Evaluating ALWadHA for Providing Secure Localisation for Wireless Sensor Networks

Adnan M. Abu-Mahfouz[1,3]
Advanced Sensor Networks Research Group
CSIR Meraka Institute
Pretoria, South Africa
A.AbuMahfouz@ieee.org

Gerhard P. Hancke[2,3]
[2]Information Security Group, Royal Holloway
University of London, UK
[3]Department of Computer Engineering
University of Pretoria, South Africa
ghancke@ieee.org

***Abstract*—Most of the proposed localisation algorithms studied the problem of location discovery in a non-adversarial environment. Although these types of algorithm are vulnerable to several types of security attack, less work has been done to implement secure localisation algorithms that are able to work in a hostile environment. An attacker could compromise, or masquerade as, a beacon node and send incorrect location information. Localisation in a hostile environment is a critical problem in wireless sensor networks (WSNs) because compromising the localisation system could disturb and subvert the entire functioning of the WSN. In this paper we investigate the security of recently proposed localisation algorithm, called ALWadHA, which enables nodes to live with the malicious reference nodes without disturbing the location estimation.**

Keywords—ALWadHA, attack resitance, malicious node, secure localisation

I. INTRODUCTION

Localisation systems play a key role in wireless sensor networks (WSNs), because in addition to locating events they could be used as the base for routing, density control, tracking and other services and protocols. This role makes the localisation system a target of attackers. An attacker that compromises the localisation system could disturb the entire functioning of WSN and lead to incorrect plans and decisions. Therefore, WSNs require a secure localisation algorithm, which not only solves the problem of localisation, but should also be resistant to the presence of fraudulent, malicious and/or compromised nodes.

One approach that has been followed by localisation algorithms is to use special nodes called "beacons", which know their location (e.g. through a GPS receiver or manual configuration). The other nodes that do not know their location, sometimes referred to as "unknowns", use different techniques to compute their own position based on the location information of the beacons and the measured distance to these beacons. The term "reference nodes" or simply "references" will be used in this paper to refer to the sensor nodes which are willing to help other nodes to estimate their position. Therefore, the reference set includes beacons and knowns (i.e. unknowns which have obtained their position) which are willing to act as a reference for other unknowns.

Localisation systems consist of three main components: distance/angle estimation, position estimation and localisation algorithm. These components are strongly dependent on one another. Malfunctioning in any of these components could affect the entire localisation system, and lead to incorrect estimation. Because of the strong relationship between them, any of these components can be targeted by an attack on a localisation system, making these systems very fragile and hard to secure [1].

Different approaches can be used for distance/angle estimation, such as directional antennas, RF fingerprinting (communication neighbour authentication), connectivity (in range) and distance bounding. Practically, these approaches use several techniques, including receive signal strength, time of arrival, time difference of arrival, angle of arrival, round trip time and hop-count based ones. The authors of [2] investigate the security aspects of these different approaches and techniques.

In addition to the distance estimations of at least three references, the node also needs to know the location of these references in order to estimate its position. An attack on the distance estimation can indirectly affect the position computation. However, some attacks can affect this component directly by advertising incorrect information about the compromised node's location. As illustrated in Fig. 1, an attacker may provide incorrect location information by either pretending to be an honest reference node or compromising beacon nodes. In both types of attack, unknown nodes which received the incorrect location information will determine their locations incorrectly. The second type of attack is more difficult to achieve than the first one, since an attacker would have to be able to compromise a beacon node first to perform the second attack, while in the first type an attacker can directly advertise the incorrect location information, pretending to be an honest reference node.

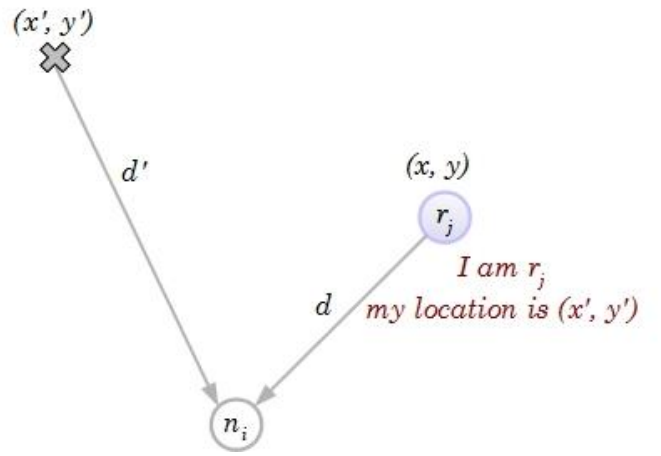

Fig. 1. Attack against position computation. n_i is an unknown node, where r_j is a dishonest reference node or a compromised beacon node.

In this paper we investigate the security of ALWadHA (An efficient Localisation algorithm for Wireless ad hoc sensor networks with High Accuracy) algorithm [3] (Section III). ALWadHA algorithm does not rely only on using a secure distance bounding protocol but also it uses a robust position computation component that tolerates the existence of malicious nodes. The simulation results (Section IV) prove that the ALWadHA algorithm is able to work on an adversarial environment.

II. Related Work

Secure localisation algorithms use several techniques to deal with the security problems of location discovery in WSNs. The main techniques used are cryptography, detecting and blocking compromised nodes, making statistical decisions or filtering the positions used in computations [1].

Cryptography does not solve all the security problems of a localisation system. However, it can be used as a second line of defence, where additional security techniques should be used to protect localisation systems [4-6].

The second technique for securing localisation systems is to detect and block malicious nodes. In this technique the node tries to detect malicious nodes and then does not use their location information to compute its position. Several methods are used to detect malicious nodes such as [7, 8].

Implementing a robust position computation component is another technique that can be used to deal with malicious nodes. This technique enables the nodes to estimate their position with acceptable accuracy even in the presence of malicious nodes. This technique is based on using statistical and outlier filtering methods to deal with malicious nodes. [9, 10] proposed localisation algorithms that based on this technique.

Localisation verification technique can be used only to verify the location estimation results from the overall localisation system, thus it can enhance the security level of the three localisation system components. The verification can be done by a central node [11], a small number of trusted nodes [12] or by all the nodes [13].

III. ALWadHA Algorithm

An ALWadHA algorithm was developed to enhance the accuracy and the security of position estimation. The idea is to select those references that are willing to help other nodes estimate their position. Based on this method, the node will only select those references that could contribute most to an accurate position estimate, and will eliminate irrelevant references from participating in the final position estimate. Irrelevant references include the ones with large measurement error and/or the references that intentionally aiming to undermine the localisation process (e.g. .malicious references).

The ALWadHA localisation algorithm consists of four phases, as shown in TABLE I. In the first phase, the node collects information from nearby references. In the second phase, the node selects a subset of references to estimate its initial position. In the third phase, the node checks the possibility of improving the current position. In the final phase, the node decides if it will accept this position, and if the accepted position can be considered as a final estimate.

TABLE I. ALWadHA Algorithm

1. Initialisation

If *(final = true)* then exit

Broadcast "location request" messages

Receive "location response" messages from neighbouring references (R_i)

If $(C(R_i) < 3)$ then exit.

2. Initial position estimation

Select a subset of references S_i from R_i

Measure distance to the references in S_i

Apply MMSE to determine an initial position $\hat{z}_i^0$.

3. Refined position estimation

for $(j = 1 \quad \text{to} \quad C(S_i))$

$\hat{e}_{i,j}^d = \left| \left\| \hat{z}_i^0 - \hat{z}_j \right\| - \hat{d}_{i,j} \right|$

if $(\hat{e}_{i,j}^d > e_{max}^d)$ then *(enhancement = true)*; break.

If *(enhancement = true)*

for $(j = 1 \quad \text{to} \quad C(R_i))$

$\hat{e}_{i,j}^d = \left| \left\| \hat{z}_i^0 - \hat{z}_j \right\| - \hat{d}_{i,j} \right|$

if $(\hat{e}_{i,j}^d > e_{max}^d)$ then eliminate r_j.

Estimate refined position $\hat{z}_i$ as shown in 2

else

$\hat{z}_i = \hat{z}_i^0$.

4. Position update

$D_{acc} = \sum \left| \left\| \hat{z}_i - z_j \right\| - \hat{d}_{i,j} \right|$

if $(D_{acc}^k < D_{acc}^{k-1})$

$\hat{z}_i$ will be accepted

if $(D_{acc} < T_{acc})$ then *(final = true)*.

$C(\,)$ is the cardinality, MMSE=minimum mean square estimate, D_{acc}=degree of accuracy, T_{acc}=accuracy target.

In this paper, the focus will be on phase three and the technique used by ALWadHA algorithm to exclude malicious references from participating in the localisation process. In this phase the node enhances the accuracy of position estimation by considering the distance error, where references with high distance error are eliminated from the reference list (R_i) that

will be used to estimate node position. This phase starts by checking the possibility of enhancement based on the estimated distance error $(\hat{e}^d_{i,j})$ using (1), which is the difference between the calculated distance (between the node's initial position $(\hat{z}^0_i)$ and references position $(z_j \text{ or } \hat{z}_j)$) and the measured distance $(\hat{d}_{i,j})$. The measured distance can be obtained using the received signal strength, while the actual distance is $d_{i,j} = \|z_i - z_j\|$.

$$\hat{e}^d_{i,j} = \left| \| \hat{z}^0_i - \hat{z}_j \| - \hat{d}_{i,j} \right|, \text{ where } j \in S_i \quad (1)$$

If the estimated distance error for at least one reference in S_i is greater than a certain value $(\hat{e}^d_{i,j} > e^d_{max})$, this indicates that position enhancement is required, otherwise the initial position is regarded as an accurate position $(\hat{z}_i = \hat{z}^0_i)$ and the process continues to the next phase. To enhance the position estimation, the node eliminates those references that have $\hat{e}^d_{i,j} > e^d_{max}$, where $j \in R_i$, from R_i, then a new subset of references will be selected to estimate a refined position $(\hat{z}_i)$ as described in the previous phase. It is remarked that position refinement is not required at each iteration; it is only required when at least one of the references in the subset S_i has a high distance error.

This technique is used to eliminate those references with a high distance error. On the other hand, it could be used to eliminate malicious nodes from the selected subset of references. The compromised nodes provide incorrect location information to mislead other nodes; however; pretending to be in an incorrect location increases the difference between the measured and estimated distance, which makes it easy to be detected by the technique used in phase three, and as a result these malicious nodes will not participate in the localisation process. In fact, the goal of the ALWadHA algorithm is not to detect these malicious nodes; rather it is to enable nodes to live with them without disturbing the location estimation.

To understand how this technique exactly works, let us consider the simple scenario shown in Fig. 2. In addition to the unknown node n_i there are two reference nodes; an honest reference node r_k and malicious node r_j. For the honest reference node the measured distance and $\|\hat{z}^0_i - \hat{z}_k\|$ can be represented as follows:

$$\hat{d}_{i,k} = d_{i,k} + e^d \quad (2)$$

$$\|\hat{z}^0_i - \hat{z}_k\| = d_{i,k} + e^l \quad (3)$$

Where e^d is the measured distance error while e^l is the estimated location error. Compensate (2) and (3) in (1), the estimated distance error will be

$$\hat{e}^d_{i,k} = d_{i,k} + e^l - d_{i,k} + e^d = e^l + e^d \quad (4)$$

If the estimated distance error for node r_k is greater than a certain value $(\hat{e}^d_{i,k} > e^d_{max})$ this node will be eliminated from S_i.

In the second case, the malicious node r_j pretend to be in location z'_j. The measured distance and $\|\hat{z}^0_i - z'_j\|$ can be represented as follows:

$$\hat{d}_{i,j} = d_{i,j} + e^d \quad (5)$$

$$\|\hat{z}^0_i - z'_j\| = d_{i,j} + d_{malicious} + e^l \quad (6)$$

where $d_{malicious}$ is the difference between the actual distance and the distance to the pretended location. $d_{malicious}$ does not affect the measured distance as shown in (5) because this distance is measured to the node in its actual location. Using (1), the estimated distance error will be

$$\hat{e}^d_{i,j} = d_{malicious} + e^l + e^d \quad (7)$$

From (7), one can notice that if the malicious node tries to pretend that it's in a location that far from its actual location, then the value of $d_{malicious}$ will be high. This makes it easy to eliminate such kind of malicious node from participating in location discovery process.

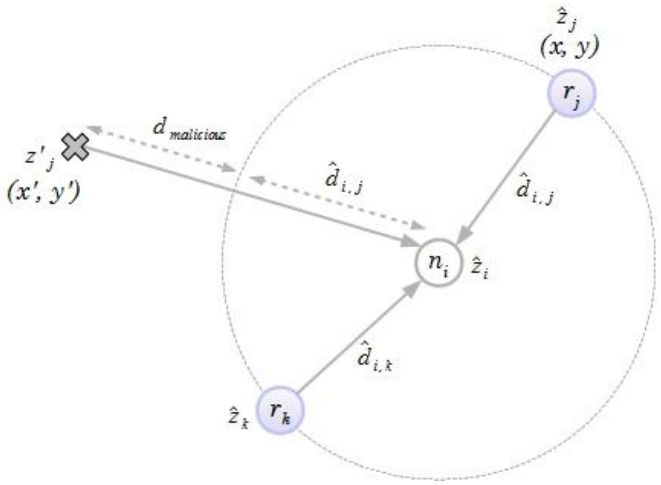

Fig. 2. Simple scinario to explain the technique used by ALWadHA to eliminate malicious nodes.

IV. Performance Comparison

This section evaluates the resistance of the ALWadHA algorithm against two types of attack; dishonest reference nodes and compromised beacon nodes. In both types the attacker provides an incorrect location reference to mislead other nodes, which could determine their location incorrectly. The performance of the localisation algorithm is evaluated based on two metrics, firstly location error created by malicious nodes, and secondly the number of malicious nodes in the network.

The Network Simulator (NS-2) was extended to simulate localisation systems in WSN [14-16]. This extension was used to implement ALWadHA algorithm. Five other localisation algorithms have been used for the performance comparison. Two algorithms based on the basic multilateration method were implemented. The first one is based on the single-estimation approach (called Single), where the node estimates its position

only once. The second one is implemented based on the successive refinement approach (called Successive), where the node keeps re-estimating its position. The other algorithms are: Nearest [17]; CRLB (Cramer-Rao-Lower-Bound) [18]; NDBL (node distribution-based localisation) [19]. 12 beacons and 64 unknowns were distributed randomly in a *200m x 200m* field.

A. *Dishonest Reference Nodes*

Four malicious nodes were distributed randomly in the network. These malicious nodes pretended to be honest references and sent incorrect location references. The error of their location was generated randomly, using a normal random variant with a mean of 0.1% of the real location and a standard deviation changed from 1% to 50% of the real location. The mean error of location estimation is recorded at the end of the run time as a percentage of transmission range (r_{tx}).

Fig. 3 shows that increasing the erroneousness of the malicious nodes' location dramatically increases the mean error of estimated location in all algorithms except ALWadHA. The maximum mean error of the ALWadHA algorithm is equal to 4.76% of the transmission range, which occurs when the standard deviation is equal to 20% of the malicious nodes' location ($L_{malicious}$). Increasing the standard deviation reduces the mean error gradually till it reaches 3.51% at the standard deviation of 50% of $L_{malicious}$. The reason for this improvement is that increasing the erroneousness of the malicious nodes' advertised location also increases the difference between the measured and the estimated distance, and so the technique used in phase three detects these nodes and eliminates them from the selected subset.

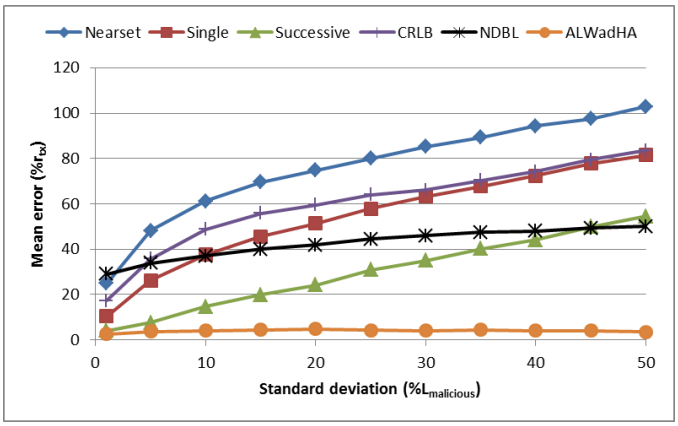

Fig. 3. Location estimation error, four dishonest reference nodes

In the second experiment, the standard deviation was fixed to 50% of $L_{malicious}$ and the number of malicious references was changed from 0 to 16, where four extra malicious nodes added each time. Note that the number of beacon nodes used in the network is only 12. Fig. 4 shows that directly after adding the first 4 malicious nodes the mean error increase dramatically for all the algorithms except for ALWadHA algorithm. ALWadHA outperforms other localisation algorithms and still achieves good accuracy of location estimation in spite of the increase in the number of malicious references. The mean error of location estimation of the ALWadHA algorithm in the presence of 16 malicious references is equal to 7.72% of the transmission range, which is much lower than that of the other localisation algorithms. Similar to ALWadHA, the NDBL algorithm is designed to work in noisy environment. Therefore, it is also less affected by dishonest references compared with other algorithms (except ALWadHA). However, the mean error of location estimation still high due to the algorithm itself. The results show that even in the absence of the dishonest references, the mean error of the NDBL algorithm is 27.71% of the transmission range.

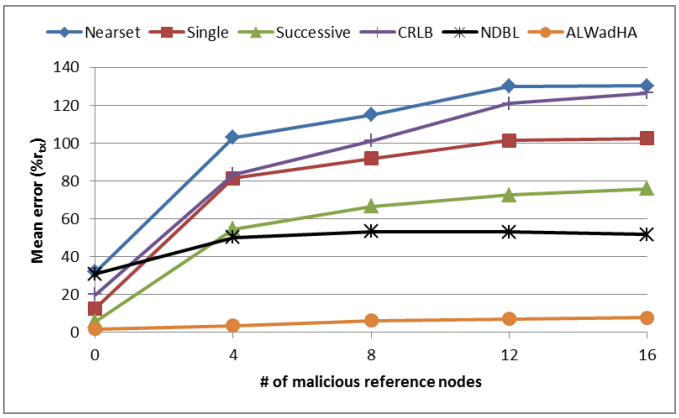

Fig. 4. Location estimation error in the existing of malicious reference nodes, standard deviation is equal to 50% of $L_{malicious}$

B. *Compromised Beacon Nodes*

The second type of attack that can be conducted by an attacker is by compromising beacon nodes. As mentioned early, this attack is more difficult to achieve than the first one. To investigate this type of attack the previous two experiments were repeated using compromised beacon nodes. From Fig. 5 and Fig. 6, one can notice that for those algorithms that do not distinguish between the beacon nodes and other references (i.e. Nearest, CRLB, Single and Successive algorithms), the mean error is the same as in the first two experiments. Therefore, an attacker can simply perform the first attack to achieve the same result. On the other hand, for the algorithms that distinguish between beacons and other references (i.e. ALWadHA and NDBL), the mean error of location estimation is higher in the second attack.

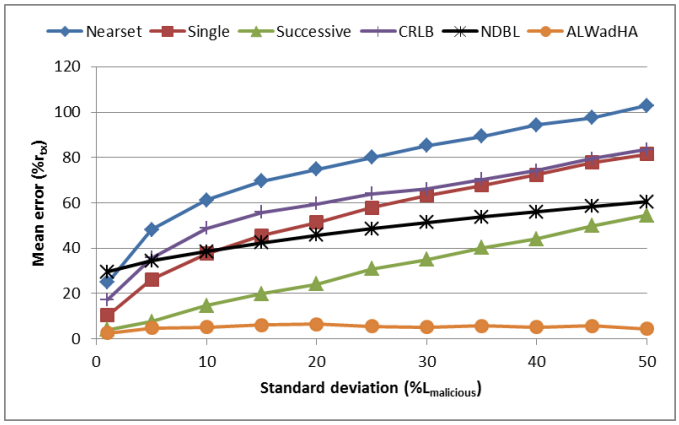

Fig. 5. Location estimation error, four compromised beacon nodes

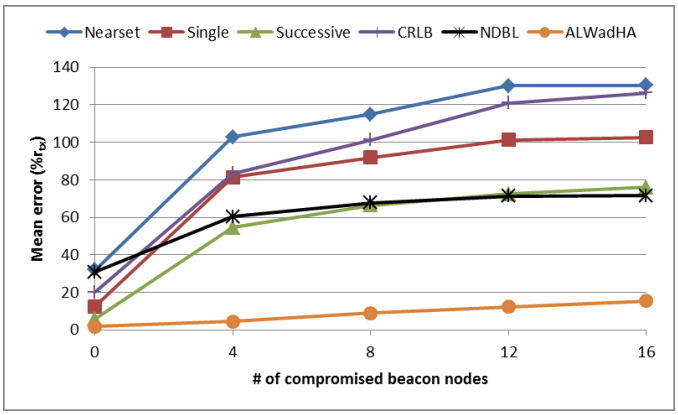

Fig. 6. Location estimation error in the existing of compromised beacon nodes, standard deviation is equal to 50% of $L_{malicious}$

In the last two experiments, the mean error of location estimation using ALWadHA is much less than that achieved by the other localisation algorithms. For example, Fig. 6 shows that, in spite of there being 16 compromised beacons, which outnumber the existing benign beacons, the mean error of location estimation using ALWadHA algorithm is only 15.39% of the transmission range, while for NDBL, Successive, Single, CRLB, Nearest it is 71.51%, 75.95%, 102.58%, 126.47% and 130.30% of the transmission range respectively.

V. CONCLUSION

This paper investigates the security of ALWadHA algorithm which uses a robust position computation technique that tolerates the existence of malicious nodes. The attack resistance of the ALWadHA algorithm was investigated simulating two types of attack. In the first type an attacker pretended to be an honest reference node, while in the second type an attacker compromised a beacon node. In both types of attack, the attacker sent incorrect location information to neighbouring nodes to mislead them in their location estimations. Simulation results showed that ALWadHA is able to determine the location of nodes where malicious nodes exist without undermining accuracy. Moreover, increasing the advertised location erroneousness of these malicious nodes makes it easier to detect these nodes and prevent them from taking part in the position computation. The security of ALWadHA will be investigated using WSN testbed [20, 21] and real sensor nodes [22] to emphasise the simulation results.

REFERENCES

[1] A. Boukerche, H. Oliveira, E. F. Nakamura and A. A. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Communications Magazine*, vol. 46, pp. 96-101, 2008.

[2] A. M. Abu-Mahfouz and G. P. Hancke, "Distance bounding: A practical security solution for real-time location systems ?" *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 16-27. 2012.

[3] A. M. Abu-Mahfouz and G. P. Hancke, "An efficient distributed localization algorithm for wireless sensor networks: Based on smart reference-selection method," *International Journal of Sensor Networks*, vol. 13, no. 2, pp. 94-111, 2013.

[4] L. Loukas and P. Radha, "HiRLoc: High-resolution robust localization for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 233-246. 2006.

[5] Y. Zeng, S. Zhang, S. Guo and X. Li, "Secure hop-count based localization in wireless sensor networks," in *Proceedings of the International Conference on Computational Intelligence and Security — CIS '07*, December 15-19, Harbin, Heilongjiang, China, 2008, pp. 907-911.

[6] S. Capkun and J. P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies — INFOCOM '05*, March 13-17, Miami, Florida, USA, vol. 3, 2005, pp. 1917-1928.

[7] A. Srinivasan, J. Wu and J. Teitelbaum, "Distributed reputation-based secure localization in sensor networks," *Journal of Autonomic and Trusted Computing*, 2008.

[8] S. Zhong, M. Jadliwala, S. Upadhyaya and C. Qiao, "Towards a theory of robust localization against malicious beacon nodes," in *Proceedings of the 27th IEEE Conference on Computer Communications — INFOCOM '08*, April 13-18, Phoenix, AZ, USA, 2008, pp. 1391-1399.

[9] S. Misra, G. Xue and S. Bhardwaj, "Secure and robust localization in a wireless ad hoc environment," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1480-1489. 2009.

[10] D. Liu, P. Ning, A. Liu, C. Wang and W. K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Transactions on Information and System Security*, vol. 11, no. 4, 2008.

[11] Y. Wei, Z. Yu and Y. Guan, "Location verification algorithms for wireless sensor networks," in *Proceedings of the 27th International Conference on Distributed Computing Systems — ICDCS '07*, June 25-27, Toronto, Canada, 2007, pp. 70-77.

[12] E. Ekici, S. Vural, J. McNair and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," *Ad Hoc Networks*, vol. 6, no. 2, pp. 195-209. 2008.

[13] J. Hwang, T. He and Y. Kim, "Detecting phantom nodes in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications — INFOCOM '07*, May 06-12, Anchorage, AK, USA, 2007, pp. 2391-2395.

[14] A. M. Abu-Mahfouz, "Localisation system in wireless sensor networks using ns-2," , 2012 .

[15] A. M. Abu-Mahfouz, G. P. Hancke and S. J. Isaac, "Positioning system in wireless sensor networks using NS-2," *Software Engineering*, vol. 2, no. 4, pp. 91-100. 2012.

[16] A. M. Abu-Mahfouz and G. P. Hancke, "Ns-2 extension to simulate localization system in wireless sensor networks," in *Proceedings of the IEEE AFRICON 2011 Conference*, 13-15 September, Livingstone, Zambia, 2011, pp. 1-7.

[17] K. Y. Cheng, V. Tam and K. S. Lui, "Improving aps with anchor selection in anisotropic sensor networks," in *Proceedings of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services — ICAS-ICNS '05*, October 23-28, Papeete, Tahiti, 2005, pp. 49-54.

[18] D. Lieckfeldt, J. You and D. Timmermann, "An algorithm for distributed beacon selection," in *Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communication — PerCom '08*, March 17-21, Hong Kong, China, 2008, pp. 318-323.

[19] S. Han, S. Lee, S. Lee, J. Park and S. Park, "Node distribution-based localization for large-scale wireless sensor networks," *Wireless Networks*, vol. 16, no. 5, pp. 1389-1406. 2010.

[20] A. Dludla, A.M. Abu-Mahfouz, C.P. Kruger, and S.J. Isaac, "Wireless Sensor Networks TestBed: ASNTbed," in *Proceeding of the IST-Africa 2013 Conference*, 29-31 May, Nairobi, Kenya, 2013, pp. 1-10.

[21] A.M. Abu-Mahfouz, L.P. Steyn, S.J. Isaac and G.P. Hancke, "Multi-level Infrastructure of Interconnected Testbeds of Large Scale Wireless Sensor Network (MI2T-WSN)," in *Proceedings of the International Conference on Wireless Networks — ICWN '12*, 16–19 July, Las Vegas, Nevada, USA, 2012, pp. 445-450.

[22] C.P. Kruger, A.M. Abu-Mahfouz and S.J. Isaac, "Modulo: A modular sensor network node optimised for research and product development," in *Proceedings of the IST-Africa 2013 Conference*, 29-31 May, Nairobi, Kenya, 2013, pp. 1-9.