Survey of Robustness Strategy for Scale Free Wireless Sensor Networks

K.Gowthami S.Vijay kumar
M.Phil Research Scholar, Assistant Professor
Department of Computer Science
Kongu Arts and Science College
Erode, Tamilnadu, India

Abstract In this paper is improving the robustness of the network topologies for WSNs. The objective of the paper is preserved after certain node failures resulting from cyber attacks for wireless sensor communication. In paper define the terms of target selection for attacks, there are two types of attack: random and malicious. In random attacks, the attacker randomly chooses nodes in the network topology as the targets, whereas in malicious attacks, the attacker chooses the nodes with high node degrees as the targets. It is known that some types of network topologies are resistant to random attacks and some are resistant to malicious attacks. This paper is proposed to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for 1) detecting attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. It is proposed to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the attacks. It formulates the problem of determining the number of attackers as a multi-class detection problem.

Keywords: Wireless Sensor Network, Cyber Attack, Network Free Toplogy, Spatial correlation,RSS,

1. INTRODUCTION

ROSE is designed to be processed in a centralized system. Before ROSE operates, each node sends its own coordinates and neighbor list to the centralized system through the multihop system. After we achieve the optimization results according to ROSE, the centralized system sends the new neighbor list to each node through the multi-hop system. The ROSE algorithm is aimed to transform network topologies to exhibit the onion-like structure. Specifically, ROSE involves two phases: a degree difference operation and angle sum operation.

In the degree difference operation and angle sum operation described next, only when a pair of edges are independent edges are they considered for swapping; otherwise, not. This not only satisfies the WSNs communication range constraint on the sensor nodes, but also dramatically reduces the pairs of edges considered.ROSE needs the information of the entire scale-free network topology to support the selection of independent edges. Therefore, the process for enhancing robustness against malicious attacks cannot directly be run in a distributed system. ROSE requires that global information be collected into the centralized calculation. Significantly high network density has a negative effect on the performance or efficiency of ROSE. Therefore, when the network density is controlled within a suitable range, this enhancing process can achieve better results and its completion requires a shorter time

- The existing detection mechanism is highly effective in both detecting the presence of attacks but considers all the location as single zone.
- Location information taken from victim as well as adversaries is directly taken from the corresponding nodes themselves. Not the neighbor nodes are queried for their location information. i.e., the spatial readings from node to base station alone. Since this approach requires fixed node locations, it cannot be used when nodes are expected to move.

The proposed system work is motivated from mitigating the limitations of previous schemes. In particular, the new system proposes a method in which the nodes are fixed as well as in movement. A reputation-based trust management scheme is designed to facilitate fast detection of compromised nodes. The key idea of the scheme is to detect untrustworthy zones and perform software attestation against nodes in these zones to detect and revoke the ones that are compromised.

Specifically, first divides the network into a set of zones, establish trust levels for each zone, and detect untrustworthy zones by using the Sequential Probability Ratio Test (SPRT). The SPRT decides a zone to be untrustworthy if the zone's trust is continuously maintained at low level or is quite often changed from high level to low level.

Once a zone is determined to be untrustworthy, the base station or the network operator performs software attestation against all nodes in the untrustworthy zone, detects compromised nodes with subverted software modules, and physically revokes them. In addition, a novel mobile replica detection scheme is proposed based on the Sequential Probability Ratio Test (SPRT). The new system uses the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. As a result, a benign mobile sensor node's measured speed will nearly always be less than the system-configured maximum speed as long as it employs a speed measurement system with a low error rate.

On the other hand, replica nodes are in two or more places at the same time. This makes it appear as if the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes' measured speeds will often be over the system-configured maximum speed. Our proposed system main contribution are,

- The main benefit of this zone-based detection approach lies in achieving fast node compromise detection and revocation while saving the large amount of time and effort that would be incurred from using periodic software attestation.

- By detecting an entire zone at once, the system can identify the approximate source of bad behavior and react quickly, rather than waiting for a specific node to be identified.
- When multiple nodes are compromised in one zone, they can all be detected and revoked at one time.
- The proposed system validates the effectiveness, efficiency, and robustness of the scheme through analysis and simulation experiments.
- The new system finds that the main attack against the SPRT-based scheme is when replica nodes fail to provide signed location and time information for speed measurement.
- To overcome this attack, the new system employs a quarantine defense technique to block the noncompliant nodes.
- It provides analyses of the number of speed measurements needed to make replica detection decisions, which shows is quite low, and the amount of overhead incurred by running the protocol.

II. RELATED WORKS

2.1 IP Spoofing

Internet Protocol (IP) is the protocol used for transmitting messages over the Internet; it is a network protocol operating at layer 3 of the OSI model. P spoofing is the act of manipulated the headers in a transmitted message to mask a hackers true identity so that the message could appear as though it is from a trusted source. The hacker manipulates the packet by using tools to modify the "source address" field. The source address is the IP address of the sender of the message therefore once an intruder forges this address and the destination server opens up a connection, this is when numerous attacks can take place.

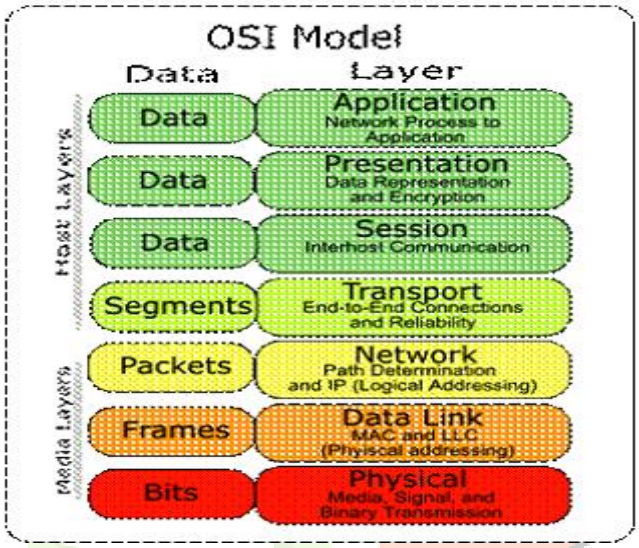

Fig 2.1 IP Spoofing

2.2 TCP and DNS Spoofing

Another class of spoofing attack, which it will not discuss here, tricks the user's software into an inappropriate action by presenting misleading information to that software3. Examples of such attacks include TCP spoofing, in which Internet packets are sent with forged return addresses, and DNS spoofing, in which the attacker forges information about which machine names correspond to which network addresses. These other spoofing attacks are well known, so it will not discuss them further.

2.3 Web Spoofing Attack

Web spoofing is a kind of electronic con game in which the attacker creates a convincing but false copy of the entire World Wide Web. The false Web looks just like the real one: it has all the same pages and links. However, the attacker controls the false Web, so that all network traffic between the victim's browser and the Web goes through the attacker.

- **Consequences:** Since the attacker can observe or modify any data going from the victim to Web servers, as well as controlling all return traffic from Web servers to the victim, the attacker has many possibilities. These include surveillance and tampering.
- **Surveillance:** he attacker can passively watch the traffic, recording which pages the victim visits and the contents of those pages. When the victim fills out a form, the entered data is transmitted to a Web server, so the attacker can record that too, along with the response sent back by the server. Since most on-line commerce is done via forms, this means the attacker can observe any account numbers or passwords the victim enters.
- **Tampering:** The attacker is also free to modify any of the data traveling in either direction between the victim and the Web. The attacker can modify form data submitted by the victim. For example, if the victim is ordering a product on-line, the attacker can change the product number, the quantity, or the ship-to address. The attacker can also modify the data returned by a Web server, for example by inserting misleading or offensive material in order to trick the victim or to cause antagonism between the victim and the server.
- **Spoofing the Whole Web:** User may think it is difficult for the attacker to spoof the entire World Wide Web, but it is not. The attacker need not store the entire contents of the Web. The whole Web is available on-line; the attacker's server can just fetch a page from the real Web when it needs to provide a copy of the page on the false Web.

2.4 MAC Spoofing Attack Model

In general, the MAC spoofing attack to consider involves an attacker, a genuine station whose MAC address is cloned by the attacker, and a victim who regards the attacker as the genuine station, as shown in Figure 2.2. A spoofing attack includes two steps. First the attacker uses 802.11 frame manipulation tools to generate the forged frames and then sends them to air using 802.11 frame injection tools. To detect attacks, to deploy an array of AMs (shown as diamonds in **Figure 2.2)** to measure the RSS of frames that can be heard at AM's antenna.

To first assume that both the attacker and the genuine station are using off-the-shelf hardware, which means that they use standard 802.11 chipsets as their transceivers. they do not assume anything about their antennas, i.e., the antennas could be integral or external, omni or directional. To further assume that sophisticated attackers may manipulate arbitrary field of 802.11 frames, such as the source and destination MAC addresses, BSSID, ESSID, sequence number, frame checksum, and so on. For each frame the attackers transmit, they may change antenna, power, and bit rate. The attacker may move freely within the area covered by AMs, which implies that an attacker could be close to the genuine station.

It also assume that an attacker needs to send enough forged frames to cause damage as discussed in previous subsection. The frames, however, can be injected at any rate. The method profiles genuine stations in advance; they assume that attacks are not present during profiling. They assume that the genuine station sends sufficient frames during the profiling period; if necessary, they may send ping or RARP requests to solicit enough frames. To recognize that the AMs may not capture all frames; AMs often miss frames in practice, due to the AMs' constrained resources, to bursty network traffic, and to collisions in the air. Finally, they assume that the genuine station has a fixed location, which is fortunately true for a common spoof target: production APs.

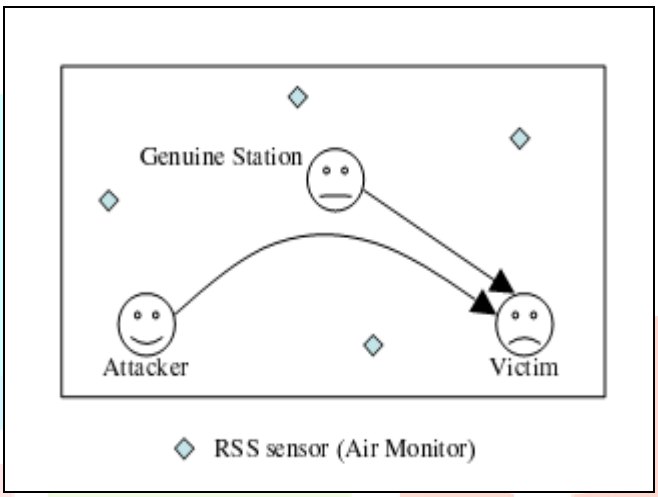

Figure 2.2: MAC Layer Spoofing

III. LITERATURE SURVEY

Shouling Ji, Raheem Beyah and Zhipeng Cai [1] describe a novel Cell-based Path Scheduling (CPS) algorithm that achieves capacity of [$\Omega(1/5\omega \ln n \cdot W)$] in the sense of the worst case and order-optimal capacity in the sense of expectation, where n is the number of sensor nodes, ! is a constant, and W is the data transmitting rate. For continuous data collection, we propose a Zone-based Pipeline Scheduling (ZPS) algorithm. ZPS significantly speeds up the continuous data collection process by forming a data transmission pipeline, and achieves a capacity gain of [$N\sqrt{n}/\sqrt{\log n}\ln n$ or $n/\log n \ln n$] times better than the optimal capacity of the snapshot data collection scenario in order in the sense of the worst case, where N is the number of snapshots in a continuous data collection task. The simulation results also validate that the proposed algorithms significantly improve network capacity compared with the existing works.

Arslan Munir, Ann Gordon-Ross, , and Sanjay Ranka [2] describe a multi-core embedded sensor nodes enable energy savings over traditional single-core embedded sensor nodes in two ways. First, reducing the energy expended in communication by performing in-situ computation of sensed data and transmitting only processed information. Second, a multi-core embedded sensor node allows the computations to be split across multiple cores while running each core at a lower processor voltage and frequency, as compared to a single-core system, which results in energy savings. Utilizing a single-core embedded sensor node for information processing in information-rich applications requires the sensor node to run at a high processor voltage and frequency to meet the application's delay requirements, which increases the power dissipation of the processor. A multicore embedded sensor node reduces the number of memory accesses, clock speed, and instruction decoding, thereby enabling higher arithmetic performance at alower power consumption as compared to a single-core processor.

Salvatore Scellato, Ilias Leontiadis, Cecilia Mascolo, Prithwish Basu, Murtaza Zafer [3] has presented a study of temporal robustness in time-varying network: we adopt temporal network metrics to assess network performance in presenceof increasingly larger random failures. We have investigated the performance of our method both analytically on a random temporal network model and via simulations in a Markov-based and in two mobility-based models, exploring how the temporaldimension provides more redundancy to communication systems compared to static evaluation. Finally, we have shown how temporal robustness gives a more realisticestimation of the resilience of a real-world temporal network than standard static approaches.

Xuqing Huang, et.al[4] describe a theoretical framework to develop the process of cascading failures in interdependent network caused by random initial failure of nodes. They show that due to the coupling between networks, interdependent

networks are extremely vulnerable to random failure. However, when we consider real scenarios, initial failure is mostly not random. It may be due to a targeted attack on important hubs (nodes with high degree). It can also occur to low degree nodes because important hubs are purposely defended, e.g., in internet networks, heavily connected hubs are purposely more secured. Indeed, it was shown that targeted attacks on high degree nodes or high betweenness nodes in single networks have a dramatic effect on their robustness. The question of robustness of inters dependent networks under targeted attack or defense has not been addressed.

Guanfeng Liu, et.al [5] presented a complex social network structure that takes trust information, social relationships and recommendation roles into account, reflecting the realworld situations better. For selecting the optimal social trust path with end-to-end QoT constraints in complex social networks, which is an NP-Complete problem, we first analyzed the advantages and the disadvantage (i.e., the imbalance problem of QoT attributes) of our previously proposed H_OSTP that is one of the most promising algorithms for the MCOP selection problem. Based on H_OSTP, they analyze MFPB-HOSTP, an efficient heuristic algorithm, where multiple foreseen paths are formed, helping avoid a failed feasibility estimation of a foreseen path caused by the imbalance problem of QoT attributes. The results of experiments conducted on a real data set demonstrate that MFPB-HOSTP outperforms existing methods in optimal social trust path selection with good efficiency

Rong-Hua Li, et al [6] measuring robustness of complex networks is a fundamental task for analyzing the structure and function of complex networks. In this paper, we study the network robustness under the maximal vertex coverage (MVC) attack, where the attacker aims to delete as many edges of the network as possible by attacking a small fraction of nodes. First, we present two robustness metrics of complex networks based on MVC attack. We then propose an efficient randomized greedy algorithm with near-optimal performance guarantee for computing the proposed metrics. Finally, we conduct extensive experiments on 20 real datasets. The results show that P2P and co-authorship networks are extremely robust under the MVC attack while both the online social networks and the Email communication networks exhibit vulnerability under the MVC attack. In addition, the results demonstrate the efficiency and effectiveness of our proposed algorithms for computing the corresponding robustness metrics.

IV.METHODOLOGY

A. Introduction

Generally compromise occurs once an attacker has found a node, and then directly connects the node to their computer via a wired connection of some sort. Once connected the attacker controls the node by extracting the data and/or putting new data or controls on that node.

The first step required to solve the problem is the identification of the problem. As the success of the system depends largely on how accurately a problem is identified. At present, the algorithms deal with detection of mobile replica attacks which does not yield better results. The result produced is not efficient and accurate; thus existing system needs some additional options for yielding better results. There is no algorithm with this feature to detect mobile replica attack in fast manner. So, this project identifies that and helps for fast detection of mobile replica attacks. The problem is stated first and the network assumptions for the proposed scheme and the attacker models are described.

A mobile replica node u_0 is defined as a node having the same ID and secret keying materials as a mobile node u. An adversary creates replica node u_0 as follows: He first compromises node u and extracts all secret keying materials from it. During the base station collecting all the nodes' location information, the attacker node sends its id (the attacker node) as id of mobile node 'u' (the affected node). Now the goal is to detect the fact that both u and u_0 operate as separate entities with the same identity and keys.

A two-dimensional mobile sensor network is considered where sensor nodes freely roam throughout the network. It is assumed that every mobile sensor node's movement is physically limited by the system-configured maximum speed, Vmax. It is also assumed that all direct communication links between sensor nodes are bidirectional. This communication model is common in the current generation of sensor networks. It is assumed that every mobile sensor node is capable of obtaining its location information and also verifying the locations of its neighboring nodes. It is also assumed that the clocks of all nodes are loosely synchronized.

It is also assumed that the nodes in the mobile sensor network communicate with a base station. The base station may be static or mobile, although we focus on a static base station for the simulations, as long as the nodes have a way to communicate reliably to the base station on a regular basis.

B. Theoretical Analysis Of The Spatial Correlation Of RSS

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. The proposed 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 RSS value vector as s ={s_1, s_2,….. s_n}where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations. Generally, the RSS at the ith landmark from a wireless node is lognormally distributed

$$s_i(d_j)[dBm]=P(d_0)\ [dBm]-10\ \gamma log(\ d_j/d_0)+X_i \quad \text{----- Equ 1} \qquad (4.1)$$

where $P(d_0)$ represents the transmitting power of the node at the reference distance d_0, d_j is the distance between the wireless node j and the i_{th} landmark, and γ is the path loss exponent, X_i is the shadow fading which follows zero mean Gaussian distribution with standard deviation.

C. Attack Detection Using Cluster Analysis

The non-hierarchical method initially takes the number of components of the population equal to the final required number of clusters. First, the final required number of clusters is chosen such that the points are mutually farthest apart. Next, it examines each component in the population and assigns it to one of the clusters depending on the minimum distance.The centroid's position is recalculated every time a component is added to the cluster and this continues until all the components are grouped into the final required number of clusters. K-means (MacQueen, 1967) is one of the simplest unsupervised learning algorithms that solve the well known clustering problem.

The procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume k clusters) fixed a priori. The main idea is to define k centroids, one for each cluster. These centroids should be placed in a cunning way because of different location causes different result. So, the better choice is to place them as much as possible far away from each other. The next step is to take each point belonging to a given data set and associate it to the nearest centroid. When no point is pending, the first step is completed and an early groupage is done.

At this point they need to re-calculate k new centroids as barycenters of the clusters resulting from the previous step. After they have these k new centroids, a new binding has to be done between the same data set points and the nearest new centroid. A loop has been generated. As a result of this loop they may notice that the k centroids change their location step by step until no more changes are done. In other words centroids do not move any more.

The k-means approach to clustering performs an iterative alternating fitting process to form the number of specified clusters. The k-means method first selects a set of n points called cluster seeds as a first guess of the means of the clusters. Each observation is assigned to the nearest seed to form a set of temporary clusters. The seeds are then replaced by the cluster means, the points are reassigned, and the process continues until no further changes occur in the clusters. The algorithm is composed as following steps,

- Place K points into the space represented by the objects that are being clustered. These points represent initial group centroids.
- Assign each object to the group that has the closest centroid.
- When all objects have been assigned, recalculate the positions of the K centroids.
- Repeat Steps 2 and 3 until the centroids no longer move. This produces a separation of the objects into groups from which the metric to be minimized can be

D. K-Mean Cluster

- The dataset is partitioned into K clusters and the data points are randomly assigned to the clusters resulting in clusters that have roughly the same number of data points.
- For each data point:
- Calculate the distance from the data point to each cluster.
- If the data point is closest to its own cluster, leave it where it is. If the data point is not closest to its own cluster, move it into the closest cluster.
- Repeat the above step until a complete pass through all the data points results in no data point moving from one cluster to another. At this point the clusters are stable and the clustering process ends.
- The choice of initial partition can greatly affect the final clusters that result, in terms of inter-cluster and intracluster distances and cohesion.

E.Network Model

The compromised node detection in a two-dimensional static sensor network is studied in which the locations of sensor nodes do not change after deployment. It is assumed that all direct communication links between sensor nodes are bidirectional. This communication model is common in the current generation of sensor networks.

F. Attacker Model

It is assumed that an adversary may attempt to find as many different regions as possible and compromise a few sensor nodes in each region. However, limits are placed on the attack capability such that the attacker does not compromise a majority of the nodes in each region. This is reasonable, since compromising a majority of sensor nodes in a region is far from optimal.

This is mainly because the attacker's influence is limited to the region while he spends substantial time and efforts to compromise many nodes. The same time and effort could instead be used to spread out compromised nodes over a wider area and cause greater disruption to the network. Moreover, it is worth noting that he can easily defeat any node compromise detection scheme if the adversary could compromise a major fraction of the region. This is because a large number of compromised nodes in a region can prevent relatively small number of benign nodes from performing node compromise detection in the region.

G. Design Goals

The three key design goals for compromised node detection are under the above system and attacker models. First, compromised nodes should be detected with minimal communication, computational, and storage overheads. Second, the detection schemes should be robust and highly resilient against the attacker's attempt to break the scheme. Finally, compromised node detection should be performed at the cost of minimal false positives and negatives. This is important to prevent turning the compromised node detection scheme into a tool for denial of service attacks.

H. Techniques To Detect Compromised Nodes In Zones

Reputation-based trust management schemes do not stop compromised nodes doing malicious activities in the network. Also, the existing schemes based on software attestation require each sensor to be periodically attested because it cannot be predicted when attacker compromises sensors. The periodic attestation of individual nodes will incur large overhead in terms computation and communication overhead.

To mitigate the limitations of both approaches, a zone-based node compromise detection scheme is proposed which facilitates node compromise detection and revocation by leveraging zone trust information. Specifically, the network is divided into a set of zones, establish trust per zone, and detect untrustworthy zones in accordance with zone trust values.

Once a zone is determined to be untrustworthy, the network operator attests the software modules of all sensors in the untrustworthy zone, and detects and revokes compromised nodes in that zone. A straightforward approach for untrustworthy zone detection is to decide a zone as untrustworthy by observing a single evidence that its trust value is less than a predefined threshold. However, this approach does not consider the zone trust measurement error. Due to the error occurrence in the zone trust measurement, trustworthy (resp. untrustworthy) zone could be detected as untrustworthy (resp. trustworthy).

To minimize these false positive and negatives, we need to make a decision with multiple pieces of evidence rather than a single evidence. To meet this need, the Sequential Probability Ratio Test (SPRT) is used, which is a statistical decision process that makes a decision with multiple pieces of evidence. The SPRT benefits in the sense that the SPRT reaches a decision with a small number of evidences while achieving the low false positive and negative rates. The SPRT can be thought of as one-dimensional random walk with lower and upper limits.

Before the random walk starts, null and alternate hypotheses are defined in such a way that the null one is associated with the lower limit and the alternate one is associated with the upper limit. A random walk starts from a point between the two limits and moves toward the lower or upper limit in accordance with each observation. If the walk reaches or exceeds the lower or upper limit, it terminates and the null or alternate hypothesis is selected, respectively. It is believed that SPRT is well-suited for tackling the compromised node detection problem in the sense that a random walk with two limits can be constructed in such a way that each walk is determined by the trust value of a zone; the lower and upper limits are properly configured to be associated with the excess and shortfall of a predefined trust threshold, the proposed protocol to find the compromised zones proceeds in three phases:

1) Phase I:

Zone Discovery and Trust Aggregator Selection: After deployment, every sensor node u finds out its location and determines the zone to which it belongs. This zone is called the home zone. From u 's point of view, other zones are called as the foreign zones. Node u discovers every other node residing in the same zone. After the zone discovery process, the Trust Aggregator (TA) is selected in a round robin manner.

Specifically, the time domain of a zone is partitioned into time slots. An initial duty time slot is assigned to each node u in the zone according to the ascending order of the nodes' IDs. Each node u then acts as trust aggregator every S time slots starting from its initial duty time slot, where S is the number of nodes residing in the zone.

2) Phase II:

Trust Formation and Forwarding: For each time slot T i , each node u in zone Z computes neighborhood-trust that is defined in accordance with the difference between the probability distributions of the information generated by u and the information sent to u by u 's neighboring nodes in zone Z.

3) Phase III:

Detection and Revocation: Upon receiving a zone-trust report from a TA in zone Z , the base station verifies the authenticity of TA's report with the secret shared key between TA and itself and discards the report if it is not authentic. The base

station also maintains a record per TA associating each TA's ID with its home zone. This prevents compromised TAs from claiming multiple home zones.

I. ALGORITHM TO FIND REPLICA NODE

To find the replicated nodes, the following algorithm is used.

1. Create a network of 'n' nodes and save the information in the database table.
2. Draw the network with the available node information.
3. Random walk procedure is worked out so that the nodes' mobility is carried out by just moving its location with 'n' pixels below (the given speed) in both x and y direction. For example, if the speed is given as 10 units, then a random value below 10 is chosen, and the node is moved in x or y direction. This is carried out for all nodes. For simulation, the timer is set to 5 seconds. So once each 5 seconds, all the nodes are moved within the given speed horizontally or vertically.
4. The nodes are sending their location to their neighbor nodes. The node is treated as neighbor to one, if it is within the given pixel units. For example, the unit is given as 50, then a node with left position in the space with 150 x value and another node with 180 x value is treated as neighbor nodes. This is applicable to y axis also. So in the rectangular area of 50 units (side), when the two nodes fall inside, then they are treated as neighbor nodes.
5. The nodes are updating their location information once in 10 seconds. The arrow lines are drawn during the animation such that from all nodes, the line is drawn to the base station. The area located at left bottom corner of the drawing space in the form.
6. Replica Attack: When a button is clicked, a node is chosen randomly which behaves as attacker node; a node is chosen randomly which behaves as affected node. The attacker node through sends the current location information, it sends its id as the affected node. So the base station receives updates with two ids at single update. Now, the base station needs to identify which node is correct and which is attacker.
7. If two nodes send same id, then the base station, collects the previous location information of the same id. Any one of the entry will have wrong previous location. At the same time, the neighbor nodes location data is also used such that, the affected nodes neighbors update correct location of suspected id whether the attacker nodes neighbor nodes update wrong location and the attacker node will be identified.
8. Then the node is revoked from the network.

V. CONCLUSION

This paper proposed to use received signal strength-based spatial correlation, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks. It provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. It derived the test statistic based on the cluster analysis of RSS readings. The approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them.

In addition, a zone-based node compromise detection scheme is proposed used and furthermore, several possible attacks are described against the proposed scheme and proposed counter-measures against these attacks. The scheme is evaluated in simulation under various scenarios.

The test result show that the scheme quickly detects untrustworthy zones with a small number of zone-trust reports.

- Deployed nodes must be able to establish secure node-to-node communication.
- The scheme should be functional without involving the base station as an arbiter or verifier.
- Additional legitimate nodes deployed at a later time can form secure connections with already-deployed nodes. This implies that bootstrapping information must always be present and cannot simply be erased after deployment to prevent compromise in the event of capture.
- Unauthorized nodes should not be able to establish communications with network nodes and thus gain entry into the network.
- To identify malicious nodes through trust management schemes and thereby revoke the compromise node.
- To find out the most affected i.e., compromised zones.
- Since wireless sensor net-works usually need to be controlled remotely by the network operator, they are often deployed in an unattended manner. The unattended nature of wireless sensor networks can be exploited by attackers. The node could inject falsified data to corrupt monitoring operation of the sensors. So the compromised nodes should be detect as soon as possible before the nodes form group and continue the attack.
- An adversary with com-promised nodes can paralyze the deployed mission of sensor networks. So it is very important to detect and revoke compromised nodes as soon as possible in the network.

In future, the scheme may evaluate against various types of attacker models. It is believed that a game theoretic model is suited for this evaluation. A variety of strategies novel hypothesis testing applying for multiple zone base network to finding number of spoofing attacker detected and that may be taken by detector and adversary.

REFERENCES

1. J.Bellardo and S. Savage, "802.11 Denial-of-Service Attacks. Real Vulnerabilities and Practical Solutions". In Proceedings of the 12th USENIX Security Symposium, Washington, D.C., August 4-8, 2003.

2. F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," Proc. IEEE Wireless Comm. and Networking Conf., 2004.

3. D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

4. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.

5. A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

6. J. Sheng, K. Tan, G.Chen, D.Kotz and A. Campbell "Detecting 802.11 Mac Layer Spoofing Using Received Signal Strength", Proc of Google. Inc at Dartmouth ISTS.

7. [7] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in Proc. WiSe, Sep. 2003, pp. 1–10.

8. S. Brands andD. Chaum, "Distance-bounding protocols," in Proc.Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, 1994, pp. 344–359.

9. ["Packet leashes: A defense against wormhole attacks in wireless networks," in Proc. INFOCOM, San Francisco, CA, Apr. 2003, pp. 1976–1986.

10. J. S.Warner and R. G. Johnston, "Think GPS cargo tracking=High security? Think again," Los Alamos National Lab., Los Alamos, NM, Tech. Rep., 2003.

11. R. Anderson and M. Kuhn, "Tamper resistance—A cautionary note," in Proc. 2nd Usenix Workshop on Electronic Commerce, 1996, pp. 1–11.

12. R. Fontana, "Experimental results from an ultra wideband precision geolocation system,"Ultra-Wideband, Short-Pulse Electromagnetics,May 2000.

13. S. Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. In ACM SASN, October 2004.

14. Y. Yang, X. Wang, S. Zhu, and G. Cao. Distributed software-based attestation for node compromise detection in sensor networks. In IEEE SRDS, October 2007

15. A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005