DETECTION OF SPOOFING AND JAMMING ATTACKS IN WIRELESS SMART GRID NETWORKS USING RSS ALGORITHM

K.Suganthi[1],K.Sahana[2],G.Santhiya[3],S.Swathi[4].

[1] *Assistant Professor Dept. Computer of Science and Engineering, Arasu Engineering College, Tamil nadu, India.*
[2,3,4] *Students Dept. of Science and Engineering, Arasu Engineering College, Tamil nadu, India.*

---***---

Abstract- *Wireless power grid networks consist of numerous small home nodes and power production nodes that can collect, and disseminate information for the processing of information of power consumption. Several of these applications involve the communication of sensitive information that must be protected from unauthorized parties. Although the wireless network communications could be secured via standard cryptographic methods, the communication patterns alone leak contextual information, which refers to event-related parameters that are inferred without accessing the report contents. Under a global model, all communications within the wireless networks are assumed to be intercepted and collectively analyzed. State-of-the-art countermeasures conceal traffic associated to real events by injecting dummy packets according to a predefined distribution. In these methods, real transmissions take place by substituting scheduled dummy transmissions, which decorrelates the occurrence of an event from the eavesdropped traffic patterns. However, concealment of contextual information comes at the expense of high communication overhead and increased end-to-end delay for reporting events. In this section, we propose a general traffic analysis method using Received Signal Strength for inferring contextual information from jamming attacks and spoofing attacks. Our method is meant as a baseline for evaluating the performance of protection mechanisms with varying underlying assumptions. Therefore, it relies on minimal information, namely the packet interception times, jamming attacks and eavesdroppers' locations.*

Key words: SVM, Spoofing, Jamming, contextual information, Traffic analysis

1. Introduction

As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless and sensor networks, they are especially vulnerable to eavesdropping attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Eavesdropping attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of eavesdropping and eliminate them from the network. The traditional approach to address eavesdropping attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network.In this project, we take a different approach by using the physical properties associated with wireless transmissions to detect eavesdropping. Specifically, we propose a scheme for both detecting eavesdropping attacks, as well as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform eavesdropping detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes.Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and further utilize the identity information to launch identity-based attacks, in particular, the two most harmful but easy to launch attacks: 1) eavesdropping attacks and 2) Sybil attacks. In identity-based eavesdropping attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks. For instance, in an IEEE 802.11 network, it is easy for an attacker to modify its Media Access Control (MAC) address of network interface card (NIC) to another device through vendor-supplied NIC drivers or open-source NIC drivers. In addition, by masquerading as an authorized wireless access point (AP) or an authorized client, an attacker can launch denial-of-service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.Therefore; identity-based attacks will have a serious impact to the normal operation of wireless and sensor networks. It is thus desirable to detect the presence of identity-based attacks and eliminate them from the network. The traditional approach to address identity-based attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication.Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and utilize the identity information to launch identity based eavesdropping attacks in wireless and sensor networks. For instance, in an 802.11 network, it is easy for a wireless device to acquire a valid MAC address and masquerade as another device. The IEEE 802.11 protocol suite provides insufficient identity verification during message exchange, including most control and management frames. Therefore, the adversary can utilize this weakness and request various services as if it were another user. Identity-based eavesdropping attacks are a serious threat in the network, because they represent a form of identity compromise and can facilitate a series of traffic injection attacks, including eavesdropping-based attacks. For instance, an adversary can launch a de authentication attack. After a client chooses an AP for future communication, it must authenticate itself to the AP before the communication session starts. Both the client and the AP are allowed to explicitly request for de authentication to void the existing authentication relationship with each other. Unfortunately, this de authentication message is not authenticated. Therefore, an attacker can spoof this de authentication message, either on behalf of the client or on behalf of the AP. The adversary can persistently repeat this attack and completely prevent the client from transmitting or receiving. Furthermore, an attacker can utilize identity eavesdropping and launch the rogue AP attack against the wireless network. In the rogue AP attack, the adversary first sets up a rogue AP with the same MAC address and service set identifier as the legitimate AP but with a stronger signal. When a station enters the coverage of the rogue AP, the default network configuration will make the station automatically associate with the rogue AP, which has a stronger signal. Then, the adversary can take actions to influence the communication. For example, it can direct fake traffic to the associated station or drop the requests made by the station. Aside from the basic packet-flooding attacks, the adversary can make use of identity eavesdropping to perform more sophisticated flooding attacks on APs, such as probe request, authentication request, and association request flooding attacks. Received Signal Strength 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 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. 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 different locations in physical space are distinctive.

During the localization process, the following steps will take place:

1. A Transmitter sends a packet. Some number of Landmarks observes the packet and records the RSS.
2. Each Landmark forwards the observed RSS from the transmitter to the Server.
3. The Server collects the complete RSS vector for the transmitter and sends the information to a Solver instance for location estimation.
4. The Solver instance performs localization and returns the coordinates of the transmitter back to the Server.

1.1 literature survey

Muhammad Akhlaq et al [1]RTSP: An Accurate and Energy-Efficient Protocol for Clock Synchronization in WSNs. Recursive Time Synchronization Protocol (RTSP) which accurately synchronizes all the nodes in a network to a global clock using multi-hop architecture in an energy-efficient way. RTSP Algorithm Used. Reducing the number of time synchronization requests through the adaptive re-synchronization interval and aggregation of synchronization requests.

Another approach is Muhammad Akhlaq [2] proposed the study of Statistical Framework for Source Anonymity in Sensor Networks. It introduces the notion of "interval in distinguish ability" and provides a quantitative measure to model anonymity in wireless sensor networks; second, it maps source anonymity to the statistical problem of binary hypothesis testing with nuisance parameters. We then analyze existing solutions for designing anonymous sensor networks using the proposed model analyze existing solutions for designing anonymous sensor networks using the proposed model. Anonymity, hypothesis testing, nuisance parameters.We transform the problem from analyzing real-valued sample points to binary codes, which opens the door for coding theory to be incorporated into the study of anonymous sensor networks.

Another approach is Frederik Armknecht and Joao Girao [3] proposed the study of Privacy at link layer..The widespread usage of these technologies comes at the price of location privacy, be it by observing the communication patterns or the interface identifiers. Although a number of network level solutions have been proposed, describes a novel approach to location privacy at the link layer level. Re-synchronization Mechanism. Used in conjunction with a pseudonym mechanism to prevent tracking by active communicating peers, this could be an interesting new direction for our work. Nevertheless, our approach provides privacy at the link layer without significantly undermining the performance of the network.

Another approach is Matthias Fruth [4] proposed the study of Probabilistic Model Checking of Contention Resolution in the IEEE 802.15.4 Low-Rate Wireless Personal Area Network Protocol. Verify correctness properties, compare different operation modes of the protocol, and analyze performance and accuracy of different model abstractions.

Used IEEE 802.3 for Ethernet and IEEE 802.11 for Wireless LAN. New scenarios could contain a larger number of stations and more complex behaviors' of the stations, such as transmitting more than one message per station and allowing stations to send and to receive.

Another approach is Xi Luo, Xu Ji [5] proposed the study of Location Privacy against Traffic Analysis Attacks in Wireless Sensor Network. Firstly, a random routing scheme (RRS) is proposed to provide path diversity. Secondly, we combine RRS with a dummy packet injection scheme (DPIS) to confuse the adversary by tracing or tracing back the forwarded packet to reach the receiver or source. Finally, an anonymous communication scheme (ACS) is proposed to hide the identities of all nodes that participate in packets transmission. Random Routing. Through the security analysis and performance analysis, we can see our proposed scheme can effectively prevent the traffic analysis attacks, and has the less delivery time and energy consumption compared

Another approach is Ben Greenstein [6] proposed the study of Improving Wireless Privacy with an Identifier FreeLink Layer Protocol. Nearly as efficient as existing schemes such as WPA for discovery, link setup, and data deliverydespite its heightened protections; transmission requires only symmetric key encryption and reception requires a table lookup followed by symmetric key decryption. Anonymity. Showed how a link layer could use two mechanisms, Tryst and Shroud, to perform this obfuscation while still achieving efficient discovery, link establishment, and data transport, and without sacrificing other crucial link layer functions such as higher layer name binding

Another approach is Yong Xi [8] proposed the study of Preserving Source Location Privacy in MonitoringBased Wireless Sensor Networks. They propose GROW (Greedy Random Walk), a two-way random walk, i.e., from both source and sink, to reduce the chance an eavesdropper can collect the location information. We improve the delivery rate by using local broadcasting and greedy forwarding. Privacy protection is verified under a backtracking attack model. The message delivery time is a little longer than that of the broadcasting-based approach, but it is still acceptable if we consider the enhanced privacy preserving capability of this new approach. GROW Algorithm. Can monitor the traffic and deduce the approximate location of monitored objects in certain situations.

Another approach is Celal Ozturk [7] proposed the study of Source Location Privacy in Energy Constrained Sensor Networks. While developing and evaluating our privacy-aware routing protocols; we jointly consider issues of location-privacy as well as the amount of energy consumed by the sensor network. Motivated by the observations, we propose a flexible routing strategy, known as phantom routing, which protects the source's location. Source-Location Privacy. Our investigations have shown that phantom routing is a powerful technique for protecting the location of the source during sensor transmissions

2. PROPOSED WORK

In this proposed work, we build a efficient traffic randomization for hiding contextual information in event-driven WSNs, under a global adversary may study. Our main contributions are summarized as follows: This system presents a general traffic analysis method for inferring contextual information that is used as a baseline for comparing methods with varying assumptions and it can obtain the Received Signal Strength in receiver end from the signal transmission of the sender. It can calculate the signal variation to obtain the location of the eavesdropper.

Our method relies on minimal information, namely packet transmission time and eavesdropping location. This system proposes traffic normalization methods that hide the event location, its occurrence time, and the sink location from global eavesdroppers. Compared to existing approaches, our methods reduce the communication and delay overheads by limiting the injected bogus traffic. This is achieved by constructing minimum connected dominating sets (MCDSs) and MCDSs with shortest paths to the sink (SSMCDSs). Here a loose transmission coordination scheme that reduces the end to end delay for the reporting events. The schemes in LTC cannot be combined with each other these techniques send the optimal packets appropriate times or through appropriate paths.

Advantages:

- Overcome the drawback of eavesdropper's localization.
- The proposed system reduces the communication and delay overheads by limiting the injected bogus traffic.
- The proposed system reduces the forwarding delay

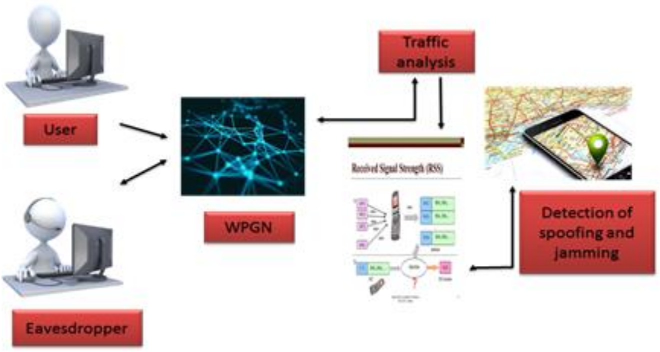

User
Eavesdropper
WPGN
Traffic analysis
Received Signal Strength (RSS)
Detection of spoofing and jamming

Fig. 1 System Architecture

Fig. 1 shows the architecture of our model.users send the message to the other user using WPGN(wireless power grid network).At the same time eavesdropper view the message from WPGN. So that hacker can easily gather the information. Attacker can be detected based on the traffic analysis using RSS algorithm(received signal strength) sometimes referred as RSSI (Received signal strength indicator) is a measurement of the power present in a received radio signal. The nodes used by the Accurate WiFi Location Monitor and Bluetooth Beacon Tracker are capable of measuring the RSS of nearby Wi-Fi and BLE devices.The RSS values are measured in dBm and have typical negative values ranging between 0 dBm (excellent signal) and -110 dBm (extremely poor signal). By using RSS we can analysis both active and passive attack .finally the location of the hacker can be analysed and mitigation them.

2.1 PROBLEM FORMULATION

To formulate our problem, Moreover, our attack strategy, RSS, is designed on the basis of the features of jamming and spoofing attacks. The attack effects can be counted in either probability or return values the operating principles of jamming and spoofing attacks in SVM. This shows the characteristics of SVM the various power levels are required for classify the attack strategy. The threshold value can determine the location of attacker. The height of each cube illustrates the power level required by adversaries. The distinctness of the heights shows the variety of demanded powers. The adversarial positions are marked in the figure. In addition, represents a SVM frame structure that consists of a sensing and a transmission message. In SVM, the vulnerabilities often address.

The periodic sensing stage in which the secondary users are searching available location.

Max [V wtotal; Prtotal] = Max [Xs (i) V w (i);Y s(i) Pr(i)] (1)
Where
Xs (i)V w (i) =Xs(i)=0V w(i) +Xs(i)=1V w(i) (2)
and Ys(i)Pr(i) =Ys(i)=0Pr(i) -Ys(i)=1Pr(i) (3)

Under a power constraint (Pw).Furthermore, our approach aims to find out an optimal adversarial plan when the level of available power Pw is fixed.To consider the total return value, we give the objective function

Of the problem in Eq. (1), which shows that the goal is to maximize the pair (V wtotal, Prtotal) under the given power constraint Pw. Given a binary function s(i), s(i) = 1 when J attack is applied and s(i) = 0 when S attack is applied.The total attack return value V wtotal is a sum of all return values from all frequency spectrums, expressed in Eq. (2).Additionally, the adversarial strategy will depend on the attack success probabilities. The method of calculating total Prtotal is shown in Eq. (3) that is a production of all probabilities.Using our proposed approach can dynamically switch attack methods between jamming and spoofing in order to reach the Optimum attack performance and mitigate them.

Generate Algorithm:

Notations used in algorithms are given as follows: Pk I;j denotes

The probability of ith frequency spectrum with the power value j. k is the index number. V ki;j denotes the value weight of ith frequency spectrum with the power value j. Additionally, we define an operator "_" for calculating probabilities and value weights, which is used for the purpose of pair alternatives. The_ definition is given in 9 two pairs (Pi, Vi) and (Pj , Vj). then (Pi, Vi)_ (Pj , Vj) = (Pi _ Pj , Vi + Vj) 9 two pair lists Li, Lj , then Li _ Lj will _ all random pairs from Li and Lj . RSS, is designed to generate a D-Table. Input of this algorithm is a Basic Table (B-Table) that maps all the values of Pr and Vw for each spectrum within all power constraints. In the D-Table, all optimal solutions with Parameters Pr and Vw are provided, which represents an attack Strategy plan. An efficient attack strategy to WSGN can be obtained by selecting one solution matching the attack preferences. The attack plan generated from MAS algorithm is an optimal solution, which relies on Theorem 5.1. The proof of generation of the RSS algorithm

Theorem 5.1 is also given below.

Algorithm 5.1 RECEIVED SIGNAL STRENGTH (RSS) Algorithm

```
Require: Attacker location
Ensure:   Mitigation of attack
A1;j   M1;j
for 8 Fi, i>1 do
    for 8 Power j do
        for 8 Power k in Mi;k do
            if Ai⍰1;j⍰k != null then
                Ai;j = Ai⍰1;j⍰k _ M i;k
            end if
        end for
        Mitigation of the attacker applying Algorithm 5.2
    end for
end for
Return Location of the attacker (contains the attack strategy plan)
```

2.2 METHODOLOGY

1. Wireless Network Formation:

Two Bluetooth devices are considered with the code application come into each other communication range, in order to set up a communication link.This simple"single-hop" network is called a piconet. Bluetooth technology is used for both neighbor discovery and data communication in the created piconets

2. Data collection: Detection of Eavesdropping Attacks:

Using received signal strength (RSS)-based spatial correlation, utilizing spatial information to address spoofing attack.unique power to not only identify the presence of these attacks but also localize adversaries.An added advantage of employing spatial correlation will not require any additional cost or modification to the wireless devices themselves. The above analysis provides the theoretical support of using the RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection.

3. DETERMINATION OF NUMBER OF ATTACKERS:

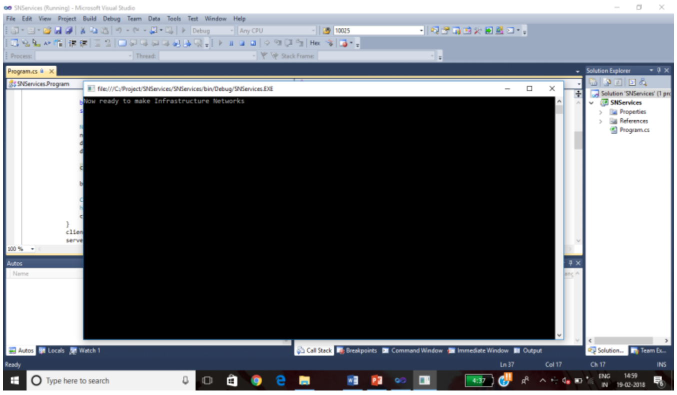
To determining the number of attackers becomes a multiclass detection problem and is similar to determining how many clusters exist in the RSS readings.A Silhouette Plot is a graphical representation of a cluster that used to determine the number of attackers. The System Evolution method performs well under difficult cases, such as System Evolution and SILENCE. Support Vector Machines to classify the number of the spoofing attackers. it can combine the intermediate results.

4. MITIGATION OF SPOOFING ATTACKS:

In this module, using traffic correlation analysis, the spoofing attackers should be monitored and mitigated from the wireless networks .It does not affect the wireless network legitimate mobile nodes by means of proposed novel approach for mitigating the multiple spoofing attacks.

3. EXPERIMENTAL RESELT

A set of experiments carried out on spoofing and jamming attack .The performance evaluation of the system is performing using this dataset. The screenshots of various phases of Detection of spoofing and jamming attack are as follows:


SNServices (Running) - Microsoft Visual Studio
File Edit View Project Build Debug Team Data Tools Test Window Help
Program.cs
SNServices.Program
file:///C:/Project/SNServices/SNServices/bin/Debug/SNServices.EXE
Solution Explorer
Solution 'SNServices'
SNServices
Properties
References
Program.cs
Autos
Type here to search

```
Now ready to make Infrastructure Networks
```

FIG.2 REPRESENT THE NETWORK FORMATION AND THE EXCUTION SERVICE

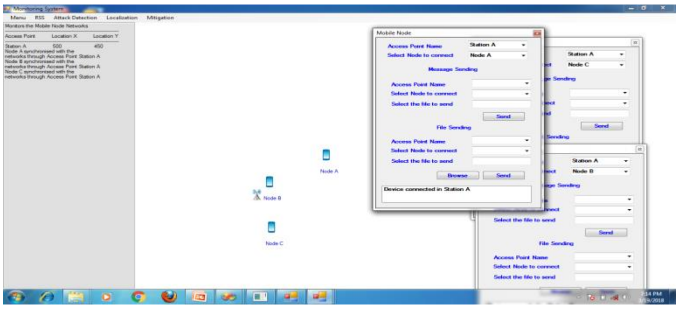


FIG-3 REPRESENT THE MOBILE NODE FORMATION

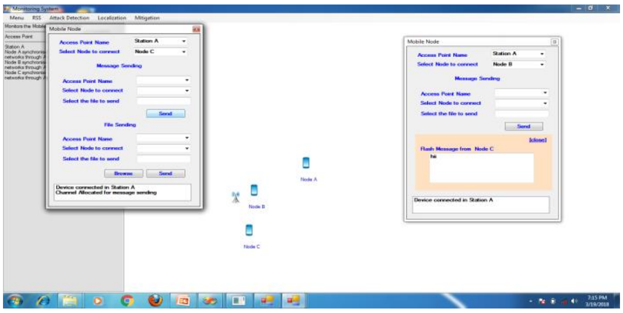
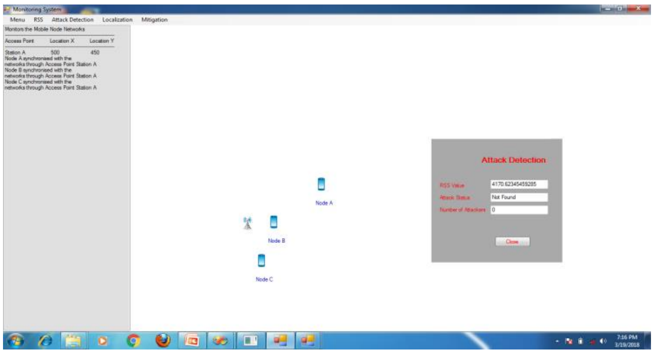
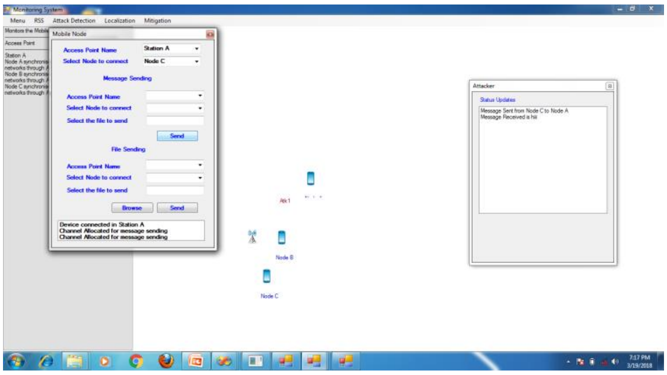

Monitoring System
Menu RSS Attack Detection Localization Mitigation
Mobile Node
Access Point Name
Select Node to connect
Message Sending
File Sending
Send
Browse
Flash Message from Node C
Device connected in Station A
Channel Allocated for message sending
Node A
Node B
Node C

FIG-4 REPRESENT THE MESSAGE PASSING THROW ONE NODE TO ANOTHER NODE



RSS Value: 4170.62345459285
Attack Status: Not Found
Number of Attackers: 0

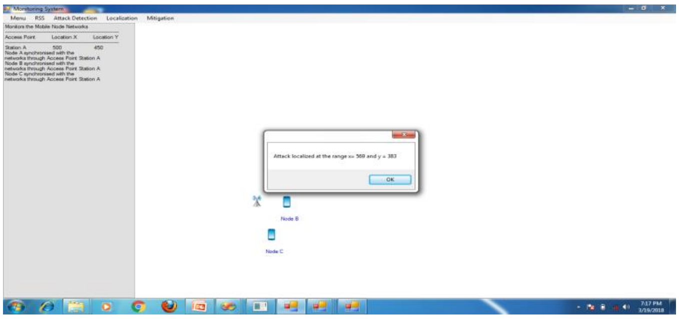
FIG-5 REPRESENT THE DETECTION OF ATTACKS



Device connected in Station A
Channel Allocated for message sending
Channel Allocated for message sending

Message Sent from Node C to Node A
Message Received is hiii

FIG-6 REPRESENT THE MESSAGE CAN RECEIVED BY THE ATTACKER



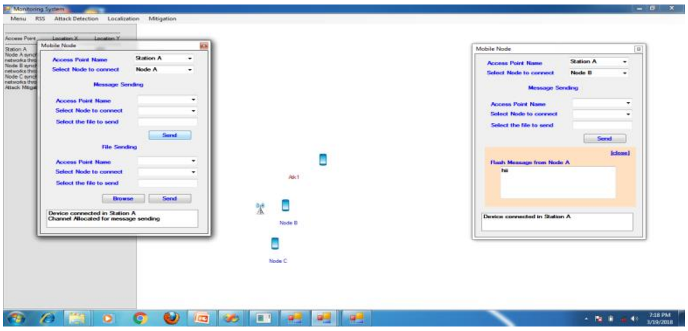
Monitors the Mobile Node Networks

Access Point	Location X	Location Y
Station A	500	450

Node A synchronised with the networks through Access Point Station A
Node B synchronised with the networks through Access Point Station A
Node C synchronised with the networks through Access Point Station A

Attack localized at the range x= 569 and y = 383

FIG-7 REPRESENT LOCATION OF THE ATTACKER (LOCALIZATION)



Access Point Name: Station A
Select Node to connect: Node A
Access Point Name:
Select Node to connect:
Select the file to send:

Device connected in Station A
Channel Allocated for message sending

Access Point Name: Station A
Select Node to connect: Node B

Flash Message from Node A
hii

Device connected in Station A

FIG-8 REPRESENT THE MITIGATION OF ATTACKS

4. CONCLUSION

In this work, here the system 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. Our approach can detect 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.

5. FUTURE ENHANCEMENT

In addition to the spoofing attacks, the insider attacks will be considered in future to mitigate and identify the legitimate user resemblance. The cryptographic techniques should be used in future if the eavesdropper obtained the data

REFERENCES:

[1] J. Muhammad Akhlaq."IEEE Std. 1588-2008", *IEEE* Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, 2008.

[2] J. Muhammad Akhlaq "Statistical Framework for Source Anonymity in Sensor Networks", Proc. IEEE Globe Com, 2013.

[3] Frederik Armknecht and Joao Girao, IEEE Standard 802.11. IEEE standard for information technology - telecommunications and information exchange between systems -local and metropolitan area networks - specific requirements, part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 2007.

[4]Matthias Fruth, "IEEE Standard 802.15.4–2003: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", IEEE Computer Society, 2007

[5] Xi Luo, Xu Ji,"A Novel Scheme for Protecting Receiver's Location Privacy in Wireless Sensor Networks", Proc. of IEEE Teansactions on Wireless Communications, vol. 7, no. 10, October 2010

[6] Ben Greenstein, "Improving Wireless Privacy with an Identifier-Free Link Layer Protocol, 2008

[7] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy constrained sensor network routing," in SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, (New York, NY, USA), pp. 88-93, ACM, 2004

[8]Yong Xi, "Preserving source location privacy in monitoring-based wireless sensor networks." in IPDPS, IEEE, 2006.

BIOGRAPHIES:

Suganthi.K recehived B.TECH Degree in Information Technology from Anna University affiliated college in 2005and M.Tech Degree from Prist University in 2014. She is currently working as Assistant Professor in the Dept. of Computer Science and Engineering, Arasu Engineering College, Kumbakonam.

Sahana.K pursuing B.E Degree in the stream of computer science and engineering at Arasu engineering college kumbakonam

Santhiya.G pursuing B.E Degree in the stream of computer science and engineering at Arasu engineering college kumbakonam

Swathi.S pursuing B.E Degree in the stream of computer science and engineering at Arasu engineering college kumbakonam