack and compromised nodes. Again Loukas Lazos has proposed one new approach [8] for secure localization in WSN HiRLoc (High-Resolution Range-Independent Localization) This scheme provides the highest accuracy as collate to the previous approaches with the use of less resources and this approach provide the best localization in the presence of the unsecure environment in which worm-hole attack, Sybil-attack and the compromise of network organization. Avinash Srinivasan has proposed novel-reputation based scheme [9] known as DRBTS (Distributed-Reputation-Based-Beacon-Trust-System) for localization in WSN. This approach uses the idea reputation for prohibiting the anchor-node. Yingpei Zeng has proposed new algorithm [10] based on hop-count is known as SHOLOC (Secure-Hop-Count based Localization). Results defined that hop-count-increment attacks are not effective for hop-count-based schemes and also narrates that LMS scheme not feasible to defend the worm-hole-attack. V. Vijayalakshmi has proposed [11] one new secure localization approach for WSN known as secure localization with ECC (Elliptic Curve Cryptography). This

 DOI : 10.18231/2454-9150.2018.0110

approach uses the ECC with ToA. ECC has chosen over the RSA (Rivest, Shamir-Adelman) and DSA.

Ting Zhang has proposed a new security approach [12] for localization is known as A Signcryption based Secure Localization in WSN. The author has proposed this approach that permits the sensors to make sure about the confidentiality and integrity of their position in detail. Jingsha has proposed [13] a Reputation Based Security scheme for node localization in WSN. In this approach author has proposed a reputation model for the security risks. . A simulation results narrates that this approach increases the security and improves the localization in an unsecured environment. Honglong Chen has proposed a new approach [14] that secures the basic DV-Hop localization from the worm-hole attack in WSN. In this paper author narrates the effect of the worm-hole attack on basic DV-Hop algorithm after that on the basis of these impacts new approach Label Based DV-Hop secure localization scheme has proposed.

Hongbin Wang has proposed secure localizing algorithm [15] based on DV-Hop known as SDV-Hop. In this paper two methods are there the first method is against the masquerade attack and second is average-per-hop-distance calculation method on the behalf of security-processing. A simulation results narrates that this proposed algorithm gives higher location accuracy and prevent the attacks such as worm-hole attack, masquerading-attack and block-attack. Wei Shi has proposed [16] algorithm that is decentralized designed to find the position of the unknown-node in the presence of the colluder. This approach permits the sensor to identify its position and identify the colluder those are within the bi-directional transmission range. So it is clearly seen from the literature work that almost all the schemes try to defend against some of the potential attacks on the network through various approaches. So the next section defines the new approach for secure localization against most of the active attacks that are possible during the localization process.

III. PROPOSED APPROACH

Security is also imperative to localization issue in wireless sensor networks. Any node can act as anchor maliciously and broadcast fake/incorrect position information to other sensor nodes in its radio range. That would lead to inaccurate location computation by those nodes and hence could affect other processes such as routing, data forwarding and data gathering at Base Station or Sink Node (SN). Hence it is important that nodes must validate or authenticate the identity of the anchor node from which it has received beacon, before it can proceed with the localization process. In this section we propose a novel secure localization scheme incorporating mutual node authentication with El Gamel digital signature scheme. We decided to choose El Gamel as it is the most simple signature scheme among available authentication methods, and thus would not put too much additional burden on the nodes computational efficiency and the constraint on resources at their disposal.

Node Authentication Based on Digital Signature

The localization process is totally dependent on the position determined by the nodes is involved in the process. There are anchor nodes who knows their location and there are unknown nodes whose position are to be determined with the help of anchor nodes using any localization scheme under the range free localization algorithms. If the nodes that are taking participation in the localization process are malicious one because of any reason then they will compromise the whole process and wrong positions will be computed at the end. This can be very dangerous in those applications that liking position centric the defense services using the missile target identification to surveillance. Hence there is a need of authentication of the nodes with respect to each other before applying the process of localization so that only the trusted nodes take the participation in the process and thus improves the accuracy of the localization process. The proposed algorithm describes below the procedure that is used to initiate for the node authentication approach based on digital signature.

The key generation part of the algorithm is taken care by SN as it required computations in finite fields. Any computation in finite field (GF (Z)) is hard and requires extensive resources which only base station or SN (Sink Node) can possess. The rest of the parts of algorithms can be implemented on each node independently. The proposed algorithm is explained below with the following steps from 1 to 4 mentions below:

STEP 1)

Input: A set of anchors/landmarks {A} and set of unknown sensor nodes {U} deployed randomly as per the parameters provided in Section 3.

SN provides IDai to each anchor and IDuj for each unknown node in {A} and {U} respectively.

After this step all the nodes, whether they are anchored or unknown will get the unique id from the base station. This is required in order to differentiate one node from other and the base station will maintain the database of the assigned id's.

The step 2 is useful for the generation of public and private keys for each node so that communication can be possible among them. So a pair of keys are generated, one is public pair and other is private pair . Here below describes the process for key generation.

 DOI : 10.18231/2454-9150.2018.0110

STEPT 2)

Key Generation Subroutine:

SN chooses a large Prime number p in field Zp and generator g1 of Zp

1. SN creates private key PRai for each anchor node Ai as

Select random number d

If (d<p-1)

Proceed

Else

Choose another d

2. Compute $g_2 = g_1^d \bmod p$
3. Exit Subroutine

Anchor Ai public key PUai= {g_1, g_2, p} and private Key PRai= {d}

After this step once the keys are determined, then signatures are generated as per the step 3 below :

STEP 3)

Signature Subroutine:

1. A_i chooses a secret random number r (obtained From random number generator) unique for each beacon it broadcasts.
2. Compute:

$$SIG_1 = g_1^r \bmod p$$

$$SIG_2 = (ID_{ai} - d \times SIG_1) * r^{-1} \bmod (p-1)$$

3. A_i encrypts the Signature pair $E_k(SIG_1, SIG_2)$ with 16 bit key.
4. Exit Subroutine

Ai sends (IDai,K, Ek(SIG1, SIG2)) to each Uj in its radio range.

Later on in step 4 verification is done for the signature by the nodes as mentioned in the step 4 below.

STEP 4)

Verification Subroutine:

1. U_i decrypts the signature pair D_k (SIG_1, SIG_2)
2. U_j determines if $0 < SIG_1 < p$
3. U_j determines if $0 < SIG_2 < (p-1)$

If ($SIG_2 < (p-1)$)

Proceed to 4.

Else

Malicious anchor. Discard beacon.

Exit.

4. Uj computes

$$\gamma_1 = g_1^{IDai} \bmod p$$

$$\gamma_2 = g_2^{SIG_1} * SIG_1^{SIG_2} \bmod p$$

5. $If\ (\gamma 1 == \gamma 2)$

Genuine anchor.

Else

Malicious anchor.

Exit.

6. Exit Subroutine

After the signature verification is complete, unknown sensor node is assured that the beacon it received was from a genuine anchor in the deployment area. It can then proceed with the localization process by employing the improved DV Hop localization with Least squares estimation.

IV. RESULTS AND DISCUSSION

The proposed secured localization scheme is simulated in MATLAB 2015a with parameters like 100×100 m deployed area with a radio range value 30 m and nodes are randomly deployed and some of the anchors are malicious in nature. With the help of digital signature scheme the unknown sensor nodes were able to authenticate the true or genuine anchors/landmarks. In case of malicious anchors (denoted by a red dot in simulation diagram), the unknown sensor nodes in its radio range discarded the beacons received from that malicious landmark. But they too can localize by another true anchor by deploying the cooperative localization scheme. Figure 1 below represents the scenario with true anchors, malicious anchors and unknown sensor nodes along with a radio communication range of each node as mentioned below to test the proposed algorithm in real time scenario. Once this scheme is deployed before the localization process by any algorithm, it will have the protection against the various attacks that are mentioned below along with the description of the attack working nature.

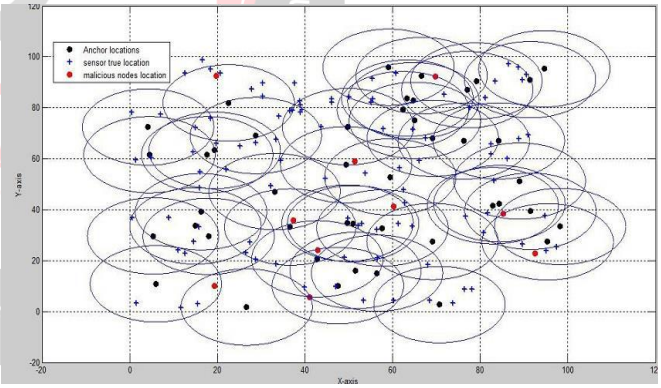

Fig 1: Resultant Graph of the Proposed System

It proves that the proposed algorithm has the capability to protect it against the various attacks that are not taken care by the various approaches developed earlier in the field of secure localization. So the various attacks that are not able to affect the localization process are mentioned below in table 1.

Type of Attack	Brief Description	Protection by Proposed Scheme
Sybil Attack	A node broadcasts with multiple	Not possible as IDs are predetermined by SN and

 DOI : 10.18231/2454-9150.2018.0110

	identities	authentication is also used.
Flooding Attack	An anchor opens too many half connections by sending repetitive SYN	Limited probability as radio range is very small and once anchor sends SYN its ID_{ai} is identified
Key Related Attacks	Using brute force or factoring techniques to find Public and Private keys	Keys are with SN and computation done in the Zp finite field which is hard to factor
Exhaustion	Transmitting on necessary beacons to consume receiver's resources	Limited radio range ensures no scope for such attack
Tampering	Broadcasting false beacons	Authentication via digital signature is used

Table1: Attacks and their Prevention by Proposed Scheme

It is inferred that the various attacks like the Sybil, flooding, tempering and brute force are not able to show their impact on the proposed approach for the node authentication as most of the attacks try to use the identity of the node and create duplicate copies of the true node and then compromise the system. Cryptanalysis is not possible in linear time for this approach as it is difficult to compute the discrete logarithms used by the digital signature approach.

V. CONCLUSION

The success of any localization approach is based on the position determination by the nodes. If the nodes are compromised, then they will affect the whole process of the localization. Identification of nodes into two categories, whether true or malicious is very important as they are involved in the position determination. Security of the information in the form of beacon signals is very important aspect in the localization process. Node authentication based on the digital signature approach mentioned in the paper can prove to be a better solution for the secure localization and also has the capability to protect the network against the various attacks like the Sybil, flooding etc. because of the algorithmic features of the digital signature. Future research work will be the integration of the proposed scheme in the calculation of unknown node position through the modified DV Hop algorithm and then the analysis of the scheme in the presence of malicious nodes.

ACKNOWLEDGEMENT

Authors are highly thankful to the department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, vol. 38, pp. 393–422, 2002.

[2] R. Stoleru, T. He, and J. A. Stankovic, "Range-Free Localization," pp. 1–31.

[3] "Applications of Sensor Networks," 2017.

[4] I. Paper Jinfang Jiang, Guangjie Han, "Secure Localization in Wireless Sensor Networks: A Survey," vol. 6, no. 6, pp. 460–470, 2011.

[5] H. Chawla, "Some issues and challenges of Wireless Sensor Networks," vol. 4, no. 7, pp. 236–239, 2014.

[6] A. Srinivasan and J. Wu, "A Survey on Secure Localization in Wireless Sensor Networks," pp. 1–26.

[7] L. Lazos and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," pp. 21–30, 2004.

[8] L. Lazos and R. Poovendran, "HiRLoc: High-resolution Robust Localization for Wireless Sensor Networks."

[9] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation-based Beacon Trust System," pp. 0–6, 2006.

[10] Y. Zeng, S. Zhang, S. Guo, and L. Xie, "Secure Hop-Count Based Localization in Wireless Sensor Networks," pp. 907–911, 2007.

[11] V. Vijayalakshmi and T. G. Palanivelu, "Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks," vol. 8, no. 6, pp. 255–261, 2008.

[12] T. Zhang, J. He, X. Li, and Q. Wei, " Signcryption-based Secure Localization Scheme in Wireless Sensor Networks," International Conference on Medical Physics and Biomedical Engineering , vol. 33, pp. 258–264, 2012.

[13] J. He, J. Xu, X. Zhu, Y. Zhang, T. Zhang, and W. Fu, "Reputation-Based Secure Sensor Localization in Wireless Sensor Networks," vol. 2014, 2014.

[14] H. Chen, W. Lou, Z. Wang, J. Wu, and Z. Wang, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," Pervasive Mob. Comput., pp. 1–14, 2014.

[15] Hongbin Wang, Liping Feng,C. Science and X. City, "The Secure Localization Algorithm of SDV-HOP in Wireless Sensor Networks," vol. 14, no. 3, pp. 65–74, 2016.

[16] W. Shi, "Secure Localization in the Presence of Colluders in WSNs," pp. 1–15, 2017.

 DOI : 10.18231/2454-9150.2018.0110