electronics

MDPI

Article

SDSWSN—A Secure Approach for a Hop-Based Localization Algorithm Using a Digital Signature in the Wireless Sensor Network

Deepak Prashar [1], Mamoon Rashid [2,*], Shams Tabrez Siddiqui [3], Dilip Kumar [4], Amandeep Nagpal [1], Ahmed Saeed AlGhamdi [5] and Sultan S. Alshamrani [6]

1 School of Computer Science and Engineering, Lovely Professional University, Jalandhar 144001, India; deepak.prashar@lpu.co.in (D.P.); amandeep.nagpal@lpu.co.in (A.N.)
2 Department of Computer Engineering, Faculty of Science and Technology, Vishwakarma University, Pune 411048, India
3 Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan 45142, Saudi Arabia; stabrezsiddiqui@gmail.com
4 Department of Electronics and Communication, SLIET, Sangrur 148106, India; dilip.k78@gmail.com
5 Department of Computer Engineering, College of Computer and Information Technology, Taif University, Taif 21994, Saudi Arabia; asjannah@tu.edu.sa
6 Department of Information Technology, College of Computer and Information Technology, Taif University, Taif 21944, Saudi Arabia; susamash@tu.edu.sa
* Correspondence: mamoon.rashid@vupune.ac.in; Tel.: +91-7814346505

Citation: Prashar, D.; Rashid, M.; Siddiqui, S.T.; Kumar, D.; Nagpal, A.; AlGhamdi, A.S.; Alshamrani, S.S. SDSWSN—A Secure Approach for a Hop-Based Localization Algorithm Using a Digital Signature in the Wireless Sensor Network. *Electronics* **2021**, *10*, 3074. https://doi.org/10.3390/electronics10243074

Academic Editors: Mohit Mittal, Rocío Pérez de Prado and Valentina E. Balas

Received: 13 October 2021
Accepted: 6 December 2021
Published: 9 December 2021

Abstract: Localization and security are among the most dominant tasks of wireless sensor networks (WSN). For applications containing sensitive information on the location parameters of the event, secure localization is mandatory and must not be compromised at any cost. The main task, as if any node is malicious, is to authenticate nodes that are involved in the localization process. In this paper, we propose a secure hop-based algorithm that provides a better localization accuracy. In addition, to maintain the security of the localization process, the digital signature approach is used. Moreover, the impact of malicious nodes on the proposed scheme has also been observed. The proposed approach is also contrasted with the basic DV-Hop and improved DV-Hop based on error correction. From the simulation outcomes, we infer that this secure digital-signature-based localization strategy is quite robust against any node compromise attacks, thereby boosting its precision. Comparisons between the proposed algorithm and the state of the art were made on the grounds of different parameters such as the node quantity, ratio of anchor nodes, and range value towards the localization error.

Keywords: DV-Hop; digital signature; localization; wormhole; wireless

1. Introduction

A WSN is a network where assorted nodes work together and feel the phenomena around them to achieve a common objective [1,2]. After the phenomenon has been detected, all sensors forward this information to the base station (BS), where the BS investigates all the occurrences in the environment and takes appropriate action [3]. A WSN has several characteristics—such as being self-organized, fault-tolerant, and scalable—but the most challenging part is the BS' awareness of the location of the event. That is, if a BS has the details that a particular operation is taking place, and a sensor transfers these attributes to the BS and the location of the BS is not known, then the BS cannot take the best possible action depending on the event [2]. To gather the location of sensor nodes, localization comes into the picture, through which the coordinates of the sensor node are determined. Security is another key issue that needs to be addressed—as without security, the true location of the nodes cannot be known or estimated. When the gathered information is sent by the sensors to the BS, there is a chance of an unauthorized entity reading and altering

the data to hamper its integrity [4–6]. WSNs also allow for a variety of attacks, such as wormhole attacks, black-hole attacks, flooding attacks, and many others. Whenever the receiver receives the information, it should be compulsory to authenticate the source, and information should be encrypted to decrease the impact of any malicious activity on it.

A WSN is fabricated from a vast number of sensing nodes and is positioned within a particular target area or nearby target area [1]. Sensor nodes are a very censorious part of a WSN. Localization identifies the position of a particular event where it is occurring. In WSN, there are two types of sensor nodes: one is an anchored node and the other one is an unknown node [7]. Localization algorithms are classified into different dimensions, such as range-based (RB) or range-free (RF), and further categorized into centralized or distributed algorithms [8–10]. Various range-free algorithms have been developed, including the centroid, approximate point in triangulation (APIT), distance vector (DV-Hop), and convex position estimation (CPE) algorithms [9,11,12]. As the range-free methods are not based on the global positioning system's (GPS) requirements, as the range-based methods are, that reduces the overall cost of their deployment. The traditional localization algorithm used in a WSN is the DV-Hop [12]. The DV-Hop has abundant enhancements that yield the most precise results, but security is still a major concern with these localization algorithms [13–19]. Regarding the security in the localization process, this is the security of data that is shared among the sensor nodes for the position estimation using any type of algorithm. Also, the authentication of the nodes engaged in the localization process is the primary task, as if any one of the nodes is malicious, the whole system can be compromised easily.

1.1. Contributions of Paper

This paper proposes a secure hop-based localization algorithm that provides a better accuracy in terms of the localization error. Further, the digital signature approach is utilized to maintain the security of the localization process. The significant insights and contributions of this paper can be listed as follows:

- An enhanced, secure approach based on node authentication using the concept of a digital signature is proposed, and this provides a defense against most of the possible attacks based on the node identity.
- An improved DV-Hop approach based on an error correction metric, along with a hyperbolic and mid-perpendicular technique, which provides better accuracy than basic and other improved variety of DV-Hop algorithms.
- The effect of malicious nodes on the improved DV-Hop and the proposed secure approach is analyzed.
- A comparative performance evaluation of the proposed algorithm on the parameters of node quantity, anchor node ratio, and range value towards the localization error is carried out with state-of-art literature.

1.2. Organization of Paper

The rest of the paper is categorized into various sections as defined. Section 2 addresses the work that has already been done in the field of secure localization. Section 3 covers the model for numerous possible attacks on the localization system. Section 4 covers the proposed secure approach based on a digital signature along with the improved DV-Hop algorithm, on which the proposed secure approach is applied. The simulation and implementation are covered in Section 5 and a security analysis is discussed in Section 6. Results are discussed in Section 7, and the conclusion of this paper is finally expressed in Section 8.

2. Related Work

The existing work carried out in the area of secure localization is described in this section, along with the major outcomes. Security in localization involves different approaches

that are created to enhance its security and decrease the impact of various attacks on the process of localization.

Loukas Lazos et al. [20] have proposed SeRLoc (secure range-independent localization) in a WSN, which is a range-free approach and uses antennas. Four steps are there to determine unknown node coordinates. This approach provides security by encrypting the messages during transmission with symmetric pairwise keys and using a hash function for authentication and to prevent various attacks. This approach yields the best accuracy, but because of the cost of using antennas, the network is more expensive. By contrast, in our proposed approach we have used digital signatures instead of hash functions to authenticate the anchor nodes, and antennas are not required for the position computation, which reduces the cost of the network and yields the best results. Our proposed approach never allows any unauthenticated anchor to enter the localization process, and it also does not allow dangerous attacks such as wormholes, black holes, replay attacks, etc. To address the security issue in the localization process, the authors added another approach called robust position estimation (ROPE) [21]. This method determines the location without any centralized computation. It is based on location verification for checking the claims made by the sensor nodes before taking data from them. Our proposed approach mitigates almost all possible attacks that are not taken care of by the ROPE, and hence it is more scalable.

Loukas Lazos et al. also proposed HiRLoc (high-resolution range-independent localization), a new approach for secure localization in WSN [22]. As in SeRLoc, an unknown node finds out its position in the region of intersection (ROI) from every sector. HiRLoc reduces the ROI by changing the orientation of the antenna and changing the transmission range of the power control. This approach uses encryption during the transmission of the detail by anchor nodes and yields the best accuracy. As this approach uses antennas, the cost of the network is high. Our proposed approach is superior, because it does not demand antennas, which means the cost is lower compared to existing approaches, and the use of keys with digital signatures provides stronger security compared to HiRLoc. This is because malicious anchor nodes are detected in the initial step of the localization process and do not impact the localization process further.

Avinash Srinivasan et al. [23] suggested a distributed-reputation-based beacon trust system (DRBTS) for localization in a WSN. This approach uses a reputation for prohibiting the anchor node. Here, each anchor maintains the neighbor routing table (NRT). Each anchor checks the first-hop neighbor for any kind of misbehavior by an anchor and then updates the same on the NRT. Each anchor directs the neighboring nodes to update their NRT and enables the anchor nodes to know whether to use the details of the anchor or not. The disadvantage of this type of localization is that, initially, no one trusts each other. In this way, the sensor uses the details of the malicious anchor for localization and this scheme adds a lower overhead. In our proposed approach, there is no concept of trust and the sensor nodes do not demand any details about malicious anchors. Here in our proposed approach, the use of digital signatures in an initial step does not permit any malicious node to be part of the localization process. Honglong Chen et al. [24] proposed a secure localization approach that is known as temporal-spatial-consistent-based detection (TSCD). In this approach, a WSN becomes secure with secure features. TSCD works by using these four properties to determine malicious anchor nodes. During the localization process of TSCD, these strategies need to be used on the basis of the number of attacked anchor nodes that have been identified by this scheme. After removing the attacked locators, this approach uses the maximum likelihood estimation (MLE) method for the localization of sensors. As our proposed approach does not demand any security properties initially, it is a better solution than the TSCD approach. Furthermore, checking the number of malicious nodes is not required in our approach, which results in a reduction of the overall overhead and an increased efficiency.

The latest research that has been done in this regard is also described here. To check the integrity and confidentiality of the nodes, a cryptographic approach was defined [25]. In this approach, the authors used the hash-based message authentication code (HMAC)

along with an elliptic curve; the position computation is then done using trilateration. This approach does not address the impact of malicious nodes in the localization process. But our proposed solution looks after that issue as well and uses a hyperbolic function instead of trilateration while providing more precise results; hence, it is more effective.

X. W. Wang et al. [26] proposed an approach to security from wormhole attacks in a WSN. It consists of three steps: anchor node labelling, sensor node labelling, and secure localization using DV-Hop. They used some properties for labelling the anchor node. This approach works perfectly when the range of the nodes is equal and there is no packet loss. Unlike to this research, our proposed approach not only prevents attacks but also contributes to the encryption that secures data from scanning or modification by any unauthenticated person. With the prevention of this attack, our proposed approach also works on the correction of distance, which makes the algorithm more resilient. Another strategy based on securing the DV-Hop is provided by H. Wang et al., which analyses the weight factor of the beacon nodes and the effect of the nodes capture attack [27]. But in our proposed approach, the effect of various attacks is addressed and their countermeasures are also taken care of. The impact of the radio model and the faulty nodes is done by the author on the basic DV-Hop, correction-based DV-Hop (CDV-Hop), and improved DV-Hop (IDV-Hop) [28]. It addresses the issue that results and must be investigated in realistic scenarios. But it does not provide an alternative to mitigate the effect of faulty nodes. However, our proposed approach provides a node-authentication-based concept that can furthermore be implemented on any localization algorithm and thus reduces the impact of any types of attacks that can be executed on localization algorithms. The author also presents a mutual-authentication-based approach for security in localization that is also presented by the author, in which two major issues are addressed: the random deployment and mobility of nodes [29]. It uses certificate values that are provided by the BS to each one of the nodes involved in the localization process. Similarly, another approach based on vector refinement and outlier elimination is given by the author that improves the localization process further [30].

Xiaole Liu et al. [31] proposed a secure localization approach in a WSN based on the basic localization algorithm DV-Hop. In this scheme, there is an assumption that all the anchor nodes communicate to the BS in a confidential manner and with an authentication scheme based on intrusion detection and random keys. This approach works with DV-Hop and finds the location with the weighted least squares (WLS) method. This approach combats the attacks on DV-Hop schemes by reducing the effect of attacks on localization. During broadcasting, it contains a detailed demand, which is to be passed through the authentication process. By contrast, our proposed approach also works with the DV-Hop algorithm due to its simplicity. Our proposed approach secures the network initially, because the BS generates the keys and assigns the keys to the nodes during the deployment only. All the sensor nodes maintain the table for keys and are going to receive the message from only authenticated anchor nodes with the use of digital signatures. Our algorithm is better because there is no need for any intrusion detection schemes, but it still prevents the network from the attacks.

Trust-based localization was given by the author [32]. In this approach, they implemented the secure algorithm in an underwater WSN. It comprises five main steps: first of all, trust evaluations are done for anchor nodes. Afterwards, a trust calculation for the reference nodes is followed by their selection. In the end, secondary localization is executed for the unknown nodes. This work does not address the issue when multiple attacks are executed on the algorithm, and most of the position values are taken with the help of GPS for an underwater WSN. However, in our proposed algorithm there is no need for GPS for position estimation, and it tries to mitigate the effect of all possible kinds of attacks. This makes the algorithm more robust and less costly due to the absence of hardware constraints.

As in our proposed algorithm, the basic DV-Hop localization approach is modified by adding an error correction factor and then using the mid-perpendicular and hyperbolic

techniques. Thus, some research work oriented towards DV-Hop localization is also described below.

Zhang et al. [33] proposed a DV-Hop based on a weighted centroid approach. This approach improves the second step by using the average of the anchor's average-hop size of those that are selected in the initial step. This approach also uses the weight factor—whereas although our proposed approach also finds the average of all anchor nodes' average hop size, it furthermore considers the correction on the distance that further improves the accuracy of the location and does not demand a weight factor. With the use of a correction for the distance and average network hop distance, it yields the best results. The letter by C. Fu et al. [34] improved the conventional DV-Hop and proposed the Fu DV-Hop, which changes the second and third steps of the conventional DV-Hop. This approach improves the result by correcting the distance, finding the weight for anchor nodes, and, in the third step, validating the coordinates. By contrast, our proposed approach also uses the conventional DV-Hop and works by correcting the distance, because the error in the location occurs only due to the error in the distance. Our approach is better, as it does not demand the weight of every anchor node, thus having a lower overhead. Xiaoxu Ma et al. [35] proposed the approach that works with the secondary correction error and uses the orthogonal polynomial fitting algorithm. The approach corrects the distance error with a polynomial fitting algorithm and, in the last step of coordinate calculation, it uses the weight matrix. This approach yields the best result. However, our proposed approach does not demand any additional requirements or weight matrix; it uses the average network distance. Because of that, our approach corrects the distance error further and yields the best result as compared to the given approach.

In the same vein, the author of the current paper completed work in the form of a survey paper, in which he investigates the possibilities of distributed range-free localization algorithms as well as the proficiency of various secure localization methods that are already available [36]. One framework developed by the same author demonstrated the impact of attacks on the localization scheme and also implemented the optimization strategy for the precise result computation [37].

Some work in order to cater to the issues associated with localization in terms of unreliable measurements and intranode conflict has been addressed by the authors. In [38], the authors considered a device-less localization for monitoring multiple bodies in a region of interest. They utilized data pertaining to electromagnetic radiation and some inference techniques. They pointed out that some disturbances in measurements are observed on account of the RSS deviation due to the signal usage. Similarly, some recent work to take care of the issues pertaining to the node count and hop count has been addressed by the authors [39], where they provided an approach based on a virtual partitioning, along with its integration with the distance error concept to reduce the overall error. This scheme also proved beneficial apart from the other similar approaches.

Localization approaches also need to consider other major aspects. First, they must consider the higher accuracy in the presence of adverse conditions (e.g., multipath propagation, presence of outliers, etc.). Second, there are important drawbacks that need to be taken into account when designing localization algorithms for WSNs. In this direction, some work has been done by the authors. In [40], the authors have worked on the issue of the maximum likelihood (ML) under the impact of multiple antennas in multipath propagation. They formulated a less complex approach to the analysis with the intent to increase the ML. One other work on detecting the abnormalities arising due to the outliers present in the network on account of RSS deviation has been executed [41]. That approach was able to reduce the error to some extent even in the presence of outliers. Chuku et al. [42] later on provided an approach for the outlier identification using density-based clustering. In [43], the authors provided an approach for reducing the error based on the RSS and TOA. They noticed that the ML was not able to provide the solution in the presence of obstacles, so they used two-step approaches based on a calibration computation followed

by an RSS/TOA estimation. This approach reduced the complexity and cost to a minimal level. The comparative analysis of the prominent literature is presented in Table 1.

Table 1. Comparative analysis of secure localization methods.

Work Reference	Type (RB/ RF)	Security Technique Used	Attacks Considered	Challenges
[20]	RF	Symmetric key and hash function	Wormhole, sybil, and compromised nodes	Antenna cost is high
[21]	RF	Cryptographic primitives & distance bounding	Wormhole, sybil, and selective Jamming	Antenna cost is high
[22]	RF	Cryptographic primitives	Wormhole, sybil, and compromised nodes	Antenna cost is high
[23]	RF	Reputation value of node based on quorum voting	Malicious beacon node behavior	Overhead of storing the nodes information in tables
[24]	RB	Maximum likelihood estimation and locators	Spoofing	Limited locators are used
[25]	RF	HMAC and elliptic curve	No attacks are considered	Attacker model is not defined
[26]	RF	Credibility of node	Wormhole	Mobility is not considered
[27]	RF	Password-based symmetric encryption	Node capture and masquerade	Mobility is not considered
[28]	RF	Irregular radio approach	Faulty nodes	Accuracy is not good
[29]	RF	Mutual authentication	All major TCP /IP layer based attacks	Base station is considered as the trusted one
[30]	RF	Outlier elimination	Malicious beacon node behavior	Complexity is high
[32]	RB	Trust calculation	All major TCP /IP layer based attacks	GPS requirement and limited malicious nodes are deployed

Judging from the above literature review, it is clear that there is a demand for new secure approaches that are better and more efficient than the present ones. They should have a lower overhead and greater resilience to attacks. Moreover, there is a need for amendments that are required by the basic DV-Hop localization approach for a greater accuracy.

3. Attack Model

We cannot underestimate the presence of attackers in the network, and thus there is a need to understand the functionality of various attacks on the system that can be possible in order to design secure methods to mitigate their effects on the localization process. Different types of attacks can be executed on any localization system, which is presented below along with their modes of operation. Some of the prominent attacks that are possible on the localization process are described here.

Wormhole attack: In a wormhole attack, the attacker sniffs the data packet from one location on the network and transfers it to another location where the attacker is present through a fake link [44]. Afterwards, it broadcasts the packets to the entire network. This process affects the localization and routing. Figure 1 demonstrates a wormhole attack instance. In the figure, one anchor node is placed in the network along with sensor nodes. Yet two attacker nodes are also there, thus creating the wormhole link between the two attacker nodes C1 and C2. In this network node, S1 and S7 are considering each other as neighboring nodes due to the wormhole attack. Furthermore, S6 is going to consider its hop count as three up to the B11 anchor node via S6 to S7, then S7 to S1 and S1 to B11. In this way, the attackers C1 and C2 are not visible. However, the correct hop count is five, as S6–S5–S4–S3–S2–B11 is the actual path. The DV-Hop algorithm considers the hop count value for the distance estimation, so if the hop count were not correct, then the overall localization process would not give the correct result in the presence of such an attack.

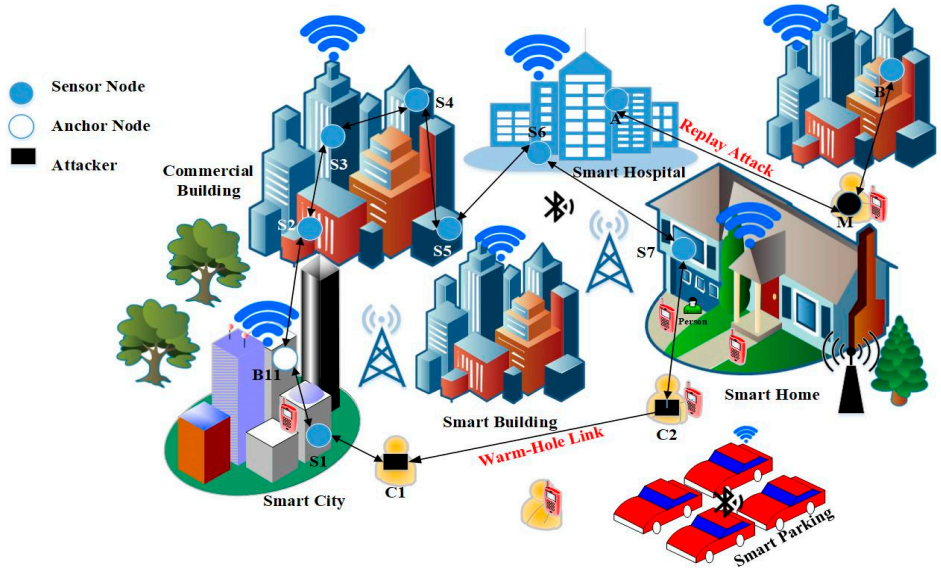

Figure 1. Representation of a wormhole attack and replay attack.

Blackhole attack: This is one of the WSN's simple routing attacks. In this attack, the malicious node set up by the attacker in the network receives all the messages and does not forward those messages in a network any further, exactly similar to a black hole [45]. As the malicious node refuses to forward the message in the network, it thus affects the overall traffic that is passing through it. The throughput of the nodes neighboring the malicious node is decreased. If the position of the attacker is very close to the BS, then all the traffic going to the BS needs to pass through the attacker. In this situation, the black hole attack breaks the overall communication of the WSN through the BS and stops the WSN from performing its specific work. On the other hand, if the attacker's position is on the edge of the WSN, then the loss is limited, as at the edge few sensors communicate with the other sensors.

Replay attack: The replay attack is easy to deploy, so most of the time this attack is performed by the attacker, particularly when the attacker does not have enough capability and the attacker cannot compromise more than one sensor node in a network [46]. The attacker jams the communication between A and B in the replay attack, as shown in Figure 2, and then sends the same message or replays the message to the receiver (B) while pretending to be the sender (A). The replay attack is shown in Figure 1, where A is the sender and B is the receiver and, in between A and B, there is an attacker represented by M.

Flooding attack: In this attack, the attacker continuously sends connection buildup requests to the particular target or victim node [46]. When the target node accepts the request, all the resources held by the target node are allocated to the attacker. The result of this attack is that the memory and energy resources of the target node become a deluge.

Sybil attack: In this attack, the compromised node holds more than one identity in the network [46]. In the localization, a localizing node gets more than one location reference from a specific node, which results in an incorrect location estimate. Hence, one malicious node is enough for this attack, and there is no need for nodes to collude. In this attack, a malicious node can send the message with different IDs and thus affect the whole localization process.

Selective forwarding: The compromised node functions as a black hole in this attack and either does not further send important messages or drops those messages [46]. It is not easy to detect, as the attacker drops only selected messages instead of every message. There can be some other reasons for packet dropping, such as unreliable wireless communication, or there can be the possibility of a sensor node being in sleep mode for reasons concerning energy efficiency.

Alteration attack: This attack is carried out on the data in the center of the unknown node and anchor node [46]. In the message, the attacker may alter the coordinates or hop count between the nodes, and may even alter the time. Due to this, the overall localization process is compromised.

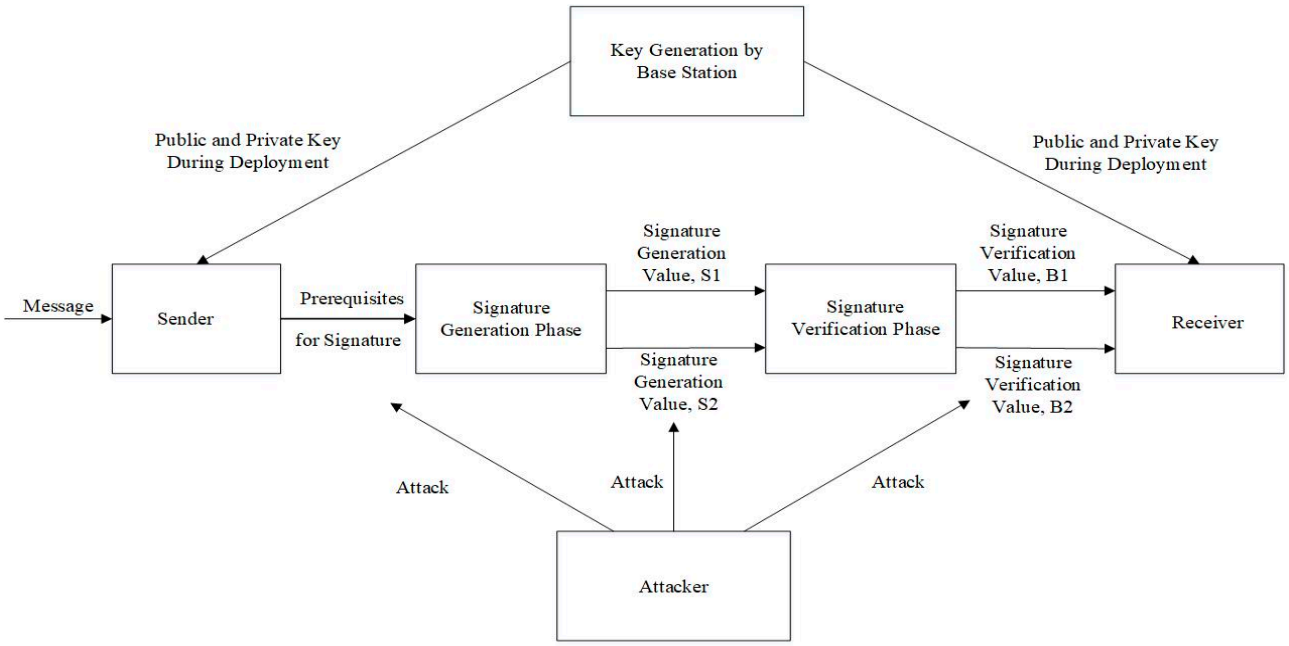

Figure 2. Signature generation and verification process.

4. Proposed Scheme

In this part of the paper, two schemes are defined: one is the proposed secure approach based on the authentication of nodes using digital signatures; the other is the improved DV-Hop approach based on a distance error correction factor using the hyperbolic function [47,48]. Most importantly, the localization involves two kinds of nodes. One is the anchor nodes that know their position and the other are unknowning nodes that can find their position with the help of anchor nodes. Malicious nodes are also there, which are unauthenticated anchor nodes. So, to find out the position of the unknown sensors, there is a need to transfer messages from anchor nodes to unknowing nodes, and these messages should have the authenticated source. The unknowing node should receive the data only from authentic anchor nodes rather than from malicious nodes. Therefore, to provide authenticity during the transfer of the messages, the BS and a digital signature are used. The whole process is divided into various phases: from key generation, key allocation, signature creation and verification, and then, at last, the position computation using the improved DV-Hop localization. The working of the signature generation and verification phase is represented in Figure 2 [49]. Here, the variables S1 and S2 are the signature generation values for the message sent by the sender while B1 and B2 are the verification values that match at the receiving end.

4.1. Network Model and Assumptions

We deploy the sensor node in the 2D area randomly in a particular area with the following Equation (1) [50].

$$ff\left(\frac{w}{\mu}, \sigma\right) = \frac{1}{\sqrt{2\mu}} e^{\frac{(w-\sigma)^2}{2\sigma^2}} \quad (1)$$

In the above Equation (1), w is the normal-distribution-based random variable, σ is the standard deviation, σ^2 is the variance, and μ μ is the mean.

$$|N| = |A| \cup |U| \quad (2)$$

In the Equation (2), we have a total of N nodes in the network, which are divided into two categories: A represents the size of the anchor nodes and U represents the size of the unknowing nodes. The issue here is to determine the U position through the A place in the network using some localization approach, and, moreover, there may be some malicious nodes be present in the same network that can impersonate U.

Assumptions

Anchor nodes are the nodes that knows their positions. Anchor nodes help the other unknowing nodes to determine their positions. Malicious nodes are also there, which are not authenticated. So, to find out the position of unknowing sensors there is a need to transfer the messages, and these messages should be authenticated. This means that the unknowing node will receive the data only from authentic anchor nodes rather than from malicious nodes. In this paper, the BS and a digital signature are used to provide authenticity during the transfer of messages. Some assumptions are taken into account in our proposed approach, as mentioned below:

(i) The base station generates a public and private key for all nodes, and it is assumed that it is a trusted entity in the network.
(ii) Initially, the BS will generate a public key (pu_{ni}) and private key (pr_{ni}) for each of the anchor and unknowing nodes in the network.
(iii) No external factors affect the process of localization.

The source of a malicious node can be an attack that is deployed on the localization process.

4.2. The Initialization Phase

Initially, the BS is generating a public key (pu_{ni}) and private key (pr_{ni}) for each of the nodes in this phase of the proposed scheme. Here, first of all, it generates a random integer with the pseudo-random function that acts as a private key for n_i, where n_i describes all of the nodes in the network. Equations (3) and (4) are used to represent the public and private key:

$$\text{Private Key} = pr_{ni} \quad (3)$$

This formula is used to calculate the public key:

$$\text{Public Key } (pu_{ni}) = \alpha^{pr_{ni}} \bmod q \quad (4)$$

where q is the prime number and α is q's primitive root.

Now, the private key for node n_i is pr_{ni} and the public key is [q, α, pu_{ni}].

In this way, the BS generates public and private keys for n_i and stores the keys in its database. The BS assigns the private keys to n_i at the deployment time. Now, whenever any node transfers information, the sending node generates the signature, as shown in Section 4.3, to provide the authenticity of data, and the receiving node ensures the authenticity by verifying the signature.

The sending node sends the message hash value (m) that contains data such as id, (X_a, Y_a), and h_cont; m is the integer in the range of $0 \leq m \leq q-1$, id is the unique identifier given to each node, (X_a, Y_a) is the anchor node's position coordinate, and h_cont is the hop between the anchor node and other network nodes.

4.3. Generate Signatures (S_1,S_2) Phase

Here, in this phase a random integer h is chosen with the pseudo-random function, such that $1 \leq h \leq q - 1$ and gcd $(h, q - 1) = 1$ [35,36] (h is relatively prime for $q - 1$):

$$\text{Then, calculate } s_1 = \alpha^h \ mod \ q \tag{5}$$

$$\text{Again, calculate } w = h^{-1} \ mod \ (q - 1) \tag{6}$$

$$\text{Now, calculate } s_2 = (m - pr_{ni} * si) * w \tag{7}$$

Now the receiving node ensures the authenticity with signatures: first of all, it receives the data, a node checks the sender ID within the data, and then the receiving node determines the sending node's public key through the table. The receiving node now executes the signature verification through the public key and the data (q, α, puni) of the sending node.

4.4. Signature Verification Phase

In this phase, two verification variables are generated using Equations (8) and (9) [49,51]:

$$\text{Calculate } B_1 = \alpha^m \ mod \ q \tag{8}$$

$$\text{Again, calculate } B_2 = (pu_{ni})^{s1} * (s_1)^{s_2} \ mod \ q \tag{9}$$

Now, if $B_1 = B_2$ then the signatures are valid, and this means the data are coming from an authenticated node. In this way, signature generation and verification are done for all the nodes that are involved in the location estimation, and this thus eliminates the possibility of any malicious node being part of the system, because its signature cannot be verified. Now the main task would be the location estimation through the authenticated anchor nodes that have passed the secure verification process mentioned above.

4.5. Empirical Analysis of Signature Generation and Verification

In this case, we choose the primitive root (α) equal to 10, a prime number (q) taken as 19, and the private key (pr_{ni}) is taken as 16. Then, using Equation (4), the public key (pu_{ni}) is calculated as $\alpha^{pr_{ni}} \ mod \ q$ ($\alpha^{16} mod$ 19), and the resultant is 4. Hence the private key is 16 and the public key set contains $\{q, \alpha, pu_{ni}\}$, which is represented as {19, 10, 4}. Now suppose the sender wants to sign the message (m) as having the hash value equal to 14, computed using any hash generator available online. Now the signatures (S_1, S_2) are generated using the pseudorandom function (h) taken as 5, which is relatively prime to $q - 1$ and is determined to be 18. Now, by using the Equations (5)–(7) the signatures are calculated. Here, S_1 is computed as $10^5 mod$ 19, which turns out to be 3, and then w is calculated as $5^{-1} mod$ 18, which is equal to 11. Now, S_2 is calculated, which turns out 4. So, at the end of the signature generation phase, the final pair of signature values is 3 and 4. This signature pair is sent by the sensor node during data transmission, and they need to be verified by the node that is to receive the information. Now, the signature verification phase is started, and two verification variables (B_1, B_2) are calculated using Equations (8) and (9). First of all, B_1 is calculated as $10^{14} mod$ 19, which turns out to be 16, and then B_2 is calculated as $(4^3)\ (3^4)\ mod$ 19, with the resultant value 16. Here, B_1 and B_2 are equal, so the signatures are verified and the information is accepted. If there is any malicious node somehow able to get the signatures, it will not able to be the part of the system, because during the verification process the signatures will not be verified, as the private keys are only allocated to the nodes by the BS at the beginning; thus, the malicious node is not going to get the same value. This makes the system secure even when malicious nodes are present in the network.

4.6. Proposed Localization Technique Using Improved DV-Hop Based on Error Correction

Now, the unknowing node coordinates are computed through the proposed algorithm—named hyperbolic and mid-perpendicular with centroid (HAMPC)—by incorporating an error correction factor [34] instead of the trilateration technique used in other DV-Hop localization methods. Similar to other DV-Hop methods, the proposed approach also has the three basic steps—i.e., a hop count calculation, followed by an average hop size determination, and then at last a distance estimation technique. We modified the steps of the basic DV-Hop localization algorithm in the proposed approach. In addition to these common steps, a mid-perpendicular along with centroid approach is used when the anchor node is an immediate neighbor of the unknowing node, otherwise a hyperbolic approach is to be used. This will enhance the accuracy and reduce the computation time of the localization process. Now, the steps are explained in a detailed manner along with their working.

4.6.1. Find Hop Count among the Nodes

Anchor nodes are now broadcasting the information throughout the network to discover the minimum hop count among the network nodes:

$$K_a \rightarrow *: ID(A), P(A), H_i(A) \tag{10}$$

Here $ID(A)$, is the ID of the anchor node, $P(A)$ represents the coordinates of the anchor node, and $H_i(A)$ is the hop count, which is initially set at 0 [52]. Whenever any node receives the packet, the node updates the hop count by one and further broadcasts it. If the same packet is received via a different path, the node verifies the hop count initially. If the value of the hop count is lower compared to a previously received packet, then the node receives the packet and update the hop count. In addition, if the hop count of a newly received packet is greater, then the node discards that packet. The node thus maintains minimum hop count value.

4.6.2. Find Updated Hop Size and Node Distance

Some modifications were made to the basic DV-Hop algorithm during this phase. After calculating the hop size value, the average hop value calculated with Equation (11) is calculated again as shown in Equation (12), where the coordinate points of an anchor and unknowing nodes are (X_a, Y_a) and (X_j, Y_j), respectively; h_cont represents the number of hop between the anchor nodes; and T signifies total anchor nodes.

$$AHD_a = \frac{\sum \sqrt{\left(X_a - X_j\right)^2 + \left(Y_a - Y_j\right)^2}}{\sum h\_cont} \tag{11}$$

$$ANH\_D = \frac{\sum_{a=1}^{T} AHD_a}{T} \tag{12}$$

The further distance error (D_E_a) is calculated using Equation (13) [34]:

$$D\_E_a = (ANH\_D \times h\_cont) - \sqrt{\left(X_a - X_j\right)^2 + \left(Y_a - Y_j\right)^2} \tag{13}$$

The average error of each anchor is found using Equation (14):

$$AVg\_E\_Anchr_a = \frac{\sum_{a=1}^{T} D\_E_a}{T} \tag{14}$$

Last, the updated distance is calculated by Equation (15) below [34]:

$$Dist_{u,a} = Dist\_E_a - AVg\_E\_Anchr_a \tag{15}$$

Hence, after receiving the packet the unknowing node checks the hop count table to know whether or not there are three anchor nodes available; it also checks whether or not those nodes that are available are in the immediate neighborhood of the unknowing node using the hop count value, which is always one in the case the nodes are neighbors. If three anchor nodes are accessible, the unknowing node will assess the position using the mid-perpendicular strategy with centroid as defined in Section 4.6.4; otherwise the hyperbolic approach is used, as defined in Section 4.6.3. There is thus no need to execute multiple calculations with the addition of the mid-perpendicular with centroid approach when the unknowing node is not an immediate neighbor of the anchor node using the hyperbolic method. So, this improves the overall efficiency of the algorithm by reducing some steps by checking the condition beforehand. Moreover, the computational cost and complexity of the mid-perpendicular and centroid approach are lower compared to the hyperbolic technique, due to a simple and minimum number of steps that need to be performed in the former. So, in the proposed algorithm, this feature of adding the check on an immediate neighbor ultimately improves the overall accuracy.

4.6.3. Position Value Estimation using a 2D Hyperbolic Approach

In our proposed algorithm, the hyperbolic approach is used instead of the multilateration method as used by DV-Hop. This step improves the accuracy of the algorithm further, and less computation is required compared to normal methods used in many variants of the DV-Hop algorithm. Here, (X_u, Y_u) are the coordinate values of an unknowing node, (X_a, Y_a) are the coordinates of the anchor, and T is the complete quantity of the anchor node. $Dist_{u,}$ represents the distance between the anchor and unknowing node. If we expand Equation (16), then it is further defined as Equations (17)–(24), as described below [53]:

$$Dist_{u,a} = \sqrt{(X_a - X_u)^2 - (Y_a - Y_u)^2} \tag{16}$$

$$X_a^2 + Y_a^2 - 2X_aX_u - 2Y_aY + X_u^2 + Y_a^2 = Dist_{u,a}^2 \tag{17}$$

$$Dist_{u,a}^2 - e_i = -2X_aX_u - 2Y_aY_u + k \tag{18}$$

$$\text{where } e_a = X_a^2 + Y_a^2 \tag{19}$$

$$k = X_u^2 + Y_u^2 \tag{20}$$

$$M_c = [X_u, Y_u, k]^t \tag{21}$$

$$g_c = \begin{bmatrix} -2X_1 & -2Y_1 & 1 \\ -2X_2 & -2Y_2 & 1 \\ & \vdots & \\ & \vdots & \\ -2X_a & -2Y_a & 1 \end{bmatrix} \tag{22}$$

$$h_c = \begin{bmatrix} D_1^2 & -e_1 \\ D_2^2 & -e_2 \\ & \vdots \\ & \vdots \\ D_a^2 & -e_a \end{bmatrix} \tag{23}$$

$$g_cM_c = h_cM_c = \left({g_c}^t g_c\right)^{-1} {g_c}^t h_c \tag{24}$$

Here, M_c includes the unknowing node's coordinates.

4.6.4. Position Value Estimation using the Mid-Perpendicular with the Centroid Approach

This step is executed when the anchor nodes are immediate neighbors of the unknowing node as mentioned before. Further, it contains three scenarios based on an obtuse triangle, right triangle, and acute triangle. Using this method, the unknowing node's coordinates will be the mid-perpendicular intersection point of three lines (*Line1*, *Line2*, and *Line3*) [44]. Here (X_1, Y_1), (X_2, Y_2), and (X_3, Y_3) are the three anchor node coordinates, and (X_m, Y_m) is the unknowing node's coordinates used in Equations (25)–(30). Now the positions are calculated by considering the various possibilities described below.

Coordinate Calculation Using an Acute Triangle

Here, first of all, we are investigating the overlapping region point as in Figure 3. *Line1* is the mid-perpendicular of the right angle to the line between *A2* and *A3*. In the same fashion, *Line 2* and *Line 3* are the mid-perpendiculars of the line between *A1* and *A3* and line between *A1* and *A2*, respectively. All these lines pass through the center of the overlapping regions. The center of the intersection is defined as *Nmid*, which uses the mid-perpendicular approach to represent the unknowing node's estimated position, and *Nx* is the normal node represented in Figure 3.

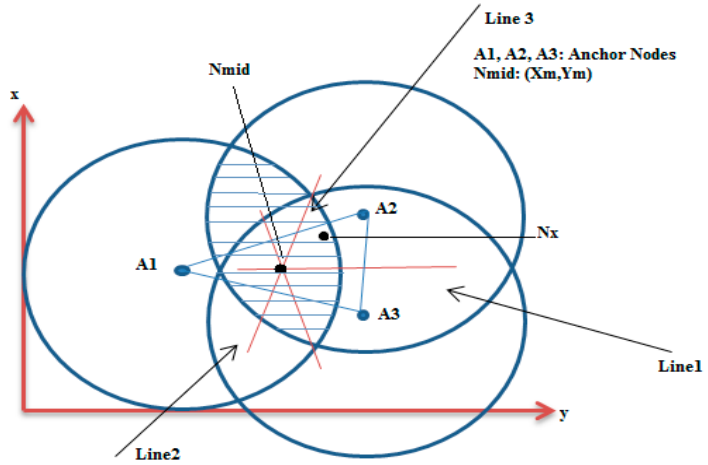

Figure 3. Mid-perpendicular using an acute triangle.

Now, for the acute triangle, the *Nmid* (X_m, Y_m) is determined by the following Equations (25) and (26) [54]:

$$X_m = \frac{(X_1^2 - X_2^2)(Y_3 - Y_1) + (X_1^2 - X_3^2)(Y_1 - Y_2) + (Y_1 - Y_2)(Y_2 - Y_3)(Y - Y_1)}{2[Y_1(X_2 - X_3) + Y_2(X_3 - X_1) + Y_3(X_1 - X_2)]} \quad (25)$$

$$Y_m = \frac{(Y_1^2 - Y_2^2)(X_3 - X_1) + (Y_1^2 - Y_3^2)(X_1 - X_2) + (X_1 - X_2)(X_2 - X_3)(X_3 - X_1)}{2[X_1(Y_2 - Y_3) + X_2(Y_3 - Y_1) + X_3(Y_1 - Y_2)]} \quad (26)$$

Coordinate Calculation Using a Right Triangle and an Obtuse Triangle

The midpoint of the longest side of the right triangle would be *Nmid* (X_m, Y_m) for the right angle triangle [55]. As if the longest side consisted of joining *A1* and *A2*, then (X_1, Y_1) and (X_2, Y_2) are the coordinates of *A1* and *A2*. The *Nmid* (X_m, Y_m) for the right triangle would now be determined by the following Equations (27) and (28) and as represented in Figure 4.

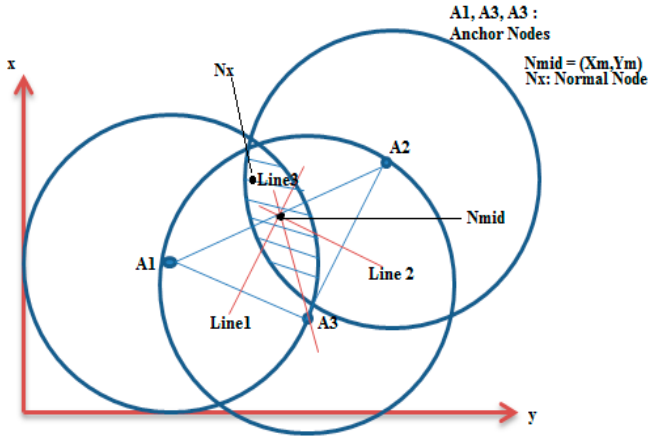

Figure 4. Mid-perpendicular using a right triangle.

Similarly, the midpoint (*Nmid*) of the longest side (*A1* to *A2*) of the triangle would again be the unknowing node's coordinates, as represented in Figure 5 [55] for an obtuse triangle.

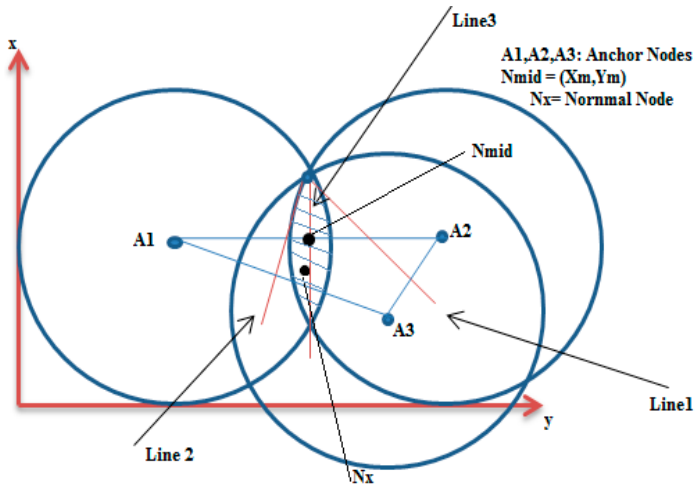

Figure 5. Mid-perpendicular using an obtuse triangle.

$$X_m = \frac{X_1 + X_2}{2} \tag{27}$$

$$Y_m = \frac{Y_1 + Y_2}{2} \tag{28}$$

After finding the mid-perpendicular, one can calculate the centroid using the following Equation (29):

$$X_c = \frac{X_1 + X_2 + X_3}{3}, Y_c = \frac{Y_1 + Y_2 + Y_3}{3} \tag{29}$$

Now the average of (X_m, Y_m) and (X_c, Y_c) can be found using Equation (30):

$$X_u = \frac{X_m + X_c}{2}, \; Y_u = \frac{Y_m + Y_c}{2} \tag{30}$$

Here, (X_u, Y_u) are the unknown coordinates calculated using the centroid approach applied over the calculated mid-perpendicular coordinates.

This method decreases the general computation time and complexity, as fewer steps are performed in the proposed approach by introducing a hyperbolic and centroid approach rather than the multilateration approach used in the basic hop-based algorithms.

5. Security Analysis

Various attacks can be carried out in a WSN, such as a wormhole attack, black hole attack, and flooding attack. So, when a receiver receives the data, the authentication of the data should be there and the data should be in an encrypted form. The various attacks that are common and affect the localization in WSNs are listed below, along with the defense through the proposed scheme in Table 2.

Table 2. Attacks and their defense by the proposed scheme.

Attack Type	The Behavior of the Attack	Defense Against the Attack Using the Proposed Scheme
Jamming attack	The attacker sends the jamming signal with the same frequency of the current signal in progress.	The signal frequency is changing as the range is changing with a random deployment.
Tampering attack	Tampering with the anchor nodes to have the wrong position computation for the unknowing node	Digital signatures are used to authenticate the beacon node.
Exhausting attack	Unnecessary messages are sent in the network only to consume the bandwidth.	Only the message from authenticated nodes is taken, all others are discarded, and with every message the hop count value is verified.
Collision attack	The same message is sent many times in the network by the sensor node.	There is no possibility, as all messages are controlled through the BS and even the hop count value is verified for each message processed and thus retains the minimum hop count messages.
Insider attack	Involvement of the malicious node inside the network.	No chance of any malicious node entering the system, as authentication is added and key pairs are shared during the deployment of the nodes by the BS. The only possibility is that the BS is compromised.
Selective forwarding	Only selected messages are forwarded and thus some necessary messages are not taken into account.	Here hop-by-hop data is propagated, so there is little possibility of this attack.
Sybil attack	Multiple identities of the same nodes are formed.	Each node has the unique private key which is authenticated during the signature verification stage.
Blackhole attack	A fake promising node is established that absorbs all the information and drops the same later on.	The malicious node cannot be part of the system due to the deployment of keys in the beginning only, and all are authenticated by signature generation and verification.
Wormhole attack	The faster fake route is propagated in the network and other nodes are convinced to use the same.	Fake nodes cannot be part of the system, which thus eliminates the possibility of this attack.
Flooding attack	False connections are established.	Connections are established based on key verification, and also each node is broadcasting the information within the specified range.

The proposed scheme primarily uses the concept of a digital signature for adding the security feature into the localization approach beforehand, so that the malicious nodes are not able to superimpose their operations onto the localization phases involved. Thus, it enhances the accuracy of the localization approach as precise values of localization error and average localization error are being formulated, because malicious nodes are prevented from participating during the position determination phase. Furthermore, the security approach used in this work is quite effective in dealing with the various attacks as mentioned in the Table 2 above. This is because the onus lies with the BS that distributes the keys to the nodes involved in the localization process, and, moreover, there are two signatures generated (*S1 & S2*) while the message (location information) is transmitted between the sender and the receiver; in addition, the verification is done through the two verification entities (*B1 & B2*) that are computed and compared at the receiver's end. Thus, even if some tampering is done by the intruder with the message and the signature during the communication, then the same is taken into account, as the verification entities is not

equal and thus the information is discarded. Although the approach is not a new one, its applicability in the current localization approach is quite effective against the various attacks mentioned.

In addition, care must be taken that while implementing the digital signature approach as used in this paper, the values of the prime number and random number taken must be large enough to handle some of the latest attacks such as Bleichenbacher's and the one that is based on solving the discrete logarithm problem, as used in the digital signature approach. The main reason for the execution of these attacks is due to the wrong choice of the prime and primitive roots during the signature generation. However, by using the very large value of prime numbers it is not possible to do the cryptanalysis without involving high computation machines in the present times.

6. Simulation and Implementation

In this section, the proposed approach is first simulated, then the proposed algorithm is implemented and evaluated in the presence and absence of malicious nodes. As per the parameters mentioned in Table 3, the execution of the proposed secure localization algorithm is done. The new algorithm is also contrasted with algorithms such as the basic DV-Hop and the proposed improved DV-Hop in MATLAB 2015 by varying the node number, anchor number, and range. There is also an analysis of the effect of the malicious node ratio.

Table 3. Simulation parameters.

Area	100 m Square Area
Total node number	100–500
Anchor node number	5%–30%
Unknown node number	70%–95%
Malicious node number	10%–30%
A range of anchor node in a circular form	20–40 m
Deployment	Random deployment

In the 100 m × 100 m area, nodes are placed randomly in the 2D region. As represented in Figure 6, 100 nodes are deployed in the same region, including 20 nodes represented by red stars as anchor nodes and the remaining 80 are unknowing black dot nodes. A set range of 30 m is allocated to each node. Simulations are made for 50 occasions to obtain the accurate error value during the computation stage of the different algorithms, owing to a node position shift due to a random node deployment as shown in Table 3. The random deployment is chosen here instead of a uniform distribution of nodes as it gives more real insights, as in practice the nodes are distributed in a random fashion owing to the area based on a particular scenario. Although the deviation will be observed in the factor for analysis but it clearly embarks the efficiency of the proposed scheme.

Factors for Analysis

As we have discussed, for the various parameters that need to be analyzed for various algorithms above, their impact on the localization scheme is calculated using the factors. One of the factors is the localization error (LE), and its significance can be deduced by using the Equation (31) for each unknown node, where (X_i^u, Y_i^u) are the computed coordinates and (X_i^{ac}, Y_i^{ac}) are the actual unknowing nodes coordinates:

$$Error_i = \sqrt{\left(x_i^u - x_i^{ac}\right)^2 - \left(y_i^u - y_i^{ac}\right)^2} \quad (31)$$

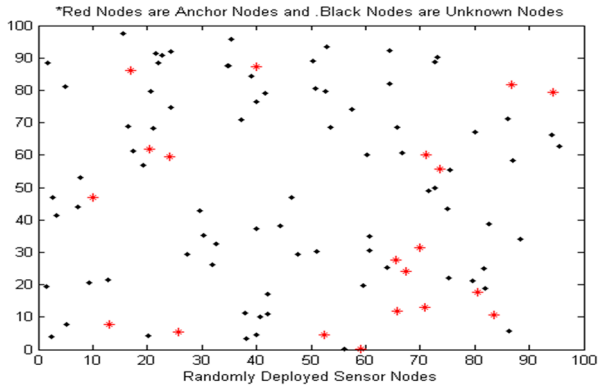

Figure 6. Node distribution diagram.

Similarly, the average localization error (ALE) is another factor. With Equation (32) it can be calculated:

$$\text{LocalizationErr} = \frac{\sqrt{\left(x_i^u - x_i^{ac}\right)^2 - \left(y_i^u - y_i^{ac}\right)^2}}{UN \times R} \tag{32}$$

where $(X_i^u,\ Y_i^u)$ are the computed coordinates, (X_i^{ac}, Y_i^{ac}) are the actual coordinates, and the range value is defined as R. UN is the unknowing node quantity. In addition, the induced value of the ALE can be correlated with the complexity and cost involvement in the localization process. A low value of the ALE means that the localization process chosen is more stable and thus less costly, which further strengthens the less complex nature of the scheme. As the nodes deployed are mostly low powered once deployed in the hostile environments, the ALE must be minimal in order to get a better output from the localization scheme.

7. Results and Discussion

Here, first of all, we are evaluating the effect of the malicious node percentage on our proposed improved DV-Hop based on the distance error correction metric. Here, the localization error value was calculated by raising the malicious node ratio from 10% to 30%. The comparisons were done for the various parameters, such as the range value, anchor node ratio, and total node number, against the same ratio of malicious nodes. All the results were tested using the graphical user interface (GUI) being developed that includes the functionality to apply malicious nodes to the improved DV-Hop, as mentioned in this paper. In addition, the secure approach proposed in this paper is embedded in this interface in order to mitigate the attack on the localization process.

7.1. Impact of Malicious Nodes Corresponding to the Range

Figure 7 shows the effect of the communication range on the error concerning the changing proportion of malicious nodes from 10% to 30% of the total quantity of nodes. The total number of nodes in this case was 100, and the number of anchor nodes was taken as 10. It was noted that as the number of malicious nodes increased, the value of the localization error showed the same trend line for different malicious node ratios. Initially, the error value was high concerning the range value of 20 to 25 m and, subsequently, the error value decreased beyond 25 m for different malicious ratios. This is because as the range value increased, more nodes came under each anchor node, and thus the estimated distance came nearer to the real distance. However, it is noted that as the ratio of malicious node increased, the amount of error also increased, as there were fewer true nodes available that participated in the position computation and thus the quantity of error increased. Table 4 shows an average localization error under the impact of malicious nodes corresponding to the range.

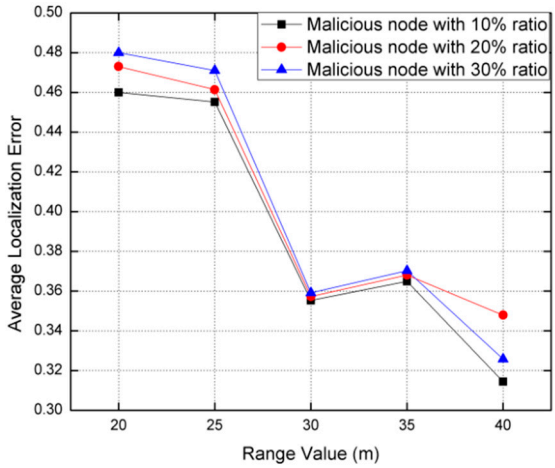

Figure 7. Error variation with the range according to malicious node ratio.

Table 4. Average localization error under the impact of malicious nodes corresponding to the range.

Range of Node (m)	Average Localization Error (Malicious Node Ratio at 10% of Total Nodes)	Average Localization Error (Malicious Node Ratio at 20% of Total Nodes)	Average Localization Error (Malicious Node Ratio at 30% of Total Nodes)
20	0.460	0.470	0.480
25	0.458	0.460	0.472
30	0.356	0.358	0.360
35	0.364	0.368	0.370
40	0.316	0.350	0.326

7.2. Impact of Malicious Nodes Corresponding to the Anchor Node Ratio

The effect of the anchor node ratio on the localization error value corresponding to the total node value of 100 is shown in Figure 8, and the range value is taken as 30 m. The quantity of the anchor node was boosted from 5% to 30%. The effect on the error value of the malicious node according to the anchor node ratio as shown in Figure 8 is noted. It is seen from the results that as the number of anchor node increased, the value of the localization error decreased in all the different scenarios of the malicious node number. However, when the malicious ratio was greater, the corresponding value for the error was also high, as depicted in Figure 8. For the anchor node ratio of 5%, the value of error corresponding to 10% malicious node ratio was 0.50; it was 0.55 for a 20% malicious node ratio and 0.57 for a 30% malicious node ratio. The error value decreased as the number of the anchor nodes increased, as more anchor nodes were closer to the unknowing node and could measure the error value with more precision. Table 5 shows the average localization error under the impact of malicious nodes corresponding to the anchor node ratio.

Table 5. Average localization error under the impact of malicious nodes corresponding to the anchor node ratio.

Total Node Number	Average Localization Error (Malicious Node Ratio Is 10% of Total Nodes)	Average Localization Error (Malicious Node Ratio is 20% of Total Nodes)	Average Localization Error (Malicious Node Ratio Is 30% of Total Nodes
100	0.343	0.374	0.376
200	0.358	0.340	0.348
300	0.359	0.346	0.354
400	0.367	0.378	0.387
500	0.369	0.387	0.392

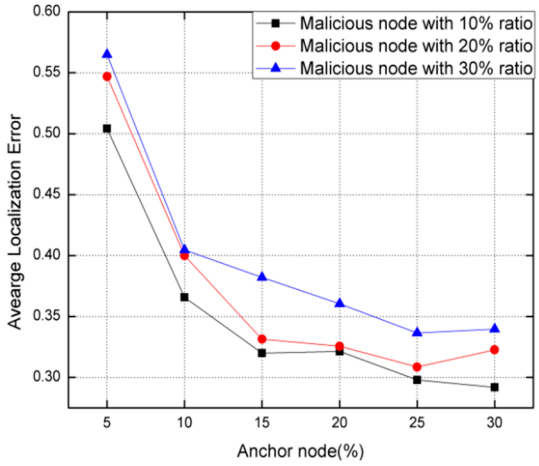

Figure 8. Localization error versus anchor node ratio under the malicious.

7.3. Impact of Malicious Nodes Corresponding to the Total Node Number

Again, the total number of nodes increased from 100 to 500 while the anchor node value was kept at 10% of the total nodes and the range value was fixed at 30 m. It can be observed in Figure 9 that as the number of total node increased, the value of the localization error decreased, as more nodes were available that were nearer to the anchor node and thus the connectivity between them was increased. The error value showed a decrease up to 200 nodes and the error value increased beyond 300 nodes. This is because in the beginning the number of malicious nodes was at the minimum of the total deployed nodes, and thus the anchor nodes could localize them efficiently. As the number was increased further, the ratio of malicious nodes also increased, though the anchor node number remained the same, which led to an increase in the error value. Table 6 shows the average localization error under the impact of malicious nodes corresponding to the total node number.

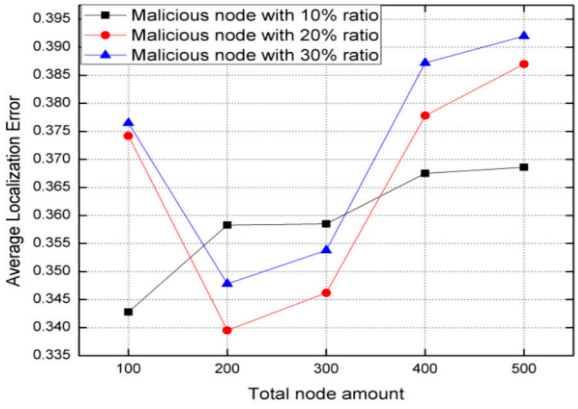

Figure 9. Localization error versus total number by ratio.

Table 6. Average localization error under the impact of malicious nodes corresponding to the total node number.

Anchor Node Ratio	Average Localization Error (Malicious Node Ratio Is 10% of Total Nodes)	Average Localization Error (Malicious Node Ratio Is 20% of Total Nodes)	Average Localization Error (Malicious Node Ratio Is 30% of Total Nodes)
5	0.505	0.545	0.570
10	0.370	0.400	0.405
15	0.325	0.335	0.380
20	0.328	0.330	0.362
25	0.290	0.315	0.338
30	0.280	0.334	0.340

From the above implementations, it is concluded that for the proposed improved DV-Hop algorithm, the value of the localization error increases as the ratio of a malicious node increases for various parameters such as the node number, anchor node ratio, and range value. Hence, there is a need for a secure localization approach to reduce the effect of a malicious node on the localization process. In this context, a signature-based approach is used in the proposed algorithm and a new secure improved DV-Hop approach was developed. For measuring the efficiency of the proposed secure algorithm, it was tested on the same parameters as mentioned above under the impact of malicious nodes. Here, in this case, the malicious node number was taken as 20% of the total node number.

Figure 10 presents the impact on the localization error value of the anchor node number corresponding to the total node number of 100 and the range value of 30 m. It is inferred that the value of the error decreased for all the algorithms as the number of anchor nodes increased. When malicious nodes were introduced into the network, the value of the error increased as these nodes tried to provide a false location estimation. However, when we used the proposed secure approach, the value of the error decreased, because the malicious nodes were not able to authenticate themselves and were not able to participate in the localization process further. Due to the distance error correction factor and the hyperbolic function used in the proposed approach, the error in the case of a proposed improved DV-Hop approach was lower in the presence of malicious nodes compared to the basic DV-Hop. Table 7 shows the average localization error variation corresponding to the anchor node number with and without malicious node for the proposed algorithm and other variants.

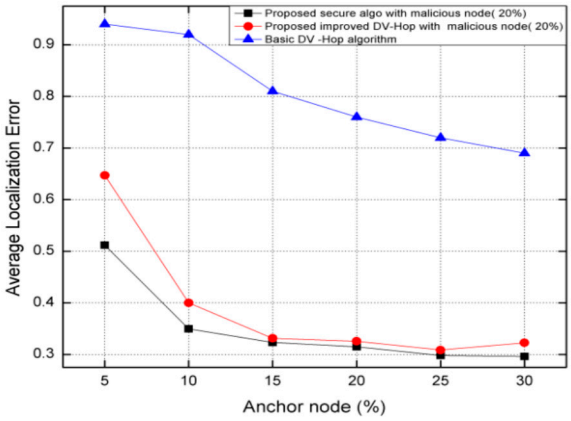

Figure 10. Error with the changing anchor number under the impact of malicious nodes.

Table 7. Average localization error variation corresponding to the anchor node number with and without malicious nodes for the proposed algorithm and other variants.

Anchor Node Ratio	Average Localization Error for the Proposed Secure Algorithm (Malicious Nodes Are 20% of Total Nodes)	Average Localization Error for the Proposed Improved DV-Hop Algorithm (Malicious Nodes Are 20% of Total Nodes)	Average Localization Error for the Basic DV-Hop Algorithm (without Malicious Nodes)
5	0.510	0.656	0.980
10	0.356	0.400	0.925
15	0.318	0.322	0.805
20	0.312	0.318	0.780
25	0.300	0.310	0.715
30	0.298	0.320	0.690

Figure 11 provides the variance of the localization error with the rise in the range value assessed with the total node number of 100 and the anchor node ratio of 10%. It is observed that the value of the error decreased for all the algorithms as the range value

increased. The reason for this is that with the increase in the range value, more nodes came within the anchor nodes' proximity and thus became more linked to the network. This also reduced the variation in the estimated and actual position of the unknowing nodes computed [50] by the anchor nodes. However, in the case of the proposed improved DV-Hop with malicious nodes, the error value was greater compared to the secure proposed algorithm, because in the latter case malicious nodes were identified and removed from the localization process due to the authentication process involved in it. Table 8 shows the average localization error variation corresponding to the range value with and without malicious nodes for the proposed algorithm and other variants.

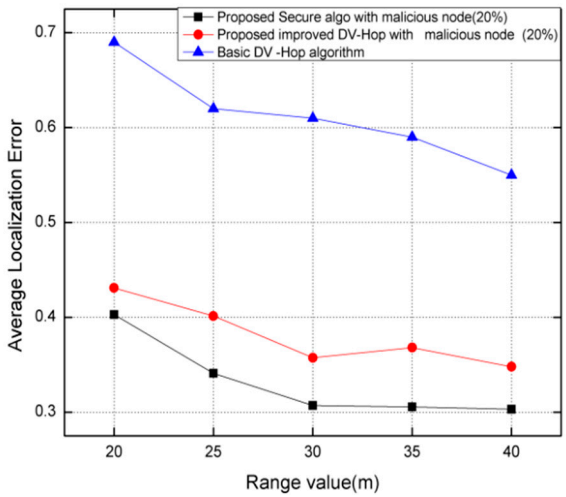

Figure 11. Variation of error by range.

Table 8. Average localization error variation corresponding to the range value with and without malicious nodes for the proposed algorithm and other variants.

Range Value (m)	Average Localization Error for the Proposed Secure Algorithm (Malicious Nodes Are 20% of Total Nodes)	Average Localization Error for the Proposed Improved DV-Hop Algorithm (Malicious Nodes Are 20% of Total Nodes)	Average Localization Error for the Basic DV-Hop Algorithm (without Malicious Nodes)
20	0.400	0.430	0.685
25	0.375	0.400	0.620
30	0.308	0.365	0.610
35	0.306	0.375	0.590
40	0.303	0.362	0.550

Again, it is inferred that, as the number of nodes increased from 100 to 500 as shown in Figure 12, the value of localization error decreased. The reduction in the error value was due to a rise in the neighbors value around each unknowing node with the rise in node number. A high error value for the malicious nodes was due to the miscalculation of the estimated location of the unknowing nodes due to the different attacks outlined in Table 2. However, it was found that the localization error value decreased when we used the secure algorithm because of the authenticating mechanism used in the algorithm. Furthermore, the error value in the case of the basic DV-Hop was high in all cases compared to other algorithms, due to the usage of a distance error correction factor in the other algorithms [39]. Table 9 shows the average localization error variation corresponding to the total node number with and without malicious nodes for the proposed algorithm and other variants.

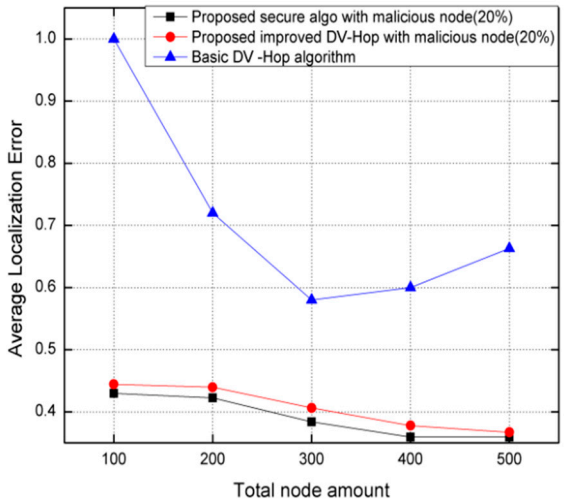

Figure 12. Variation of error by node number.

Table 9. Average localization error variation corresponding to the total node number with and without malicious nodes for the proposed algorithm and other variants.

Total Node Number	Average Localization Error for the Proposed Secure Algorithm (Malicious Nodes Are 20% of Total Nodes)	Average Localization Error for the Proposed Improved DV-Hop Algorithm (Malicious Nodes Are 20% of Total Nodes)	Average Localization Error for the Basic DV-Hop Algorithm (without Malicious Nodes)
100	0.440	0.450	0.100
200	0.430	0.450	0.720
300	0.380	0.405	0.580
400	0.360	0.380	0.600
500	0.350	0.365	0.670

8. Conclusions and Future Work

The localization error produced by various localization algorithms is one of the prime criteria and evaluation factors. However, the security of the localization process is also very important and cannot be overruled, as many attacks are possible in the localization process that can jeopardize the whole system. So, there is a need for secure localization approaches at this point. One of the algorithms thoroughly investigated by researchers is DV-Hop. This paper presents the HMPAC approach based on distance error correction as one of the new improved DV-Hop algorithms that have been developed and implemented. Compared to the basic hop-based algorithms, the proposed algorithm has a greater precision, due to the error correction metric and hyperbolic function used during its position computation. In addition, a secure approach based on the authentication of the nodes involved in the localization process is proposed in this paper. It was evaluated under the impact of malicious nodes with a varying ratio to evaluate the effectiveness of the proposed secure scheme. The proposed algorithm was analyzed for its average localization error value corresponding to the changing node number, anchor node ratio, and range value. The proposed approach was efficient against the several types of attack with and without malicious nodes with a localization error of 0.298—in comparison to 0.690 and 0.320 for the basic DV-Hop and the improved DV-Hop algorithms, respectively. The proposed secure approach was more effective than the basic DV-Hop and the improved DV-Hop, with an average localization error of 0.350 in comparison to 0.670; it was 0.365 when nodes numbered 500. In addition, future research will be on the mobility and implementation of the proposed approach in a three-dimensional environment. Furthermore, the effect of energy and other constraints will be evaluated.

Author Contributions: Conceptualization, D.P.; methodology, D.K.; validation, D.P. and M.R.; formal analysis, D.P. and A.N.; writing—original draft preparation, D.P.; writing—review and editing, M.R. and S.T.S.; supervision, S.S.A.; funding acquisition, A.S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Taif University Research Supporting Project number TURSP-2020/311 (Taif University, Taif, Saudi Arabia).

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Acknowledgments: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number TURSP-2020/311 (Taif University, Taif, Saudi Arabia).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. *Comput. Netw.* **2002**, *38*, 393–422. [CrossRef]
2. Du, T.; Qu, S.; Guo, Q.; Zhu, L. A simple, efficient anchor-free node localization algorithm for wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717705784. [CrossRef]
3. Priya, A.M. A review on localization algorithms in wireless sensor networks. *Int. J. Comput. Sci. Eng. Technol.* **2014**, *5*, 677–682.
4. Chauhdary, S.H.; Hassan, A.; Alqarni, M.A.; Alamri, A.; Bashir, A.K. A twofold sink-based data collection in wireless sensor network for sustainable cities. *Sustain. Cities Soc.* **2019**, *45*, 1–7. [CrossRef]
5. Srivastava, A.; Kumar, R.; Gupta, S.K.; Rashid, M.; Umrao, L.S. Novel technique to detect network error or modification of votes during transmission in online voting system. *J. Discret. Math. Sci. Cryptogr.* **2021**, *24*, 729–743. [CrossRef]
6. Bashir Syed, F.; Gupta, S.K.; Hamood Alsamhi, S.; Rashid, M.; Liu, X. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e4133.
7. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Comput. Netw.* **2008**, *52*, 2292–2330. [CrossRef]
8. Savarese, C.; Rabaey, J.; Langendoen, K. Robust positioning algorithms for distributed {ad-hoc} wireless sensor networks. In Proceedings of the USENIX Technical Annual Conference, Carlsbad, CA, USA, 11–13 July 2002; pp. 317–328.
9. He, T.; Huang, C.; Blum, B.M.; Stankovic, J.A.; Abdelzaher, T. Range-free localization schemes for large scale sensor networks. In Proceedings of the 9th Annual International Conference on MOBILE Computing and Networking, San Diego, CA, USA, 14–19 September 2003.
10. Stoleru, R.; He, T.; Stankovic, J.A.; Luebke, D. A high-accuracy, low-cost localization system for wireless sensor networks. In Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, New York, NY, USA, 15–17 November 2005; pp. 13–26.
11. Bulusu, D.E.N.; Heidemann, J. GPS-less low-cost outdoor localization for very small devices. *IEEE Pers. Commun. Mag.* **2000**, *7*, 28–34. [CrossRef]
12. Niculescu, D.; Badri, N. The ad hoc positioning system (APS) using AOA. In Proceedings of the Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies, San Francisco, CA, USA, 30 March–3 April 2003; IEEE: Manhattan, NY, USA, 2003; pp. 1734–1743.
13. Cai, C.; Yuan, L. DV-hop localization algorithm improvement of wireless sensor networks. *J. Theor. Appl. Inf. Technol.* **2013**, *48*, 1546–1551.
14. Wang, F.; Wang, C.; Wang, Z.; Zhang, X.Y. A hybrid algorithm of GA + simplex method in the WSN localization. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 731894. [CrossRef]
15. Singh, S.P.; Sharma, S.C. Implementation of a PSO based improved localization algorithm for wireless sensor networks. *IETE J. Res.* **2018**, *65*, 502–514. [CrossRef]
16. Chen, H.; Sezaki, K.; Deng, P.; So, H.C. An improved DV-Hop localization algorithm with reduced node location error for wireless sensor networks. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2008**, *91*, 2232–2236. [CrossRef]
17. Zhang, J.; Ning, G.; Jian, L. An improved DV-hop localization algorithm based on node deployment in wireless sensor networks. *Int. J. Smart Home* **2015**, *9*, 197–204. [CrossRef]
18. Sharma, D.; Gupta, S.K.; Rashid, A.; Gupta, S.; Rashid, M.; Srivastava, A. A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e4114. [CrossRef]
19. Patel, H.; Singh Rajput, D.; Thippa Reddy, G.; Iwendi, C.; Kashif Bashir, A.; Jo, O. A review on classification of imbalanced data for wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720916404. [CrossRef]
20. Lazos, L.; Poovendran, R. SeRLoc: Secure range-independent localization for wireless sensor networks. *J. ACM* **2004**, 21–30.

21. Lazos, L.; Poovendran, R. HiRLoc: High-resolution robust localization for wireless sensor networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 233–246. [CrossRef]
22. Lazos, L.; Poovendran, R.; Čapkun, S. ROPE: Robust position estimation in wireless sensor networks. In Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, Los Angeles, CA, USA, 24–27 April 2005.
23. Srinivasan, A.; Teitelbaum, J.; Wu, J. DRBTS: Distributed reputation-based beacon trust system. In Proceedings of the Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium, Indianapolis, IN, USA, 29 September–1 October 2006; pp. 277–283.
24. Chen, H.; Lou, W.; Ma, J.; Wang, Z. TSCD: A novel secure localization approach for wireless sensor networks. In Proceedings of the Second International Conference on Sensor Technologies and Applications, Cap Esterel, France, 25–31 August 2008; pp. 661–666.
25. Zhang, T.; He, J.; Li, X.; Wei, Q. An encryption-based secure localization scheme in wireless sensor networks. *Phys. Procedia* **2012**, *33*, 258–264. [CrossRef]
26. Wang, X.W.; Hu, F.; Zhai, C.X.; Zhang, Y.; Su, X.X.; Li, Y.; Deng, Z.H. Research on improved DV-HOP algorithm against wormhole attacks in WSN. In Proceedings of the ITM Web of Conferences EDP Sciences, Moscow, Russia, 19 September 2016.
27. Wang, H.; Feng, L.; Li, R.; Zhang, Y. The secure localization algorithm of SDV-hop in wireless sensor networks. *TELKOMNIKA* **2016**, *14*, 65–74. [CrossRef]
28. Ran, X.; Shu, L.; Mukherjee, M.; Wu, Y.; Chen, Y.; Sun, Z. Impact of irregular radio and faulty nodes on localization in industrial WSNs. In Proceedings of the International Wireless Internet Conference, Thessaloniki, Greece, 25–27 May 2016; pp. 36–48.
29. Kumar, G.; Rai, M.K.; Kim, H.J.; Saha, R. A Secure localization approach using mutual authentication and insider node validation in wireless sensor networks. *Mob. Inf. Syst.* **2017**, *2017*. [CrossRef]
30. Li, X.; Yan, L.; Pan, W.; Luo, B. Secure and robust DV-Hop localization based on the vector refinement feedback method for wireless sensor networks. *Comput. J.* **2017**, *60*, 810–821. [CrossRef]
31. Liu, X.; Yang, R.; Cui, Q. An efficient secure DV-Hop localization for the wireless sensor network. *Int. J. Secur. Its Appl.* **2015**, *9*, 275–284. [CrossRef]
32. Han, G.; Liu, L.; Jiang, J.; Shu, L.; Rodrigues, J.J. A collaborative secure localization algorithm based on the trust model in underwater wireless sensor networks. *Sensors* **2017**, *16*, 229. [CrossRef]
33. Tao, Q.; Zhang, L. Enhancement of DV-Hop by weighted hop distance. In Proceedings of the Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Shanxi, China, 5 October 2016; pp. 1577–1580.
34. Fu, C.; Qian, Z.; Ji, G.; Zhao, Y.; Wang, X. An improved DV-HOP localization algorithm in the wireless sensor network. In Proceedings of the 2013 International Conference on Information Technology and Applications, Chengdu, China, 16–17 November 2013; pp. 13–16.
35. Ma, X.; Liu, W.; Wang, Z. Node localization of wireless sensor network based on secondary correction error. In *International Symposium on Parallel Architecture, Algorithm, and Programming*; Springer: Singapore, 2017; pp. 142–151.
36. Prashar, D.; Jha, N. Review of secure distributed range-free hop-based localization algorithms in the wireless sensor networks. In *Multimedia Security*; Springer: Singapore, 2021; pp. 283–302.
37. Prashar, D.; Jyoti, K.; Kumar, D. SDRFHBLoc—A secure framework for localization in wireless sensor networks. *Recent Adv. Comput. Sci. Commun.* **2020**, *13*, 1158–1171. [CrossRef]
38. Rampa, V.; Nicoli, M.; Manno, C.; Savazzi, S. EM model-based device-free localization of multiple bodies. *Sensors* **2021**, *2*, 1728. [CrossRef]
39. Meng, Y.; Zhi, Q.; Dong, M.; Zhang, W. A Node localization algorithm for wireless sensor networks based on virtual partition and distance correction. *Information* **2021**, *12*, 330. [CrossRef]
40. Fascista, A.; Coluccia, A.; Ricci, G. A Pseudo Maximum likelihood approach to position estimation in dynamic multipath environments. *Digit. Signal Process.* **2021**, *181*, 107907. [CrossRef]
41. Chuku, N.; Nasipuri, A. RSSI-Based localization schemes for wireless sensor networks using outlier detection. *J. Sens. Actuator Netw.* **2021**, *10*, 10. [CrossRef]
42. Abid, A.; El Khediri, S.; Kachouri, A. Improved approaches for density-based outlier detection in wireless sensor networks. *Computing* **2021**, *103*, 2275–2292, 1–18. [CrossRef]
43. Coluccia, A.; Fascista, A. Hybrid TOA/RSS range-based localization with self-calibration in asynchronous wireless networks. *J. Sens. Actuator Netw.* **2019**, *8*, 31. [CrossRef]
44. Meghdadi, M.; Ozdemir, S.; Güler, I. A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. *IETE Tech. Rev.* **2011**, *28*, 89–102. [CrossRef]
45. Singh, S.K.; Singh, M.P.; Singh, D.K. A survey on network security and attack defence mechanism for wireless sensor networks. *Int. J. Comput. Trends Technol.* **2011**, *1*, 9–17.
46. Jiang, J.; Han, G.; Zhu, C.; Dong, Y.; Zhang, N. Secure localization in wireless sensor networks: A survey. *J. Commun.* **2011**, *6*, 460–470. [CrossRef]
47. Prashar, D.; Jyoti, K.; Kumar, D. Design and analysis of distance error correction based localization algorithm for wireless sensor networks. *Trans. Emerg. Telecommun. Technol.* **2018**, *29*, e3547. [CrossRef]
48. Prashar, D.; Jyoti, K. Distance error correction based hop localization algorithm for wireless sensor network. *Wirel. Pers. Commun.* **2019**, *106*, 1465–1488. [CrossRef]

49. Stallings, W. *Cryptography and Network Security, 4/E*; Pearson Education India: Noida, India, 2006.
50. Sergeev, A.V.; Goodson, D.Z. Self-consistent field perturbation theory of molecular vibrations. *Mol. Phys.* **2008**, *93*, 477–484. [CrossRef]
51. Li, G. Application of an improved DV-Hop algorithm on the wireless sensor network of the mine shaft. *Appl. Mech. Mater.* **2013**, *273*, 537–541. [CrossRef]
52. Song, G.; Tam, D. Two novel DV-Hop localization algorithms for randomly deployed wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 187670. [CrossRef]
53. Sharma, G.; Kumar, A. Dynamic range normal bisector localization algorithm for wireless sensor networks. *Wirel. Pers. Commun.* **2017**, *97*, 4529–4549. [CrossRef]
54. Gui, L.; Val, T.; Wei, A.; Taktak, S. An adaptive range-free localization protocol in wireless sensor networks. *Int. J. Ad Hoc Ubiquitous Comput.* **2014**, *15*, 38–56. [CrossRef]
55. Shit, R.C.; Sharma, S.; Puthal, D.; Zomaya, A.Y. Location of things (LoT): A review and taxonomy of sensors localization in IoT infrastructure. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2028–2061. [CrossRef]