Detection and Localization of Multiple Spoofing Attackers Using Asymmetric Key Cryptography Algorithm for Wireless Sensor Network

Cherukuri Srikanth, K. Vadivukkarasi

Abstract— **Due to the openness of the wireless transmission medium, adversaries can monitor any transmission. Further, adversaries can easily purchase low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with little effort .These attacks affect the network performance and leads to easy access of secured data .The main aim of this project is to detect and prevent unauthorized access of wireless data from spoofed using Zigbee technology. Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, these approaches are not always desirable because of their overhead requirements .In this project, we propose to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity, and localizing multiple adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks.**

Keyword— **Mac Address, Cryptography, Encryption, Decryption, WSN, Zigbee, RSSI.**

I. INTRODUCTION

A Wireless sensor network (wsn) 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 network are bi-directional, also enabling control of sensor activity. The development of wireless sensor network was motivated by 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.

And security also is very important this is 1.detect the presence of spoofing attacks, 2. Determine the number of attackers, and 3.localize multiple adversaries and eliminate the them. Most existing approaches employ cryptographic schemes to address potential spoofing attacks. However, the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods. Because of its infrastructural, computational, and management Overhead. Further, cryptographic methods because of its infrastructural, computational, and management overhead further, cryptographic methods are susceptible to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be Easily scanned. This paper proposes to use RSS-based spatial Correlation, a physical property associated with each wireless node that is heard to falsify and not relent on cryptography as the basis for detecting spoofing attacks. Since the concern is on the attackers who have different location then legitimate wireless node, utilizing spatial

Information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. An added advantage of employing spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves.

II. SYSTEM MODEL

The CC2530 comes in three different flash versions CC2530F32/64/128, with 32/64/128 KB of flash memory respectively, the CC2530 is a true system on chip solution specifically tailored for IEEE 802.15.4 and ZigBee applications. It enables ZigBee nodes to be built with very low total bill of material cost. The CC2530 combines the excellent performance of the leading CC2530 RF transistor with an industry standard enhanced 8051 MCU, 32/64/128 KB flash memory, 8KB RAM and many other powerful features combined with the industry leading ZigBee protocol stack (z-stack) from Texas instruments, the CC2530 provides the market's most competitive ZigBee solution. The CC2530 is highly suited for systems where ultra low power consumption is required. This is ensured by various modes further ensure

Manuscript received March 25, 2015

Cherukuri Srikanth is currently pursuing masters degree program in embedded system technology in SRM University, India, PH-+919043638514.

K. Vadivukkarasi is currently pursuing masters degree program in electric power engineering in SRM University, India, PH-+918939055377.

low power consumption.

In Figure 1. Three nodes are being used, one coordinator node and two end devices. Each node consists of 8051 microcontroller, CC2530 RF Transceiver and battery. Authorized end device is interfaced with PIR (Passive Infrared Sensor) sensor and GPS (Global Positioning System). Coordinator node is interfaced with PC.

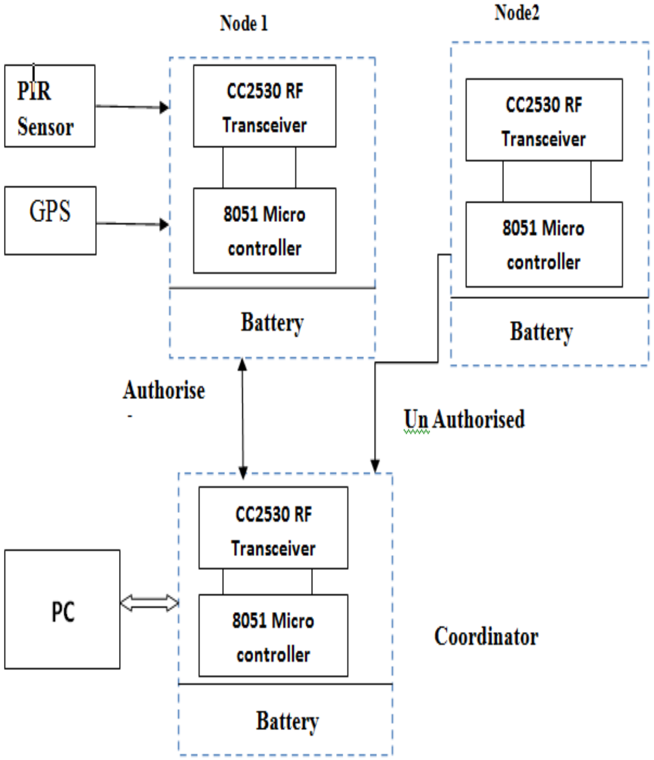


Fig. 1

III. CRYPTOGRAPHY

Cryptography an art of hiding the text intelligence, is used to resolve crucial security issues. Cryptography is way of secret writing where original meaningful data is transformed to a non meaningful data. Cryptography is done in two types of algorithm. That is

1. Asymmetric,
2. Symmetric.

A. *Public key cryptography*

Public key cryptography or asymmetric cryptography employs different keys for encryption and decryption. The key used for encryption is public key. Sender can encrypt the data using public key which is open for everyone, but only receiver has the private decryption key to obtain the original message.

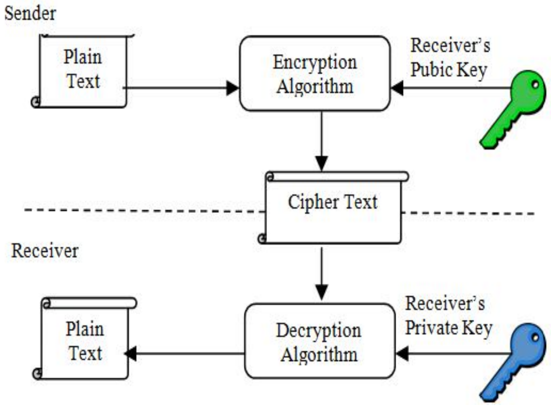


Fig .2

B. *Symmetric key cryptography*

Symmetric key cryptography uses the single key for both encryption and decryption. It is shared by parties at both the ends. As represented in fig.2, the same key has been used by both sender and receiver.

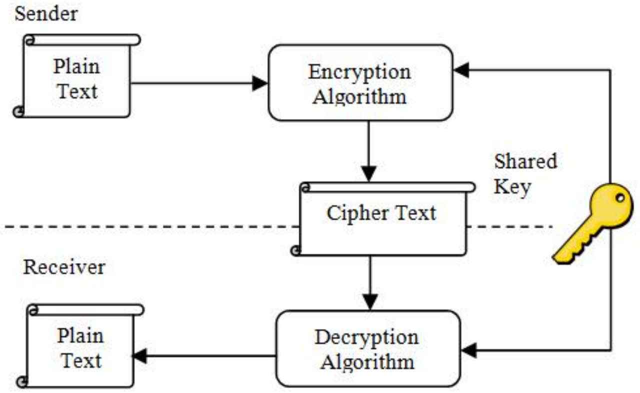


Fig .3

Compare to the both algorithms for secured algorithm is asymmetric key cryptography algorithm. So I have chosen Asymmetric key cryptography.

C. *Proposed algorithm*

Step 1: End device (slave node) will send its MAC (media access Control) address to the coordinator (master node).
Step 2: Coordinator takes the MAC address and checks for authentication.
Step 3: If authenticated, it will send the encrypted code to respective end device.
Step 4: End device will decrypt the received code and sends back to the coordinator.
Step 5: coordinator will compare the decrypted code send by end device (slave node) and its code.

Step 6: If the code matches, it is authorized and then data transmission will take place.
Step 7: If the code doesn't match, it will be considered as unauthorized node

D. *Flow chat*

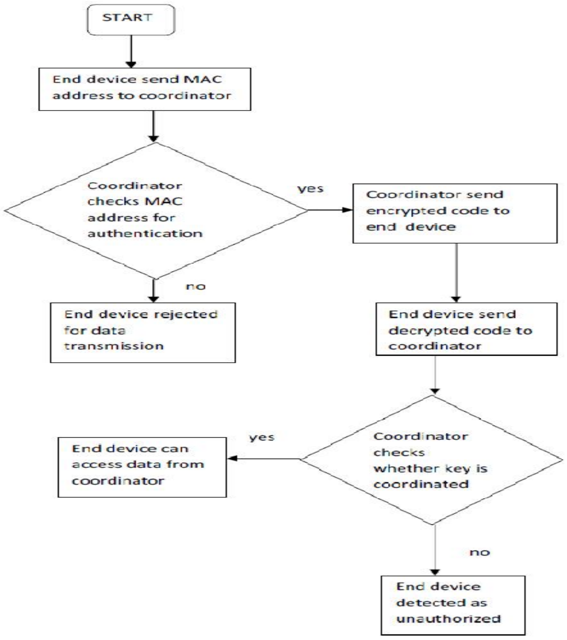
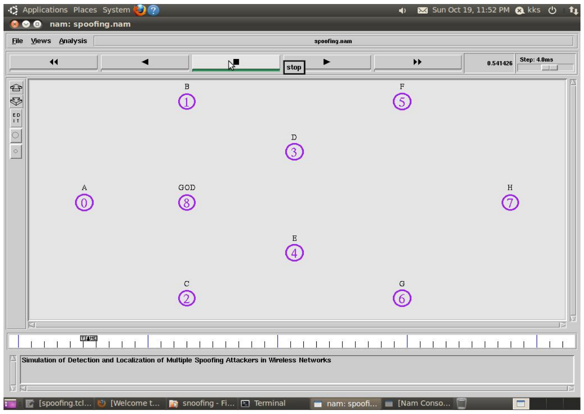

START
End device send MAC address to coordinator
Coordinator checks MAC address for authentication
yes
Coordinator send encrypted code to end device
no
End device rejected for data transmission
End device send decrypted code to coordinator
Coordinator checks whether key is coordinated
yes
End device can access data from coordinator
no
End device detected as unauthorized

Fig .4

IV. RESULT

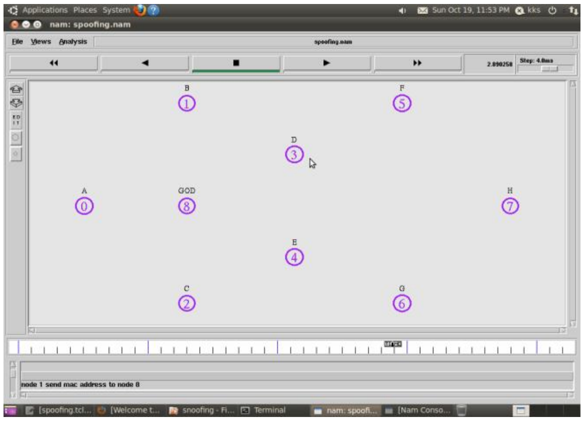
A. Simulation result



Simulation of Detection and Localization of Multiple Spoofing Attackers in Wireless Networks

Fig .5

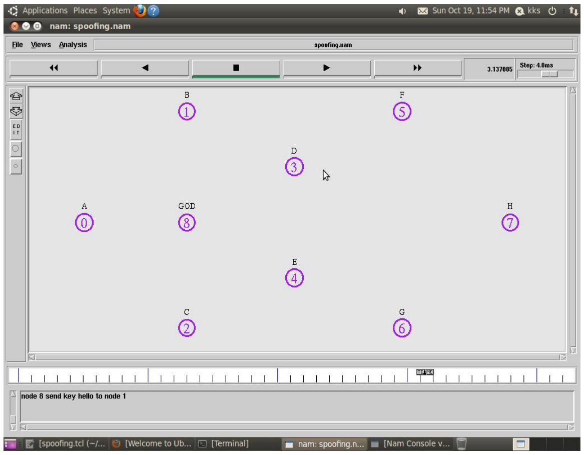
1. Detection and localization of multiple spoofing attackers in wsn.
2. fixed the nodes in x and y axis.



node 1 send mac address to node 8

Fig .6

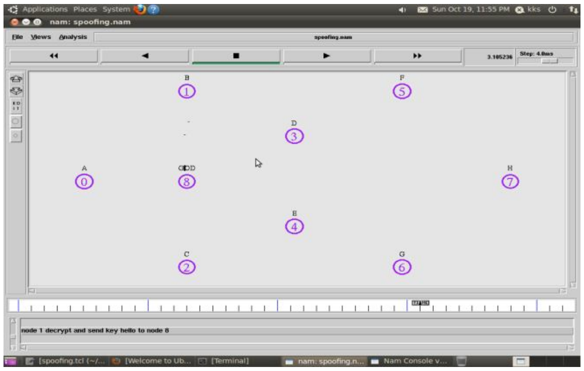
1. Node 1 sends Mac address to Node 8.
2. Node 8 is the coordinator.
3. Node 1 is the end device.



node 8 send key hello to node 1

Fig .7

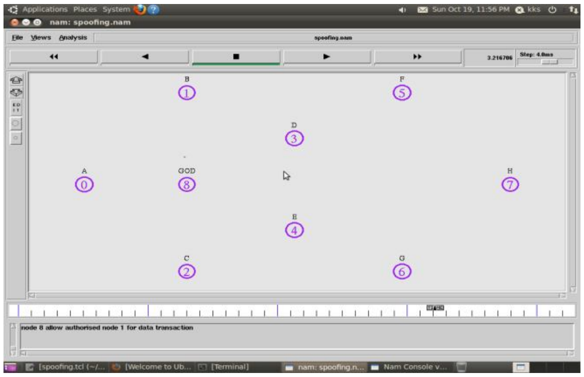
1. Node 8 send key to Node 1
2. That key should be in encrypted mode.



node 1 decrypt and send key hello to node 8

Fig .8

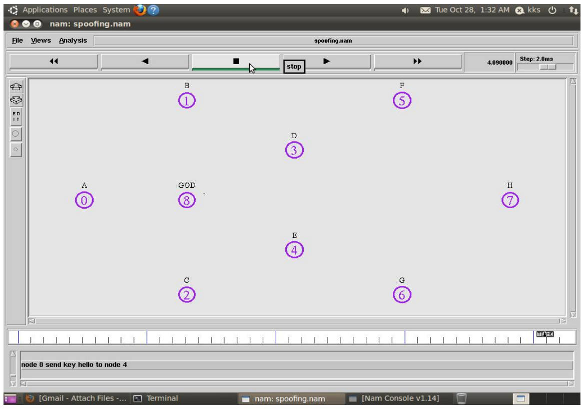
Node1 decrypt and send key hello to node



node 8 allow authorised node 1 for data transaction

Fig .9

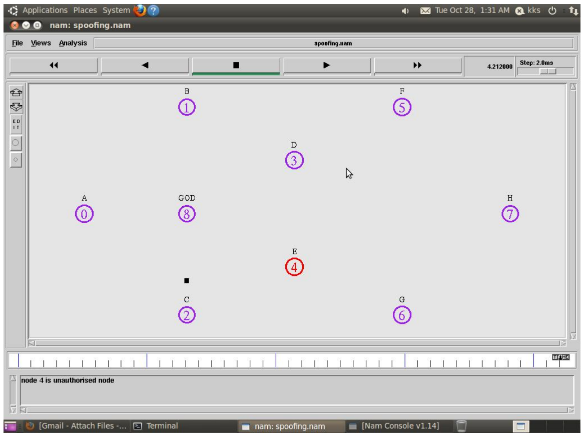
1. Node 8 declared Node 1 is authorized
2. Node 1 sending the data to Node 8.



node 8 send key hello to node 4

Fig .10

1. Node 8 will send the encrypted code to Node 4.
2. Node 4 decrypt the code and send key hello to Node 8.



node 4 is unauthorised node

Fig .11

1 .The encrypted code and decrypted code is not matched.
2. It will show Node 4 is unauthorized.

B. *Hardware result*

In the CC2530 kit first end device send the Mac address to coordinator. Coordinator will check the Mac address. If it is authorized data start transmitting, end device will send the RSSI vale to coordinator. If it is not authorized communication won’t be start.

Fig .12(CC2530 kit)

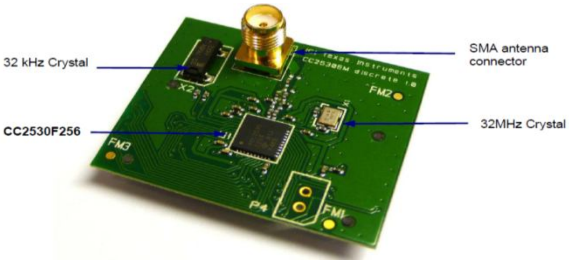


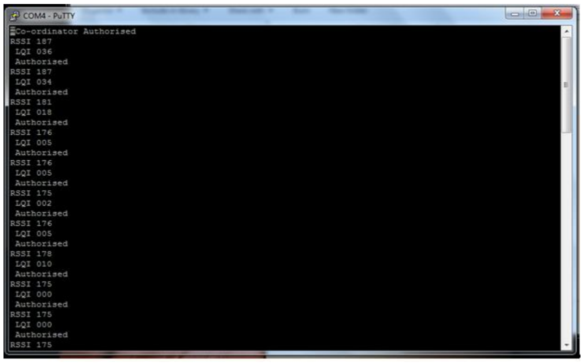
Fig .13(CC2530 EM)

C. *MAC (media access control) address*

A media access control address is a unique identifier assigned to network interfaces on the physical network segment. MAC address are used as a network address for most IEEE 802 network technology, including Ethernet and wifi logically, Mac address are used in the media access control protocol sub layer of the OSI reference model.MAC address are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card’s read only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer’s registered identification number and may be referred to as the burned in address. It may also be known as an Ethernet hardware address, hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

D. Spatial correlation of RSSI

Uniqueness of spatial information is the challenge in spoofing detection, it does not using the attackers location directly position are unknown. RSS measured the landmarks through the transmitter's physical location and governed by landmark distance.



```
Co-ordinator Authorised
RSSI 187
 LQI 036
 Authorised
RSSI 187
 LQI 034
 Authorised
RSSI 181
 LQI 018
 Authorised
RSSI 176
 LQI 005
 Authorised
RSSI 176
 LQI 005
 Authorised
RSSI 175
 LQI 002
 Authorised
RSSI 176
 LQI 005
 Authorised
RSSI 178
 LQI 010
 Authorised
RSSI 175
 LQI 000
 Authorised
RSSI 175
 LQI 000
 Authorised
RSSI 175
```

Fig .14

V. COMPARING EXISTED SYSTEM AND PROPOSED SYSTEM

Existed paper is the web based data center monitoring and alerting system. In this paper we are providing high level security using MAC and cryptography algorithm for data center monitoring, alerting and finding location.

VI. CONCLUSION

In this paper we briefly discussed about MAC address authentication, asymmetric key cryptography algorithm for security in wsn and simulated that in network simulator 2, and implemented MAC address authentication using ZigBee, if it is authorized the RSSI distance will be found.

VII. REFERENCES

[1]kiran nayak nanda, tulasi dwarakanath, haribabu,"data centre monitoring and alerting system using wsn" in 2014 IEEE conecct 1569825779.

[2]junbeom hur and kyungtae kang, "secure data retrieval for decentralized disruption tolerant military network",member,IEEE,acm vol.22 no.1 february 2014.

[3]archana tayal, prachi,'energy efficient new symmetric key algorithm for wsn"

[4]zibee alliance, zigbee specification version 17,jan 2008.

[5]D.baghyalakshmi,jemimahEbenezer,s.a.vsatyamurthy, 2011 "wsn based temperature monitoring for high performance computing on recent trends in information technology", ICRTIT.

[6]Ritika Sharma, kamalesh gupta, oct 2012," international journal of computer applications (0975-8887) volume 56-no.15.

[7] ravindra navanath puche for nisha p.sarwade , February 2014 "sensor node failure selection based on round trip delay for paths in wsn" IEEE sensor, Journal, vol 14, no.2.