International Journal of Electrical and Electronic Engineering & Telecommunications

ISSN 2319 – 2518 www.ijeetc.com
Special Issue, Vol. 1, No. 1, March 2015
National Level Technical Conference P&E- BiDD-2015

Research Paper

NODE RELIABILITY AND AUTHENTICATION TO IMPROVE NETWORK PERFORMANCE FOR WIRELESS SENSOR NETWORK USING RECEIVED SIGNAL STRENGTH (RSS)

Marie Claude[1]* and R Kalaivani[1]

*Corresponding Author: Marie Claude, ✉ nmclaude@yahoo.com

Wireless attacks are generally easy to launch and can significantly impact the performance of Wireless Sensor Networks (WSN). Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. We propose to use spatial information, a physical property associated with each node, hard to falsify. To use the spatial correlation of Received Signal Strength (RSS) in the form of energy inherited from wireless nodes to detect the attacks. We formulate the problem of determining the number of attackers as a multiclass detection problem. Cluster-based mechanisms are developed to determine the number of attackers. We evaluated our techniques through real time network for active and asleep node by putting spoof attack. Our experimental results show that our proposed methods can achieve over 90% Hit Rate and Precision when determining the number of attackers. Our localization result using a representative set of algorithm provides strong evidence of high accuracy of localizing multiple adversaries and plots the energy graph for the node in the network.

Keywords: Wireless sensor networks, Received signal strength

INTRODUCTION

A Wireless Sensor Network (WSN) (sometimes called a Wireless Sensor and Actor Network (WSAN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by

[1] Department of CSE, IFET College of Engineering, Villupuram, India.

military applications such as battlefield surveillance. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes"—from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

PROBLEM STATEMENT

Existing System

Secure data transmission is a critical issue for Wireless Sensor Networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. Two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. A secure data transmission for Cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. The outputs are checked for network security overhead and energy consumption.

Drawbacks

- Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks
- Not self-defensive
- Effective only when implemented by large number of network
- Deployment is costly
- Incentive for an ISP is very low

PROPOSED SYSTEM

In this project to show that our proposed system deals with the real time creation of network and its weight analysis. After providing the network topology we prioritize the node for connection. We check our network efficiency against perfect data transmission and against spoofing attack. We check for active and inactive node on the complete network to provide attack. Then we finally analyze the network for complete packet loss on network and energy used graph plot to finally examine the network efficiency.

Advantages

GADE: A generalized attack detection model (GADE) that can both detect spoofing attacks

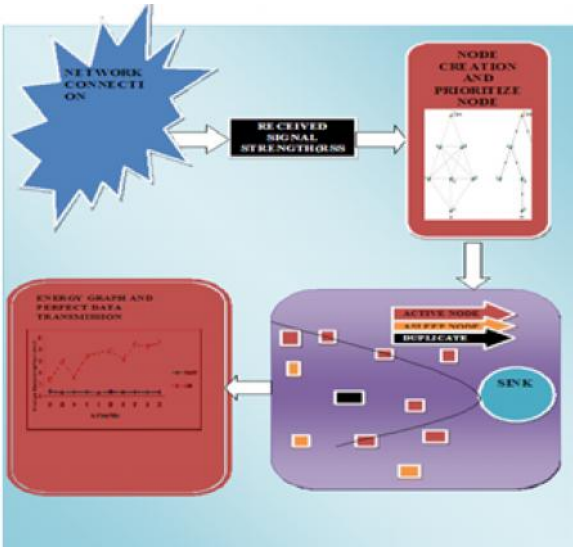
as well as determine the number of adversaries using cluster analysis methods grounded on RSS-based spatial correlations among normal devices and adversaries

IDOL: An integrated detection and localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. Damage Reduction under SPM Defense is high. Client Traffic. Comparing to other methods the benefits of SPM are more. SPM is generic because their only goal is to filter spoofed packets.

SYSTEM ARCHITECTURE

The System Architecture is shown in Figure 1.

Figure 1: System Architecture



RECEIVED SIGNAL STRENGTH (RSS)

Received Signal Strength is a radio frequency Signal which analyzed energy consumption of the WSN's. When used RSS algorithm real time weight analysis and check perfect data transmission and network efficiency. It is short time solution and cost effective.

RSS Calculation

In telecommunications, Received Signal Strength Indicator (RSSI) is a measurement of the power present in a received radio signal. RSSI is a generic radio receiver technology metric, which is usually invisible to the user of the device containing the receiver, but is directly known to users of wireless networking of IEEE 802.11 protocol family. RSSI is often done in the Intermediate Frequency (IF) stage before the IF amplifier. In zero-IF systems, it is done in the baseband signal chain, before the baseband amplifier. RSSI output is often a DC analog level. It can also be sampled by an internal ADC and the resulting codes available directly or via peripheral or internal processor bus.

RSS Formula

$$P(d)[dBm] = P(d0)[dBm] - 10 \text{ ylog}_{10} (d/d0)$$

where,

P(d) is the signal strength at distance d P(d0) is the signal strength reference distance d0 (dBm). Unknown node receives a plurality of RSSI value of anchor nodes, then, it calculates the distance between nodes according to the channel model. Firstly, three anchor nodes first received are used to preliminary calculate positions of unknown node. For all the received messages, each group of three, namely to calculate the position of the unknown node. Finally, all calculations position in the collection is averaged, which is the estimated position of unknown nodes.

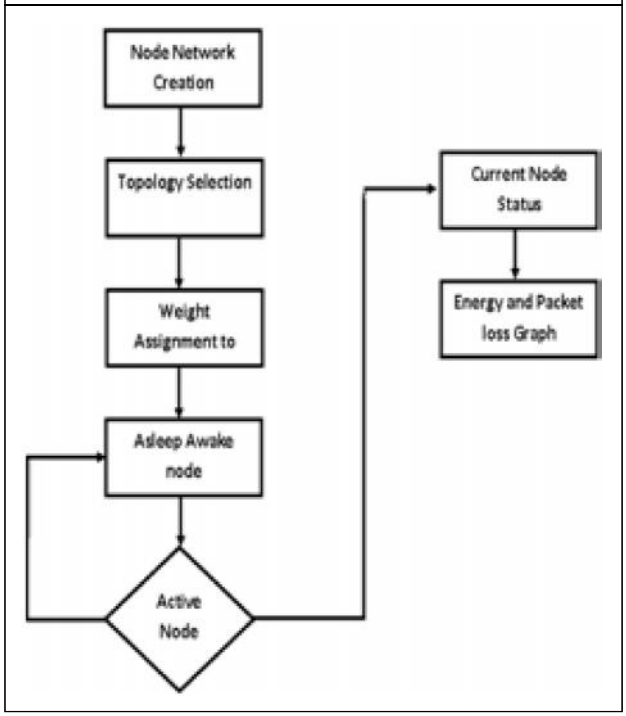
As can be seen, location positioning algorithm first rough calculates position of

unknown nodes, and then gradually Increases the positioning accuracy of unknown nodes by a plurality of similar process. As the number of nodes increases, the computational complexity will grow exponentially, not suitable for sensor network localization requirements.

MODULE DESCRIPTION

- Blind and Non-Blind Spoofing
- Man in the Middle Attack
- Constructing Routing Table
- Finding Feasible path
- Inter-Domain Packet Filter Construction
- Packet Validation

Figure 2: Dataflow Diagram



Blind and Non-Blind Spoofing

Spoofing detection is to devise strategies that use the uniqueness of spatial information. In location directly as the attackers' positions are unknown network RSS, a property closely correlated with location in physical space and is readily available in the wireless networks. The RSS readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive. The number of attackers when there are multiple adversaries masquerading as the same identity.

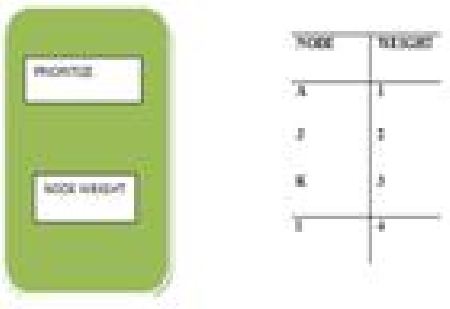
Man in the Middle Attack

Localization is based on the assumption that all measurements gathered Received Signal Strength (RSS) are from a single station and, based on this assumption, the localization algorithm matches a point in the measurement space with a point in the physical space. The spoofing attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings of that ID is the mixture readings measured from each individual node.

Constructing Routing Table

The channel frequency response is sensitive to each multipath. An impulse in the time domain is a constant in the frequency domain, and thus a change to a single path may change the entire multiple tone link of Network. In wireless networks classes that provide automatic reconfiguration of APs, adjusting power levels and channel assignments to

Figure 3: Node Weight Analysis



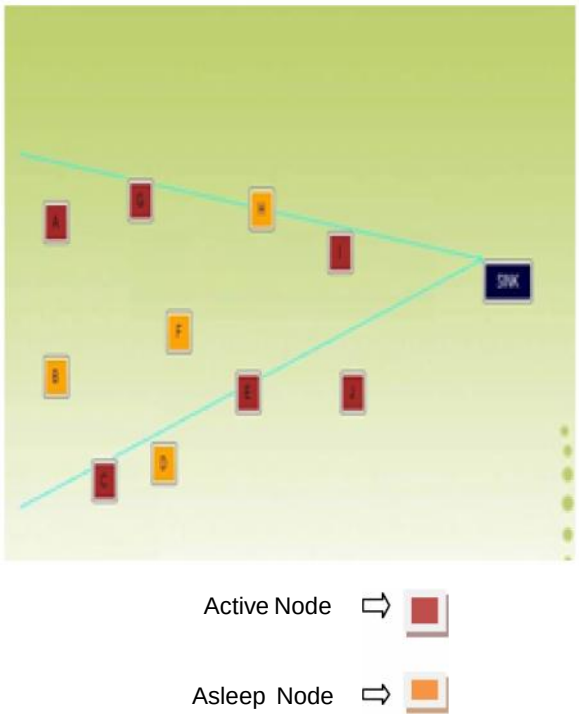
optimize coverage while minimizing contention between neighbors.

To propose Received Signal Strength prioritized each sensor nodes. When it analyzed received packet and dropped packet. It checks to network efficiency and data transmission for received packet.

Finding Feasible Path (Attack Computation)

Converting the large dataset into medium format for the computation purpose. In this medium the rows consists of http request and columns consists of time for a particular user (IP address). 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 active and asleep nodes range shown in Figure 4.

Figure 4: Active and Asleep Nodes Range



Inter-Domain Packet Filter Construction

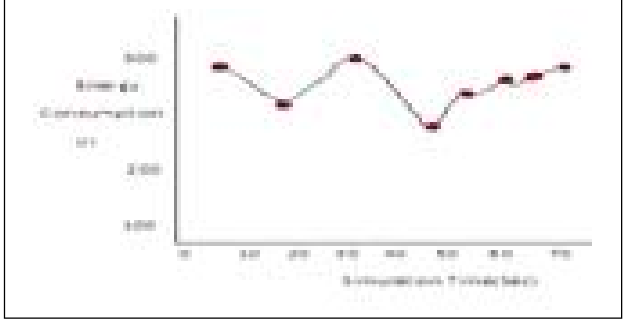
The clustering algorithms cannot tell the difference between real RSS clusters formed by attackers at different positions and fake RSS clusters caused by outliers and variations of the signal strength. The minimum distance between two clusters is large indicating that the clusters are from different physical locations.

Packet Validation

The transmission power levels when performing spoofing attacks so that the localization system cannot estimate its location accurately. The CDF of localization error of RADAR Gridded and ABP when adversaries using different transmission power levels. In detection mechanisms are highly effective in both detecting the presence of attacks with

Detection rates over 98% and determining the number of network.

Figure 5: Energy Graph

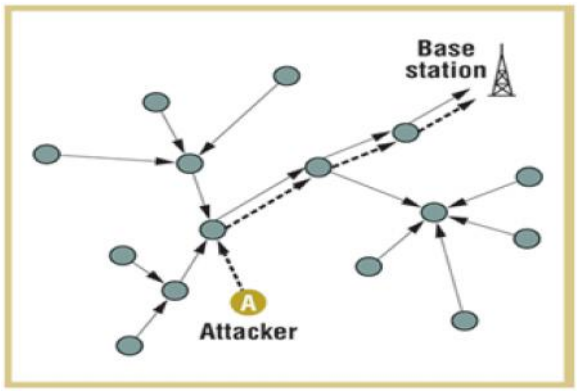


SECURITY ANALYSIS

Spoofing Attack

A spoofing attack is when a malicious party impersonates another device or users on a network in order to launch attacks against network hosts, steal data, spread malware or by pass access controls. There are several

Figure 6: Spoof Attack



different types of spoofing attacks that malicious party.

We applied spoofing attack in given network when analyzed our network's efficiency and perfect data transmission.

CONCLUSION

Thus a system of RSS based security system for WSN is achieved and tested for perfect transmission against spoofing attack. The energy graph is plotted finally for the proposed project.

FUTURE ENHANCEMENT

In this work, we propose to use Received Signal Atrength (RSS) based spatial correlation, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. In future we can increase the efficiency of detecting the attacker and also we have to drop the attacker level actions. For this, we should for the efficient algorithm

REFERENCES

1. Abbasi A A and Younis M (2007), "A Survey on Clustering Algorithms for Wireless Sensor Networks", *Computer Comm.*, Vol. 30, Nos. 14/15, pp. 2826-2841.
2. Hara T, Zadorozhny V I and Buchman E (2010), "Wireless Sensor Network Technologies for the Information Explosion Era", *Studies in Computational Intelligence*, Vol. 278, Springer-Verlag.
3. Heinzelman W, Chandrakasan A and Balakrishnan H (2012), "An Application-Specific Protocol Architecture for Wireless Micro Sensor Networks", *IEEE Trans. Wireless Comm.*, Vol. 1, No. 4, pp. 660-670.
4. Manjeshwar A, Zeng Q-A and Agrawal D P (2010), "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol", *IEEE Trans. Parallel & Distributed Systems*, Vol. 13, No. 12, pp. 1290-1302.
5. Wang Y, Attebury G and Ramamurthy B (2012), "A Survey of Security Issues in Wireless Sensor Networks", *IEEE Comm. Surveys & Tutorials*, Vol. 8, No. 2, pp. 2-23, 2nd Quarter.
6. Yi S *et al.* (2013), "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks", *Computer Comm.*, Vol. 30, Nos. 14/15, pp. 2842-2852.