DISCOVERY AND VERIFICATION OF NEIGHBOR POSITIONS IN AD HOC NETWORKS

Nikhil Jadhav[1], Kushal Bang[2], Anurag Boggavarapu[3], Akshay Gaikwad[4], Zarina Y. Shaikh[5]

[1,2,3,4,5] *Dept. of Computer, JSPM's RSCOE, Pune, (India)*

ABSTRACT

Discovery of positions of neighboring nodes has become an important factor in today's world due to an increase in the use of ad-hoc network. Because of the increasing demand, security has also become an important factor as fake positioning of nodes in the ad-hoc networks is possible. So in this project we will be discovering position of nodes in ad-hoc network and we will verify it to check whether it is a trusted node or a faulty one. For distance verification we will be using signal strength and GPS co-ordinates.

Keywords: Neighbor Position Verification , Ad Hoc Network

I. INTRODUCTION

In fast growing technologies there are many applications which require location awareness. Co-ordination of the movement of robots in robotics, geographic routing, spontaneous network and traffic monitoring, vehicular networks are some of the fields which require location awareness of all the neighboring nodes.

Neighbor discovery (ND) provides an important functionality for wireless devices that is to discover other devices that they can communicate with makes it easy to abuse ND. The verification of node locations is an important issue in mobile networks and it becomes particularly challenging in the presence of adversaries aiming at harming the system.

Therefore we need a solution to 1) To correctly establish the location of nodes in spite of attack feeding false location information, and 2) To verify the position of neighbor so as to detect adversarial nodes.

In this project we are discovering the position of nodes in ad-hoc network using GPS (Global Positioning System.). RSSI (Received Signal Strength) is used for distance calculation of node from the verifier node in the network. RSSI gives the value of power strength from client to the access point, for instance. RSSI is the relative signal strength in a wireless environment and can be measured in any unit of power. It can be expressed in decibels or percentage from 1-100. The value obtained from this method can either be positive or negative [1].

II. SYSTEM AND ADVERSARIAL MODEL

Here, we consider a WiFi network and consider its nodes as communicating neighbors if it can reach other nodes directly [2]. We assume that every node knows its position in the network with some maximum error. To achieve this, the nodes are equipped with GPS receiver.

We assume each node owns a set of private key and public key as mentioned in the emerging architecture for secure and privacy-enhancing communication [3]. Node X can encrypt and decrypt data with its key and public

key of other node and can produce digital signature with its private key. Nodes can authenticate messages of other nodes through public key cryptography as mentioned in [4]. Nodes are assumed to be true if they act in accordance with the NPV protocol otherwise adversarial.

III. NPV: AN OVERVIEW

NPV is a protocol which consists of a node, hereinafter called as verifier which is used to verify and discover the position of its communication nodes. The verifier is used for starting the NPV protocol. The protocol uses a set of messages for discovering the position of the communicating nodes. The purpose of the messages is to get the information about the two communicating nodes which we can use for finding out distance between them. After collecting the information, verifier uses the signal strength information obtained from communicating neighbor to compute distance between all pairs of nodes in network [3]. After calculating the distance we classify the nodes into 2 parts for completing the verification process. The 2 parts are verified nodes, i.e., which are safe for communication, faulty nodes, i.e., which are not safe for communication. The process of verification is carried out with help of two tests, the direct symmetry test and cross symmetry test and multilateral test. Thus after carrying out the process correctly we can easily avoid the adversary from entering the network for communication and secure the network from such adversary.

IV. NPV PROTOCOL

We detail the message exchange between the verifier and the nodes connected to it in the network, and series of verification test carried out on them.

4.1 Message Exchange

Verifier starts the protocol by broadcasting message (Poll) to the all the client nodes in the network. The encryption technique used is RSA [5]. This message is encrypted using the public key of the client node. Then the client node replies to the verifier with its geological coordinates and signal strength of the ad hoc network. This message is encrypted using public key of the verifier. Upon receiving the message from the client node, the verifier carries out verification test on the information obtained from client node. A list of trusty nodes (true node) is prepared by the verifier and is sent to all trusted client nodes in the network. All the false nodes are removed from the network and are labeled as false node.

We consider following notations for message exchange.

S=Verifier

X=Client node

Ns=List of all the Clients

Rx=RSS value of X

Latx & Longx= Latitude and Longitude values of X

True_nodes= List of nodes which are verified/Valid

Faulty_nodes=List of nodes which are faulty

We use the following algorithms where algorithm 1 is used by the verifier node i.e., S and algorithm 2 is used by communicating neighbor of S.

Algorithm 1: Message Exchange: Verifier

1. Node S do
2. S→* : {Poll,Ks}
3. When receive REPLY from X ∈ Ns do
4. S: stores Rx, Latx ,Longx
5. After verification of X
6. If (X==Verified then
7. True_node ← X
8. Else Faulty_node ←X

Algorithm 2: Message Exchange: Client

1. when receive Poll from S do
2. X: find Rx
3. X: find Latx Longx
4. X: encrypt Rx, Latx ,Longx using Ks
5. X: send encrypted message.

4.2 Position Verification

To verify the position of the node, we take a step forward to verification process with the message exchange which takes place between the nodes in the network. The verifier decrypts the data received and finds the position of all the nodes participating in the network. To make the system safer we carry out two tests simultaneously. They are:

1. Direct Symmetry test
2. Cross Symmetry test

4.2.1 Direct Symmetry Test:

In direct test the verifier (server) sets the RSS value, the nodes in the system send their RSS value to the verifier through the message. The verifier sets a range for the values i.e., from 0-100 and the distance is calculated according to the value, the value 100 means the node is exactly next to the server and the distance between them is 0 meters. As the node move away from the verifier the value decreases and the distance between them increases. The value of the RSS changes according to the strength of the signal.

Verifier sets the RSS value according to the usage and wants to share the network area and allow the nodes in the network. If the nodes which fall outside the range of the RSS value are encountered, the verifier rejects those particular nodes because the distance between the verifier and node is greater than the Ad-Hoc range, the node is placed in the unverified nodes list.

Algorithm 3: DST

1. Node S do
2. Forall X ∈ Ns
3. If(Rx within range) then
4. S: True_node ←X
5. Else S: Faulty_node←X

4.2.2 Cross Symmetry Test

Cross Symmetry test is where the verifiers carries out a test with respect to itself. The verifier keeps record of its own geographical values i.e. longitude (v) and latitude (v), as the position of the verifier changes the

geographical value changes. The node which comes in the network through the message exchange, the node's geographical values are also sent in encrypted form to the verifier (latitude(n) and longitude(n)). Through the geographical values we calculate the distance between the verifier and the node. As the node moves inside the network the geographical values change and the distance is calculated. This process is carried out throughout the system lifetime. If the distance between the node and the verifier is different compared to the distance obtained from RSS value and the geographical value with error range the node is placed in the faulty node list.

Algorithm 4: CST

1. Node S do
2. Forall X ∈ Ns, X ∄ Faulty_node
3. If(Drx-Dlx)>Er then
4. S: True_node ←X
5. Else S: Faulty_node←X

Where,

Drx =Distance calculated through RSS value,

Dlx =Distance calculated through latitude and longitude,

Er=Error range of ± 5 meters.

V. RESULTS

We performed the simulation of this project using three laptops each with a GPS dongle and a Wi-Fi. The GPS dongle provided latitude and longitude with an accuracy of 3-5 meters. Therefore the error ratio while distance comparison in second test is ±5 meters. Initially the range considered is of 15meters. The error ratio considered for the signal strength is 3 units. The valid range for the signal strength is 0-100. Initially when both client and verifier is at same place the signal strength is 100, but as client moves away from verifier the signal strength reduces by 7units per meter. Therefore, the signal strength to distance calculation is done using the following formula:

(1) $\text{Distance} = (100 - x)/7$

Where,

x = Signal strength.

Distance calculation formula between two different geological positions is as follows:

(2) $a = sin^2\left(\frac{\Delta\varphi}{2}\right) + \cos\varphi 1.\cos\varphi 2.sin^2\left(\frac{\Delta\lambda}{2}\right)$

(3) $c = 2.atan2(\sqrt{a}, \sqrt{(1-a)})$

(4) $d = R.c$

Where,

φ = latitude,

λ = longitude,

R = earth's radius (mean radius = 6,371km) [6].

We examined this protocol at different location with the success rate of 70 percent. The following graph shows the comparative study of the ideal values and those obtained through this methodology, where the X-axis represents the RSSI Values in percentage and the Y-axis represents the Distance in meter

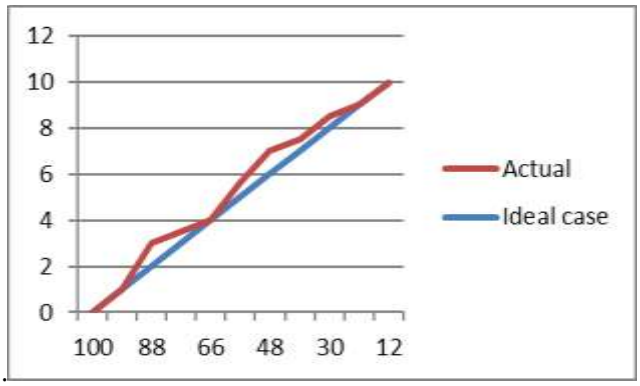

Fig.1 Comparative Study of Ideal and Actual Values

The success rate highly depends upon the accuracy of the GPS coordinates obtained from GPS dongle.

VI. CONCLUSION

In our project we are successfully able to discover the nodes in the network and verify the position of it. But, this is valid only if all the nodes are in the same plane as that of the server. If the planes of the client or server node is different (i.e. height) we are not able to find the position of the node accurately. In order to do this we require a higher level of coding and additional number of devices.

VII. FUTURE SCOPE

In our project we are using GPS for positioning i.e. for plotting. Instead of that we can use trilateration method for positioning. So that it can be used in places where GPS co-ordinates are not available (no range area, but should know coordinate of verified server). Using trilateration method we can find the position of nodes in the network and can as prepare a 3D model of it.

REFERENCES

[1] http://www.speedguide.net/faq/what-is-wireless-rssi-level-418.

[2] P.Papadimitratos, M.Poturalski, P.Lafourcade, D.Basin, S.Capkum, and J-P, Hubaux, Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad-Hod Networks," IEEE comm.Magazine, vol.46, no.2, pp.132-139, Feb.2008 (neighbor discovery based on distance).

[3] S.Capkun and J-P.Hubaux,"Secure Positioning in Wireless Networks,"IEEE J.Selected Areas in Comm., Vol.24, pp.221-232, Feb.2009.

[4] G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, "On the Performance of Secure Vehicular Communication Systems," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 6, pp. 898-912, Nov./Dec. 2011.

[5] http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29

[6] http://www.movable-type.co.uk/scripts/latlong.html