Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/8133
DOI URL: http://dx.doi.org/10.21474/IJAR01/8133

RESEARCH ARTICLE

A HYBRID APPROACH TOWARDS LOCALIZATION AND SECURITY IN WIRELESS NETWORKS.

Suraj Balwan[1], Mahesh Malwade[2] and Ajinkya Kunjir[3].
1. Faculty of Computer Science, MES College of Engineering, Pune, India.
2. Faculty of Computer Science, MES College of Engineering, Pune, India.
3. Master's in Computer Science, Lakehead University. Thunderbay, Canada..

Manuscript Info

Manuscript History
Received: 01 October 2018
Final Accepted: 03 November 2018
Published: December 2018

Keywords:
Localization, Wireless Networks, Security, Authentication, Matrix Completion, Message Digest.

Abstract

In the digital era of 21st Century, recent developments and advancements in fields of Wireless Networks and positioning technology have progressed tremendously to enhance the pervasive devices and applications. To overcome the limitations of GPS such as the need for line of sight, expensive at cost, low battery life and others of relevance, many researchers and wireless technology practitioners have devised several localization topologies based on the distance between the nodes in the network. Localization and Security play significant roles in modeling the Wireless Networks and preventing it from collateral data damage. Localization eases up the accessibility procedure by allowing the user to access its device from any remote location via internet connection without any distance limitation. Security in Wireless Networks avoids unauthorized usage of network and also prevents data leak. The previous systems deployed for localization and security suffered from poor computation speeds, high power usage, and weak authentication. In this research paper, we propose an empirical approach towards localization in Wireless Networks using a decentralized scheme based on matrix completion, MALL, which makes use of coordinates of nodes and distance between them to achieve efficient localization index. Since MALL believes in high complex optimization and low non-convex optimization, the computation of distances can be done at a faster pace. For security in Mobile Clouds, we have introduced a novel light weight authentication scheme called MDLA (Message Digest and Location-based Authentication) which is of paramount importance in mobile networks for authentication in message passing. SSH (Secure Shell) makes use of public key cryptosystem which leads to high-cost computation for mobile devices. MDLA involves symmetric key operations and the integrity of messages is preserved by hashing the information using message digest. The entire operation is catalyzed using time stamps, secret keys and Pseudo-Random Generator (PRGM). An in depth-analysis of MALL and MDLA with the end simulation implementations for both the approaches have been stated in the later part of the paper.

Introduction:-

In modern times, high-speed execution and remote localization play vital roles in all areas of computer science which consists of a wireless network. GPS (Global Positioning System) is used in every device for achieving localization of individual nodes in the networks. Apart from being so advanced, GPS requires line of sight (LOS) for locating the nodes in the network and is very expensive when it comes to the battery requirements. These few disadvantages of

Corresponding Author:-Suraj Balwan.
Address:-Faculty of Computer Science, M.E.S College of Engineering, Pune, India.

GPS has motivated the wireless network practitioners to adapt and switch to trending localization schemes for efficient implementation procedures. The existing localization schemes can be categorized into two segments such as centralized and decentralized localization schemes. In the first category, a single central hub node is responsible for monitoring and gathering information about distances and connectivity from all the other nodes in the network. Due to availability and flexibility in the centralized scheme, the result is highly efficient and localization is achieved precisely. The two main disadvantages of centralized schemes are long computation time and extremely poor scalability as the hub has to detect the location of all other functioning nodes in the network. TSL, LRL and TSLRL are the three good centralized algorithms that work with significant results in the network of nodes (S. Rallapalli et al., 2010). Speaking of Decentralized localization schemes, there is no central hub in the network. Instead, each node collects the distances and connectivity information about its neighbor nodes and locates itself in the network independently. Biggest pro about decentralized schemes is that fast computation is obtained as limited information is collected from a set of nodes to obtain locations in the network. However, the localization results are less precise as compared to centralized algorithms. Three typical decentralized localization schemes can be listed as IMCL, MSL (M. Rudafshani and S. Datta, 2007) and Monte Carlo Localization (L. Hu and D. Evans, 2004).

In this research, we present a unique decentralized location scheme based upon matrix completion and localization for wireless and mobile networks. The short abbreviation would be called as 'MALL' (Matrix Completion and Localization). The authors proposed a decent matrix completion approach in which the unknown entries in the matrix are filled if the rank is low and other known samples are randomly distributed in the plane (B. Recht et al., 2010). In 'MALL' every node uses a two-step procedure to locate itself accurately in the network. In our approach the first step comprises of exhibiting the low-rank features where the samples are not randomly distributed in the plane. The second step of MALL incorporates an effective matrix completion algorithm to localize mobile nodes in the network. The end result is obtaining a lightweight non convex optimized algorithm which high precision and fast computation. In the lower section we will describe more about MALL and its technical features in stepwise representation. Over the past few years, mobile cloud computing has imprinted a niche for itself in the software Industry. Several cloud services such as PAAS (Platform as a service), SAAS (Software as a service) and CAAS (Cloud as a service) have remodelled the cloud computing organization by providing these services for free usage for limited time and a paid subscription for long as you use it for deploying instructions for mobile clients. For implementing security measures for mobile clients in wireless networks, we are using mobile cloud computing services offered by the cloud service providers. The services work in a traditional format where the client needs to register for a service to the cloud providers and then the server responds an acknowledgment to the client by sending an encrypted confirmation message to the client. The transmission of messages in a cloud infrastructure discards the need of installing any other external memory unit and also can be dangerous at the same time due to leak of data in the network. The security parameters are needed to be taken into consideration for preventing network from unsafe passage and making it a secure channel for exchange of information. Mobile cloud computing makes use of USIM (Universal Subscriber Identity module) chip which is embedded in the motherboard of every mobile client device. The USIM chip is responsible for establishing secure communication between a device and a cloud server. Every smart device is not necessarily supposed to have a USIM chip in it as there are many threats associated with USIM authentication concerns (A.M.Talib et al., 2011).

To eliminate the use of USIM in mobile device, we propose a reliable authentication scheme "Message digest and location-based authentication (MDLA)" which uses a message digest (md5) hashing function to validate the transmissions of information between a mobile device and a cloud server. This technique is independent of a USIM module and does not require the registered user to memorize the password. Moreover the location of user is enough for logging in the application. MDLA uses message digest generated by the cloud servers, timestamps, a few secret keys, and other parameters such as dynamic locations of mobile devices for authentication. We will elaborate more on MALL's problem formulation, distance matrix and others of relevance in the second half of the paper. MDLA architecture and equations of different phases along with scythe analysis has been discussed in later sections. The later part of the part focuses on simulations, results, future scope, conclusion and the references referred for aiding our research.

Theoretical background:-

Proposed approach: MALL

The proposed approach for the decentralized localization scheme MALL involves of a central node which is responsible for collecting information regarding distances and connectivity from the neighboring nodes and locating itself in the network. The architecture consists of anchor nodes and normal nodes in which the anchor nodes are the

ones which are equipped with GPS and normal nodes are the random samples distributed in the network. The normal nodes strive to locate itself in the network by computing the distances of anchor nodes within two hops of its radius and one hop for the other normal nodes. The non-convex optimization algorithm helps the normal nodes for localization by forming two matrices i.e *Coordinate matrix* and *distance matrix*. The detailed architecture of MALL single hop is described in section III. For obtaining security in wireless networks via cloud servers, MDLA has been suggested which emphasizes more on using message digest (md5) as a cryptographic hashing function for secure message passing between the mobile client nodes and cloud server. The overall MDLA implementation consists of three phases listed as Registration phase followed by Authentication and Update phase. The user registers with the mobile cloud server in the first phase where then after the cloud server provides an acknowledgment feedback by hashing the information using message digest. All the three phases have been described with important features in lower section of MDLA.

Architecture and Working

As shown in the architecture below for MALL, the time is divided into equal interval time slots such as t1, t2, t3….tn. All the samples are distributed in equal interval at t1….tn in a 2D Euclidean space. To achieve precise localization every node stores its own distance and coordinate matrix.

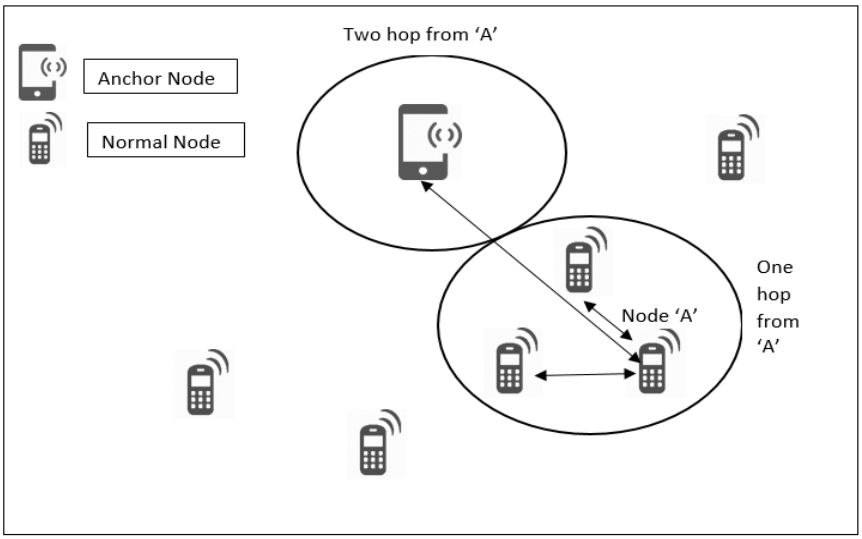

Figure 1:- Local Subnet showing one hop and two hop

As shown in the figure 1, the node A (which is a normal node), and forms a local subnet in the network computes its distance and connection from all the other normal nodes in its one-hop radius and connects to anchor node which is situated within two-hop radius of its position in the local subnet. The distances are computed using Euclidean distance formula for vector norms. Like node 'A', every other normal node follows the same procedure and locates itself precisely in the network with high computation power.

$$\sum_{i=1}^{n} ti\,(qi - pi)^2 \qquad (1)$$

Referring to Eq (1) above, the Euclidean vector distance formula is used by the nodes to calculate the distance between the nodes and store in their individual distance matrices. Note that '*ti*' in Eq (1) denotes the current timeslot at time 't' and all the past time slots can be denoted as T – 1 slots. In our research we have set T = N, where N can be 1, 2, 3…N. Maximum limit or threshold is not being specified as the testbeds experiments were not performed for the same.

Matrix Formulations

In this section, we form the mathematical equation problem for mobile network localization. Assume that there are M nodes in a network under investigation. These nodes move and communicated in a 2D Euclidean space. Being a

generic multidimensional approach, every node in MALL based network is assigned a global ID ranging from I to M. We use the following notations to describe the anchor and normal nodes formally:

1. E (i,t) denotes the 2D Euclidean space of node *i* at time *t.*
2. E (k,,i, t) denotes the k^{th} dimension for node *i* at time *t.*
3. (N, tc) denotes the set of nodes at current time tc
4. N can be a node set consisting of nodes from N_i, N_{i+1}…..N_{i+n}.
5. $N_r = |N_i, T_r|$ denotes the neighbor nodes in a local subnet of node N_i
6. $N = |N_{i,} t_{cw}|$ denotes the number of neighbor nodes that appear at final current time slot $t_{cw.}$

In any wireless network the nodes tend to move around quite frequently as there is a dynamic change in the environment due to any feedback. Hence, the neighbors of any node N_i will change with time accordingly. Therefore, the node set of current and former neighbors change to grow and shrink by time. Ideally, the equation $(Ni, tc \in Ni, tr \in Ni, tcw)$ summarizes the frequent changes in the network.
Adding to the notations, we will be describing three matrices which are used for MALL:

Distance Matrix: Every local subnet L has a set of nodes N_s at current time t_c. According to the research, each globally assigned normal node *i* forms a N × N matrix of size N and name N to store all the Euclidean distance computed. Generally, an intrusion of N, N (a, b) can be calculated mathematically using eq (2):

$$N(a,b) = || N(m,t_c) – N(n,t_c)||^2 \quad (2)$$

Here ||.|| stands for Euclidean norm of a vector, and $||.||^2$ for Euclidean square of norm. N(a,b) are the global ID's of nodes and N(m,n) are the local ID's used for computation of distances. Distance matrix of size 5 × 5 (N=5) is shown below:

N(a1,b1)	……	…..	……
N(a2,b2)			
N(a3,b3)			
…..			
N(an,bn)	….	…..	N(atc,btc)

Figure 2:- Distance Matrix

Coordinate Matrix: For each normal node N_i, there are a few neighbors over time t_{cw}. In our approach, each neighbor uses a specific matrix X to store coordinates of its neighbors in $N_{i,}$ T. Locally each node is assigned a unique local ID j^x, which has a range from 1 to N. Each local ID corresponds to respective global ID for t_{cw}. The node uses E(k, j^x,t^x) to represent the k^{th} dimension and corresponding to E(k,j,t) at t_{cw}. To be noted, E is an 3D matrix, hence we need to convert this 3D matrix into 2D matrix. The matrix X^i can be formally obtained using Eq (3):

$$X(j^x + (k-1)N, t^x) = X^i(k, j^x, t^x) \quad (3)$$

Object Matrix: Object matrix is quit the same replica of coordinate matrix. The only difference is that for a node N_i, the object matrix stores the coordinates of its neighbors over a local subnet at time t_{cw} at $N_iT_{r.}$ The mathematical equation for object matrix Y will be same as above Eq (3):

$$Y(j^y + (k-1)N, t^y) = Y^i(k, j^y, t^y) \quad (4)$$

Authors in their research article on "A Matrix-Completion Approach to Mobile Network Localization" stated that the object matrix Y is a subset or a submatrix of coordinate matrix X. The matrices can be constructed using a '(.)' operator with any variable (Qiang Ye et al., 2014). The authors concluded a relation between both the matrices X and Y using Eq (4) and derived Eq (5):

$$Y = P(X(:;T-T_r+1,T)) \quad (5)$$

The matrix representation of X and Y as dimension coordinates is shown below in figure 3.

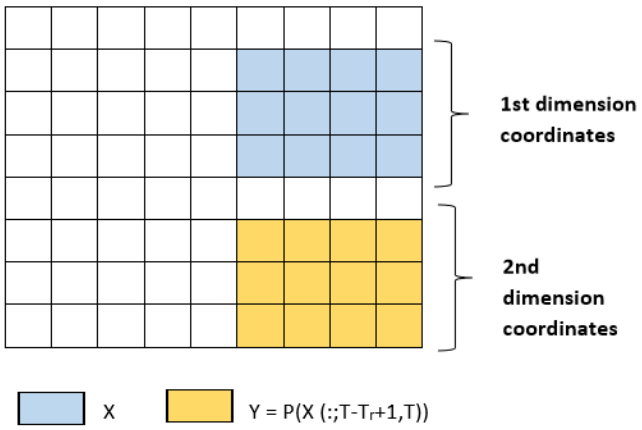

Figure 3:-Relation between Object(Y) and Coordinate Matrix(X)

With all the gathered data, each normal node determines its coordinates at current time by computing the unknown entries in the object matrix Y using two-step procedure. A brief about the two-step procedure is presented below:

1. *Step 1*: Use a matrix completion algorithm which involves only convex optimization approach to approximate X(:;1 : T-1). The computations are simplified and executed on OMnet++ and MATLAB. Therefore, X(:;1:T-1) denotes the submatrix of coordinate matrix X, where, T-1 are first few columns of X.
2. *Step 2*: Precisely calculate the unknown random entries in the object matrix Y using a decent matrix completion approach which utilized the approximated X(:;1:T-1) to its full potential. Once the estimated samples of Y are available, the coordinates of normal node *i* can be fetched. The complexity of this step is low as it involves a non-convex optimization method.

As our concern in this paper is relations between 2D matrices therefore we won't dig deep in the relations between 3D matrices in k^{th} dimension space. The unknown entries in Y matrix can be found using rank and temporal stability features of the approximated X matrix at time (T-1). The authors gave a detailed description for relation between X and Z along with MALL's time complexity and Simulation results (Saurabh Dey et al., 2014).

MDLA (Message Digest And Location-Based Authentication)

As mentioned in the proposed approach, MDLA is a lightweight authentication scheme which uses message digest for hashing the information shared and the procedure takes place in three phases formally as Registration, authentication and update. We will describe each phase in detail with its mathematical equation and technical characteristics. The operation begin with mobile user client being registered to the cloud server. The registration phase stores the user's credentials such as username, password and others to the cloud server for authorized access. The phase is also accompanied by few other elements such as a message digest md_{client}, a secret random number key $sec_{key,}$ and a primary key $prim_{key}$ along with hashed client ID ($h\{cid\}$) and password (h{pass}). The hashed client ID and password is supported with user's previous location ϕ_{prev} Eq(6). During the authentication phase the cloud server is responsible for providing the resources responsible for authentication to the cloud server Eq(7). The authentication request provides user an authentication key $auth_{key}$ which is generated using current timestamp and new current location ϕ_{new} Eq (8).

$$h\{cid\} \oplus h\{pass\} \rightarrow PRNG \xrightarrow{\phi prev} prim_{key} \qquad (6)$$

Here, PRNG is the Pseudo Random generator is a random number sequence generator which generates an anonymous unique string of numbers which supports and enhances the quality in the authentication process.

$$\delta time \rightarrow PRNG \rightarrow auth_{key} \qquad (7)$$

The new timestamp is passed through the PRNG to generate the authentication key. This process usually takes place at the cloud server for granting the authentication request.

$$auth_{reg} =$$

$$E_{primkey}\ (E_{authkey}\ (md_{client})||\phi_{new}\ ||\delta time\ ||\text{ref} \qquad (8)$$

The cloud server decrypts the message using the primary key to obtain the user's current new location and time stamp in generating the authentication key Eq (7). The basic architecture for MDLA which highlights all the three phases is shown below:

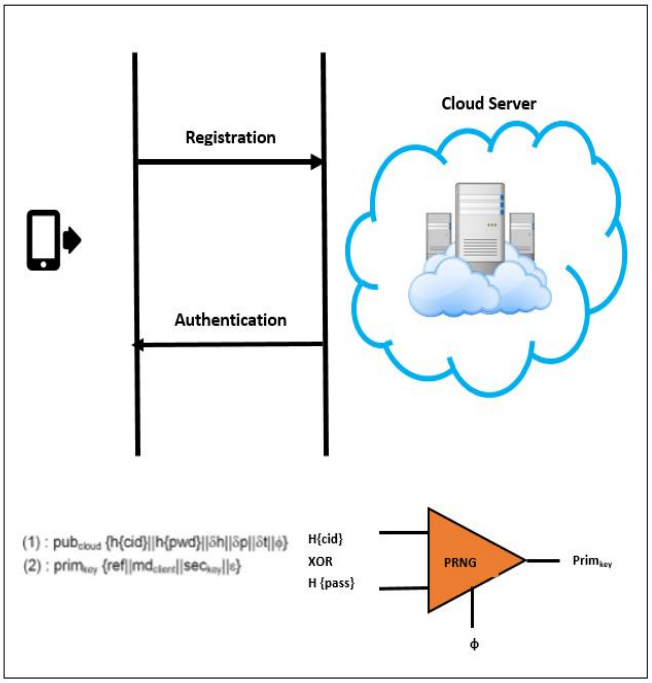

Figure 4:-MDLA Architecture

Three different types of updates take place after authentication phase performed by the methodology to assure confidentiality and secure access. Updation only takes place if there's a sudden loss of connection or change of values in between the authentication process.

Scyther Analysis for Security

The recommended protocol analyzer to validate the registration and validation phases is called as 'Sychter protocol analyzer'. Saurabh Dey et al. in their paper summarized the scythe analysis in two tables for both registration and authentication phases. They obtained a security score of '0' which indicated that the gateway is secure (Saurabh Dey et al., 2014). The score was labeled as $secure_{score.}$

$$secure_{score} = \frac{failed\_case}{total\_case}$$

The two tables given below represented the authentication and registration phases [7]:

Table 1:- Security Scyther Analysis for Registration phase

Sl.Num.	Claim	Status	Comment
1	secret $prim_{key}$	Ok	No Attacks
2	secret sec_{key}	Ok	No Attacks
3	secret cid	Ok	No Attacks
4	secret pwd	Ok	No Attacks
5	secret δt	Ok	No Attacks
6	secret δh	Ok	No Attacks
7	secret δp	Ok	No Attacks
8	secret ϕ	Ok	No Attacks
9	secret md_{client}	Ok	No Attacks
10	secret ϵ	Ok	No Attacks
11	Alive	Ok	No Attacks
12	Weakagree	Ok	No Attacks
13	Niagree	Ok	No Attacks
14	Nisynch	Ok	No Attacks

Table 2:- Security Scyther Analysis for Authentication Phase

Sl.Num.	Claim	Status	Comment
1	secret $prim_{key}$	Ok	No Attacks
2	secret sec_{key}	Ok	No Attacks
3	secret $sec_{key_{new}}$	Ok	No Attacks
4	secret $auth_{key}$	Ok	No Attacks
5	secret δt_{new}	Ok	No Attacks
6	secret ϕ_{new}	Ok	No Attacks
7	secret md_{client}	Ok	No Attacks
8	Alive	Ok	No Attacks
9	Weakagree	Ok	No Attacks
10	Niagree	Ok	No Attacks
11	Nisynch	Ok	No Attacks

Results and Implementation:-

Flowchart for MALL:-

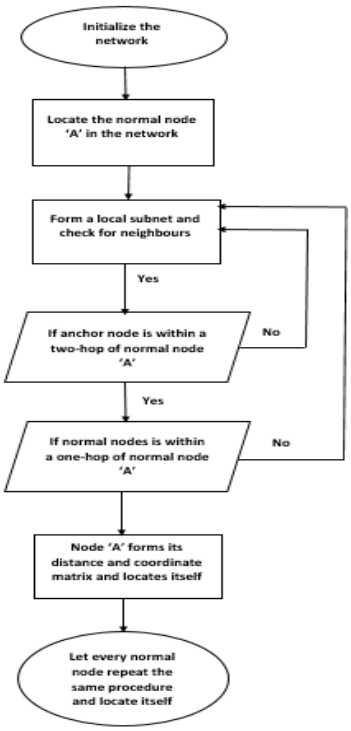

Figure 5:- Flowchart for working of MALL

The steps explained in the above section have been summarized into a flowchart which eases up the implementation process. The flowchart for the working of MALL has been displayed in figure 5.

OMnet++ IDE for Simulation:

Omnet++ is a discrete event simulator based on the foundations of C++. Omnet++ can be for modeling simulations for microcontrollers, wireless networks, and other parallel architectures. Omnet++ is a free open source software available at https://omnetpp.org/ and available as a standalone IDE for Windows/Mac/Linux. We have referred a few documents from the core site for learning about the IDE (Internet Source, 2018). A simulation in Omnet++ can be defined as a set of modules interacting with each other for a secure message flow. For implementing MALL, we have created several simulation models based on client-server architecture which are capable of passing the message coded in C++ without any interaction channel. The node detects its neighbor node and interacts with it by passing messages in equal interval time slots. As we would need an actual grid of sensors in a network for implementing MALL scheme, we have just created a visual representation of two nodes interacting with each other and trying to locate themselves in the network. Below given are some snaps of the simulation model created in Omnet++:

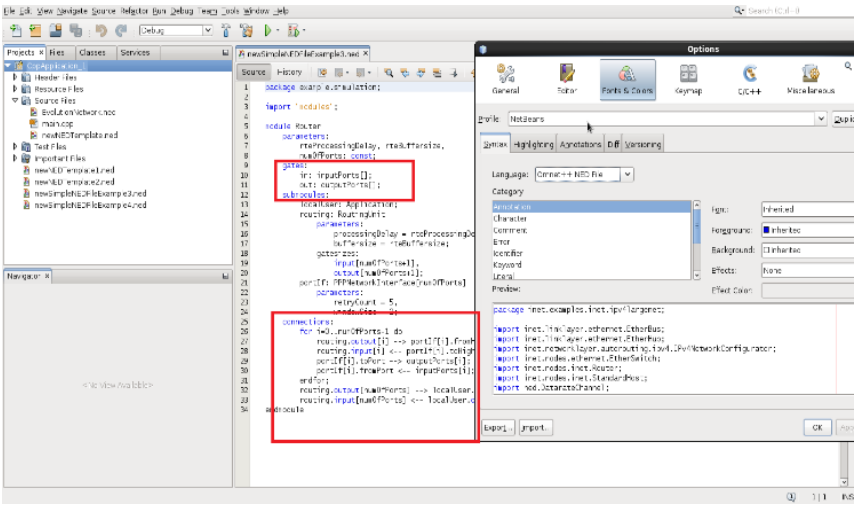

Figure 6:- Sample code for the architecture in Omnet++ IDE

Figure 7:- Interaction between a normal and anchor node in a local subnet

As shown in figure 6, the image from IDE is cropped to obtain a clear view of interaction between the nodes. The ‘gps’ node is the normal node and ‘nogps’ is the anchor node in a local subnet of ‘network1’ hosted communication network.

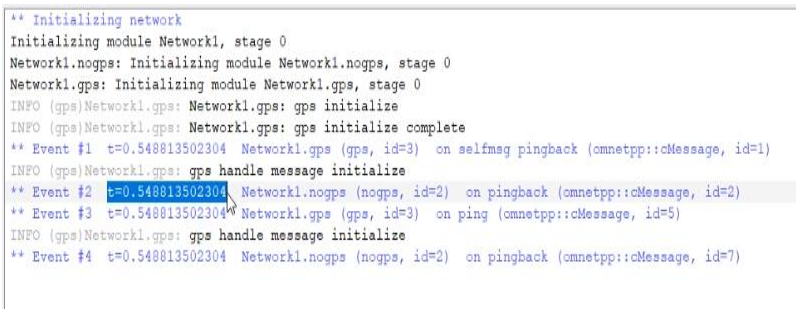

Figure 8:- Message passing in equal time events

Referring figure 7, the highlighted text in blue is the time taken for a node to interact with the anchor node. The time generated is used to calculate the Euclidean distance between the two nodes and form a distance matrix. The coordinate matrix is formed later after getting the coordinates in the network.

Flowchart for MDLA:-

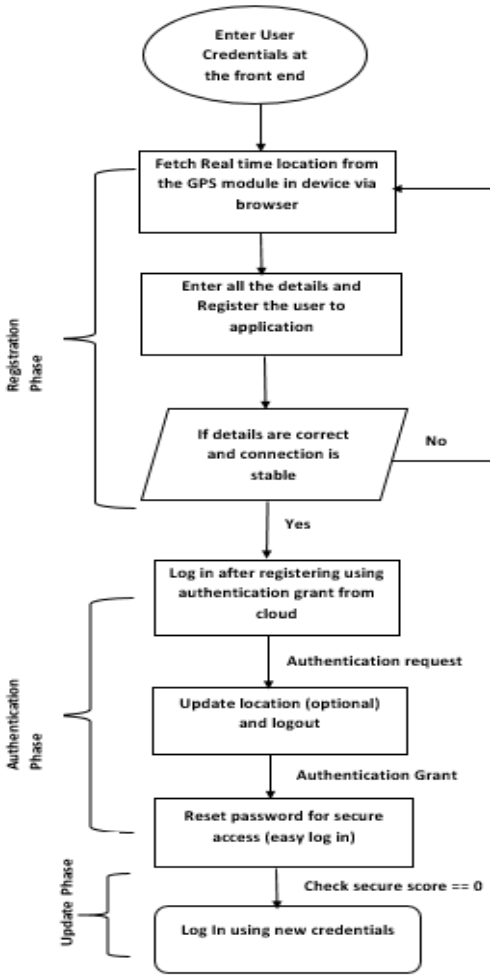

Figure 9:- Step wise Representation of MDLA with its three phases

The flowchart in figure 8 explains the working of our implementation for MDLA. The three phases have been explained in brief in the previous section and implemented the exact same way in our local system using XAMPP.

1. Tools used for System: The set of tools and technologies used for implementing MDLA consists of XAMPP on a local system (as an alternative to a real cloud server hosting). Database preferred for storing the user's records is

MySQL of XAMPP. PHPMyAdmin is used for visually accessing the database and making changes if situation demands.

2. Registration phase: The user end enters the user credentials such as username, email ID, password and real-time location of the user as were stated in the 'Registration phase' of MDLA. The registered details deflect in the database at the backend after hitting 'submit' button.

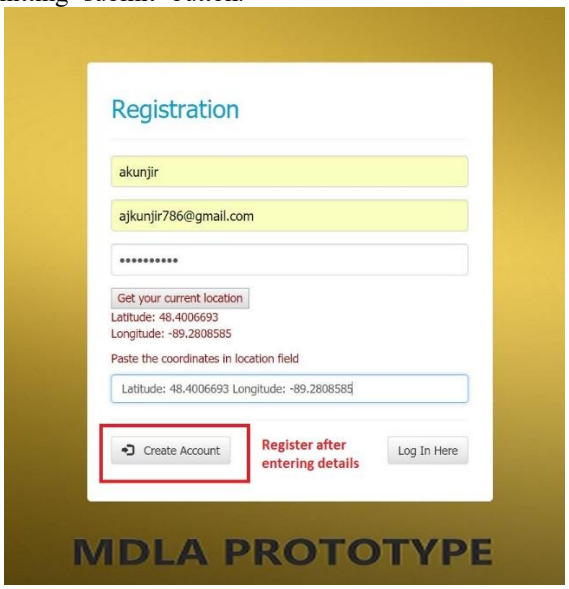

Figure 10:- Registration phase on the front end

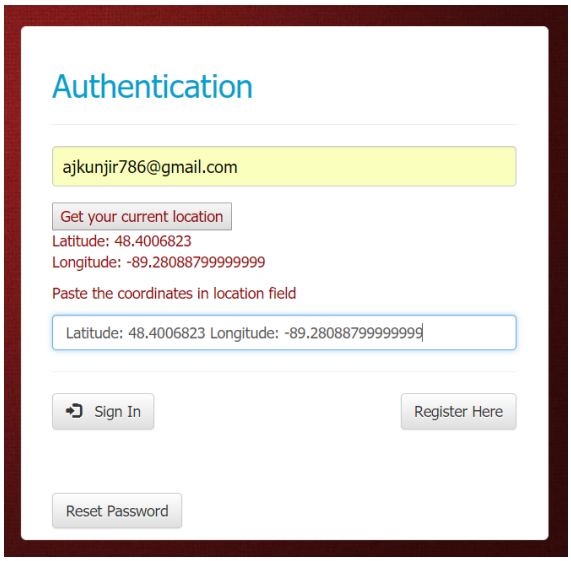

Figure 11:- Authentication phase

1. Authentication phase: After creating the account, the user is successfully registered to the system. User has to enter the registered email ID and live location to log in, after logging in, you land on the home page and also can update your location to avoid de-registration. For MDLA, the cloud server provides authentication grant to client's authentication request while logging in. In our case, our local system just matches the exact letters and allows user to enter in if they are same and not equal to '0'.
2. Update: The user can update his/her location after logging in and can also reset the password for enhancing the security.

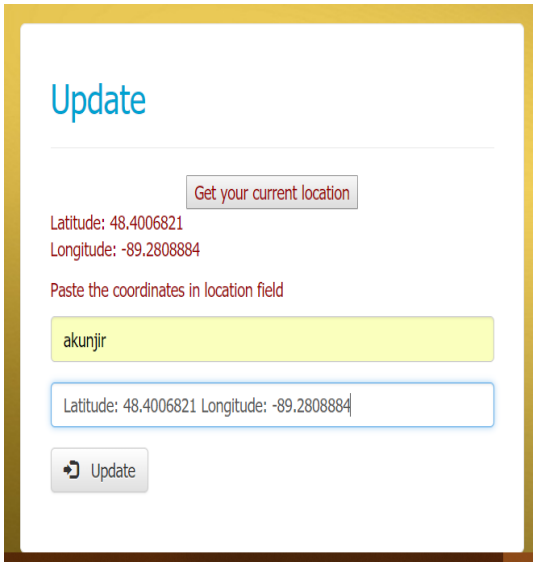

Figure 12:- Update Location Phase

Future Scope:-

Being a novel multi-disciplinary generic approach, MALL has been tested in fields of dynamic decentralized schemes. Shortly, MALL can also be configured to monitor and function in Ad-hoc networks. MALL can be applied in IoT (Internet of things) to remotely control various devices. MALL emphasize more on multi-hops for anchor nodes, the limitation on area of nodes can be decreased to make it able to gather information from anchor nodes within a single hop radius. The number of GPS nodes in the network can be decreased as of to make the computation efficiency reach its highest limit. As discussed in the earlier sections, MDLA has its applications for mobile device clients. MDLA and MALL can be combined to fetch location of mobile devices in the network without using GPS and user credentials. This can be achieved by doubling the use of location vector for authentication for communication.

Conclusion:-

In our research we elaborated on a decentralized localization approach 'MALL' which uses a two-step algorithm to localize a normal node in a wireless network using its neighbor normal and anchor nodes. Every nodes invoke its distance and coordinate matrices for storing the distance and locations of all its nodes in its neighborhood or local subnet formed. We also discussed about MDLA with its architecture. MDLA's three phases of working such as registration, authentication and update were enlightened in this article. After doing our research, we can conclude that MDLA can be used as a standard protocol in mobile clouds. MDLA is a secure and resource efficient protocol for authentication in mobile cloud servers. Unlike other approaches which rely on USIM chips in mobile devices for safe pathway, MDLA makes use of hashing function for encrypting the user credentials i.e username, password and email. MDLA incorporates location and timestamp vector in existing hashing algorithms that make our authentication system more secure. MDLA is based on 128-bit symmetric key authentication, it is also very resource efficient which results in low power usage for mobile devices.

Acknowledgment:-

We would like to thank all the co-authors for helping with the research suggestions and recommendations which helped us write this research paper. I appreciate Mr. Qiang Ye for providing us with resources via email and aided us understand the two approaches MALL and MDLA in wireless networks.

Abbreviations:-

MALL: Matrix completion and Localization
MDLA: Message Digest for Location based Authentication

References:-

1. S. Rallapalli, L. Qiu, Y. Zhang, and Y.C. Chen. Exploiting temporal stability and low-rank structure for localization in mobile networks. In Proc. of the sixteenth annual international conference on Mobile computing and networking, pages 161–172. ACM, 2010
2. M. Rudafshani and S. Datta. Localization in wireless sensor networks. In Proc. of the 6th international conference on Information processing in sensor networks, pages 51–60. ACM, 2007.
3. L. Hu and D. Evans. Localization for mobile sensor networks. In Proc. of the 10th annual international conference on Mobile computing and networking, pages 45–57. ACM, 2004.
4. B. Recht, M. Fazel, and P.A. Parrilo. Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization. Society for Industrial and Applied Mathematics Review, 52(3):471–501, 2010
5. A.M.Talib,R.Atan,R.Abdullah,and.Azrifah,"CloudZone:Towards an integrity layer of cloud data storage based on multi-agent system architecture," 2011 IEEE Conference on Open Systems, pp. 127–132, Sep. 2011.
6. Qiang Ye, Jie Cheng, Hongwie Du, Xiaohu Jia, Jing Zhang,"A Matrix Completion Approach to Mobile Network Localization", ACM Digital Library, 2014
7. Saurabh Dey, Srinivas Sampalli, Qiang Ye, "A Light-weight Authentication Scheme Based on Message Digest and Location for Mobile Cloud Computing", IEEE 2014. https://omnetpp.org/documentation/.