Prevention of Spoofing using ZKP in Wireless Networks

Rashmi T V
Department of Information Science and Engg
BNM Institute of Technology
Bangalore,India
rashmitv@bnmit.in

Mona
Department of Information Science and Engg
BNM Institute of Technology
Bangalore,India
mona@bnmit.in

Abstract—Wireless networks are more prone to attacks and especially spoofing attack which in turn can lead to many other kinds of attacks. It is very simple to launch spoofing attacks in a wireless environment and have a significant effect on the performance of network. So, there is a need to identify the attackers and prevent spoofing. A cluster based technique is employed to identify the various attackers and prevent spoofing attacks using zero knowledge protocol (ZKP). Also, securiry which is necessary in a wireless netwoks is achieved using Elliptic curve cryptography (ECC) by taking the constrained nodes into consideration.

***Keywords*—Elliptic Curve Cryptography (ECC), Spoofing Attacks, Wireless Networks, Zero Knowledge Protocol (ZKP).**

I. INTRODUCTION

The research is going on to optimize the routing protocols in wireless networks and security is a factor that has to be given more importance in a wireless network but majority of the protocols haven't taken security into consideration. It is believed that routing protocols should be designed by keeping security in mind. Also, the nodes in wireless networks are constrained nodes with limited capabilities and the attacker may be with higher capabilities. But encrypting techniques have perpetually difficult calculation that requires more processing power. so, not fit for all forms of networks. Lately, to detect spoofing attacks, received signal strength (RSS) has been used. RSS represents the physical characteristics of wireless nodes and stations those are unique to each device and it represents the 6 signal strength at which the frame is received by the antenna. RSS value cannot be spoofed and it has correlation with the site of message sender, closer the sender is signal strength is high, far is the sender from the receiver signal strength will be low.

Attacks that spoof traffic can also result in other traffic injection attacks, including Denial-of-Service (DoS) attacks, attacks on access control lists, and attacks on rogue access points [10], [11]. [12] and [13] provide a thorough overview of potential spoofing attacks. Additionally, in a tidy network, multiple attackers may adopt the same identity and work together to launch risky attacks, like a denial-of-service attack and an attack on network resource utilisation, more quickly. As a result, it is critical to spot the presence of spoofing assaults, count the number of attackers, identify the various attackers, and locate and eradicate them.

The remainder of the essay is structured as follows: Section 2 describes a literature review and various spoofing attack techniques; The technique for the proposed system is presented in Section 3, which also covers network initialization, cluster formation, fingerprint generation, data encryption, data transmission, and decryption. The experimental findings made utilizing the suggested procedures are presented in Section 4. Section 5 offers conclusions and discusses potential future improvements.

II. RELATED WORK

We have examined many ways that have been used in this field by various researchers. Seyedeh Zahra Rajabi et al. [5] presented a unique received signal strength (RSS)- 1 based fuzzy logic methodology for identifying spoofing attacks in wireless networks.

Using four 802.11 access points, this technique collects RSS values from nodes.Fuzzy approaches are utilised to distinguish between various signal strength levels and to determine the location of each node in 11 wireless networks. Sushil Yadav et al. [6] have developed a technique to identify spoofing attacks that makes use of the spatial correlation of the received signal strength (RSS) inherited from numerous wireless nodes. Following the development of a multiclass detection and a Cluster-based approach, it determines the number of attackers.

An approach that uses a different authentication method in addition to MAC address filtering and regularly re-authenticates the client has been proposed by Wesam S. Bhaya and Samraa A. AlAsady [7]. This is supported by two factors. Using the computer name, CPU ID, and the current time as the inputs to a hash function (one-way function), this hash value is then inserted in the slack fields of the header of the frame (steganography) in the first step.

V Bharath Srinivas and Dr Syed Umar [11] have proposed a technique that does both the tasks of detecting spoofing attacks, as well as locating the positions of attackers forming the attacks. In this, they first use an attack detector for checking wireless spoofing that utilizes K-means cluster analysis. Next, they have described how attack detector mechanism is integrated into a real time indoor localization system, which is also capable of localizing the positions of the different attackers.

P. Kiruthika Devi and Dr. R. Manavalan have 5 offered a complete review of the various spoofing attack detection techniques utilised in wireless sensor networks [8]. B.VidhyaM.E [9] has proposed a method for detecting spoofing attacks, when more attackers use the identicalness of the same node, and localising multiple attackers that uses spatial information, the physical property corresponding with each wireless node that is difficult to falsify but is not based on cryptographic authentication schemes. The suggested solution in this scenario uses spatial correlation of the received signal strength (RSS), inherited from numerous wireless nodes, to detect the spoofing assault.

III. PROPOSED SYSTEM

In the proposed approach, we guard against spoofing attacks using the zero knowledge protocol (ZKP). We additionally protect data using elliptic curve cryptography (ECC). If the link between the source and the destination is long, any node can be compromised, and there is a higher probability of attacks, we construct clusters in the network and transfer data directly between nodes and their cluster leaders. To identify if a node is valid or not, every node in the network has a fingerprint established. In this case, attacks are less likely and communication node verification comes before data transmission.

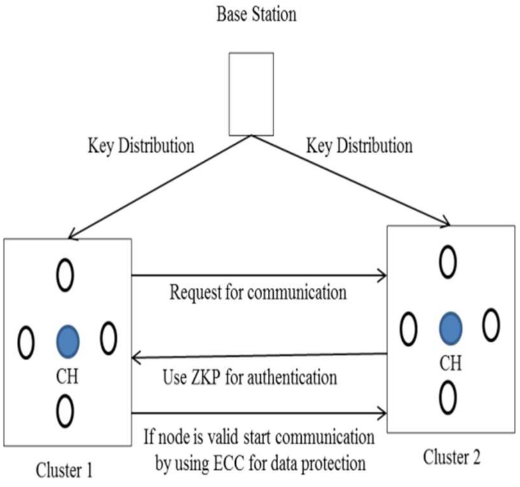
Base Station
Key Distribution
Key Distribution
Request for communication
Use ZKP for authentication
If node is valid start communication by using ECC for data protection
CH
CH
Cluster 1
Cluster 2

Figure 1: System Architecture

Nodes will begin communicating through the cluster heads once the nodes have been placed in the network and the clusters have formed. The ZKP technique will be used to authenticate whether a node is a legitimate node or a faked node after the nodes begin talking. If it is a legitimate node, the message may be sent throughout the network; otherwise, the packets from that specific node would be dropped. following the provision for communication, the ECC algorithm will be applied to avoid the data access from unauthorized user present in the network.

a) Pseudo code for selecting cluster head

For choosing the cluster head, Weighted Clustering Algorithm will be used. In this algorithm, the neighbors will verify the weights of nodes on the basis of distance among the neighbor, movement angle and the speed and chooses the best possible cluster head.

```
For (every node in the network)
    Calculate the Angle difference Av
    Calculate the Degree difference Dv
    Calculate the Speed difference Sv
    Calculate the weight Wv = C1*Dv+C2*Av+C3*Sv
If (Wv > Weight of neighbor node)
  Select Wv as the cluster head
Else
  Neighbor node is the cluster head
```

b) Pseudo code for Spoofing attack detection

The Zero Knowledge protocol is the method employed in this case to detect the spoofing attempt. In this protocol, each node will initially receive a key, after which it can be validated by answering a series of questions based on the key without ever disclosing the key. The node is a legitimate node if it responds to every query; otherwise, it is a fake node.

The verifier and prover are the two persons involved. The verifier will check to see if the node can be trusted. Prover will demonstrate its reliability. The following is the pseudo code for the ZKP and ECC algorithms. Verifier

```
In the Verifier side initialize the state as false.
Verifier Step1:
 If (ChallengeSoved1)
    Proceed for the next step of challenge
Else
    Reject the packets from that particular node
Verifier Step2:
If (ChallengeSolved1 is correct)
    Gives the challenge based on the step1 challenge
If (ChallengeSolved2)
If (ChallengeSolved1==1 && ChallengeSolved2)
    Accept the node as an original node
Else
    Reject the packets from that particular node
```

Prover

```
It will answer for the verifier challenges.
Prover Step1:
Receive the challenge
If (ChallengeAccepted)
    Send Proof to the Verifier by avoiding the communication with key
Prover Step2 :
If ( NextChallengeAccepted)
     Generate a proof Return to Verifier
```

ECC Algorithm

In ECC algorithm, it defines the curve in the finite field Fp and generate a point on the curve which will be consisting of two elements in the Fp. The ECC algorithm will be used for data encryption and decryption to avoid the data to be stolen by third party. Pseudo code The range used here is 0 to p-1 and the equation is y2 mod p=(x3 +ax+b) mod p.

```
For (Each value of x)
    Choose the value of y within 0 to p-1 which satisfies the
    equation Display the required point
Generate the public key Q and private P by using the point on
the curve
If (keys generated)
    Distribute the keys
If (Sender starts sending message)
    Encrypt the message using the equations,
    C1 = k*P and
    C2 = M + k*Q
    Where, C1 & C2 are Cipher texts k is generated randomly
    within the range 0 to p-1 M is a point on the curve with the
    message.
 If (Message received at the destination)
    Decrypt the message M = C2 – r1* C1
    Where r1 is the random number within the range 0 to p-1
```

IV. Results & Discussion

The proposed security approach discussed in the preceding part is tested using simulation to determine its viability. How to assess the proposed system's performance in terms of (a) latency, (b) packet delivery ratio, (c) routing overhead, and (d) throughput is described in this section. The attack is compared before and after the solution is applied to create a performance graph, which is then evaluated using the aforementioned metrics.

a) Delay: The typical time it takes for a package of information to arrive at its destination. It also accounts for delays brought on by the transmission of information packages and the course disclosure process. Just the data packets that successfully went to the numbered locations. The end-to-end latency estimate is predicted to be lower the better the convention performs.

b) Packet Delivery Ratio: This measures the ratio of correctly received packets to all packets sent and received. It delivers parcels. The evaluation graph is shown in Figure 3.

c) Routing Overhead: Routing overhead is the number of routing packets necessary for network communications. The evaluation graph is shown in Figure 4.

d) Throughput: One of the performance measures is throughput, which is the average quantity of data received per unit of time. The evaluation graph is shown in Figure 5.

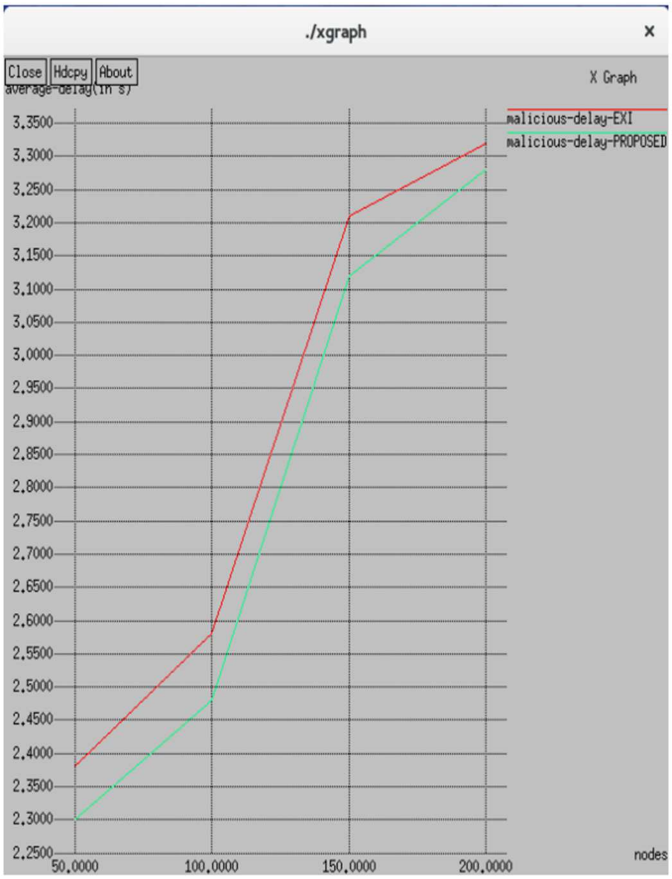

Figure 2: Evaluation of delay

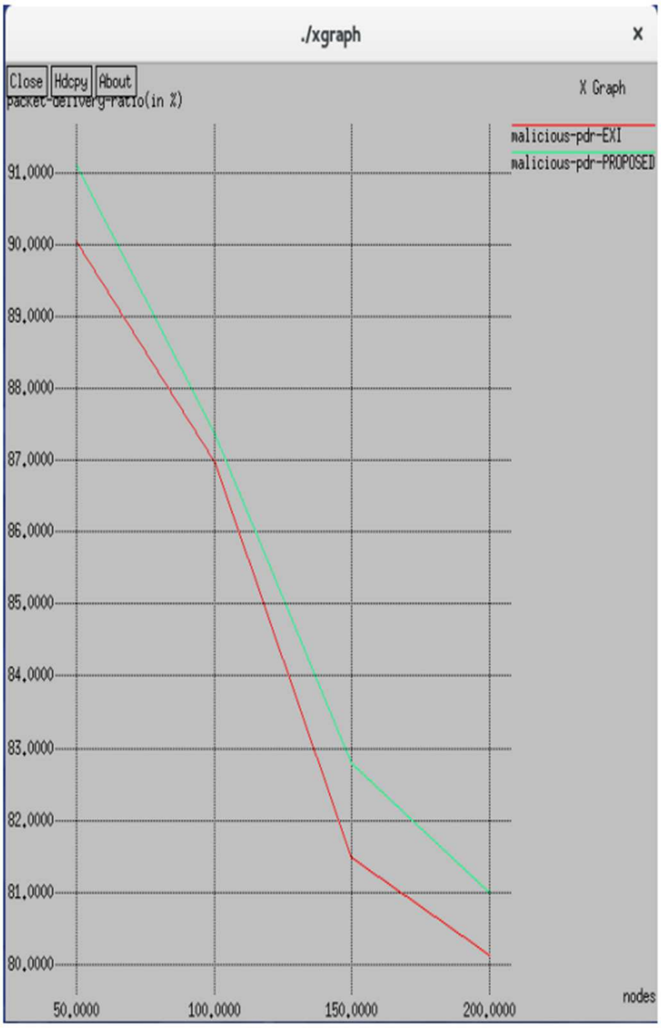

Figure 2: Evaluation of Packet Delivery Ratio

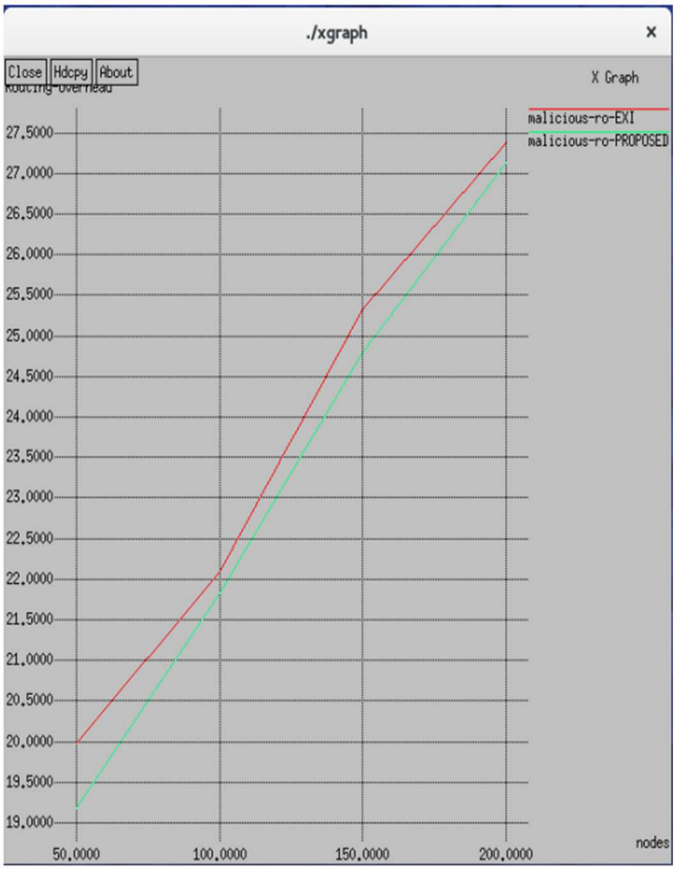

Figure 4: Evaluation of Routing Overhead

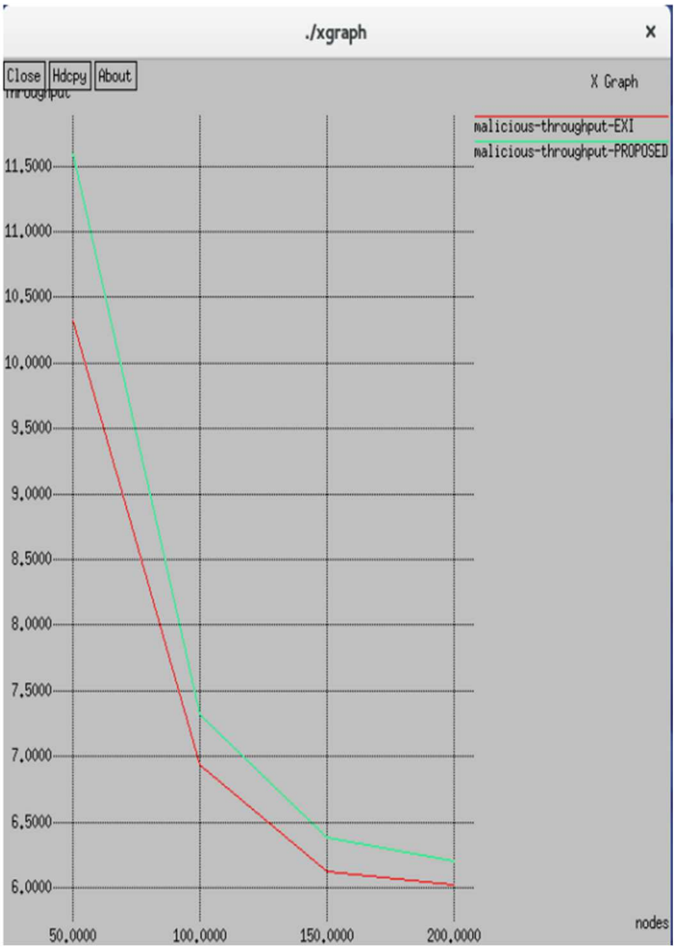

Figure 5: Evaluation of Throughput

V. CONCLUSION & FUTURE WORK

The suggested approach is an effective network security system that focuses on protecting against spoofing attacks, potential DoS assaults, and Man-In-The-Middle attacks in wireless networks while also offering data protection. The findings demonstrate that the adopted technique offers increased protection against spoofing attacks with little delay and minimal routing overhead. And the suggested technique uses less memory and operates effectively.

The suggested method offers protection in small networks against spoofing, potential DoS assaults, and Man-In-The-Middle attacks. It may be improved for medium- and large-scale networks as well as other comparable attacks including phishing, jamming, and sybil attacks, among others.

REFERENCES

[1] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and PracticalSolutions,”Proc. USENIX Security Symp., pp. 15-28, 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 UsingSignalprints,” Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[4] Q. Li and W. Trappe, “Relationship-Based Detection of Spoofing- Related Anomalous Traffic in Ad Hoc Networks,” Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[5] Seyedeh Zahra Rajabi, Seyed Javad MirabediniShirazani and Ali Haronabadi, “Detection of Spoofing Attack in Wireless Networks Using Fuzzy Logic”, International Journal of Mechatronics, Electrical and Computer Technology, Volume 4, Issue 12, 2014.

[6] Arjunsingh Sushil Yadav, Deshana Manoj Sethia, Amruta Balaji Mundkar and Pooja Milind Natu, “Detection, Localization And Prevention Of Spoofing Attacks In Wireless Network”, International Journal of Electrical, Electronics and Computer Systems, Volume 2, Issue 8, 2014.

[7] Wesam S. Bhaya and Samraa A. AlAsady, “Prevention of Spoofing Attacks in the Infrastructure Wireless Networks”, Journal of Computer Science, Volume 8,Issue10, 2012.

[8] P. Kiruthika Devi and Dr. R. Manavalan, “Spoofing Attack Detection And Localization In Wireless Sensor Network: A Review”, International Journal of Computer Science & Engineering Technology, Volume 5,Issue 09, 2014.

[9] B.Vidhya M.E, “Prevention Of Multiple Wireless SpoofingAttack Protocols”, International Journal of Advanced Research, Volume 2, Issue 3, 2014.

[10] Arjunsingh, Sushil Yadav, Pooja Milind Natu, Deshana Manoj Sethia, Amruta Balaji Mundkar, Prof. Santosh S Sambare, “Prevention of Spoofing Attacks in Wireless Networks”, 2015 International Conference on computing communication control and Automation.

[11] Pallavi D Sontakke, Prof. Dr. C A Dhote, “Spoofing Attacks Detection and Localizing Multiple Adversaries in Wireless Networks”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2015.

[12] R Vijayakumar, K Selva kumar, K Kulothungan, A Kannan, “Prevention of Multiple Spoofing Attacks with Dynamic MAC Address Allocation for Wireless Networks”, 2014.

[13] B Dinesh babu, T Thirunavukarasu, “Prevention of Spoofing Attacks in Wireless Sensor Networks”, International Journal

of Computer Science and Information Technologies, Vol. 5(3), 2014.

[14] S Raguvaran, “Spoofing Attack: Preventing in Wireless Networks”, International Conference on Communication and Signal Processing, April 3-5, 2014, India.

[15] M Soniya, P Sabarinathan, S Visnudharsini, “Enhancing Security in Wireless Ad-Hoc Network Using ZKP”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014.

[16] Shikha Goel , “Wireless LAN (WLAN) Spoofing Attack- A Proposed Detection Method in Victim Silent Case”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013.

[17] Fereydoun Ramezani Zangi, Sajjad mavizy, Javad Badali, “A Stable Distributed Clustering Algorithm For Mobile Adhoc Networks”, IJCSI (International Journal of Computer Science Issues), Vol. 9, Issue 5, No 3, September 2012.

[18] P Ramesh Babu, D Lalitha Bhaskari, CH Satyanarayana, “A Comprehensive Analysis of Spoofing”, International Journal of Advanced Computer Science and Applications Vol. 1, No.6, December 2010.