ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2015**

# Distance Based Localization and Detection of Scattered Nodes in WNS

B.Somasundaram [1], A.Sathiya Raj [2] , S.Krubakaran [3] , K.Sivagurunathan [4]

U.G. Student, Department of ECE, Dr. SJS Paul Memorial College of Engineering and Technology, Puducherry, India [1]

U.G. Student, Department of ECE, Dr. SJS Paul Memorial College of Engineering and Technology, Puducherry, India[2]

U.G. Student, Department of ECE, Dr. SJS Paul Memorial College of Engineering and Technology, Puducherry, India[3]

Assistant Professor, Department of ECE, Dr. SJS Paul Memorial College of Engineering and Technology, Puducherry, India [4]

**ABSTRACT**: Spoofing attacks are one of the approaching threats in open source networks where the attacks are beyond the scrutinizing range. Spoofing attacks can be localized and based on localization; it can be eradicated such that the spoofer is over whelmed in a particular network coverage region. The previous approaches based on frequency face a storm when the number of data transferred from source to destination is not constant. The TOA fails in examining the exact location of the spoofer. The new approach of DALD (Distance based Attack Localization and Detection) is a counter measure to the spoofing and a methodology to overcome the drawbacks of the existing frequency based approaches.

**KEYWORDS**: Mobile Sensor Navigation, RSS, AOA, DALD

## I. INTRODUCTION

A computer network, often simply referred to as a network, is a collection of computers and devices connected by communications channels that facilitates communications among users and allows users to share resources with other users. In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

The word ad-hoc is highlighted from Latin which means “for this purpose only”. A mobile ad-hoc network is an autonomous network system of routers and hosts connected by wireless links. They can be setup anywhere without any need for external infrastructure like wires or base stations. The routers are free to move randomly and organize themselves arbitrarily. Acronym is MANET. Each device in the network is called an NODE.
Mobile Ad hoc Network (MANET) compromises of a set of wireless devices that can move around freely and cooperate with each other in relaying packets without the support of any fixed infrastructure or centralized administration. Hence they are known as infrastructure less networks.

A mobile node can be laptop computer, personal digital Assistant or a cellular phone. The mobile nodes operate with the help if battery power and they communicate each other through antennas (transceiver – a transmitter and receiver) and the radio waves acts as the medium of communication. There are two types of antennas commonly used by the mobile nodes: 1. Directional antennas 2. Omni-directional antennas. In Omni-directional the data packets are broadcasted in all directions whereas in directional antennas the packets are flooded in a fixed direction. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2015**

## II. LITERATURE SURVEY

The Challenge of target tracking and mobile sensor navigation arises when a mobile target does not follow a predictable path. Successful solutions require a real-time location estimation algorithm and an effective navigation control method. Target tracking can be viewed as a sequential location estimation problem. Typically, the target is a signal emitter whose transmissions are received by a number of distributed sensors for location estimation. There exist a number target localization approaches-based various measurement models such as received signal strength(RSS), time of arrival (TOA), time difference of arrival (TDOA), signal angle of arrival (AOA), and their combinations [2],[3].For target tracking, Kalman filter was proposed in [4], where a geometric-assisted predictive location tracking algorithm can be effective even without sufficient signal sources. Li et al. [5] investigated the use of extended Kalman filter in TOA measurement model for target tracking. Particle filtering has also been applied with RSS measurement model under correlated noise to achieve high accuracy [6].

In addition to the use of stationary sensors, several other works focused in mobility management and control of sensors for better target tracking and location estimation. Zou and Chakrabarty [7] studied a distributed mobility management scheme for target tracking, where sensor node movement decisions were made by considering the trade-off among target tracking quality improvement, energy consumption, loss of connectivity, and coverage. Rao and kesidis [8] further consider the cost of node communication and movement as part of the performance trade-off. To enable target tracking by a mobile sensor with a prior knowledge on target motion, [9], [10] presented a proportional navigation strategy and several variants. In [11], a continuous nonlinear periodically time-varying algorithm was proposed for adaptively estimating target positions and for navigating the mobile sensor in a trajectory that encircles the target. Belkhouchet et al. [12] modelled the robot and the target kinematics equations in polar coordinates, and proposed a navigation strategy that attempts to position the robot in between a reference point and the target so as to successful follow the target. Using the similar set of nonlinear kinematics equations, Vargas navigation et al. [13] proposed cubic Navigation function, which is both simple and effective. In our work, we adopt this simple navigation function.

## III. RSS BASED ATTACK DETECTION

The challenge in spoofing detection is to devise strategies that use the uniqueness of spatial information, but not using location directly as the attackers' positions are unknown. We propose to study RSS; a property closely correlated with location in physical space and is readily available in the existing wireless networks. Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks (i.e., reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks. The RSS readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive. Thus, the RSS readings present strong spatial correlation characteristics.

The detection power of the so far approach is by using the RSS-based spatial correlation. There are four landmarks deployed at the four corners of the square area. The physical distance between two wireless devices is 16, 20, and 25 feet, respectively. The path loss exponent _ is set to 2.5 and the standard deviation of shadowing is 2 dB. The ROC curves shift to the upper left when increasing the distance between two devices. This indicates that the farther away the two nodes are separated, the better detection performance that our method can achieve. This is because the detection performance is proportional to the no centrality parameter, which is represented by the distance between two wireless nodes together with the landmarks. A larger standard deviation of shadowing causes the two distributions, i.e., no central chi-square and central chi-square, to get closer to one another.

In particular, we utilize the received signal strength (RSS) measured across a set of landmarks (i.e., reference points with known locations) to perform detection of identity-based attacks. We focus on static nodes, which are common for most identity-based attacks scenarios. Our scheme can detect both spoofing and Sybil attacks by using the same set of techniques and does not add any overhead to the wireless devices and sensor nodes.

**Cluster Analysis for Attack Detection**

RSS is widely available in deployed wireless communication networks, and its values are closely correlated with location in physical space. In addition, RSS is a common physical property used by a widely diverse set of

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2015**

localization algorithms. In spite of its several-meter-level localization accuracy, using RSS is an attractive approach, because it can reuse the existing wireless infrastructure, and it is sufficient to meet the accuracy requirement of most applications. For example, during health care monitoring, a doctor may only need to know in which room the tracked patient resides. We thus derive an attack detector for identity-based attacks by utilizing properties of the RSS.
The aforementioned analysis provides the theoretical support of using the spatial correlation in RSS inherited from wireless nodes to perform attack detection. It also showed that the RSS readings from a wireless node over time fluctuate under different and should cluster together. In particular, the RSS readings from the same physical location over time will belong to the same cluster points in the n-dimensional signal space, whereas the RSS readings from different locations over time should form different clusters in signal space, which presents RSS reading vectors of three landmarks from two different physical locations. This observation suggests that we can conduct cluster analysis on top of RSS readings to find out the distance in signal space in practice. Furthermore, we can detect the identity-based attacks based on the observed RSS distance between clusters.

## IV. INTEGRATED DETECTION AND LOCALIZATION FRAMEWORK (IDOL)

### Framework

The traditional localization approaches are based on averaged RSS from each node identity inputs to estimate the position of a node. However, in wireless spoofing attacks, the RSS stream of a node identity may be mixed with RSS readings of both the original node as well as spoofing nodes from different physical locations. The traditional method of averaging RSS readings cannot differentiate RSS readings from different locations and thus is not feasible for localizing adversaries.

Different from traditional localization approaches, our integrated detection and localization system utilize the RSS medoids returned from SILENCE as inputs to localization algorithms to estimate the positions of adversaries. The return positions from our system include the location estimate of the original node and the attackers in the physical space. Handling adversaries using different transmission power levels. An adversary may vary the transmission power levels when performing spoofing attacks so that the localization system cannot estimate its location accurately.

### Area-based probability

ABP also utilizes an interpolated signal map. Further, the experimental area is divided into a regular grid of equal-sized tiles. ABP assumes the distribution of RSS for each landmark. Area-based algorithms return the most likely area in which the true location resides. Compared with point-based methods, one major advantage of area-based methods is that they return a region, which has an increased chance of capturing the transmitter's true location. ABP returns an area, i.e., a set of tiles on the floor, bounded by a probability that the transmitter is within the returned area. ABP assumes that the distribution of RSS for each landmark follows a Gaussian distribution. The Gaussian random variable from each landmark is independent. ABP then computes the probability that the transmitter is at each tileLi on the floor by using Bayes' rule.

### False Alarms

A cloud system with hundreds of nodes will have huge amount of alerts raised by Snort. Not all of these alerts can be relied upon, and an effective mechanism is needed to verify if such alerts need to be addressed. Since Snort can be programmed to generate alerts with CVE id, one approach that our work provides is to match if the alert is actually related to some vulnerability being exploited. If so, the existence of that vulnerability in SAG means that the alert is more likely to be a real attack. Thus, the false positive rate will be the joint probability of the correlated alerts, which will not increase the false positive rate compared to each individual false positive rate. Moreover, we cannot keep aside the case of zero day attack where the vulnerability is discovered by the attacker but is not detected by vulnerability scanner. In such case, the alert being real will be regarded as false, given that there does not exist corresponding node in SAG. Thus, current research does not address how to reduce the false negative rate. It is important to note that vulnerability scanner should be able to detect most recent vulnerabilities and sync with the latest vulnerability database to reduce the chance of Zero-day attacks.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2015**

## V. DISTANCE BASED ATTACK LOCALIZATION AND DETECTION (DALD)

The DALD approach is based on the distance of each data that travels from source to destination. For one cycle of data transmission, the distance is calculated based on the TOA and the sender node's position. The frequency parameter is excluded from the scenario. It means the node can operate in any frequency or 2 or more nodes can exist in a same frequency or in a same frequency region. The difference is that each node has different physical locations despite they even share the common frequency or exist in the same frequency region.

**Localization System**

We have developed a general-purpose localization system to perform real-time indoor positioning. This system is designed with fully distributed functionality and easy-to-plug-in localization algorithms. It is built around four logical components:
1) Sender
2) Location Receiver
3) Central Node
4) Dispatcher.

Sender: Any device that transmits packets can be localized. Oftentimes, the application code does not need to be altered on a sensor node to localize it.

Location Receiver: The location component listens to the packet traffic and extracts the RSS reading for each transmitter. It then forwards the RSS information to the Server component. The Landmark component is stateless and is usually deployed on each landmark or AP with known locations.

Central Node: A centralized node collects RSS information from all the Landmark components. The identity-based detection is performed at the Server component. The Server component summarizes RSS information such as averaging or clustering and then forwards the information to the Solver component for localization estimation.

Dispatcher: The dispatcher takes the input from the Server component, performs the localization task by utilizing the localization algorithms that are plugged in, and returns the localization results back to the Server component multiple Solver instances available, and each Solver instance can simultaneously localize multiple transmitters

The DALD works as follows:

- Compute the sender node's location with respect to the co-ordinates.
- Compute the location of the receiver (Self Known)
- Calculate the distance between source and destination using the co-ordinate positions of both the source and destination.
- Store the difference in distance of the request packet in a localization table.
- For every "i" in "n" cycle of data transfer, check if the data is arriving from the same destination (based on distance).
- If any of the data is occurring from a different localization value then drop the packet and terminate the connection.

**NEIGHBORSHIP-BASED DETECTION**

In this scheme, each node has a set of monitoring nodes. For ease of presentation, we refer to the node being monitored as monitee and the nodes that monitor it as monitors in the rest of the paper. The basis of the neighbor ship-based scheme is that different transmission power levels correspond to different transmission ranges. Thus, a certain neighbour can hear from the monitee only when the monitee transmits packets with a transmission power higher than a certain level. By having the monitee transmitting with all possible transmission power levels, each of its neighbours can record the power level from which the packets sent from the monitee start to be heard (note that any message sent using

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2015**

a power level higher than that can also be heard). If later a neighbour can overhear a packet from the monitee with a lower power level or only with a higher power level, it can suspect that the monitee is redeployed.

**Distance Based Detection**

The distance-based redeployment detection is based on the following insight: without node redeployment attack, the monitee's location will not change and the distance measurements at its neighbouring nodes should be consistent, respectively. Thus, if the monitee is redeployed into a different location, a monitor can detect the redeployment by noticing the inconsistency in the distance measurements. In other words, the distributions of the distance measurements before and after redeployment are different. More specifically, if a monitor makes before and after distance measurements on the monitee, it can calculate the difference between the before and after distance-measurement pairs and determine whether that monitee has been redeployed or not. The before measurement, which consists of a set of distance measurements, is collected after the initial deployment. We denote the set of data in before measurement as the reference-set. The after measurement is done at sometime thereafter and we denote the collected data set at this time as the testing-set.

**DISTANCE ESTIMATION IN PROXYS**

Caching under proxy routing works like this:

1. The client requests an on-demand stream, through the child Helix Universal Proxy. The child Helix Universal Proxy proxies the request and sends it to the parent Helix Universal Proxy outside the subnet. The parent Helix Universal Proxy makes the request of the origin Helix Universal Server. The origin server sends the data to the parent Helix Universal Proxy.

2. The parent Helix Universal Proxy caches the data and streams the request to the child Helix Universal Proxy.

3. The child Helix Universal Proxy caches the data and streams the request to the client.

A new communication mechanism is RandomCast, via which a sender can specify the desired level of overhearing, making a prudent balance between energy and routing performance. In addition, it reduces redundant rebroadcasts for a broadcast packet, and thus, saves more energy. In random casting, the server gets request from the client and gives response back through the IP address. In mobile ad hoc networks (MANETs), every node overhears every data transmission occurring in its vicinity and thus, consumes energy unnecessarily. However, since some MANET routing protocols such as Dynamic Source Routing (DSR) collect route information via overhearing, they would suffer if they are used in combination with PSM. Allowing no overhearing may critically deteriorate the performance of the underlying routing protocol, while unconditional overhearing may offset the advantage of using PSM.

In such a routing the packet is denied of its forward approach. So the packet will be withheld in the same node. The node can be assumed to be out-of-range in that particular network. In such a case we can use two methods in either or choice to deliver the packet. The first and best method is reverse step shortest path finding.

**Advantages**

- It is been build in a decentralized architecture so it will be autonomous and infrastructure less.
- On using decentralized network, additional delay consumed by VM profiling is been avoided.
- Attacker's link failures are addressed by using IDS.
- Data consistency is been overcome by using encryption method.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2015**

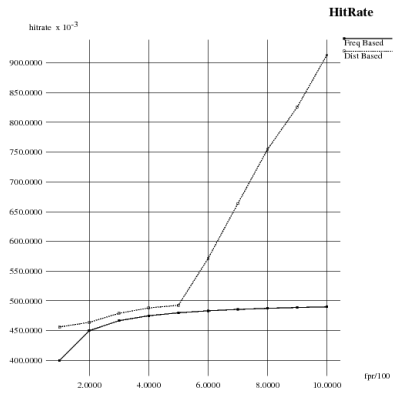
**Region-Link Failure Detection**

Link failures are not generally addressed, but here the attacker's link failures are been noticed based on the IDS nodes. The attacking nodes are been found using this IDS. And here, we can find the attacked path and we can avoid it and use a new path so that the delivery ratio will be comparatively high. Here the distance between the source and the destination and also the distance between the attacker with the source and destination are been known.
IDS being a detection system monitor and alerts all the source and destination by a periodic broadcast regarding the behaviour of the nodes. It monitors the number of broadcasts, data handover, node's inactive time period and log. Based on the parameters monitored, it detects the suspicious node and broadcasts the information to the source and destination.

Region and location can be geographical, network topological, geometric or administrative entities depending on the metric we use to define a space and construct a hierarchy. Locality of nodes refers to their proximity relations in the metric space. One can construct a hierarchy of arbitrary number of levels. We use region, sub-region and leaf region levels of the hierarchy. We use physical space and distance to refer to the metrics pace and its metric.

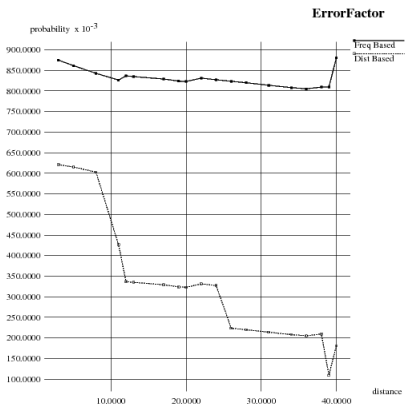
## VI. SIMULATION RESULTS

**Hit Rate Graph**




Hit Rate is the detection probability of the attacks in the network. From the graph it is seen that, distance based detection is more reliable than the frequency based detection technique. As the false positive rate increases, the detection probability also increases.

**Error Factor**




Error factor is the misdection in localization of the node. When more than one frequency meets at some point, the misdetection probability increases, whereas in distance based localization, the error factor is less.

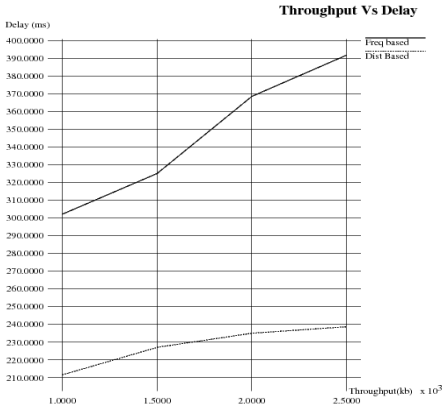
ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 3, March 2015**

**Delay Graph**




Due to the computational complexity in frequency based detection, end to end delay observed is higher. Due to single phase computation, the delay is comparatively less in distance based detection.

## VII. CONCLUSION

Here we propose to detect and mitigate attacks in the wireless ad-hoc networking environment. We utilize the distance based detection model to conduct attack detection and prediction. The proposed solution investigates how to use the detection and localization techniques to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks. The system performance evaluation demonstrates the feasibility of DALD and shows that the proposed solution can significantly reduce the risk of the Ad-Hoc Nets from being exploited and abused by internal and external attackers. But the above only investigates the network IDS approach to counter zombie explorative attacks. To improve the detection accuracy, host-based IDS solutions are needed to be incorporated and to cover the whole spectrum of IDS in the Ad-Hoc system.

Every dropping attack can also be isolated from the network by forming a secure and non-secure zone using dynamic partitions. The zone is differentiated using secure path and non secure path based on maximum connectivity and the distance at which the end node communicates at each instance, reducing the possibility of the attackers.

## REFERENCES

[1] M.cetin, l.chen, J.Fisher, A.Ihler III, M. wainwright, and A.Willsky, "distributed Fusion in sensor Networks," IEEESignal provessing magazine, vol/23, no.4, pp.42-55, Dec.2006.
[2] A.H. Sayed, A.Tarighat, and N. Khajehnori, "Network-Based Wireless Location: Challenges Faced in Developing Techniques for Accurate Wireless Location Information," IEEE sigal processing magazine, vol.22, no. 4, pp.24-40, July 2005.
[3] N.patwari, J.N. Ash, S. kyperountas, A. Hero, R.L. Moses, and N.s. correal, "Locating the Nodes: Cooperative Localization n wireless sensor network," IEEE sigal processing magazine, vol.22, no. 4, pp. 54-69, July 2005.
[4] P.H. Tseng, K.T. feng, Y.C. lin, and C.L. chen,"wireless location tracking algorithms for environments with insufficient signal sources," IEEE trans. Mobile computing, vol.8, no.12, pp. 1676-1689, dec.2009
[5] T.li, A.ekpenyong, and Y.F. huang, "source localization and tracking using distributed asynchronous sensors," IEEE trans. Signal processing, vol.54, no.10, pp. 3991-4003, oct. 2006.
[6] L.mihaylova, d.angelova, D.R.bull, and n.canagarajah, "Localization of mobile nodes in wireless networks with correlated in time measurement noise," IEEE Trans. Mobile compting, vol. 10, no. 1, pp. 44-53, jan.2011.
[7] Y. Zou and k. chakrabarty, "Distributed moility management for target tracking in mobile sensor networks," IEEE Trans. Mobile computing, vol. 6, no. 8, pp. 872-887, aug. 2007
[8] R.Rao and G. kesidis, "Purposeful mobility for relaying and surveillance in mobile Ad Hoc sensor networks," IEEE Trans. Mobile computing, vol. 3, no.3, pp. 225-231, Mar. 2004.
[9] C.D. yang amd C.C. yang, "A unified approach to proportional navigation," IEEE Trans. Aerospace and Electronic system, vo;.33, no.2, pp. 557-567, apr.1997.
[10] M. mehrandezh, M.N sela, R.G fenton, and B.Benhabib, "proportional navigation guidance for robotic interception of moving objects," J. robotic systems, vol. 17, no.6, pp. 321-340,2000.