J. Sustain. Wireless Syst., vol. 03, no. 2, pp. 87-96
https://doi.org/10.36548/jsws.2021.2.003

Detection of Localization Error in a WSN under Sybil Attack using Advanced DV-Hop Methodology

Dr. V. Suma
Professor,
Department of Information Science & Engineering,
Dayananda Sagar College of Engineering,
Bangalore, India.

Abstract: Localization is one of the most important aspects of Wireless Sensor Networks that make it applicable in a number of fields and areas. WSN advances in the technological aspects the number of attacks on the nodes of the WSN have also increased proficiently resulting in a number of security issues. One such attack is the Sybil attack which uses multiple pseudonymous identities to disrupt the reputation of the system. This paper is used to analyse the Sybil attacks using a detection and defence algorithm based on distance vector hop. Simulation of the results using the algorithm will be useful in effectively enhancing security of WSN nodes. In this proposed work based on the experimental analysis we have found out that with 50 beacon nodes, we have been able to decrease the average localisation error buy a solid 4% when compared with previous methodologies.

Keywords: WSN; Sybil Attack; Security localization; Location node; Location error; DV-HOP

1. Introduction

The Wireless sensor networks (WSN) carry out multiple tasks like tracking, objective positioning, data transmission and network state. However, the security of a WSN needs to be considered seriously and any discrepancies in this aspect should not be ignored. One of the most common attacks faced by a WSN is the Sybil attack. During this attack, pseudonymous identities are introduced to disrupt the credibility of the system, hindering with the services provided by the network. Recently a number of research works has been carried out on WSN security localisation technology. Some of the typical WSN attacks include denial of service

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021

Sybil attack wormhole attack [1], spoofing [2] etc. To find these attacks focus is on security enhancement strategies to strengthen localisation of wsn. In this proposed work we have categorised localisation algorithm into two types namely tolerated attack algorithm and safety class algorithm [3]. The distance vector algorithm is a classic free-ranging wsn localisation algorithm is analysed in this work. To further enhance system and protect it against sybil attacks on localisation problem, a new DV hop based algorithm [4] is developed. In this paper we have considered static WSN with localisation issues.

The major contributions of this work can be summarized as below:

- In this paper, we have introduced the concept of neighbour list and hop difference as a part of the security measures against Sybil attack.
- The major difference between our proposed work and the traditional methodology is that we have incorporated the same fake node with same neighbour list.
- The rest of the paper is arranged such that section 2 gives a brief overview of the various security localization algorithms that exist.
- Section 3 outlines the proposed methodology and section 4 shows the experimental results observed and analyzed.
- Section 5 concludes the work and compares the proposed work with other methodologies to determine the efficiency of the proposed scheme.

2. Related Works

As the demand for security in localization of WSN [5] has gained importance in recent years, many research works has been carried out in this aspect [6]. To enhance security, many approaches have been proposed and carried out. In [7] the authors have introduced a mechanism using distance verified approach that is VM based to stop attacks by means of interaction between the beacon nodes. Authors in [8] have used a more advanced approach SLS program that is an improvement over the VM approach in terms of robustness and flexibility. The drawback with this approach is that it has a very complex program structure that requires larger overhead. Similarly, a Covet Base Station hidden approach is proposed in [9] as a solution to attacks on localizations in WSN. In this methodology, the

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021

signals are positioned in a more secure manner depending on the strength of the signal. It also takes into assumption that CBS location privacy is used during execution of the program[10]. However, this approach cannot be implemented in real time. Hence, an SLA security localization methodology is incorporated in [11] such that it is possible to determine the variation in transmission range. But, this methodology faced the issue of scalability since the location of the nodes is calculated by the sink nodes.

In [12], HiRLoc protocol, ROPE protocol and SeR-Loc protocol are proposed. HiRLoc protocol faces the issue of computing complexity and high communication overhead. On the other hand, ROPE protocol [13] will be able to improve the drawbacks realised in SeR-Loc protocol though it increases the cost of the system with increase in hardware requirement. Similarly, SeR-Loc protocol demonstrates requirements like identification of the deployment density of the nodes which are not apt for securing the system against attacks [14]. A PLC algorithm is proposed in [15] that need periodic calculation of the node positioning along with the overloads. A conflicting set mechanism is used in the positioning methodology to prevent wormhole attacks [16]. The apt output is possible only if there is no package loss during transmission of information. This will be prominent when an attacker who attacks the system discards an information packet on purpose. To overcome these drawbacks, a sign cryption-based secure localization scheme [17] is enforced ensuring integrity and confidentiality in holding the location data. But, if a malicious node captures [18] the normal node, this technique will fail. To overcome these discrepancies, a novel scheme using distance vector hop is introduced to improve the security of the WSNs, protecting them from Sybil attacks.

3. Proposed Work

3.1 DV-HOP Algorithm

The minimum hop distance between the beacon nodes is calculated using the DV-Hop algorithm [19], in a WSN. It was Niculescu et al. who proposed this algorithm initially. This methodology is determined using a range-free strategy. The first step in this process involves broadcasting of a message that consists of three components: HopSize_a initialised to ‘0’,

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021

Coordinates and the ID. The minimum wireless hops that take place between the beacon node ‘a’ and the sensor node ‘b’ is used as the value of HopSize$_a$. In case the packet that is received holds a smaller value with respect to a beacon node, this value is updated in the table. Moreover the packet is also sent with an increment count to the network. However if the hop count value is higher the packet is not taken into consideration [20]. Using this methodology every note the network will hold the minimum hop count value. The next step involves calculation of the average of distance as shown in the expression given below:

$$HopSize_a = \frac{\sum_{a\neq b}\sqrt{(x_a-x_b)^2+(y_a-y_b)^2}}{\sum_{a\neq b} h_{ab}} \tag{1}$$

The true beacon node coordinates, h_{ab} and the coordinates of the beacon nodes a and b is represented by (x_a,y_a) and (x_b,y_b). On calculating, every beacon node broadcasts the value using controlled flooding. When this hop size is received by an unknown node, the first message is only saved and further sent to the other nodes. On receiving the hop-size, the node will compute the distance between the beacon node and itself using the formula:

$$d_{pk} = HopSize_a \times hop_{pk} \tag{2}$$

Finally, a polygon method is used to identify the position of the unknown node. If there are a total of ‘n’ beacon node used and the unknown node is assigned ‘m’, then it is possible to determine the location using the following equation:

$$\begin{gathered}(x-x_1)^2+(y-y_1)^2 = d_1^2\\(x-x_2)^2+(y-y_2)^2 = d_2^2\\(x-x_n)^2+(y-y_n)^2 = d_1^2\end{gathered} \tag{3}$$

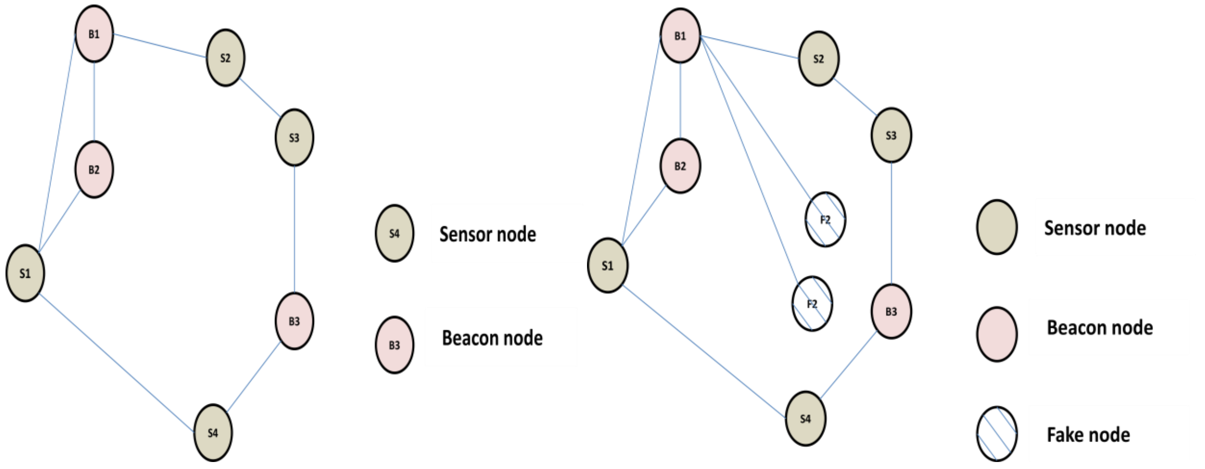
Using least squares, we can reduce the equation taking the form AX=B such that $X = (A'A)^{-1}A'B$.

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021

3.2 Sybil Attack and Defence

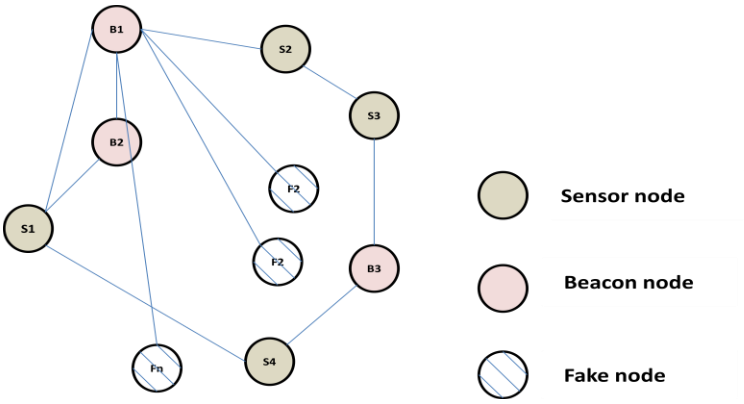
The primary goal of this paper is to decrease the effect of Sybil attack that occurs on localized nodes. Hence sensor nodes S1, S2, S3 and S4 while beacon nodes are taken as B1, B2 and B3. Similarly the malicious nodes that are initiate the attack are represented as F1, F2, F3, F4,... Fn. A secure network is represented in the Fig.1.a.The simultaneous attack is a type of Sybil attack that occurs when the attack is launched by all the fake nodes at the same time such that the hop difference is the same for the malicious node as well as the fake nodes. In Fig.1.b, since B1 node is in a communication range with S2 and S, the hop distance is HopD (F1,S1)= HopD(F2,S2). Here, F1 and F2 have the same location as that of B1 and so the nodes F1 and F2 are said to be at equivalent distance [21] from S1 and S2. However, if the attack timings vary and these two distances are found to be the same, then some of the fake nodes will be missed and this proposed methodology will not pass. Hence to overcome this drawback, the neighbour list is introduced into this algorithm such that one node get different neighbour list. Based on this analysis, the following steps are involved in the proposed algorithm:

- **Step 1:** Test information is broadcasted by the beacon node such that a neighbour list is established with the neighbouring nodes. For every node a, if the neighbour list is different, it indicates that the node is under Sybil attack.
- **Step 2:** The malicious nodes are saved in a blacklist represented as BL.
- **Step 3:** DV hop localisation is carried out by all the nodes that are normal.



(a) No Sybil Attack **(b) (Sybil Attack 2 Malicious Nodes)**

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021



(c) S8ybil Attack (n malicious nodes)

Fig.1. Different Stages of the Sybil Attack

Using these steps, the proposed algorithm using DV-Hop localization proves to identify the Sybil attack in a more efficient manner. When there is 'n' number of malicious nodes, the system can be represented as shown in Fig.1.c.

4. Results and Discussion

The evaluation metrics, simulation settings and impact of malicious nodes are analysed in this section. The following observations have been carried out using the network simulator NS-2 to determine the efficiency of the proposed work.

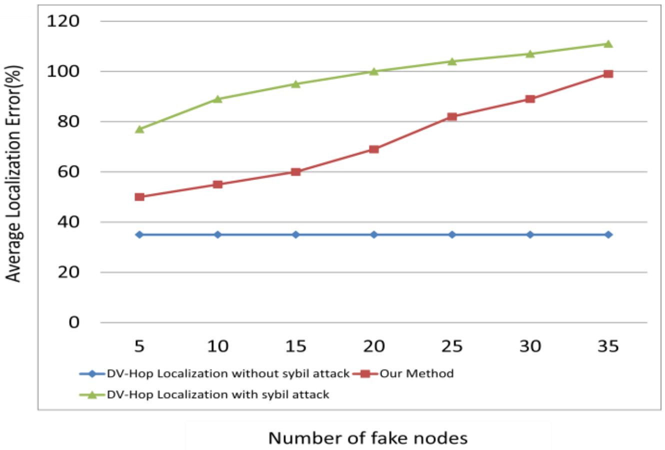


Fig.2. Location Error Identified against the Malicious Attacks

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021

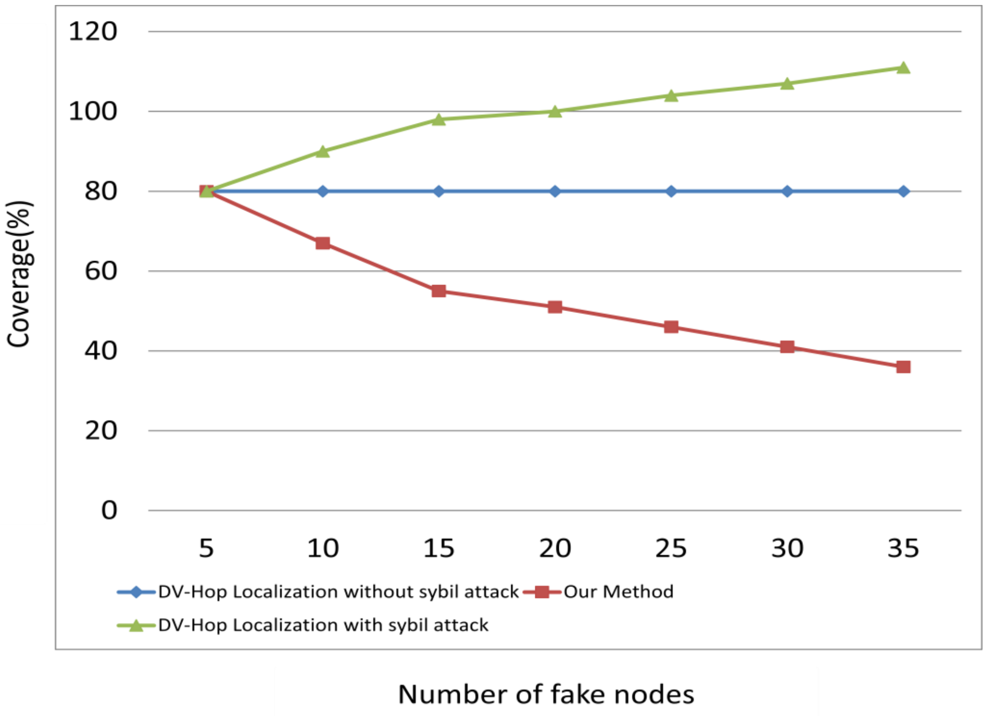


Fig.3. Coverage Percentage

Fig.2. shows the error identification in case of malicious attacks. It shows that there is an increase in localization error during Sybil attack for the proposed methodology while in the absence of the attack, it remains a constant. Similarly, Fig.3 shows the coverage percentage against the malicious nodes where our proposed methodology works towards improving the accuracy of the attack and decreasing the malicious nodes. Fig.4 shows the average localization error that varies based on the number of beacon nodes. It is observed that the number of beacon nodes vary indirectly with that of the average localization error. From the figure it can be identified that about 72% average localization error occurs when there are 35 beacon nodes. On the other hand, the traditional DV-Hop methodology observes an error of 80% while under no Sybil attack, the average localization error is very small at 30%, indicating the effectiveness of the proposed work.

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021

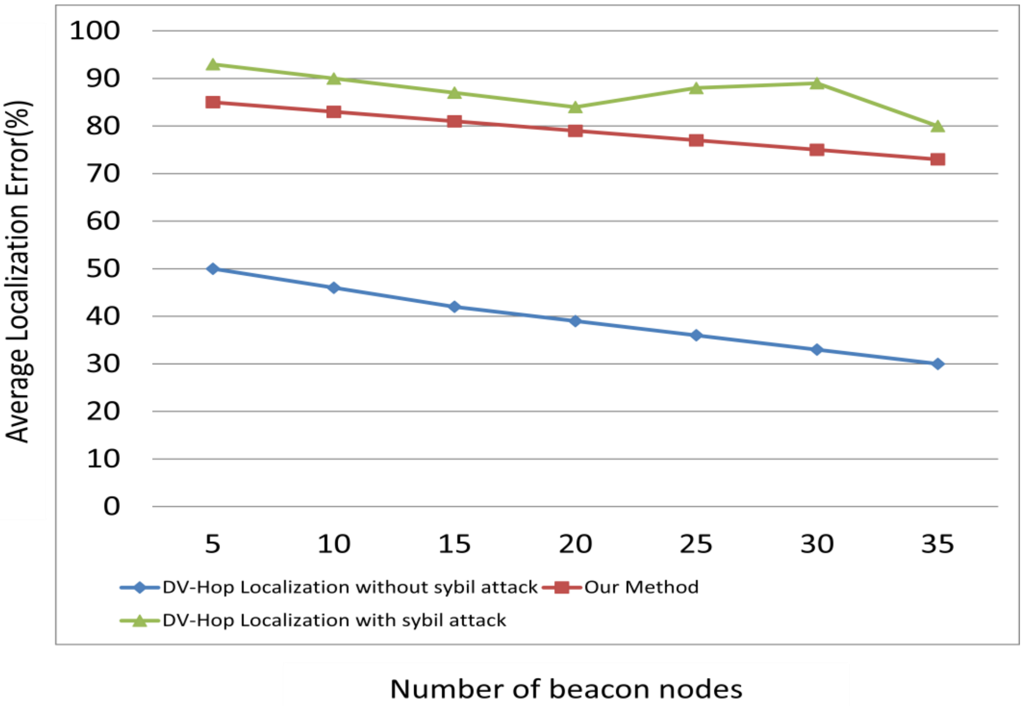


Fig.4 Beacon Attack Coverage

5. Conclusion

In this work, we have incorporated a security localization algorithm that is capable of decreasing the localization error. The positive aspect of this paper is mainly the lack of need for extra hardware. It is seen that the proposed work shows a significant improvement over the previously existing DV-Hop localization methodology and uses novel concepts of neighbour list, hop difference and black list in order to accurately identify the location of the malicious node. Here, we have used 50 beacon nodes and it is seen that the localization error has been decreased by 5% in comparison to the traditional methodologies of DV-Hop. As part of future work, it is possible to further improve the accuracy of identifying the malicious nodes.

References

[1] Dinger, J., & Hartenstein, H. (2006, April). Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration. In *First*

International Conference on Availability, Reliability and Security (ARES'06) (pp. 8-pp). IEEE.

[2] Chen, C., Wang, X., Han, W., & Zang, B. (2009, June). A robust detection of the sybil attack in urban vanets. In *2009 29th IEEE International Conference on Distributed Computing Systems Workshops* (pp. 270-276). IEEE.

[3] Suma, V., & Haoxiang, W. (2020). Optimal Key Handover Management for Enhancing Security in Mobile Network. Journal of trends in Computer Science and Smart technology (TCSST), 2(04), 181-187.

[4] Patel, S. T., & Mistry, N. H. (2017, February). A review: sybil attack detection techniques in wsn. In *2017 4th International Conference on Electronics and Communication Systems (ICECS)* (pp. 184-188). IEEE.

[5] Bhalaji, N. (2020). Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks. Journal of ISMAC, 2(02), 106-117.

[6] Baraneetharan, E. (2020). Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey. *Journal of Information Technology*, *2*(03), 161-173.

[7] Ruth Anita Shirley, D., Sasi Priya, S. (2018, August), Electromagnetic interference and its effect on the printed circuit board. Journal of Advanced Research in Dynamical and Control Systems, 2018, 10(12), pp. 684–688.

[8] Ashwini, G.V., Pandian, S.C., Shirley, D.R.A. (2019, November). Mitigating the effects of ESD using ESD capacitor and TVS diode. In International Journal of Innovative Technology and Exploring Engineering, 2019, 9(1), pp. 942–946.

[9] Piro, C., Shields, C., & Levine, B. N. (2006, August). Detecting the sybil attack in mobile ad hoc networks. In *2006 Securecomm and Workshops* (pp. 1-11). IEEE.

[10] Shakya, S., & Pulchowk, L. N. (2020). The Robust Routing Protocol with Authentication for Wireless Adhoc Networks. Journal of ISMAC, 2(02), 83-95.

[11] Guette, G., & Ducourthial, B. (2007, October). On the Sybil attack detection in VANET. In *2007 IEEE international conference on Mobile Adhoc and sensor systems* (pp. 1-6). IEEE.

[12] Kamani, J., & Parikh, D. (2015). A review on sybil attack detection techniques. *J Res*, *1*(01).

[13] Gu, P., Khatoun, R., Begriche, Y., & Serhrouchni, A. (2017, March). Support vector machine (svm) based sybil attack detection in vehicular networks. In *2017*

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021

IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[14] Pal, S., Mukhopadhyay, A. K., & Bhattacharya, P. P. (2008). Defending mechanisms against sybil attack in next generation mobile ad hoc networks. *IETE Technical Review*, *25*(4), 209-215.

[15] Al-Qurishi, M., Alrubaian, M., Rahman, S. M. M., Alamri, A., & Hassan, M. M. (2018). A prediction system of Sybil attack in social network using deep-regression model. *Future Generation Computer Systems*, *87*, 743-753.

[16] Adithya, M., Scholar, P. G., & Shanthini, B. (2020). Security Analysis and Preserving Block-Level Data DE-duplication in Cloud Storage Services. Journal of trends in Computer Science and Smart technology (TCSST), 2(02), 120-126.

[17] Smys, S., Basar, A., & Wang, H. (2020). Hybrid Intrusion Detection System for Internet of Things (IoT). *Journal of ISMAC*, *2*(04), 190-199.

[18] Chen, D. J. I. Z., & Lai, K. L. (2020). Internet of Things (IoT) Authentication and Access Control by Hybrid Deep Learning Method-A Study. *Journal of Soft Computing Paradigm (JSCP)*, *2*(04), 236-245.

[19] Smys, S. (2019). Energy-aware security routing protocol for WSN in big-data applications. *Journal of ISMAC*, *1*(01), 38-55.

[20] Raj, J. S. (2020). Machine Learning Based Resourceful Clustering With Load Optimization for Wireless Sensor Networks. *Journal of Ubiquitous Computing and Communication Technologies (UCCT)*, *2*(01), 29-38.

[21] Mugunthan, S. R. (2020). Novel Cluster Rotating and Routing Strategy for software defined Wireless Sensor Networks. *Journal of ISMAC*, *2*(02), 140-146.

ISSN: 2582-3167
Submitted: 24.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 5.06.2021