ADVANCES in NATURAL and APPLIED SCIENCES

ISSN: 1995-0772
EISSN: 1998-1090
2017 January 11(1):pages 1-7

Published BY**AENSI Publication**
http://www.aensiweb.com/ANAS
Open Access Journal

Signature Based Intrusion Detection System for Uwb Wireless Sensor Networks

[1]R. B. Aparnaa and [2]Dr. D. Sridharan

[1]Research Scholar, Department of Electronics and Communication Engineering, Anna University, Chennai, Tamil Nadu, India.
[2]Professor, Department of Electronics and Communication Engineering, Anna University, ChennaiTamilnadu, India.

Received 18 September 2016; Accepted 15January 2017; Available online 29 January 2017

Address For Correspondence:
R.B.Aparnaa. Research Scholar, Department of Electronics and Communication Engineering, Anna University, Chennai, Tamil Nadu, India.

ABSTRACT

Wireless sensor networks (WSNs) sometimes called as Wireless Sensor and Actual Network (WSAN), researchers are more interested in this topic due to its unique characteristics. LAL (Localizability-Aided Localization) based on their localizability treats their nodes differently and positioned in component tree. It also converts all non-localizable in one round. By LAL, the networks can be adjusted as localizable by existing methods. WSNs are always sensitive to different type of attacks and for safeguarding they also require security mechanisms. One solution for the existing safety problem is Intrusion Detection System (IDS). So, a fine-grained approach has been proposed. LAL is used for many sensor and network applications as an implementation technique. Deploying network in real time is not entirely localizable. The existing algorithm, abbreviated as ADLU (Anomaly based Detection and Location attribution), has committed methods for secured cluster formation, efficient cluster member consideration, and periodical re-clustering. The ADLU performance is used in establishing and localizing the intrusions using a rule-based anomaly detection procedure.

KEYWORDS: Wireless sensor networks, Security in UWB WSNs, UWB radio technology, Localizability Aided Localization (LAL),Anomaly-based detection.

INTRODUCTION

Wireless sensor networks (WSNs) are becoming evident as an optimistic technology for extensive sensing, controlling and monitoring home, city and office for wide range of applications. Recent approaches in wireless sensor network have authorized the development of low cost, multifunctional sensors and power which provide broad spectrum when networked wirelessly and also helps in the applications of monitoring, defense, traffic monitoring, etc. The use of mobile nodes and its incremental deployment adds the hardware cost which is not possible in most of the cases. Increasing the ranging capability of sensor nodes is considered to be a suitable and practical way. A recent review article on anomaly detection in WSN by Royer and Toh (1999) focuses on data anomalies, mainly due to security attacks, and the statistical approaches for revealing them. Since their tight coupling is often harsh tophysical environments, WSNs and other networks used in extreme conditions[8] (e.g. in space) are more likely than standard networks to experience anomalies related to connectivity or hardware failures. Perkins and Royer (2002) also focus on detection strategies that target network level or node and data level anomalies.

Paucityof existing strategies is that none of them comprehensively addresses network, node and data level anomalies in WSNs. Basis for this are application-specific design choices in sensor networks that tend to tailor anomalies detection procedure to a family of applications with a given set of limitations and assumptions. The lack of comprehensive anomaly detection procedure for WSNs contributes to slower adoption procedure and

ToCite ThisArticle:R. B. Aparnaa and Dr. D. Sridharan.,Signature Based Intrusion Detection System For Uwb Wireless Sensor Networks.**Advances in Natural and Applied Sciences**. 11(1);Pages: 1-7

more countering in establishing and maintaining these networks. FromaWSN user or operator outlook, it is crucial that a network managementtool embeds the required observation to detect all possible anomaly types,as the network is perceived comprehensively as an intelligent data delivery system. To plan such system-level tools demands a inclusive understanding of all types of WSN anomalies, their likely causes, and their probable solutions. Perkins and Royer (2002) also examines WSN anomalies from a systems outlook, covering anomalies that appear at the network, node and data levels.

Localization potential is necessary in most of the applications of Wireless Sensor Networks (Estimation of location);the data which is sensed is profitless without knowing the precise location from where it is acquired. Also, realization of location playsa vital role for designing protocols to obtain energy efficient routing in wireless sensor networks. Sensor nodes location can be acquired by global positioning systems(GPS) deployment on every sensor node or by positioning the nodes according to the coordinates that are already known at different points. Placing the nodes at the already known positions is not possible because the nodes are scattered randomly in the field in many numbers. The overall cost of deployment will increase at a greater rate if GPS is employed at every node. Hence, localization techniques are employed to find out the position of the nodes depending on the previous location in the network, which is defined as anchor nodes. These nodes get their position information either through GPS or by positioning at places with known coordinates. In places that require global coordinate systems, the anchor nodes find out the position of the sensor nodes in reference to the Global coordinate system and in places that require local coordinate systems, the anchor nodes are found in reference to the local coordinate system. There are many algorithms that exist which estimate the location of the sensor nodes in Wireless Sensor Network.It introduces a simple process for determining anomalies in WSNsfor detection, localization and root cause determinationas explained by Johnson and Matz [3] and Behzad et al (2002). A survey of existing anomaly detection strategies provides guidelines for tailoring new anomaly detection procedures to specific WSN application requirements and also shows their significant design choices,including architecture and user support. The distance to a large number of neighboring nodes can be calculated by enhanced nodes. By strengthening the transmitter power output the received signal strength (RSS) and time of arrival (ToA), the enhancement can be received which is considered as prevailing ranging approaches. The nodes can be localized by increasing the node's transmitting power stage-by-stage and that takes numerous rounds of configuration, communication and data collection in a network.

Problem Statement:

Before considering secure localization problems, it is always essential to take a look at some general concepts used in the localization process. Basically, there are two categories of sensor nodes: unknown and anchor nodes. The network with Unknown nodes has no awareness of their positions and also has no special hardware to acquire the positions. Anchor nodes, else called as beacon nodes, their positions are obtained by physical placement or additional hardware's such as GPS(GlobalPositioningSystem).Hence,unknown nodes can use localization information of fixed nodes to localize themselves. Normally, the localization process can be categorized into two steps: 1) information acquisition and 2) position determination.

An Information acquisition, current localization schemes of WSNs are classified into two categories: range-based ONLY schemes and range-free schemes. For range-based localization strategy, the angleor distancefeatures is evaluated into Time of Arrival(TOA), RSSI (Received Signal Strength Indicator) AOA (Angle of Arrival) and Time Difference on Arrival (TDOA) by Agrawal and Zeng, 2002. For range-free localization strategy, the localization is perceived based on network connectivity or other data, which can be acquired by DV-Hop, Convex Optimization and MDS-MAP.

Related Work:

The WSN is made up of nodes from scarce to several hundreds or even thousands as shown by Deng etal, [5]where each node is connected to one in fine grained recognition: because visual recognition research is clearly focused on two different scenarios; basic level categories (category recognition) or recognizing specific instances developing algorithm for automatically discriminating with only small subtle visual differences(fine grained recognition) as per the description by Marti et al., [9].

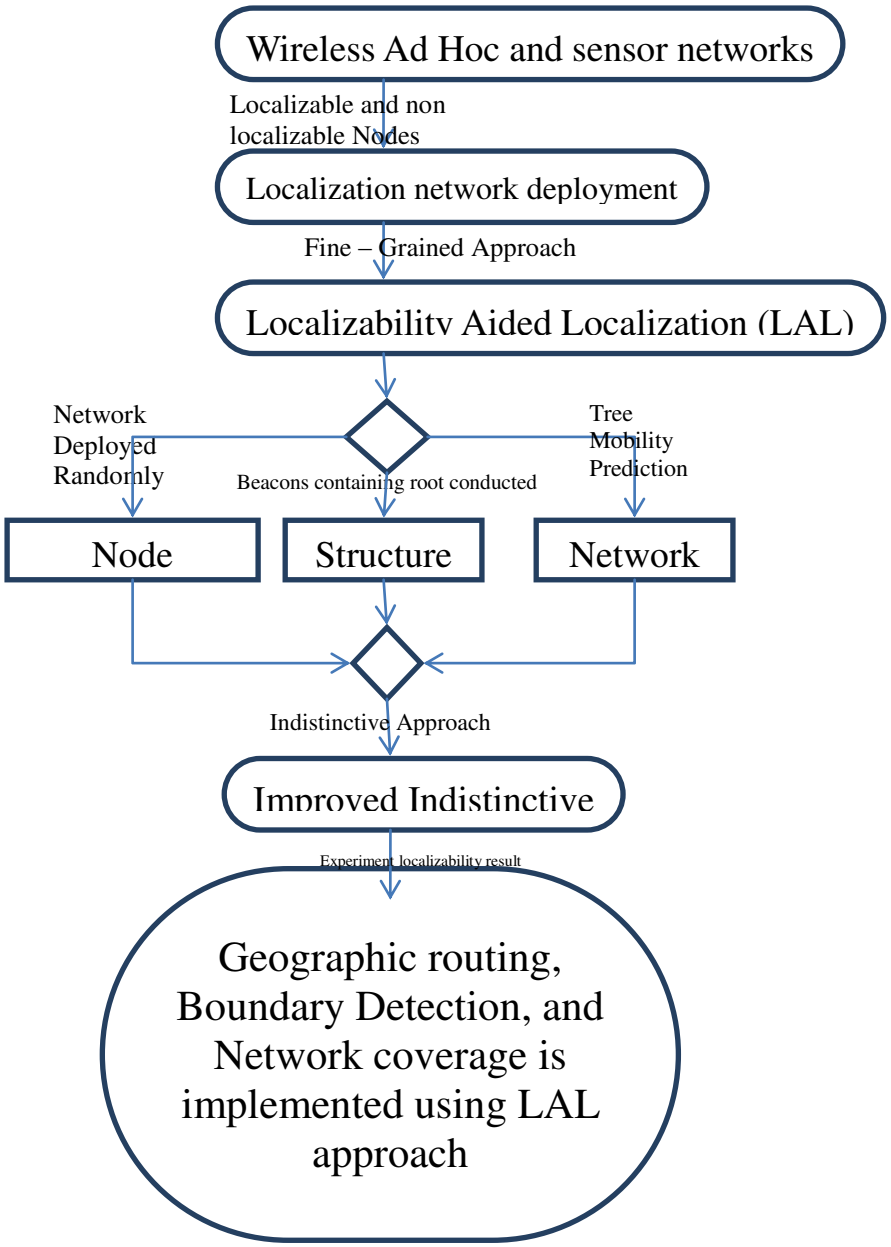

Fig. 1: LAL Protocol design

There are two methodsin localization namely, range-free method and range-based method. The majority of localization algorithms assume a dense network trilateration or multilateration can be organized. Other methods record all possible location in each step and prune the incompatible ones whenever possible. Many of the localization algorithms try to localize as many nodes as possible; however, they are not concerned with the non-localizable part of the network. Due to the existence of non-localizable networks, it leads to the research on location-uniqueness problem Goldenberg et al. has proposed nontrivial necessary condition of location uniqueness for a specific node. Vishnu and Paul, 2010further derive currently the best necessary conditions of node localizability. In recent research, a few works were published on localization for non localizable networks. Pathirana et al. used a mobile robot to localizingnodes. To obtain distance information from robot to anchored nodes RSS data has been used by Seys and Preneel, [10], to reduce the number of beacons which were required to localize a network in a unique manner. However, it requires the exact velocity and acceleration availability of a mobile robot. Sichitiu and Ramadurai used a GPS-equipped mobile node to localize the anchor nodes by measuring its distance between from the mobile node to anchornode.In the paper authored by Johnson and Maltz, [3]. The Difference from the above approaches is that, it uses a mobile node with location information known, Priyantha et al. proposed an approach, which only requires information of distance between mobile node and anchored ones and also Proposed a similar approach by assuming that even each node can move around and the distances can be measuredfrom its neighbors and the relative distances between sequential positions along its trajectory.

System Architecture:

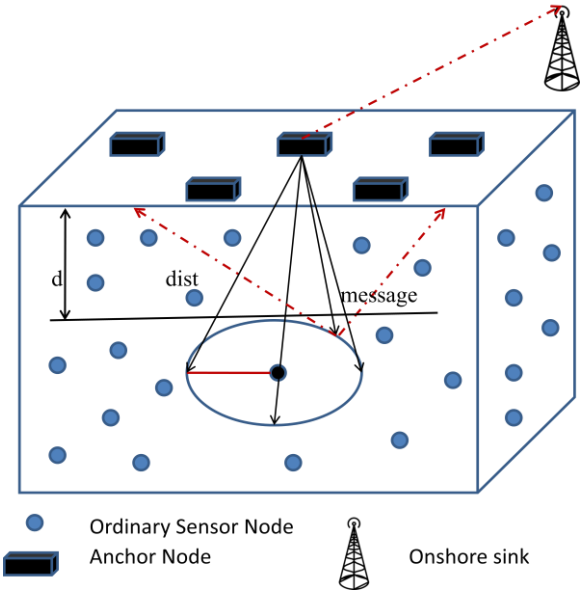

Fig. 2: System architecture

Main theme of the proposed work is to increase the nodes transmitting power stage by stage until all nodes become localizable, Which leads to multiple rounds of configuration diffusion and data collection in a network.

Detection anomaly node behavior in wireless sensor networks:

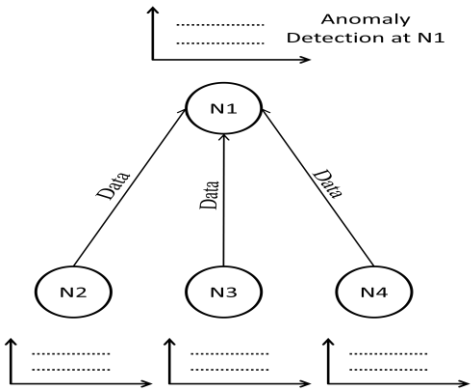

Fig. 3: Detection of anamoly node behavior

When the routing protocol does not use the position information of the mobile node, then it is topology-based routing protocol. If the information of the location is used in the routing protocol, then the routing is location-based routing protocol. There are methods for forwarding data packets in location-based routing: greedy algorithm.

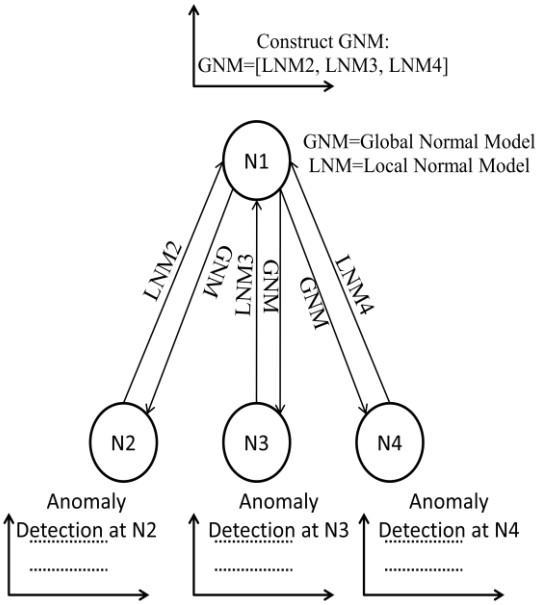

Fig. 4: Anamoly Detection

In greedy forwarding method, the destination node distance is nearby to next hop node. Nodes that are range-free are considered to be non-localized nodes, they are not used for data transmission. Greedy uses information about the location of the mobile nodes to limit the search for an alternative route to a smaller area of the network which results in reduction in the number of routing messages and the consumption of energy of the mobile nodes batteries is decreased significantly.In order to minimize the control overhead due to broadcast uproar in the network when control packets are flooded into entire network addition, simulation results show that there is a tradeoff between decreasing control overhead by extending number of areas and increasing route loss by increasing the number of network areas due to node mobility.

Background:

Wireless Sensor Networks; Security in UWB WSNs; UWB radio technology; Anomaly-based detection; Attack attribution; Ranging attacks

Node localizability testing:

By obtaining the sufficient conditions for node localizability, for the first time, it is possible for the network localizability testing.

Structure analysis:

There aretwo distinguishing themes in our contributions: first our focus will be on fine grained approach and, the second approach developed in our work is structure aware in that we design the inference.

Network Adjustment:

Thescalability limitation in the preceding centralized approaches is overcome. The extensive simulation results show that our approach outperforms the above method in adjustment efficiency.

Anamolies:

WSN anomalies from an intelligent-based system approach, which covers the anomalies that arise at the network, node and data levels. One of the main challenges in WSN anomaly detection is to determine where to embed the intelligence for detecting and localizing anomalies.

Simulation Setup and Results:

NS2 has been used for performance evaluation of the proposed schemes. The simulation has been carried out number of times and average results of simulations are used for performance evaluation. Parameters used for simulation are cited in Table 1.

Table 1: Simulation parameters

Parameter	Value
Number of sensor nodes	25
Number of anchor nodes (for non-cooperative localization)	04

Number of anchor nodes (for cooperative localization)	18
Transmission range of nodes	50 m

Proposed System Analysis:

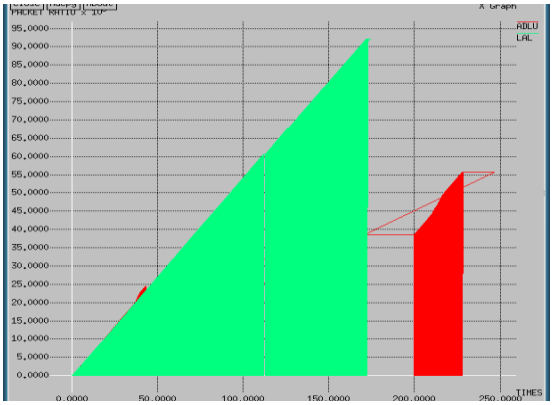

Fig. 5: Throughput

Throughput in the communication networks can be defined as the rate of successful message transmission in the communication channel/medium.

The data may be delivered over a physical or logical link or it can pass through a specific network node. Throughput is generally measured in bits per second, and erratically in data packets per second (p/s or pps) or data packets per slot. In the proposed system it is calculated using LAL protocol (Localization Algorithm applied) the graphs are simulated.

However, the assumption of mobile nodes availability is costly and not scalable, and it also restricts the application of the approach.

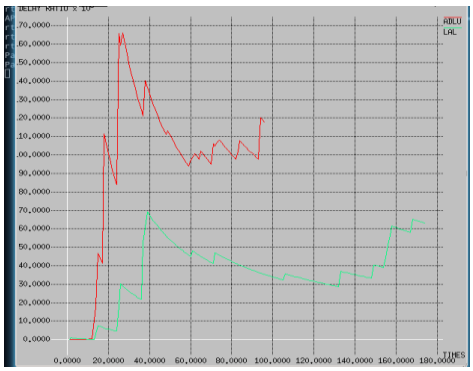

Fig. 6: Delaying Concept

Delay is always defined as the time taken to transmit a packet across a network from source to destination. Hence delay has to be reduced in LAL protocol in order to improve the reliability.

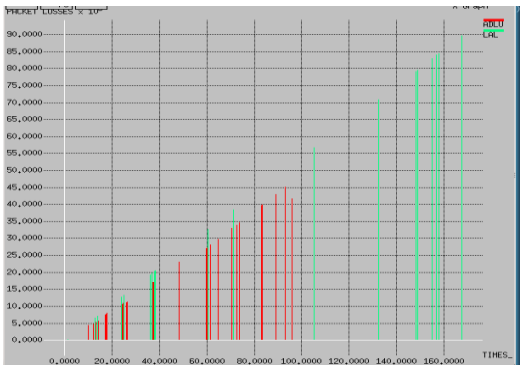

Fig. 7: Loss Properties

Packet loss will happen when data packets travel across a network fail to reach their destination. Packet loss for proposed system is simulated using LAL protocol (Localization Algorithm applied) and their graphs are simulated.

On the other extreme, Anderson et al. proposed a graph manipulation method to assure the network localizability for mobility based approaches. They also recognize graphical properties that assuring unique localizability, and proposed an approach G2 to make the two-connected graph localizable and a G3 approach to obtain a trilateration graph based on a connected graph. These two approaches treat all vertices in the graph as complete, which is more coarse-grained than LAL.

Conclusion:

The results obtained from this paper are compared with the existing techniques through simulations using NS2. The results also show the effectiveness and novelty of the proposed technique compared to the other existing schemes. These techniques require a great number of anchor nodes in the deployment. Higher the number of anchor nodes in the sensor network will increase the accuracy along with the computational cost. Hence, to reduce the computational cost, a collective localization is proposed which also receives the accuracy with less number of anchor nodes. The results thus acquired from this paper prove that the collective localization can be employed for large range localization with proper accuracy and less number of anchor nodes.

LALalways make adjustments according to localizability results of the node, other than that it considers the network as a whole. When a network is deployedon an application environment, due tounpredictable environmental factors in its design phase, it may not be ready for localization. Hence node localizability testing is done in LAL, which identifies the network with localizable and non localizable nodes for further adjustment.The Fuzzy logic will provide the solution of packet loss and data rate against the malicious attack in network. The proposed work will firstly recognize the malicious attack using the fuzzy logic. The fuzzy logic is imposed on packet loss and data rate at time of node communication. This algorithm will provide the better solution. To increase the efficiency root node is used, which could reduce the detection overhead effectively.

Future Work:

The proposed techniques could be used by the nodes to calculate the placement of the nodes and also to find out the data on distances and position. Further, to bridge the gap between the simulation and real time localization, extra research work could be carried out. For example, the physical parameters like interference, obstruction and multiple paths could be addressed to find out the original behavior of the sensor nodes in the wireless sensor network.

REFERENCES

1. Baadache,A. and A. Belmehdi, 2010.“Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks,” Intl. J. Comput. Sci. Inf.Security, 7: 1.
2. Charles, E. Perkins, and Elizabeth M. Royer, 2002.“Ad-hoc On Demand Distance Vector (AODV) Routing”, Book.
3. Johnson,D. and D. Maltz, 1996. “Dynamic source routing in ad hoc wireless networks,” Mobile Comput., pp: 153-181.
4. Elizabeth M. Royer and Chai-Keong Toh, 1999. “A Review of Current Routing Protocols for Ad-Hoc Mobile”.Wireless Networks,”IEEE Personal Communications, pp: 46-55.
5. Deng, H., W. Li and D. Agarwal, 2002. “Routing security in wireless ad hoc network,” IEEE Communication. Mag., 40: 10.
6. Rubin, I., A. Behzad, R. Zhang, H. Luo and E. Caballero, 2002. “TBONE: A mobile backbone protocol for ad hoc wireless networks,” in Proc. IEEE Aerosp. Conf., 6: 2727-2740.
7. Vishnu,K. and A. J Paul, 2010. “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,”Int. J.Comput., 1(22): 28-32.
8. Agrawal,P. and Q.-A. Zeng, 2002. “Introduction to Wireless and Mobile Systems”,Brooks/Cole Publishing, Book.
9. Marti, S., T.J. Giuli, K. Lai, and M.Baker, 2000. “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6thAnnu. Intl. Conf. Mobi Com, pp.
10. Seys, S., B. Preneel, 2009. ARM: Anonymous Routing Protocol for Mobile adhoc Networks,Int. J. Wire. Mob. Comput.,pp: 145-155.
11. Tao Chen, Zheng Yang, Yunhao Liu, Senior, Deke Guo and Xueshan Luo, 2014. “Localization-Oriented Network Adjustment in Wireless Ad Hoc and Sensor Networks”, IEEE TRANSACTIONS DISTRIBUTED SYSTEMS.
12. Whitehouse,K. and D. Culler, 2002. “Calibration as Parameter Estimation in Sensor Networks,” WSNA

'02: Proc. 1st ACM Int'l. Wksp. Wireless Sensor Networks and Apps., ACM Press, pp: 59-67.
13. Akyildiz,F. et al., 2002. "Wireless Sensor Networks: A Survey," Comp. Networks, 38(4): 393-422.
14. Savvides, A., C.-C. Han and M.B. Strivastava,2001. "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," 7th ACM/IEEE Int'l. Conf. Mobile Computing and Networking, Rome, Italy, pp: 166-79.
15. Simic,S. and S. Sastry, 2002. "Distributed localization in wireless ad hoc networks," UC Berkeley, Tech. rep. UCB/ERL M02/26.