Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 126327, 10 pages
http://dx.doi.org/10.1155/2013/126327

Research Article

Secure Actor Directed Localization in Wireless Sensor and Actor Networks

Tamleek Ali,[1] Muazzam A. Khan,[2] Amir Hayat,[3] Masoom Alam,[3] and Muhammad Ali[1]

[1] *Institute of Management Sciences, Peshawar, Pakistan*
[2] *E&ME College, National University of Science and Technology, Islamabad, Pakistan*
[3] *COMSATS Institute of Information Technology, Islamabad, Pakistan*

Correspondence should be addressed to Masoom Alam; masoom.alam@gmail.com

Received 25 January 2013; Accepted 12 April 2013

Academic Editor: Muhammad Khurram Khan

Wireless sensor and actor networks are fully automated. Actor nodes are inducted to communicate with sensor nodes directly and reduce the communication delay caused by base station or sink nodes. Sometimes, the actor node is directly accessible without the involvement of any control room. The actor node is responsible for taking a prompt action against the reported event by a sensor node. For secure communication, it is essential that sensor and actor nodes be aware of their existing location and the data must be encrypted before transmission. Due to energy constraints, secure localization in wireless sensor networks is a hot issue. To date, the researchers have proposed many approaches for localization of sensor nodes in the network. In this paper, we provide new insights for secure actor directed localization technique in wireless sensor and actor networks. A secure connectivity based localization (CBL) approach for sensor and actor nodes localization is presented. The proposed approach helps to locate a sensor node efficiently and effectively. We have also decreased the possibility of attacks and the registration of attacker nodes with other legitimate nodes in the network. The proposed technique prevents man-in-the-middle attacks and securely delivers data to the destination.

1. Introduction

Wireless sensor network (WSN) is a collection of different sensor nodes which sense certain information from its surrounding and transfer it for further processing to one or more interested nodes called sinks. A number of WSN applications have emerged to observe an abnormal activity in the sensor's deployment area, such as military movement in a battlefield, sensing environmental changes, and health monitoring. In some applications, sending the state information only to a single node is not sufficient such as bomb blast and earth quake. Therefore, it is imperative to report to a group of nodes about the sensed events/data [1]. Due to resource limitations, sensor nodes usually adopt a multihop communication paradigm in which packets are passed to the destination through multiple intermediate nodes.

It is also sometimes necessary to respond to the sensed events/data by performing corresponding actions in that environment. For instance, in a fire handling system, the actors need to turn the water sprinklers on after receiving a report of fire. This leads to the emergence of wireless sensor actor networks (WSANs) [1, 2], which are a substantial extension of sensor networks, involving coexistence of sensors and actors in the same network. Thus, wireless sensor and actor networks (WSANs) are realized to enable the application to sense, interact, and change the physical world, for example, to monitor and manipulate the temperature and lighting in a specific area or the speed and direction of a mobile robot. It is envisioned that WSANs will be one of the most critical technologies for building the network infrastructure of future cyberphysical systems [3–5].

A WSAN is a networked system of geographically distributed sensor and actor nodes that are interconnected through wireless links. On receiving the required information, the actors make the decision about how to react to this information and perform corresponding actions to change the behavior of the physical environment. Sometimes there may be a base station which is responsible for monitoring and

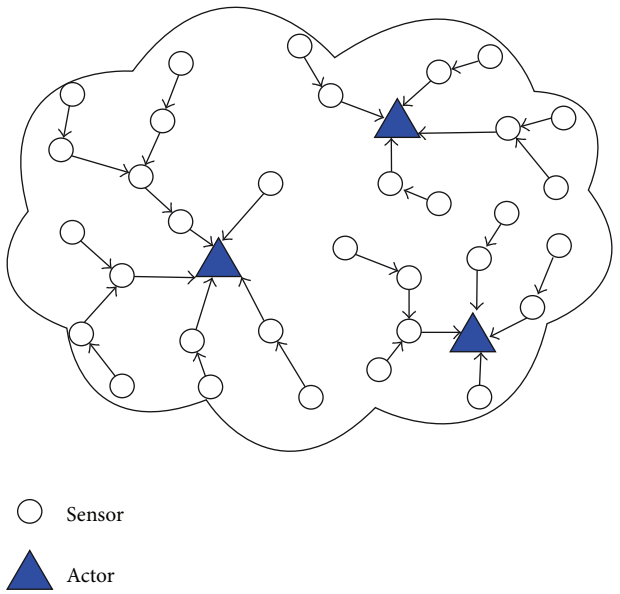

Figure 1: Wireless sensor and actor network.

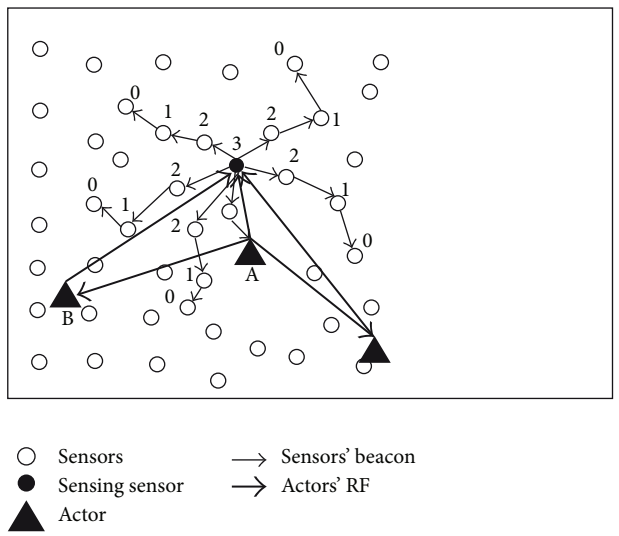

Figure 2: Actor sensor communication for localization.

managing the overall network through communications with sensors and actors. Figure 1 shows a view of wireless sensor actor network without any centralized control from a base station, but in most of the cases, there is a base station. For example, in case of fire anywhere in the network, the actor needs to turn on the water sprinkler to control the fire.

A WSAN can also monitor and manipulate the temperature and lighting in a smart office. In case of mobile robots, the actor may be able to change the velocity and direction of a mobile robot when there is any danger in a certain area [6]. Sensor nodes are generally stationary, whereas actors are mobile, for example, mobile robots and aerial vehicles. Figure 2 shows a typical scenario of actor sensor communication for localization where normal sensors are shown with their distances from sensing sensors. Sensors gather information about the state of the physical world and transmit the collected data to actors through single hop or multihop communication. On receiving the required information, actors make the decision about how to react to the event and trigger corresponding actions [7, 8].

Secure data delivery to actor nodes is very important for taking a prompt action at the right time and the right position. For data security, many encryption algorithms are proposed by researchers. These algorithms can be broadly divided into two types known as symmetric and asymmetric algorithms. In asymmetric cryptographic algorithms, two types of keys are used. Public key is used to encrypt data at the source node, while private key is used to decrypt data at the destination node. In symmetric cryptographic algorithms, there is a single key used for encryption and decryption. Both source and destination nodes should agree on that key in the start of communication. Therefore secure key distribution in symmetric algorithms is very important. Asymmetric algorithms are computationally very expensive as they need more energy and more computational power. Because these algorithms are based on high mathematical functions, they are not a suitable option for wireless sensor nodes which have lower computational power and energy. Keeping the keys secret and strong is very important in these algorithms; in case of using a weak key, the attacker can guess the used key after sniffing few data packets from the network. Once the used key is found, then the attacker can decrypt data, do any alteration, and also reencrypt it [7, 9].

Localization is a process to determine the exact locality of sensor nodes as well as actor nodes in the network. Location information of every node is very important for detection of an event to transfer any information and to record events. In a static network, it is easy to localize sensor nodes; however, in mobile networks as well as in large scale networks, manual localization is not possible. Similarly, to provide the equipment of GPS on each sensor node is quite expensive in terms of cost and energy consumption [10, 11].

The localization algorithms are divided into two categories:

(a) range based,

(b) range free.

In range based algorithms, specialized hardware is used to estimate their distance from seeds. However, range free algorithms do not use any specialized hardware, radio signal strength, angle of signal arrival, or distance measurement. Range free algorithms require that each node knows the nodes inside its radio range, estimated locations, and the ideal range of each sensor node. However, due to insecure communication between sensor and actor nodes, any attacker node can take part in this communication and later on become the legitimate member of the network. To avoid such types of attacks in Khan et al.'s [10] work, we proposed a secure localization technique where sensor and actor nodes will first encrypt their data with an efficient predecided algorithm. This technique will prevent the attacker nodes registration as well as intervention in communication among sensor and actor nodes.

In this paper, we proposed a secure connectivity based approach to localize sensor and actor nodes in the network as well as to prevent the attacker nodes from joining the group and becoming a legitimate node of the network. The proposed localization approach works efficiently in both random and precise deployed sensor nodes. The rest of the paper is organized as follows. Section 2 presents related work with different localization approaches proposed to date in the research community. Section 3 explains our proposed approach in different scenarios (an emergency scenario with normal communication and attacker scenario where an attacker node tried to get registered). Section 4 presents our simulation results and discussion. Section 5 which is the last section of this paper has the conclusion and future work.

2. Related Work

In this section, we discuss the literature survey about localization. We explain different localization protocols proposed by researchers for localization in wireless sensor networks to date. There are two main categories of these protocols: range based, which works in a limited communication range, and the range free approach, which has no such restrictions. These categories are further discussed here.

2.1. Range Free Localization. Range free localization schemes localize the sensor nodes in the network with the help of radio connection information shared with their neighbor nodes or with their ability to sense the environment which each sensor node can do easily. There are many range free approaches for localization; we can divide them into two subcategories on the basis of their characteristics:

(i) anchor based schemes, where some special nodes called anchor nodes are required in the network and have the ability to know their location

(ii) anchor free schemes, where no special anchor nodes are required for localization.

The most important aspect of range free localization is its implementation on simple sensor node instead of high-cost sensor nodes equipped with specialized hardware. Similarly, it has the same drawbacks of range based localization like radio propagation that is area and time dependent, attenuation, interference and multipath propagation causes anchor based localization schemes more costly and expensive.

He et al. [12] in 2009 proposed a new approach to localize a lost node or newly registered node in the network, and it was later improved by Wang and Jin [13]. In this scheme, a new node that is entered or may not be in range initially receives information from its neighbor nodes and then each node is connected with another node to make a triangle; every node checks either it is in a triangle or not to calculate the center of gravity (COG) of the triangle, through which a node is able to estimate its position. APIT also performs better when node placement is random as well as with irregular radio patterns. Teng et al. [14] in 2009 developed mobile beacon assisted localization (MBL) for wireless sensor networks. In this approach, all nodes are unknown and they have no information about their surrounding nodes and their own locations. Initially, for each unknown node, a set of samples is chosen randomly from the whole deployment area. A set of uniformly distrusted samples are used to represent those sets having equal weights. When the weight of a set is equal to 1, it actually represents the importance of that corresponding sample, which estimates the location of the unknown node. The current position of a beacon which may be the initial position is also chosen randomly from the whole deployment area.

Rudafshani and Datta [15] proposed new algorithms for mobile as well as for static wireless sensor networks called MSL and MSL*. Both MSL and MSL* algorithms are able to handle heterogeneous networks in a radio transmission range. MSL* maintains a list of probable locations (samples) as the location information of each node in the network, and then weight is assigned to each sample that estimates its gravity. The weight of a sample is an approximation that represents the true location of a node. In MSL*, communication is the transfer of samples between nodes, and so each node uses the sample of its neighbors for the calculation of its own samples. While in MSL they assign a weight to each node for computation of its own samples, each node uses the weight of nodes in its surrounding. After the computation of weights, MSL is responsible for estimating a single location and a closeness value. Then each node broadcasts its estimated value and closeness to its neighbor nodes.

Ma et al. [16] for the first time proposed a secure localization technique for wireless sensor actor networks (WSANs). These networks are different from simple wireless networks due to nodes heterogeneity. This approach is based on DV-Hop (the most basic scheme which employs a classical distance exchange so that all nodes in the network get distance) and hidden actors, where actor nodes are responsible for locating a sensor node in the networks. The actor node continuously receives authentication messages and minimum hop numbers from sensor nodes, and then the nearest actors collectively compute the location of sensors through actor-actor communication and maximum likelihood estimators MLE (the parameters that maximize the probability (likelihood) of the sample data). Xiao et al. [17] proposed a novel scheme for localization in irregular areas of wireless sensor networks called reliable anchor based localization (RAL). There are three important characteristics of this approach: (i) it uses an average hop length estimation algorithm, which provides tolerance against irregular radio propagation and distortion effects due to many obstacles in an irregular area, (ii) achieves high accuracy due to information received from reliable anchors, and (iii) it introduces virtual anchors. All the anchors are equipped with GPS and have the ability to know their positions. There are four basic steps in RAL: (i) propagation of anchor information in the network, (ii) calculation of average hop length and reliable anchors, (iii) determination of the area of sensors, and (iv) determination of an anchor for sensor.

DRFL uses a cluster based approach for localization of nodes in a wireless sensor network; it was proposed in 2007 by Qiu and Xu [18]. The clustering is a data mining technique which actually separates the studied objects on the basis of

distance from each other into different groups. The clustering technique also helps in security by excluding the bad possible positions of nodes, which improves the localization accuracy. A new distributed localization scheme for wireless sensor networks was proposed by Kuang et al. [19] in 2008 known as VB-ERL. Using this scheme, all nodes in the network are static except for a few nodes which can move from one location to another location. These mobile nodes use virtual beacons to broadcast their location information in the network. Each sensor node receives that beacon and estimates its own location on the basis of received information using the proposed algorithm. Mobile nodes move in the network through Guass Markov mobility model and broadcast their location information in the network.

Shah and Khan [20] proposed a time based localization approach in wireless sensor actor networks. They introduced a new algorithm called timing based mobile sensor localization (TMSL) algorithm, where actor nodes are used for localization of sensors in the network which broadcast beacons after specified intervals, and after receiving that beacon, each sensor node is responsible for using its propagation time and speed of RF signal for the calculation of its distance from actor node. These beacons have certain information like propagation time and actor identity.

2.2. Range Based Localization. Range based localization is hardware dependent. In range based approaches, each node has to estimate its point-to-point distance and angle from its neighbors. In such type of localization, the researchers mostly assume that, from signal strength, the distance between sender and receiver can be estimated or the time of flight of the data from sender to receiver can help in this regard. In contrast to range free approaches for localization which are independent of all these restrictions, here, the sensor nodes are required to be equipped with extra hardware and coordination. Energy consumption is also higher and thus overall cost of the network having a range based localization technique is higher as compared to a range free technique [21]. Han et al. [22] in 2005 proposed an efficient cooperative localization scheme for wireless sensor actor networks. The ECLS scheme is totally dependent on an event in the network because it is an event driven scheme.

The ECLS scheme works on actors' cooperation. In this scheme, the actor nodes use GPS or some other mechanisms to know their real-time location in the network, which is possible, as we have discussed in the introductory part of this paper, because these actor nodes are more powerful and have no energy constraints. After getting its position, the actor node floats its position in the network as a beacon; the mobile actor nodes actually serve as replacements for anchor nodes in the wireless sensor network. Here the lifetime of beacons is defined and every node which receives the beacon reduces it by one and forwards it to its neighbors. When its lifetime gets to 0, any node which receives this beacon will discard it. The nearest actor will receive the beacon and that will directly communicate with other actors to take part in the localization process.

Wang et al. [23] proposed a direction based localization scheme (DLS) for sensor networks. DLS uses multiple beacons to determine the direction of a sensor node. In this scheme, some anchor nodes are also deployed which work as reference nodes. For efficient and precise position measurement, DLS uses a virtual dual direction coordinate (VDDC) system. DLS estimates the direction of each sensor node on the basis of data dissemination and direction of its neighbor nodes in the network. The sink node that lies normally at the center of the network and works as a control center is responsible for originating the localization requests in the network. Therefore, DLS easily and correctly identifies the direction of all sensor nodes that are nearest to the sink node. The sink node initiates the DLS by sending a locating request (LREQ) to all neighbor nodes, and only anchors have the responsibility to send LREQ packets with their directions. However, no sensor node has to do this. When a sensor node receives an LREQ packet from an anchor in the surrounding area, it estimates its direction according to the direction information in the LREQ packet and propagates its direction information to the surrounding sensors.

Li et al. [24] in 2008 worked on localization of sensitive service discovery in wireless sensor networks. In iMesh, an information mesh is constructed by a service provider that is actually used as a localized planner structure. For this purpose, a blocking rule is used that is further enhanced with a newly proposed expansion rule. iMesh-A is the basic version of iMesh which only uses the information blocking rule, whereas the complete protocol consisting of the blocking rule and the expansion rule is called iMesh-B. In iMesh-B, the localization information is published by the service provider about all directions in the mesh like east, west, north, and south. The node may receive information from multiple nodes, but it only forwards the information from the closest nodes.

In 2008, Won and Song [25] proposed a new technique for localization, that is, anchor free localization. For this purpose, the authors used a map to map stitching approach. In this approach, the whole network is divided into small subregions that overlap each other and each creates a local map that is further refined through an optional refinement phase which improves the quality of these maps. These local maps are stitched together to form a global map; however, the map stitching order strongly influences the localization performance. Shang et al. [26] used connectivity information for localization of sensor nodes in 2004. Every sensor node is able to know its neighbor nodes which are in its communication range. This approach is based on multidimensional scaling (MDS). MDS is a data analysis approach that transforms proximity information into geometric embedding and takes advantage of distance information between nodes that have yet to be localized. MDS is very suitable for communication networks where localization of nodes is done through distance information among different nodes using their coordinates in two-dimensional and three-dimensional areas. There are two major parts of this approach: (i) MDS-MAP(C) that constructs a global map for localization in the network and (ii) MDS-MAP(P) that constructs many small maps throughout the network and then combines them

together into a global map. There are three basic steps which started with local distance measurement: (i) measure the shortest path distance of each node with other nodes, (ii) derive nodes' coordinates using MDS, and (iii) normalize the resulting coordinates to take into account any nodes whose positions are known [27, 28].

Lazos et al. [29] address the problem of enabling sensors of WSN to determine their location in an untrusted environment. As localization schemes based on distance estimation are expensive for the resource constrained sensors, they proposed a range independent localization algorithm known as SeRLoc. It was a distributed algorithm and did not require any communication among sensors. Lazos and Poovendran [30] proposed secure and robust localization. They identified the problem of verifying the location claim of a node, known as location verification, in wireless sensor networks (WSNs). Their robust positioning system, called ROPE, enables sensors to determine their location without any centralized computation. It also provides a location verification mechanism that verifies the location claims of the sensors before data collection. Li et al. [31] identified some unconventional security threats, which rather adversely affect the ability of localization schemes to provide trustworthy location information. They identified a list of attacks that were unique to localization algorithms. Since these attacks were diverse in nature and there were some unforeseen attacks, therefore, they could bypass traditional security countermeasures. They developed robust statistical methods to make localization attack tolerant. Their solution worked on two broad classes of localization, that is, triangulation and RF based fingerprinting methods. Liu et al. [32] proposed two methods to tolerate malicious attacks against beacon based location discovery in sensor networks. One method filters out malicious beacon signals on the basis of the "consistency" among multiple beacon signals, while the second method supposedly tolerates malicious beacon signals by adopting an iteratively refined voting scheme. Both methods were authentication independent and provided that the benign beacon signals constitute the majority of the "consistent" beacon signals. Jadliwala et al. [33] proposed secure distance based localization in the presence of cheating beacon nodes in mobile wireless ad hoc and sensor networks. They identified the problem of wrong location estimation and proposed a threshold value above which error free estimation would not be possible. On the bases of these values, they proposed secure localization algorithms. Attacks on the localized mobility are identified in RFC4832 [34]. It identified the impersonation and man-in-the-middle attacks. Wang et al. [35] developed a new landmark selection algorithm with incremental Delaunay refinement method that does not assume any knowledge of the network boundary and runs in a distributed manner to select landmarks incrementally until the global rigidity property is met [36, 37].

3. Emergency Scenarios

In this section, we discuss our proposed scheme for localization in rescue operations after huge destruction where we deploy sensor network. The sensor nodes are uniformly deployed; we assume medium nodes density in the network, where actor nodes play the role of anchors. The proposed scheme works on coordination among actors in the network. We assume two actors (anchors) in the network having greater signal strength, power, and energy as compared to sensor nodes. There are two anchor nodes in the network used for localization of sensor nodes.

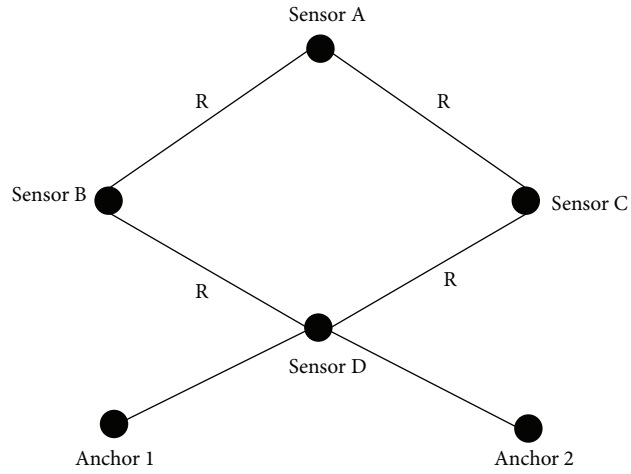

Figure 3: Simulation scenario.

3.1. Example Scenario. Figures 5 and 6 shows the localization scenarios of two and three nodes, respectively. In the first case, the two anchor nodes will flood their location information in the network. The sensor nodes closest to the anchor nodes will receive information from both anchors. The sensor node D will calculate its position on the basis of received information. Sensor nodes at far position will receive that packet through sensor node D, which will increment the packet hop count by 1. Any sensor that will receive the anchor information packet will increment the hop count and every node is able to know its position, neighbor nodes, and its distance from anchor node. If a sensor node receives an information packet from two different anchors it will join the closest anchor node. If the distance for both anchors is the same and no alternative route is available without that sensor node to access other nodes of the network as in Figure 3, then the sensor node will work as a router and forward the node for both anchors.

Figure 3 explains our simulation scenario where many nodes are deployed and they donot know their location. Therefore the initiative step will be taken by the two anchor nodes to broadcast their information and provide a starting point for sensor nodes to compute their position with respect to the anchor [9, 10].

Figure 4 shows the process when node D received information packet from both anchors 1 and 2; as discussed earlier, there is no option without node D to access sensor nodes A, B, and C. Therefore sensor node D will be responsible for forwarding anchor information to other nodes. The process will continue till all of the sensor nodes join the network and know their position as well as the position of anchors.

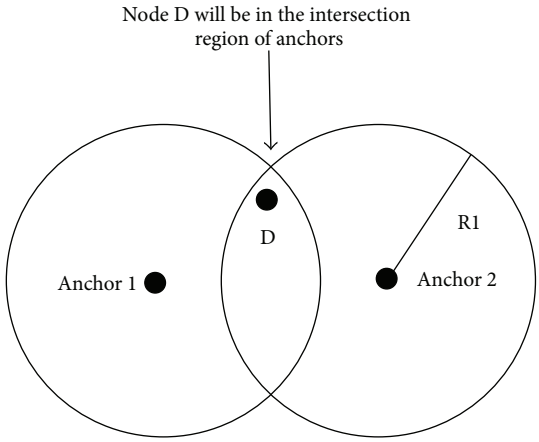

Figure 4: Connectivity of anchors with node D.

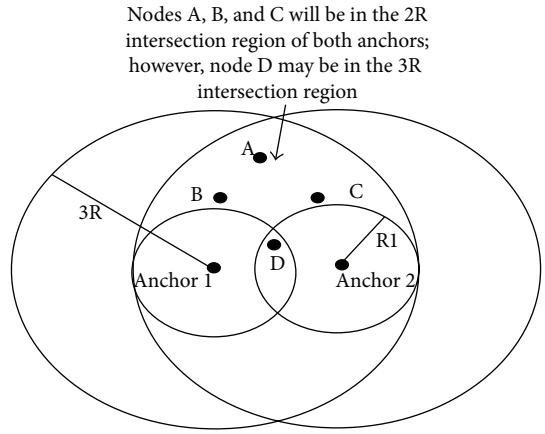

Figure 6: Localization of node A with nodes B and C.

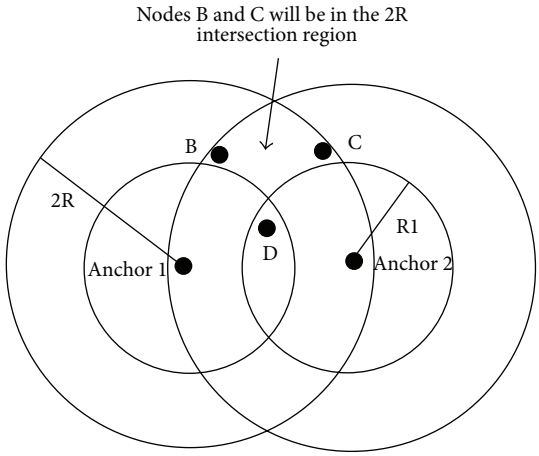

Figure 5: Localization of nodes B and C using node D.

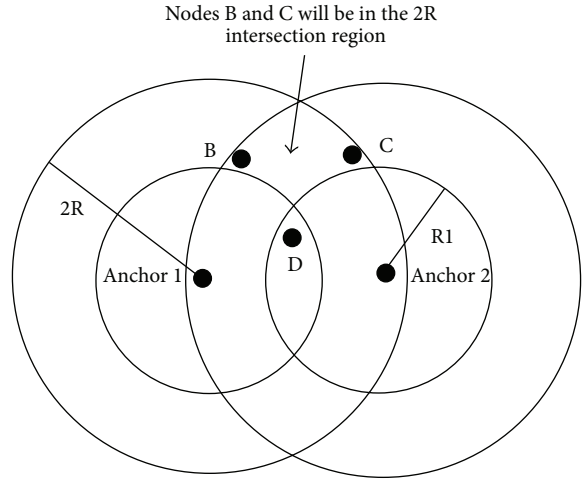

Figure 7: Attacker scenario (node D is the attacker node).

However the drawback of this approach was that many unwanted and attacker nodes could be able to join the network.

3.2. Attacker Scenario. Now we discuss an attacker scenario where the attacker node will send a join request to an anchor node. The anchor node will consider it as a legitimate node and will allow him it communicate and use the network resources because there is no mechanism to authenticate a node or to check the authorization whether the node is trustworthy to join or not. Figure 7 explains a scenario where node D is an attacker node. Due to the absence of any security mechanism in the network, node D gets registered with the anchor nodes and the other nodes in the network also consider node D as a legitimate node and join it as a forwarding/routing node to access anchor nodes.

To prevent the registration of these attackers, we use a symmetric key approach for authorization and authentication of our trusted sensor nodes. Before deployment of anchor and sensor nodes, we should provide them with a predefined key for authentic communication as well as to maintain data integrity and confidentiality. It provides end to end communication security among sensors and anchor nodes. Although this technique is in unable to handle man-in-the-middle attack, therefore, we still need a mechanism for prevention of man-in-the-middle attack. Such type of attacks can misguide our network system; the attacker can inject faulty routes in the routing table and replace the data packets and so forth.

Therefore this technique is not suitable for sensitive regions like atomic reactors and battlefields where man-in-the-middle attack can cause a big destruction. To achieve high level of security, we introduce traditional security mechanism, in which RC-6 algorithm is used for data encryption. As it consumes high energy as compared to symmetric key, however, it also provides high level security. There are many scenarios where we could not compromise security as discussed earlier.

4. Results and Discussion

In this section we discuss probabilities of the location of different nodes using our simulation scenario from Figure 3.

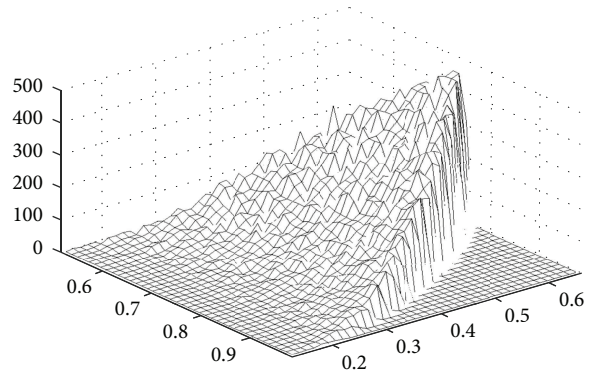

Figure 8: Probabilities for node D location.

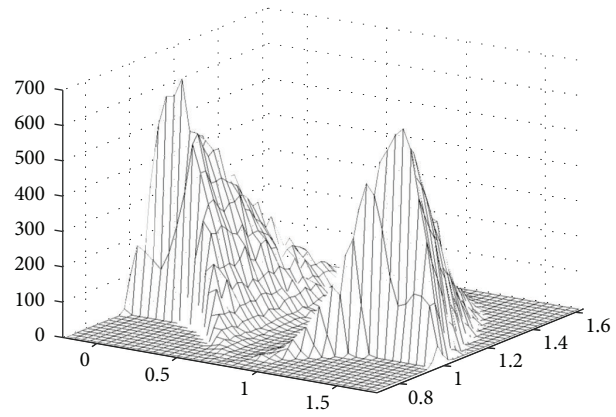

Figure 9: Probabilities for nodes B and C location.

These are found by generating random node locations and finding the frequency with which nodes are located in certain positions when they satisfy the topology constraints.

Figure 8 shows the number of times node D was located in certain positions. If normalized, this could also be viewed as a probability distribution. The probability of node D location increases in an upward direction, depending on the other nodes position as well as anchor nodes. Node D is directly connected with both anchor nodes as well as with nodes B and C.

The probabilities of nodes B and C are shown in Figure 9. We assume that nodes B and C are far away from each other that they are not directly connected. Therefore it is also clear from their probabilities diagram that there is some space between these nodes.

Figure 10 shows the probabilities of node A location in our particular scenario. Node A is directly connected with both nodes B and C; therefore, the graph is denser in the middle as compared to its edges. Figure 10 shows the position of node A that lies in the middle of both anchors 1 and 2. After localization of node D, it helps to localize nodes B and C.

Figure 11 gives another way to view the position of node B on the left side of the diagram and node C on the right side. There is a certain gap between B and C which clarifies that these nodes cannot be so close to each other.

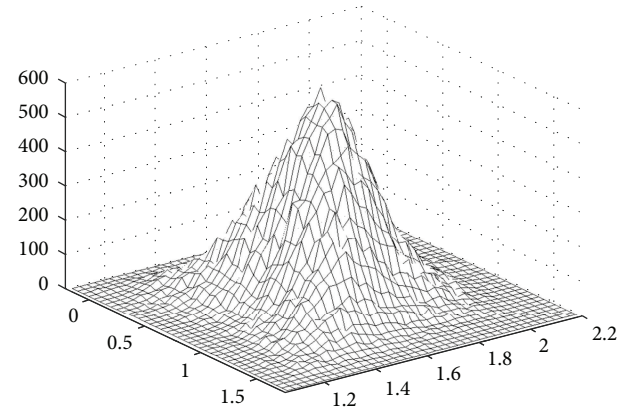

Figure 10: Probabilities for node A location.

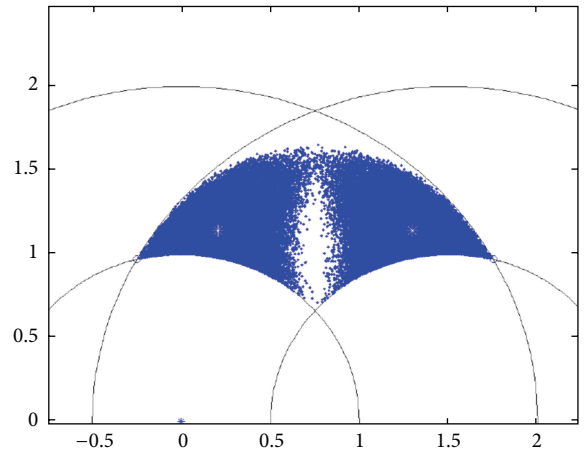

Figure 11: White dots in the middle of the blue area represent the location of node B and node C.

The diagram in Figure 12 explains the positions of both nodes D and A in their particular locations.

The mean and standard deviation (a measure of the dispersion of a set of data from its mean) values for the locations of the nodes are as follows:

Node A: (0.7493, 1.6138) σ = (0.2942, 0.1610),

Node B: (0.2045, 1.1404) σ = (0.1743, 0.1292),

Node C: (1.2949, 1.1404) σ = (0.1743, 0.1292),

Node D: (0.7499, 0.4684) σ = (0.0831, 0.0966).

The results shown above make it clear that actor nodes are very important and the localization procedure starts from actor and then onward responsibilities are shared with other nodes. From our simulation results, it is clear that beacon broadcasting by actors provides a base to sensor nodes for the computation of their position. This approach shifted the computational overhead on the actor node having high resources, and therefore this approach reduces energy consumption as well as increases networks lifetime.

The graph in Figure 13 explains memory requirements for secure approach and nonsecure approach. From the graph it is clear that as we increase the level of security, it also increases

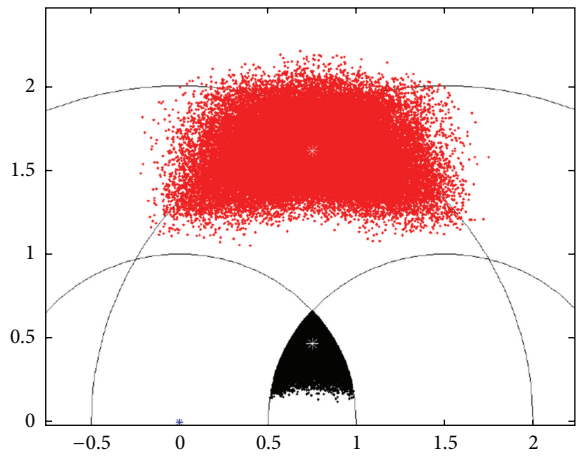

Figure 12: White dots in the middle of the red and black areas represent the location of node A and node D.

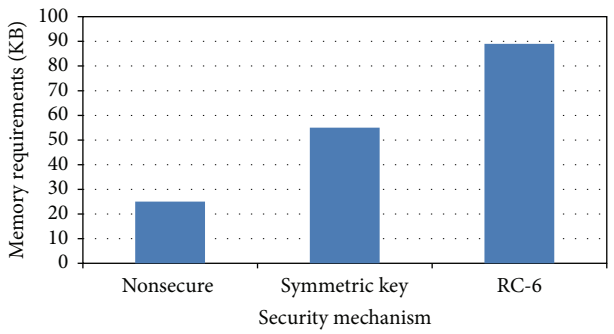

Figure 13: Memory requirements (KB) of different mechanisms.

the memory requirements at sensor nodes. RC-6 provides a high level of security as compared to the other two approaches and that is why it has high memory requirements whereas the other two approaches need lower memory than RC-6.

Figure 14 presents a relationship between compromised sensor nodes and network node density. As long as node density in the network increases, number of compromised sensor nodes also increases. However we can control the number of compromised sensor nodes with the help of a strong security mechanism. RC-6 based security mechanism minimizes the number of compromised sensor nodes in the network, while the other two mechanisms are unable to control compromised sensor nodes and gradually increase with the increase in node density.

The relationship between number of successful attacks and time is shown in Figure 15. As time passes, the attackers are successful in intruding into the network and getting registered with anchor and sensor nodes. However using a good security mechanism can reduce the number of attacks. In Figure 15 the number of successful attacks is very high in nonsecure approach, while induction of security mechanism reduces these attacks. In case of symmetric key, number of attacks is lower and minimized much more using RC-6 based security.

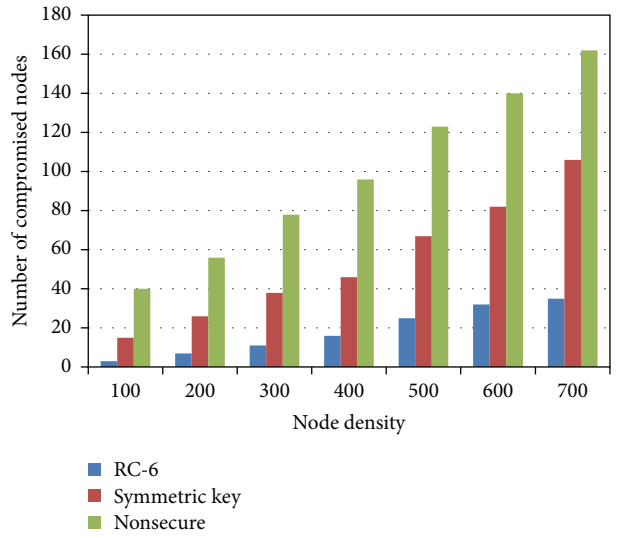

Figure 14: Node density versus number of compromised sensor nodes.

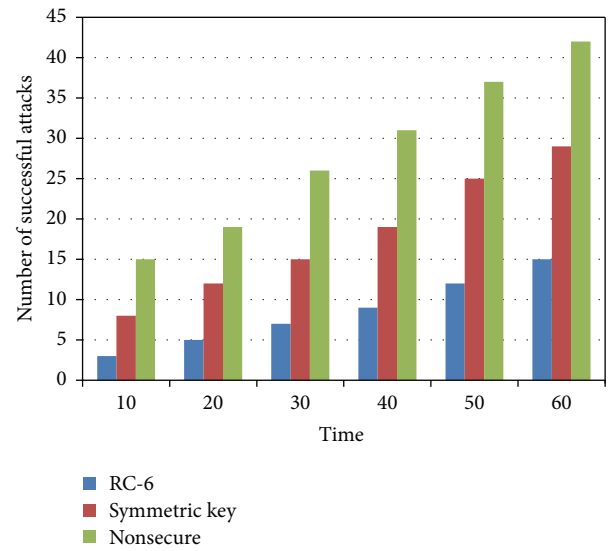

Figure 15: Number of Successful Attacks versus Time.

Figure 16 presents the impact of security mechanism on network lifetime. It is obviously clear that security algorithms increase computational time of sensor nodes and utilize more energy than a normal procedure. Therefore security strength is directly proportional to the network lifetime. High level of security will decrease the network life time because it involves more energy utilization. The graph given here also explains the same relationship; RC-6 provides high level security and it reflects back on the network life. Whereas symmetric and other mechanisms have lower energy consumption, the network life is greater than in RC-6 based networks.

Figure 17 shows a relationship between number of unknown nodes and percentage error. In case of older approaches, ADO and MSL, the percentage error rate is higher than in our proposed approach (CBL). The main

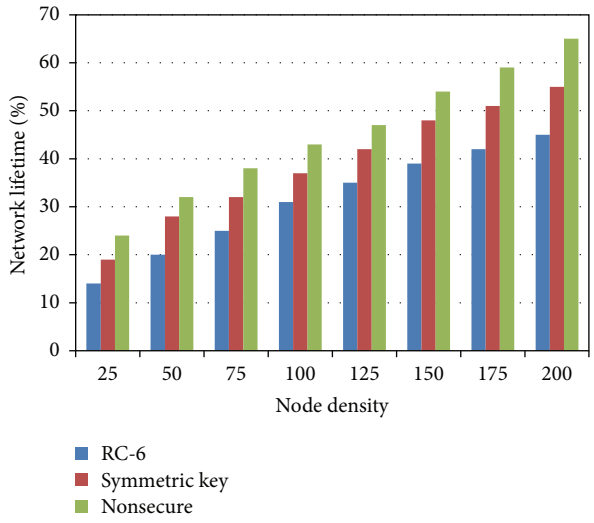

Figure 16: Network lifetime versus node density.

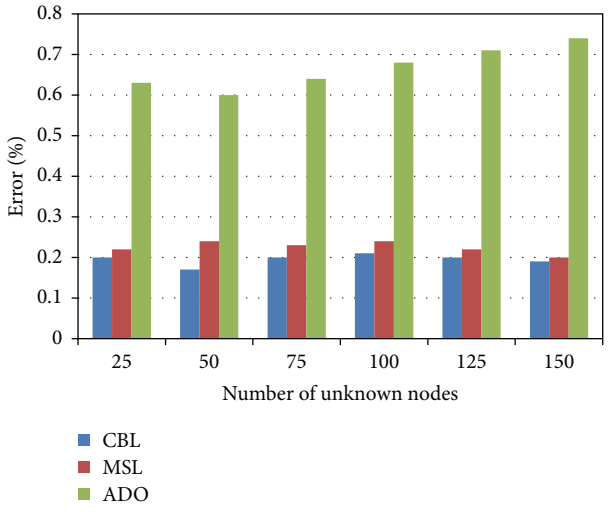

Figure 17: Error due to unknown nodes.

reason is that anchor node is able to track a sensor node due to its high transmission and receiving power than the other two approaches. An anchor node can handle the movement of nodes as well as any hurdle in the transmission.

5. Conclusion and Future Work

In this paper we proposed a secure mechanism for localization of sensor nodes in wireless sensor networks. Using an encryption algorithm for secure data delivery and registration of sensors with anchor node, we effectively minimize and block the external attacks. After simulation results, we conclude that efficient localization in sensor networks can be greatly enhanced by the understanding of both connectivity of sensor nodes and to which nodes they are not connected. The mechanism shows a particular area in which a node can be localized, and we can easily find it there. Once the anchor node locates its own position, the sensor nodes are able to localize each other. This approach is initiated by the anchor node having higher resources than sensor node; therefore, it will reduce energy consumption as well as increase networks lifetime. However the future work is to stop the internal attacks and reduce the number of compromised sensor nodes in the network.

References

[1] F. Xia, W. Zhao, Y. Sun, and Y.-C. Tian, "Fuzzy logic control based QoS management in wireless sensor/actuator networks," *Sensors*, vol. 7, no. 12, pp. 3179–3191, 2007.

[2] F. Xia, Y.-C. Tian, Y. Li, and Y. Sun, "Wireless sensor/actuator network design for mobile control applications," *Sensors*, vol. 7, no. 10, pp. 2157–2173, 2007.

[3] A. Rezgui and M. Eltoweissy, "Service-oriented sensor-actuator networks," *IEEE Communications Magazine*, vol. 45, no. 12, pp. 92–100, 2007.

[4] I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: Research challenges," *Ad Hoc Networks*, vol. 2, no. 4, pp. 351–367, 2004.

[5] "NSF Workshop on Cyber-Physical Systems, Research Motivation techniques and roadmap," October 2006, http://varma.ece.cmu.edu/cps.

[6] M. A. Khan, G. A. Shah, and M. Sher, "A survey of multicast routing in wireless sensor networks," in *Proceedings of International Conference of World Academy of Science, Engineering and Technology Conference*, Amsterdam, The Netherlands, September 2009.

[7] M. A. Khan and A. Salam, "Evaluation of different cryptographic algorithms for wireless sensor and actor networks (WSANs)," *Wulfenia Journal*, vol. 19, no. 10, 2012.

[8] M. A. Khan, A. Rehman, M. Zakaya, and G. A. Shah, "Challenges for security in wireless sensor networks (WSNs)," *Journal of Computing*, vol. 4, no. 9, 2012.

[9] M. A. Khan, C. Beard, and M. Sher, "A comparison of different localization approaches in wireless sensor networks," in *Proceedings of International Conference on Computer Communications and Networks (CCN '10)*, Orlando, Fla, USA, July 2010.

[10] M. A. Khan, M. Sher, and C. Beard, "Connectivity based localization approach for wireless sensor actor networks," in *Proceedings of International Conference on Electrical, Computer, Electronics & Communication Engineering*, pp. 21–24, Penang, Malaysia, February 2011.

[11] M. A. Khan, G. A. Shah, M. Ahsan, and M. Sher, "An efficient and reliable clustering algorithm for wireless sensor actor networks (WSANs)," in *Proceedings of the 53rd IEEE International Midwest Symposium on Circuits and Systems (MWSCAS '10)*, pp. 332–338, August 2010.

[12] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range free localization schemes for large scale sensor networks," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom '03)*, pp. 81–95, San Diego, Calif, USA, September 2003.

[13] J. Wang and H. Jin, "Improvement on APIT localization algorithms for wireless sensor networks," in *Proceedings of International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC '09)*, pp. 719–723, April 2009.

[14] G. Teng, K. Zheng, and W. Dong, "Adapting mobile Beacon-assisted localization in wireless sensor networks," *Sensors*, vol. 9, no. 4, pp. 2760–2779, 2009.

[15] M. Rudafshani and S. Datta, "Localization in wireless sensor networks," in *Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN '07)*, pp. 51–60, Cambridge, Mass, USA, April 2007.

[16] J. Ma, S. Zhang, Y. Zhong, and X. Tong, "SeLoc: secure localization for wireless sensor and actor network," in *Proceedings of International Conference on Mobile Ad Hoc and Sensor Sysetems (MASS '06)*, pp. 864–869, October 2006.

[17] B. Xaio, L. Chen, Q. Xaio, and M. Li, "Reliable anchor based sensor localization in irregular areas," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 60–72, 2009.

[18] M. Qiu and H.-M. Xu, "A distributed range-free localization algorithm based on clustering for wireless sensor networks," in *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '07)*, pp. 2633–2636, September 2007.

[19] X.-H. Kuang, H.-H. Shao, and R. Feng, "New distributed localization scheme for wireless sensor networks," *Acta Automatica Sinica*, vol. 34, no. 3, pp. 344–348, 2008.

[20] G. A. Shah and O. B. Khan, "Timing based mobile sensor localization in wireless sensor actor networks," in *Mobile Networks and Applications*, pp. 664–679, Springer, Amsterdam, The Netherlands, 2010.

[21] A. Savvides, C.-C. Han, and M. B. Strivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01)*, pp. 166–179, July 2001.

[22] P. Han, C. Gao, M. Yang, D. Mao, and B. Yu, "ECLS: an efficient cooperative localization Scheme for wireless sensor and actor networks," in *Proceedings of the 5th International Conference on Computer and Information Technology (CIT '05)*, pp. 396–400, September 2005.

[23] S.-S. Wang, K.-P. Shih, and C.-Y. Chang, "Distributed direction-based localization in wireless sensor networks," *Computer Communications*, vol. 30, no. 6, pp. 1424–1439, 2007.

[24] X. Li, N. Santoro, and I. Stojmenvoic, "Localized distance-sensitive service discovery in wireless sensor networks," in *Proceedings of the 1st International Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and Computing (FOWANC '08)*, Hong Kong, May 2008.

[25] O.-H. Won and H.-J. Song, "Localization through map stitching in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 1, pp. 93–105, 2008.

[26] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz, "Localization from connectivity in sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 11, pp. 961–974, 2004.

[27] B. Xiao, H. K. Chen, and S. G. Zhou, "A walking beacon-assisted localization in wieless sensor networks," in *Proceedings of IEEE International Conference on Communications (ICC '07)*, pp. 3070–3075, Glasgow, Scotland, June 2007.

[28] M. Rudafshani and S. Datta, "Localization in wireless sensor networks," in *Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN '07)*, pp. 51–60, Cambridge, Mass, USA, April 2007.

[29] L. Lazos, R. Poovendran, and S. Čapkun, "ROPE: robust position estimation in wireless sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 324–331, April 2005.

[30] L. Lazos and R. Poovendran, "SeRLoc: secure range-independent localization for wireless sensor networks," in *Proceedings of the ACM Workshop on Wireless Security (WiSe '04)*, pp. 21–30, October 2004.

[31] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 91–98, April 2005.

[32] D. Liu, P. Ning, and W. K. Du, "Attack-resistant location estimation in sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 99–106, April 2005.

[33] M. Jadliwala, S. Zhong, S. Upadhyaya, and C. Qiao, "Secure distance-based localization in the presence of cheating Beacon nodes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 6, pp. 810–823, 2010.

[34] C. Vogt and J. Kempf, "Security threats to network-based localized mobility management (NETLMM)RFC-4832," Network Working Group, Category: Informational, The IETF Trust, April 2007.

[35] Y. Wang, S. Lederer, and J. Gao, "Connectivity-based sensor network localization with incremental delaunay refinement method," in *Proceedings of the 28th Conference on Computer Communications (INFOCOM '09)*, pp. 2401–2409, April 2009.

[36] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[37] M. K. Khan, "Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world," *IETE Technical Review*, vol. 26, no. 3, pp. 191–195, 2009.