Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

7th International Conference
on Electrical Engineering
ICEENG 2010

Secure Localization Model in Wireless Sensor Networks

By

Prof.Dr.Mostafa Sami * Eng. Ashraf Hussein **

Abstract:

Wireless Sensor Networks (WSNs) are the key of gathering the information in a smart environment. This environment could be a building, utilities, an industrial firm, etc. WSNs have an endless list of potential applications in both military and civilian fields. One common feature shared by all of these critical applications, is the vitality of sensor location. Many techniques have been discussed for sensor localization, the simple one is based on using a Global Positioning System (GPS). Yet, it's not a feasible solution from an economic perspective. Therefore, other techniques use the known location beacon (special sensors) (BNs) to help the other sensors (SNs) to compute there location. Secure localization in WSNs has become a major focus for researchers in recent years. Since many intruders exploit the WSNs localization technique. Many secure localization techniques have been implemented, where the most recent one depends on a smart node monitoring to exclude any malicious nodes. This paper proposes an applicable Secure Localization Model (SLM) for excluding malicious BNs to ensure secure localization of SNs, by enabling BNs to monitor their neighbors, establishing a Neighbor Reputation table (NRT), and then publish it as a response of the sensor location requests, so as the SNs can avoid the malicious BNs false location. Our simulation shows that the proposed SLM provides a simple and applicable secure localization model for WSNs.

Keywords:

Wireless sensor networks, Beacon, Malicious, Secure Localization.

---

* Computer Science Department - Helwan University
** Egyptian Armed Forces

1. Introduction:

WSN is composed of a large number of sensor nodes, which are densely deployed either inside or close to a phenomenon, distributed randomly, have Self-organizing, cooperative capabilities, prone to failures, topology changes frequently[1, 2], mainly use broadcast communication, limited in power, computational memory capacities, may not have global identification (ID), and limited cost for each node[3, 4].

WSNs have attracted a lot of attention recently due to their broad applications in both military and civilian operations. The core function of a WSN is to detect and report events which can only be meaningfully assimilated and responded to, if the accurate location of the event is known. This helps in: identify the location of an event of interest, location awareness facilitates numerous application services [5, 6], and location information can assist in various system functionalities, (geographical routing, network coverage checking [7], and location-based information querying).

Location discovery consists of two components: one is the reference points, whose coordinates are known, the other is the spatial relationship between sensors and the references point. For example, in GPS, satellites are the reference points, and the time of arrival reveals the relationship between receiver and the satellites. In general, there are two kinds of localization based on the actor performing position computation. The centralized localization techniques, where sensor nodes transmit data to a central location, and computation are performed to determine the location of each node. On the other side, distributed localization methods rely on each node determining its location with only limited communication with nearby nodes. There are two subtype techniques in the distributed localization; Range-based approaches exploit Time of Arrival (TOA), Received Signal Strength Indicator (RSSI), Time Difference of Arrival (TDOA) and Angle of Arrival (AOA) to determine the distance and direction of the sensor nodes from the reference points, which is called Beacon Nodes. A range-free localization algorithm depends on the connectivity of the reference points, which is called Seeds. The connectivity parameters are denoted in the content of received messages. Solution of this type is well known as beacon less solution [8]. Many WSNs are deployed in unattended and often hostile environments such as military and border security operations. Therefore, this would allow an adversary to launch attacks from inside the system, bypassing encryption and password security systems, as the adversary would have access to all the information hold in the compromised node.

The secure localization problem has been extensively studied in wireless networks, but the idea of BNs creates a new challenge. These BNs are capable of determining their location and then providing this information to other SNs lacking this ability, but SNs can’t determine which BNs are being truthful. A future WSN is expected to consist of numerous of SNs. We proposed an applicable Secure Localization Model (SLM) for excluding malicious BNs to ensure secure localization of SNs, by enabling BNs to monitor their neighbors, building NRT then publish it as a response of sensor location requests so SNs can avoid the malicious BNs false location. Our simulation shows that

the proposed SLM provides a simple and applicable secure localization model for WSNs.The Paper is organized in six sections: Section 2 presents related work. Section 3 proposes SLM. Section 4 demonstrates simulation of SLM. Section 5 analyzes Simulation Results. We end our paper with the conclusion and future work.

2. Related work

Secure localization in WSN attracts a lot of researcher in last few years. Savvides et al [9] and extension was presented in [10] present a novel approach for localization of sensors in an ad-hoc network called Ad-Hoc Localization System (AHLoS) that enables SNs to discover their locations using set distributed iterative algorithms.

Lazos et al [11] have addressed the problem of enabling sensors of WSNs to determine their location in an un-trusted environment and have proposed a range independent localization algorithm called SeRLoc. SeRLoc is a distributed algorithm and does not require any communication among sensors. Sastry et al [12], introduced the concept of secure location verification, shows how it can be used for location-based access control.

Marti et al [13] present two techniques for improving throughput in ad-hoc networks: a watchdog, which identifies misbehaving nodes (The watchdog system has often been used as the prototypical promiscuous monitoring system in subsequent research), and the other is the path rater, which helps routing protocols to avoid these nodes.

Michiardi et al [14] proposed A COllaborative Reputation mechanism (CORE) using a watchdog with a reputation mechanism to distinguish between subjective, functional and indirect reputation, both of them are weighted to get the combined reputation. Where, nodes exchange only positive reputation information. The authors argue that this prevents a false-negative (badmouthing) attack, but do not address the issue of collusion to create false praise. In CORE, members have to contribute on a continuing basis to remain trusted or they will find their reputation deteriorating until they are excluded.

Buchegger et al [15] have presented CONFIDANT with predetermined trust, and later improved it with an adaptive bayesian reputation and trust system and an enhanced Passive ACKnowledge mechanism (PACK) in [16] and [17] respectively. Mundinger and Boudec [17] have presented a two-dimensional reputation system for protecting the system from liars to ensure cooperation and fairness in mobile ad-hoc networks. This system works based on a simple deviation test, (nodes accept second-hand information only if it does not deviate too much from the node's reputation value).

Ganeriwal et al [18] proposed a reputation-based framework for sensor networks where nodes maintain reputation for other nodes and use it to evaluate their trustworthiness. They show that their framework provides a scalable, diverse and a generalized approach for countering all types of misbehavior resulting from malicious and faulty nodes. Like CORE [14], the authors have chosen only to disseminate positive interactions, in order to block false-negative attacks, but have shown interest in extending their work with a

second metric similar to the one used by Mundinger and Boudec.
Liu et al [19], have presented a suite of techniques that detect malicious beacon signals, identify malicious BNs, avoid false detection, detect replayed beacon signals, and revoke malicious BNs. Their revocation model works on the basis of two counters maintained for each BN, namely Attack Counter (Ac) and Report Counter (Rc). This system is a very simple example of a reputation-based system, in which nodes garner negative reputation for misbehavior.
Avinash Srinivasan et al [20] extended [19] by introducing an algorithm for a reputation-based system depending on a simple deviation test, presented in [17] but they use the location deviation test to build the first hand reputation. The location deviation test count on comparing the calculated location from the transferred location of another BN only, which required at least four receivers in each BN [21]. And since WSN is limited in the node cost and has a very large number of nodes, then we find, from our point of view, that applying the location deviation test is expensive in the WSN case. It is to the best of our knowledge; this algorithm presented in [20] is the recent work addresses the specific BN model with respect to the WSNs.

3. Proposed SLM

Given WSN composed of a large number of SNs and BNs our goal is to give SN the ability of determining the trustful BNs from its neighbors and avoid the malicious BNs, so that the SN can calculate its location depending on correct information. In our proposed model, we will use the deviation test addressed in [17] and the framework algorithm used in [20] with the idea of reputation concept addressed in [19] and the main contribution in this model is using a new approach by making BN behavior monitoring technique that presents the distance deviation test instead of location deviation test used in the previous work [20], so that SLM will be applicable in the WSN. Our SLM will do the same function of the secure localization system addressed in [20], but with a lower hardware complexity needed, (where the node doesn't need more than one receiver, one transmitter, one processing unit with small memory, a power unit and a sensing unit); the matter which minimizes the cost of WSN and enhances the processing. Thus, we expect it to be more robust.
We will propose the SLM under the following assumptions:

- If two nodes are within each other's range, they will communicate without any collision loss or a back-ground noise.
- Location information is not encrypted using a pair-wise key, unlike CORE [14]. We instead assume a network-wide group key for encryption, to allow promiscuous observation in the network, while preventing outsiders from eavesdropping.
- Location information is broadcast to the requesting SN by the BN, unlike

unicasted [14].

- Considering only dense and static networks. A neighborhood can stand up to k malicious BNs only if there are at least 2k + 1 BNs in that neighborhood.

3.1. Reputation

Reputation is formed and updated along time through direct observations and through information provided by other members of the community [14]. In our novel BN behavior monitoring technique, BN makes reputation of its neighbor BNs after comparing the Calculated Distance (CDistbki) between the BN and its neighbor BN from the transferred location and compare it with the Actual Distance (ADistbki) calculated from Received Signal Strength (RSS), as the following distance deviation test in equation (1),(2).

If ($CDistb_{ki}$ - $ADistb_{ki}$) < TH then

$$R_{k,i}^{New} = \mu_1 \times R_{k,i}^{Current} + (1-\mu_1) \quad (1)$$

Else

$$R_{k,i}^{New} = \mu_1 \times R_{k,i}^{Current} \quad (2)$$

Where TH is a threshold that represents the distance deviation accuracy, $\mu 1$ $\mu 2$ and $\mu 3$ is probabilistic value from 0 to1, Rj,i is the reputation value of BN i from BN j point of view and d is the accepted reputation deviation value between two BNs opinion about other BN. By this test BN build the reputation table for its all neighbor within its range, then to update the reputation value, BN will compare between the reputation of its neighbor from his point of view and from its common neighbor point of views as the following deviation test in equation (3),(4).

If $R_{j,i}^{Current} - R_{k,i}^{Current} \leq d$ Then

$$R_{j,i}^{New} = \mu 2 \times R_{j,i}^{Current} + (1-\mu 2) \times R_{k,i}^{Current} \quad (3)$$

Else

$$R_{j,k}^{New} = \mu 3 \times R_{j,k}^{Current} \quad (4)$$

3.2. SLM Notion

The notion of the proposed model aimed to build a distributed reputation table for each BN by providing a method, i.e. BNs can monitor each other and provide information to SNs about its neighbors. SNs can choose which BN to trust, based on a Quorum voting approach. In order to trust a BN's information, a sensor must get votes for its

trustworthiness from at least half of their common neighbors. The following steps will summarize SLM idea:

- When a SN broadcast asking for location information, each BN will respond with a single broadcast.
- The BN respond contains both the reporting location and its reputation values for each of its neighbor BNs.
- Other BNs within the 1-hop neighborhood will evaluate these findings and update the reputation then send it to SN.
- The SNs will also receive these reports and use them to form an opinion of their neighborhood.
- When SN receives trust from one neighbor of BN it counts that as a positive vote. If the positive votes exceed the half of the neighbor BNs number the sensor trust these BN. By applying the simple majority (In a neighborhood of n members, when at least (n/2) +1 member has the same opinion it is known as simple major).

Table (1): *Variables Index*

$TBNs_i$	Trusted Beacon Neighbor Table of si
NRTbj	Neighbor Reputation Table of bj
$N(s_i);N(b_j)$	Neighbor Set of si / bj
$C(s_i; b_j)$	Common Neighbor(s) set of (si; bj)
$CDistb_{ki}$	Computed Distance of bki
ADistbki	Actual Distance of bki from RSS
$TLocb_j$	Location Transmitted by bj
$+veb_j$	Votes for bj
$-veb_j$	Votes against bj

In step 2 and step 3 we recognize two classifications of the information available to the reputation system for updating the reputation values.

First classification information: It is the information available by the personal experience or direct observation. A BN overhears location information transmitted by other BNs, in its communication range, in response to a location request. This is regarded as a direct observation. On the other hand, during periods of low network activity, a BN can use its pseudo-sensor IDs to disguise itself as a SN and request location information. This is regarded as a personal experience, as the flowchart in Fig.1.

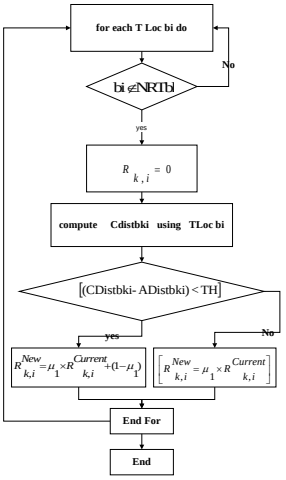

Fig (1): *Reputation initiation*

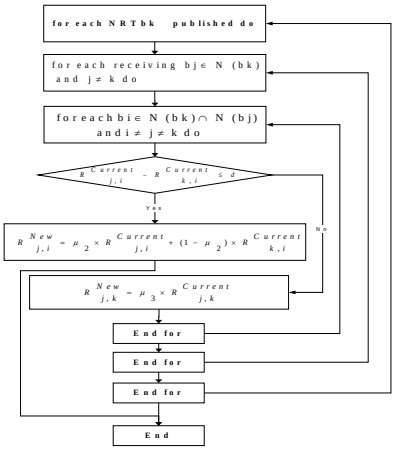

Fig (2): *Reputation update*

Second classification information: It is the information available when peers share their experiences by publishing their gathered reputation information in their 1-hop neighborhood, as flowchart in Fig.2.

By using these two algorithms BNs initiate and update the reputation of their neighbors, Now consider a network setup in which BNs b_i, b_j , and bk are 1-hop neighbors as in Fig 3. To simplify the example, we have considered a SN sA that is within the range of bi but outside of b_j and b_k's range. When sA requests location, bi responds by broadcasting its location $TLocb_i$ and $NRTb_i$.

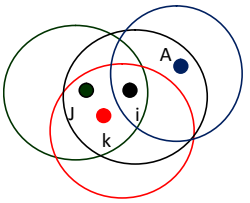

Fig (3): *Bi, Bj and Bk are within each other range but SA in Bi range only*

The SN S_i, on receiving the location information ($TLocb_j$) and $NRTb_j$ broadcast by its beacon neighbor B_j , after a certain time, assumes all BNs have answered and then tabulates the results, S_i first constructs $N(s_i)$ using the following flowchart in Fig.4. Then, for each b_j in $N(S_i)$, it counts the number of $+ve_j$ votes and the number of $-ve_j$ votes, storing them in a table called Trusted Beacon Neighbor (TBN) similar to NRT , notes that TH_{rep} is the threshold of accepted reputation value for the BN to be trusted. Then, finally location information from remaining beacon neighbors is used to calculate its location. Once the location is computed, the TBN is cleared to free up memory since the BNs are already keeping track of long term reputation.

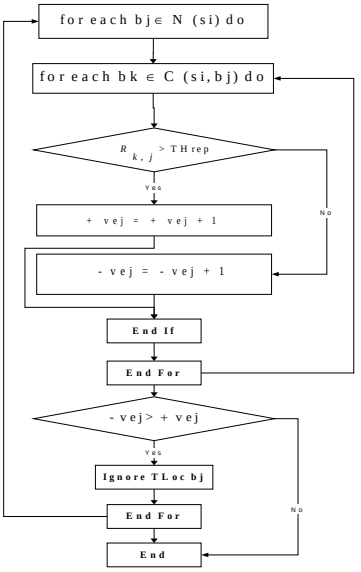

Fig (4): *Sensor Voting Process*

3.3 Mathematical Analysis of SLM

We consider a WSN consisting of n SNs s1, s2,..,sn and m BNs b1, b2,…., bm. We model the network as an undirected graph G = (V, E), with the set of vertices V = v1 ∪ v2, with v1 being the set of SNs and v2 being the set of BNs. E is the set of edges. An edge exists between any two nodes that are in each other's communication range.
The set of vertices V = v1 ∪ v2. Here, v1 = {s1, s2,…,sn} and v2 = {b1, b2,…., bm} where n and m are system dependant parameters and represent the number of SNs and BNs respectively. The sensitivity of the system and its performance for different values of n and m has been studied through simulations and results are presented in section 4.now look at how the size of C (sA, bj) affects the performance of the system and the minimum size of C (S_A, b_J) needed to defeat a collusion of k malicious nodes. We know that

$$C(S_A, b_J) = N(S_A) \cap N(b_J) \quad (5)$$

The value of ׀ C (SA, bJ) ׀ determines the limit to which the system is robust against collusion, where N (sA) and N (bj) represent the neighbor set of SN (SA) and BN (bj) respectively and neighbor set refer to the beacon neighbor set as beacon nodes.
For a network with k malicious BNs, the worst case scenario occurs when all the k malicious nodes are in the same neighborhood N (S_A). However, the chance that this scenario occurs is very unlikely. In any event, the system must have, on average, a minimum of 2k beacon nodes in every C (S_A , b_J) for a completely robust system. Therefore, the equations below give the necessary conditions for a robust system:

$$\forall[\, S_A \in v1 \,, b_J \in v2 \,,\, b_J \in N(S_A)\,] \,,\, |\, C(S_A, b_J)\,| = 2k \quad (6)$$

$$\text{Neighborhood}(S_A, b_J) = C(S_A, b_J) \cup b_J = 2k + 1 \quad (7)$$

$$\text{Maximum Malicious Nodes} = \left\lfloor \frac{|C(SA,bJ)|}{2} \right\rfloor = k \quad (8)$$

$$\text{Minimum -ve V otes} \geq \left\lceil \frac{|N\,br\,Hood\,(SA,bJ)|}{2} \right\rceil \quad (9)$$

$$\text{Minimum +ve V otes} \geq \left\lfloor \frac{|N\,br\,Hood\,(SA,bJ)|}{2} \right\rfloor \quad (10)$$

Equation 8 gives the maximum permissible number of malicious nodes in a neighborhood. Equation 9 gives the minimum number of negative votes needed to flag anode as malicious while Equation 10 gives the minimum number of positive votes needed to flag a node as trusted.

There are two scenarios here that we need to analyze. First, if $\lfloor |C(SA,bJ)| \rfloor$ is odd, then there will be no tie between positive and negative votes. But, in the second scenario, when $\lfloor |C(SA,bJ)| \rfloor$ is even, then there can be a tie between the number of positive and negative votes. When there is a tie, however, Equation 10 will always win over Equation 9. This clearly indicates the BN in question is benign and the colluding malicious nodes cannot affect its status since the minimum number of negative votes needed to flag a node as malicious is $\left\lceil \frac{|N\,br\,Hood\,(SA,bJ)|}{2} \right\rceil$ and when $\lfloor |C(SA,bJ)| \rfloor$ is even it is equal to $\left\lfloor \frac{|C(SA,bJ)|}{2} \right\rfloor$ +1. This, however, is greater than the permissible number of malicious nodes as per Equation 9.

4. Simulation and Results

4.1. Simulation Stages and conditions

We built our own SLM simulation to enable us achieving the following stages:

First, study area selection stage, which covers a subset of IKONOS satellite image with its real UTM, coordinates in Egypt, Cairo, with limits of 500 m × 500 m. *Second*, nodes distribution stage, to distribute the WSN nodes randomly with predetermined number of nodes for each trial. *Third*, throat initiation stage, by randomly chooses malicious BN and changes their behavior to act as a malicious. *Fourth*, reputation initiation stage, by building reputation table for each beacon then updates these reputations on three options: Single reputation update (on BN demand), Total reputation update and sensor neighbor's reputation update. *Fifth*, sensor voting stage, where the sensor performs the voting process then collects the WSN analyzing information.

Experiments test the following trials conditions:

- Effect of varying the total number of SNs + BNs on the Avg. No. of BN Neighbors for SN with different SN: BN ratios (50:50, 70:30, and 80:20) for different SN and BN ranges (15, 25, 35, and 45) meter. These ranges represent the different wireless data transmission technologies now exist such as, UWB (Ultra Wide Band),

Bluetooth, ZigBee, and Wireless USB (Universal Serial Bus).

- Effect of varying Malicious BN percentage on Trusted BN percentage In Neighbors with different SN: BN ratios (50:50, 70:30, and 80:20) for different SN and BN ranges (15, 25, 35, and 45) meter.

4.2. Simulation Results

Situation no.1 shows the effect of varying the total number of SNs + BNs on Avg. No. of BN Neighbors for SN with SN: BN Ratio 50:50 as in the graph Fig.5.

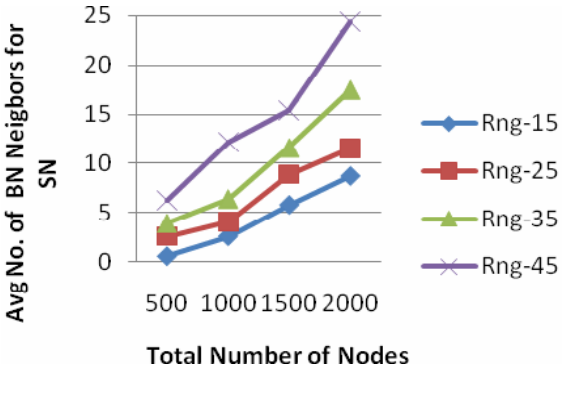

Fig (5): *Effect of varying the total number of SNs + BNs on Avg. No. of BN Neighbours for SN with SN: BN Ratio 50:50*

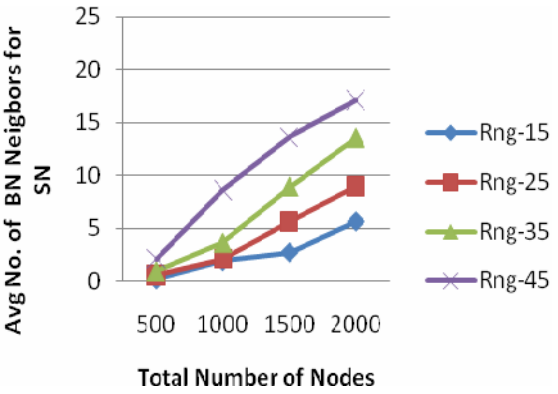

Fig (6): *Effect of varying the total number of SNs + BNs on Avg. No. of BN Neighbours for SN with SN: BN Ratio 70:30*

Situation no.2 shows the effect of varying the total number of SNs + BNs on Avg. No. of BN Neighbors for SN with SN: BN Ratio 70: 30 as in Fig.6. Situation no.3 shows the effect of varying the total number of SNs + BNs on Avg. No. of BN Neighbors for SN with SN: BN Ratio 80: 20 as in Fig.7.

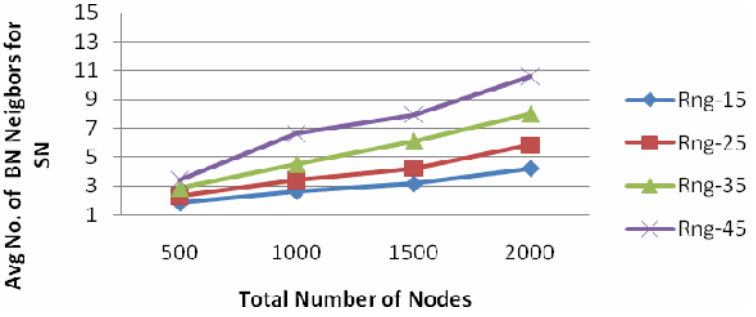

Fig (7): *Effect of varying the total number of SNs + BNs on Avg. No. of BN Neighbors for SN with SN: BN Ratio 80:20*

From the above situations we can notice the following:

- When total nodes number was 1000 nodes and SN: BN ratio was 80:20, the three ranges (25, 35, and 45) meter achieved more than AVG. of 3 BN Neighbors for each SN which makes SN qualified to calculate its location.
- We can recommend 1000 nodes in 500×500 meter^2 as the minimum distribution density for the ranges (25, 35, and 45) meter.
- SN: BN ratio 80:20 considered the minimum hard-ware cost, since the BN cost is higher than SN cost.

Situation no.4 shows the effect of varying Malicious BN % on Trusted BN % In Neighbors with SN: BN ratio 50:50 and 1000 nodes NW as in Fig.8.

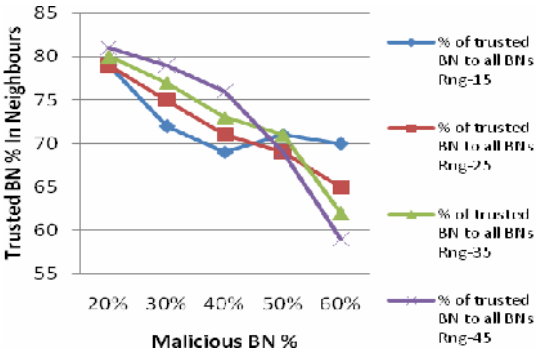

Fig (8): *Effect of varying Malicious BN % on Trusted BN % in Neighbours with SN: BN Ratio 50:50*

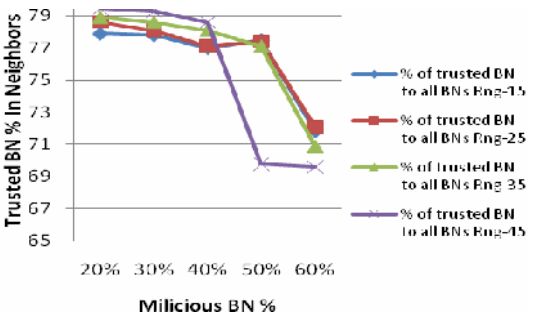

Fig (9): *Effect of varying Malicious BN % on Trusted BN % in Neighbours with SN: BN Ratio 70:3*

Situation no.5 shows the effect of varying Malicious BN % on Trusted BN % In Neighbors with SN: BN ratio 70: 30 as in Fig.9. Situation no.6 shows the effect of varying Malicious BN % on Trusted BN % In Neighbors with SN: BN ratio 80:20 as in Fig.10.

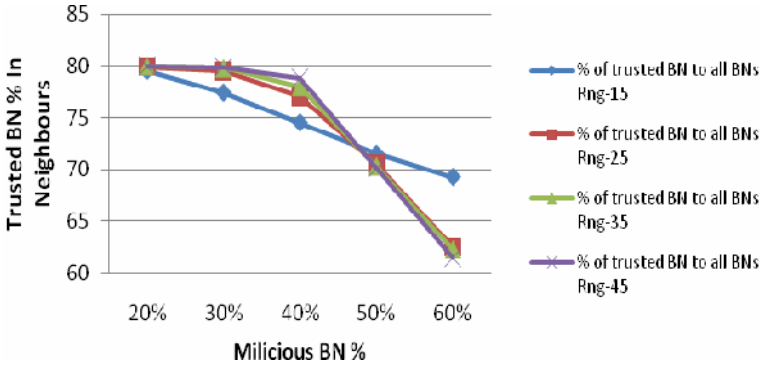

Fig (10): *Effect of varying Malicious BN % on Trusted BN % in Neighbors with SN: BN Ratio 80:20*

From analyzing the previous three graphs we can find the following:

- The WSN with ranges (45, 35) meter can still robust even at 40% malicious BN,

while WSN with ranges (15, 25) meter can still robust at 20% malicious BN.

- After the malicious BN percentage exceed the 50% the NW with range 45 meter lost its localization qualification for all SN: BN ratios.
- The range 25 meter NW can stand up to 50% of malicious BN only when the SN: BN ratio was 70:30 and the NW density was 2000 nodes on 500×500 meter^2.

5. Conclusion and Future Work

This article proposed SLM using a new BN behavior monitoring technique (distance deviation test) provides a simple and applicable secure localization model for WSNs. SLM uses the reputation systems for self-policing, the reputation systems can mitigate the deleterious effects of misbehavior in self-organized networks, which enables the nodes to make informed decisions about their response to the behavior of other nodes. The simulation results show that the SLM verifies the SN location with minimum node specification. Each node has one receiver, transmitter, power unit, sensing unit, processing unit, and a limited memory. This minimum specification reduces power consumption, hardware complexity, and WSN cost. The result analyses concluded that the suitable configuration for robust SLM consists of node density (1/250) node/meter^2 with ratio SN: BN 80:20 using Bluetooth or ZigBee technology (45 meter range). In future work we aim to extend our misbehavior model in order to consider different attacks like location information flooding causing denial of service.

References:

[1] J. C. Navas and T. Imielinski, “Geographic Addressing and Routing”, In Proceedings of MOBICOM ’97, Budapest, Hungary, September 26, 1997.

[2] Y.-B. Ko and N. H. Vaidya. “Location-Aided Routing (LAR) in Mobile Ad Hoc Networks” In the Proceedings of MobiCom ’98, 1998.

[3] B. Karp and H. T. Kung, “Greedy Perimeter Stateless Routing”, In the Proceedings of MobiCom ’00, 2000.

[4] M. Mauve, J.Widmer and H. Hartenstein, “A Survey on Position-Based Routing in Mobile Ad Hoc Networks”, IEEE Network Magazine, 2001.

[5] Y. Yu, R. Govindan, and D. Estrin, “Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks”, Technical Report UCLA/CSD-TR-01-0023, UCLA, Department of Computer Science, May 2001.

[6] Y. Xu, J. Heidemann and D. Estrin, “Geography-Informed Energy Conservation for Ad Hoc Routing”, In Proceedings of MOBICOM ’01, Rome, Italy, July 2001.

[7] T. Yan, T. He, and J. A. Stankovic, “Differentiated Surveillance Service for Sensor Networks”, In Proceeding of First ACM Conference on Embedded Networked Sensor Systems (SenSys ’03), Los Angeles, CA 2003.

[8] Pin Nie, “Location Discovery in Sensor Network”. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology.
[9] A. Savvides, C. Han, and M. Srivastava, “Dynamic fine-grained localization in ad-hoc networks of sensors”, In Proceedings of ACM MobiCom ’01, pages 166-179, July 2001
[10] A. Savvides, H. Park, and M. Srivastava, “The bits and flops of the n-hop multilateration primitive for node localization problems”, In Proceedings of ACM WSNA ’02, September 2002.
[11] L. Lazos and R. Poovendran, “Serloc: Secure range independent localization for wireless sensor networks”, In ACM workshop on Wireless security (ACM WiSe 2004), Philadelphia, PA, October 1 2004.
[12] N. Sastry, U. Shankar, and D.Wagner, “ Secure verification of location claims”, In ACM Workshop on Wireless Security, 2003.
[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “ Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks”, In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000).
[14] P. Michiardi and R. Molva, ”CORE: A COllaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks”, Communication and Multimedia Security, September, 2002.
[15] S. Buchegger and J.-Y. Le Boudec, “ Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks)” Proceedings of MobiHoc 2002, Lausanne, CH, June 2002.
[16] S. Buchegger and J.-Y. Le Boudec,” A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks”, Proceedings of P2PEcon 2004, Harvard University, Cambridge MA, U.S.A., June 2004.
[17] S. Buchegger, C. Tissieres and J.-Y. Le Boudec, “A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks - How Much Can Watchdogs Really Do?.”, Proceedings of IEEE WMCSA 2004, English Lake District, UK, December 2004.
[18] S. Ganeriwal and M. Srivastava, “Reputation-based framework for high integrity sensor networks”, In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN ’04), October 2004 pp. 66-77
[19] D. Liu, P. Ning, and W. Du, ”Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks”, 25th IEEE International Conference on Distributed Computing Systems (ICDCS’05), pp. 609-619, 2005.
[20] Avinash Srinivasan, Jie Wu, and Joshua Teitelbaum, “Distributed Reputation-based Secure Localization in Sensor Networks”, International Journal of Security and Networks, Volume 3, Number 4 / 2008 Pages: 226 – 239.
[21] Neal Patwari, Joshua N.Ash, Spyros Kyperountas et al , ” Locating the Nodes” IEEE Signal Processing Magazine (54) julay 2005.