IJCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-6 E-ISSN: 2347-2693

Estimating Localization for intruder detection in WSN

Vinolia A[1*]and Jagajothi G[2]

[1,2]IT Department, Periyar Maniammai University, Vallam, Thanjavur, Tamil Nadu, India*
vinolia7191@gmail.com:; jagajothi.g@gmail.com

www.ijcaonline.org

Received: 12/05/2014 Revised: 26/05/2014 Accepted: 17/06/2014 Published: 30/06/2014

Abstract— Today's location based provisions relies on customer's mobile device to find the present area. This licenses malignant customers to enter a continued holding or outfit fake guards by undermining their areas. To address this issue, we propose Wi-Fi Based Location Proof Updating System (WBLPUS) in which colocated mobile phones usually make location verification and send data to the location confirmation server. This schema screens the location of the customer and guarantees the assurance reliant upon the advancement of the customer in the particular moment. Furthermore similarly recognize that either the particular customer is the customary customer or the assailant by emulating the log records in the Wi-Fi framework. The source area is ensured subordinate upon the weighed customer in the particular location. Extensive experimental results demonstrate that WBLPUS can enough give location proofs, on a very basic level defend the source location security, and effectively perceive the plotting assaults.

Keywords- Location Based Services, Colluding Attacks, RSSI (Received Signal Strength Indicator), Wi-Fi, Location Privacy.

I. INTRODUCTION

Mobile devices, such as smart phones and PDAs, are playing an increasingly important role in people’s lives. Location based applications take advantage of user location information and provides mobile users with a unique style of resource and service offerings. Today, it typically is a user’s mobile device that determines the device’s location (e.g., using GPS) and that sends the location information to an application. This approach makes it possible for a user to cheat by having his device transmit a fake location, which might let the user to access a protected resource erroneously. Therefore, an application might ask a device to prove that the device really is or was at the claimed location.

Information that is produced by mobile users could be retagged, and individuals who download the content ought to have the capacity to confirm the location claim connected with the information [14]. An organization may need verification from its repairmen that they truly taken after an endorsed route throughout the day. An individual blamed for carrying out a crime is really intrigued by having the capacity to demonstrate to the police that he was some place other than the crime scene at the time of the crime was conferred.

A location proof is an electronic type of record that confirms somebody's presence at a certain location eventually in time. A location proof architecture is a mechanism with which mobile users can acquire location proofs from proof issuers and with which applications can confirm the legitimacy of these proofs [3]. With a specific end goal to be genuinely valuable, a location proof architecture must be adaptable. For example, in some application scenarios, such as the police situations specified above, users may not know while being at a specific location that they will require verification for having been at this location later on. In this way, it must be workable for users to accumulate location proofs proactively. Nonetheless, the proactive get-together of location proof evidences must be carried out deliberately, overall proof issuers can track users and individuals' protection will be in danger.

Moreover, different applications have different requirements for the contents of a location proof, such as the granularity of the certified location [25]. For example, an insurance company might want to know only that a client drives around mainly in sedate Waterloo (as opposed to busy Toronto), but not where exactly in Waterloo. When a user does not know about the application that a location proof will be used for, she also does not know about the location granularity that will be required by the application. Including fine-grained location information in any location proof would solve this problem. However, presenting such a proof to an application might reveal more information than necessary about the user, and her privacy would get violated [11], [15], [16].

In this paper we propose Wi-Fi Based Location Proof Updating System (WBLPUS), which does not rely on the expensive trusted computing module. In WBLPUS, Wi-Fi enabled mobile devices in range mutually generate location proofs, which are uploaded to an untrusted location proof server that can verify the trust level of each location proof. An authorized verifier can query and retrieve location proofs from the server. Moreover, our location proof system guarantees user location privacy from every party. The locations of the user are updated based on the distance from each other. By analyzing the distance of the user service will be provided.

Corresponding Author: *Vinolia A*

The rest of this paper is organized as follows. Section 2 briefly reviews the related work. Section 3 presents the proposed framework. The results and discussions are elaborated in Section 4.We conclude the paper in Section 5.

II. Related Works

In recent times, some frameworks have been proposed to furnish end users the capacity to demonstrate that they were in a specific spot at a specific time. The result in [2] depends on the way that nothing is speedier than the pace of light so as to register an upper bound of a client's separation. Capkun and Hubax [4] propose challenge-response scheme, which utilize various beneficiaries to correctly appraise a remote node location utilizing RF propagation characteristics. In [21], the authors portray a secure localization service that could be utilized to create unforgeable geotags for mobile contents, for example, photographs and video. However committed measuring fittings or high-cost trusted computing module is needed.

Saroiu and Wolman [19] proposed a solution suitable for outsider validation; however it depends on a PKI and the wide organization of Wi-Fi framework. Unique in relation to these results, WBLPUS utilizes a shared approach and does not oblige any change to the existing base. Smokescreen [5] presents a sharing mobile social service between colocated clients which depends on centralized, trusted agents to facilitate anonymous correspondence between strangers. SMILE [17], [18] permits clients to make missed associations and uses comparative wireless strategies to demonstrate if a physical experience happened. Notwithstanding, this administration does not uncover the real location data to the service provider accordingly can just furnish location proofs between two clients who have really experienced. WBLPUS can furnish location proofs to outsider by transferring genuine experience location to the untrusted server while supporting location privacy.

There are lots of existing works on location privacy in remote systems. In [10], the authors proposed to diminish the precision of location data along spatial or transient extents. This fundamental thought has been enhanced by a series of works [9], [13]. All the above procedures cloak a node's locations with its current neighbors by trusted central servers which is powerless against DoS attacks or to be traded off. Not the same as them, our methodology does not require the location proof server to be reliable. Xu and Cai [22] proposed a feeling based model which permits a client to express his privacy prerequisite. One essential concern here is that the spatial and temporal correlation between progressive locations of mobile nodes must be carefully dispensed with to avoid outside gatherings from trading off their location privacy. The procedures in [1], [6], [7], [8] attain location privacy by changing pseudonyms in region called mix zones. In this paper, locations of every node are changed by the node itself dynamically. Recognizing a key tradeoff between performance and privacy, Shao et al. [20], [23] proposed an idea of statistically solid source anonymity in wireless sensor systems despite anything that might have happened before, while Li and Ren [17] and Zhang et al. [24] attempted to furnish source location privacy against traffic analysis attacks through dynamic routing or unknown validation. Our scheme utilizes comparative source location unobservability concept in which the true location proof message is scheduled through statistical algorithms. Nonetheless, their focus is to produce indistinguishable appropriations between different nodes to conceal the true occasion source, while our focus is to outline different locations between distinctive nom de plumes ensure the genuine personality.

Most existing IDS (Intrusion Detection System) are optimized to detect attacks with high accuracy. However, they still have various disadvantages that have been outlined in a number of publications and a lot of work has been done to analyze IDS in Wi-Fi network. RSSI is the most attractive because reading RSSI is economical and compatible with existing component is not accepted in any case, only if the quality of the model increases or does not decrease too much. In the existing system, a mobile social service is shared between co located mobile devices of the user which relies on centralized trusted brokers. It coordinates the anonymous communication between strangers. It is difficult to establish missed connections and utilize the similar wireless techniques to prove whether a physical encounter occurred on location privacy in a wireless network or not.

III. PROPOSED APPROACH

3.1 WBLPUS Architecture

In this work, Wi-Fi Based Location Proof Updating System (WBLPUS) is proposed. This system provides the ability to the end user to prove that they are in a particular place at a particular time. The privacy of each mobile device is maintained based on their current location. In this system, the user is identified based on the Received Signal Strength Indicator (RSSI). Using Wi-Fi tracking, we can exactly say where the user currently presents. Using adjacent networks also the user can be found. The locations of the user are updated based on the distance from each other. By analyzing the distance of the user service will be provided. The proposed system reduces the accuracy of location information along spatial or temporal location. The solution in relies on the fact that nothing is faster than the speed of light in order to compute an upper bound of user interface. It offers a solution suitable for third party attestation, but it relies on a RSSI based on the moment of the user. Continuous monitoring is carried out for detecting the attackers in the network. If the user is a normal user in the Wi-Fi based monitoring movement then the RSSI value is gradually increased. If the user is an intruder, then the RSSI value is exceeds the limit of the user’s normal movements.

3.2 The Location Proof Updating System

In this section, we introduce the location proof updating architecture, the protocol, the information is extracted based on their location, the location is identified based on RSSI, and intrusion detection based on distance to achieve location privacy in WBLPUS.

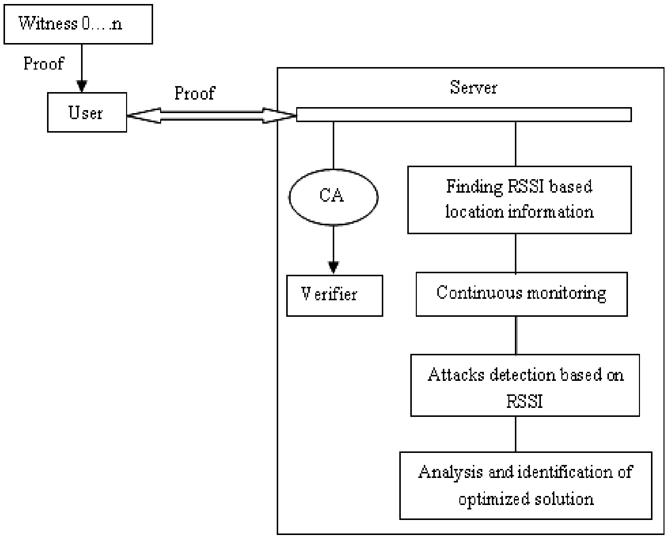
Witness 0….n
Proof
User
Proof
Server
CA
Finding RSSI based location information
Verifier
Continuous monitoring
Attacks detection based on RSSI
Analysis and identification of optimized solution

Fig.1 WBLPUS System architecture

Architecture

Mobile nodes communicate with neighboring nodes through Wi-Fi, and communicate with the untrusted server. Based on the different roles they play in the process of location proof updating, they are categorized as User, Witness, Location proof Server, Certification Authority or Verifier. The architecture of WBLPUS is shown in Fig.1

User: the node who necessities to gather location proofs from its neighboring nodes. The point when proof is required at time t, the user will broadcast an location proof to its neighboring nodes through Wi-Fi. In the event that no positive reaction is accepted, the user will create a dummy location proof and submit it to the location proof server.

Witness: When a neighboring node consents to give location proof for the user, this node turns into a witness of the user. The witness node will create a location proof and send it over to the user.

Location proof server: As our objective is to monitor the ongoing locations, as well as to recover the history of location proof data when required, a location proof server is important for saving the history records of the location proofs. It speaks specifically with the user nodes who submit their location proofs. As the source personalities of the location verifications are saved, the location proof server is untrusted as in spite of the fact that it is bargained and observed by attackers, it is impossible for the attackers to uncover the true wellspring of the location proof.

Certification authority: As regularly utilized as a part of many networks, we think about an online CA which is controlled by a free believed alternate gathering. Each mobile node registers with the CA and preloads its credentials matches before entering the network. CA is the only party who knows the mapping between the real identity and the locations. And also, it works as a bridge between the verifier and the location proof server. It can recover location proof from the server and forward it to the verifier.

Verifier: a third-party client or a requisition who is approved to check a user's location inside a particular time period. The verifier typically has close association with the user, e.g., companions or associates, to be trusted enough to increase approval.

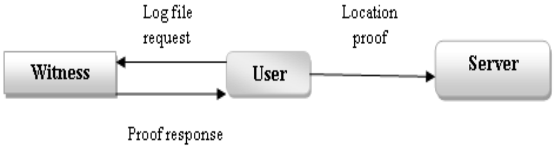

Fig.2 Location Proof Updating

When a client requirements to gather location proofs at time t, it executes location proof updating in Fig.2 to acquire location proofs from the neighboring nodes inside its correspondence range. Every node utilizes its M number of location evidences as its character all around the correspondence.

1. The user broadcasts a proof request to its neighboring nodes for its upgrade booking. The request holds the data about the user.

2. The witness chooses whether to acknowledge the log record appeal as per its witness scheduling. When concurred, it will produce a log file for both user and itself and send confirmation reaction to the user. The log file holds the data about witness nodes. This proof is signed and hashed by the witness to make sure that no attacker or user can modify the location proof and the witness cannot deny this proof.

3. After accepting the evidence reaction, the user is answerable for submitting this location proof to the location proof server.

4. Authorized verifiers can inquiry the CA for location proofs of a particular user. In place not to uncover connection between location proofs to the server, CA will dependably gather enough inquiries from k distinctive nodes before a set of questions are conveyed.

5. The location proof server just returns hashed location instead of the genuine location to the CA, who then advances to the verifier. The verifier contrasts the hashed location and the asserted location obtained from the user to choose if the guaranteed location is genuine.

6. Whenever the user moved to a new location, the proof will be generated based on the new location. The location privacy of witness nodes varies

depending on the time and location when they exchange location proofs.

3.3 Tracking based information extraction

The tracking of user is based on the Wi-Fi connected in the network. The user upon entering into the Wi-Fi network logging on to the services is allowed to use the services. The authorized user will enter the Wi-Fi services and unauthorized user is not allowed to access the services. The services will be online. The information about the tracking of user is based on network information such as longitude, latitude, actual time, actual date, SSID Name, MAC, RSSI, Quality, channel, speed, security, network type, etc., are gathered from the Wi-Fi based log files. The information is gathered from the monitored file. The movements of the user are changed time to time. So, continuous monitoring is carried out for updating the log files in the server. Whenever the user changed his position to new place, a new log file is generated based on the new location. The new movements are updated in the server.

3.4 Finding Location based on RSSI

The location of the user is based on the Received Signal Strength. The RSSI is calculated based on the movement of the user at a particular moment. The range of RSSI is different for every user. The normal movement traveled by the user from the particular place is monitored continuously. The range of RSSI will have the similar ranges for the movement of the normal user whereas it having a very high variation for attackers. The other network information also monitored for the reference of the people moment to predict the accurate location.

3.5 Intrusion detection based on distance

In Wi-Fi environment, an intruder can produce a group of colluding attacks at any time. So it is very difficult to detect the attacker easily. For this reason, a threshold value is given. The user is continuously monitored in the network [12]. The user using the services at the particular time can be a normal user or intruder. The threshold value is based on the movement of the normal user in the particular amount of time. If the moment of the particular user is normal as per the threshold value that particular user cannot be considered as the intruder. If the threshold value exceeds to certain limit, then there is an attacker entered in the network. The distance of the attacker can be varied compared to the normal user. It is calculated by,

$$d = (rssi * rssi) / q *1.92 / 2 \tag{1}$$

where, d is the distance of the user, rssi is the received signal strength indicator, q represents the quality.

IV. RESULTS AND DISCUSSIONS

4.1 Experimental setup

To evaluate the effectiveness of our system, this study included the experiments conducted in the Wi-Fi environment. Four Wi-Fi BSs/APs were placed in the target area and an SAMSUNG laptop was used to collect actual RSSI data at 55 different reference locations. RSSI data were measured 250 times for each reference location.

4.2 Performance Evaluation

In this section, we study the feasibility of deploying WBLPUS such as the computation, power consumption, and the proof exchange latency.

4.2.1 Prototype implementation

To study the feasibility of our scheme, we have developed a prototype of WBLPUS based on the techniques presented in the previous sections. The prototype has two software components: client and server. The client is implemented in JAVA on Android Developer Phone(A2DP), which is equipped with 512 MB RAM, 4 GB internal memory, Bluetooth, Wi-Fi 802.11 b/g/n, and running Google Android 4.0.4 OS. It can communicate with the server anytime through AT&T's 3G wireless data service. The server is implemented on a AMD E-300 APU with Radeon™ 1.30GHz 2GB RAM laptop. It stores the uploaded location proof records and manages corresponding indices using MySQL 5.0. We use two android phones to communicate with each other to test our solution.

This section compares the performance of the proposed system. Localization based information is taken as the cleared dataset. The possible amount of attacks can be considerably reduced in the dataset. In the cleared dataset online services are effectively produced without any internal attacks as well as external attacks in the network. Compared to the other network services, Wi-Fi produces the effective services and the performance of computation utilization is increased. The performance of the computation time is very less compared to all other networking services and the received signal strength also is increased. In Fig.3, the performances of four different networks are analyzed. The distance and the movements of the user under different RSSI at different time are analyzed. The RSSI value is dynamically changed based on the location of the user. Whenever the user switch on to a new location, a new location proof will be generated and updated in the location proof server. From the analysis, we can find the information such as the current location of the user, their privacy level, network information, neighborhood networks, and attacks to the user, and at which moment the user stops their connection from the server. And also we can evaluate the communication for the particular user.

The distance between the phones when they trade location proofs likewise influences the latency, where longer separation implies longer postpone because of the frail

Received Signal Strength. As has been built in prior studies, more than 80 percent of contact terms are not exactly 10 seconds, and therefore there is no issue for our verification trade procedure to be done inside the contact length of time. Fig. 4 measures the power utilization under different Wi-Fi status. There are three statuses: *proof Exchange, inquiry and standby*. The inquiry status is utilized to run across other Wi-Fi mechanisms inside correspondence extend, and convey confirmation demands. The inquiry methodology proceeds for a prespecified time, until a prespecified number of units have been uncovered or until it is halted unequivocally. Wi-Fi units that just listen to inquiry messages are in standby. In our framework, inquiry and standby are shared restrictive at whatever time. The mechanism enters the proof exchange status when it exchange location proofs with others. The most successive status is standby, which devours not exactly 2% of power with any correspondence distance. The proof exchange status expends the most measure of power and falls apart with expanding correspondence distance; be that as it may, it won't show up until the following location proof updating cycle.

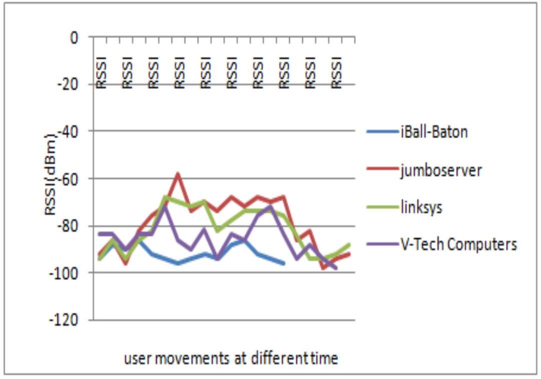

Fig. 3 Distance and the movements of the different users under different RSSI

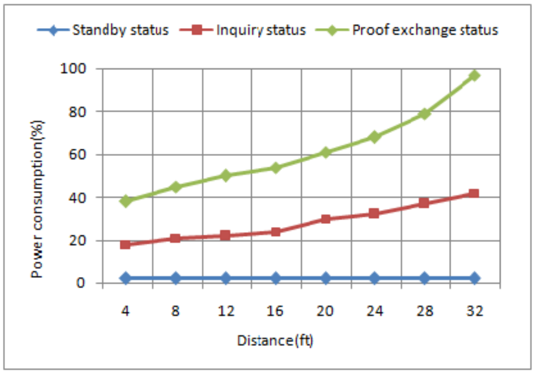

Fig. 4 Power consumption under different RSSI status and different communication distance

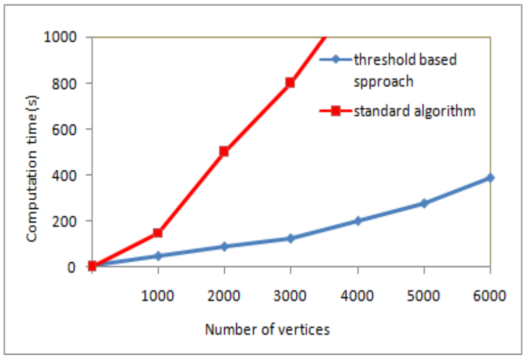

Fig. 5 Computation time with number of vertices

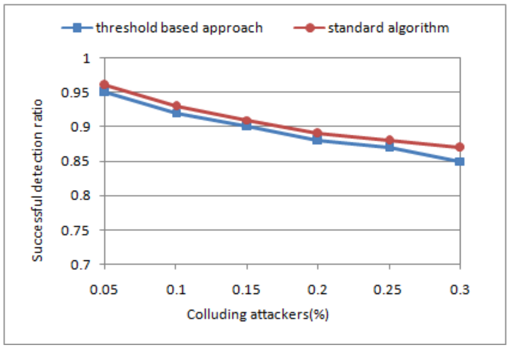

Fig. 6 Successful detection ratio

4.3 Collusion Detection

In this section, we evaluate the performance of collusion detection subordinate upon threshold based detection approaches. We consider four data sets: iBall-Baton, jumbo server, Linksys and V-Tech. We select generally joined customers (who have numerous allies) as seeds to start slithering. In the wake of collecting the customer and location data, we gain a data set of 65,346 customers and 98,129 locations. Note that each customer and location in the dataset is associated with a location which could be changed over to a geographical location (i.e., latitude and longitude) by method of Google map service.

So as to assess the performance of threshold based detection approach in light of distinguishing colluding nodes, we utilize computation time and successful detection ratio to measure the effectiveness and viability, individually. We additionally contrast this approach and a standard algorithm, in which each location proof is checked exclusively. This approach is assessed dependent upon the four square information set. As demonstrated in Fig. 5, threshold based approach is much quicker than the standard algorithm. As shown in Fig. 6, despite the fact that the detection ratio of threshold based methodology is a tiny bit lower than the standard algorithm.

V. Conclusion

In this paper, we proposed a Wi-Fi based location proof updating system called WBLPUS, where colocated mobile devices commonly create location proofs and transfer to the location verification server. We utilize dynamically changed location data for every user to secure source location protection from one another, and from the untrusted location verification server. To manage colluding attacks, we proposed threshold based detection approaches for outlier detection. Extensive experimental and simulation results demonstrate that WBLPUS can furnish real-time location proofs successfully. Besides, it conserves source location security and it is conspiracy safe.

REFERENCES

[1] A.R. Beresford and F. Stajano, “Location Privacy in Pervasive Computing,” IEEE Security and Privacy, **2003**.

[2] S. Brands and D. Chaum, “Distance-Bounding Protocols,” Proc. Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT ’93), **1994**.

[3] L. Buttya´n, T. Holczer, and I. Vajda, “On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs,” Proc. Fourth European Conf. Security and Privacy in Ad-Hoc and Sensor Networks, **2007**.

[4] S. Capkun and J.-P. Hubaux, “Secure Positioning of Wireless Devices with Application to Sensor Networks,” Proc. IEEE INFOCOM, **2005**.

[5] L.P. Cox, A. Dalton, and V. Marupadi, “SmokeScreen: Flexible Privacy Controls for Presence-Sharing,” Proc. ACM MobiSys, **2007**.

[6] E.D. Demaine, D. Emanuel, A. Fiat, and N. Immorlica, “Correlation Clustering in General Weighted Graphs,” Theoretical Computer Science, vol. 361, nos. 2/3, pp. **172-187, 2006.**

[7] N. Eagle and A. Pentland, “CRAWDAD Data Set mit/reality (v.2005-07-01),”http://crawdad.cs.dartmouth.edu/mit/reality, July **2005**.

[8] J. Freudiger, M.H. Manshaei, J.P. Hubaux, and D.C. Parkes, “On Non-Cooperative Location Privacy: A Game-Theoretic Analysis,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS), **2009**.

[9] B. Gedik and L. Liu, “A Customizable K-Anonymity Model for Protecting Location Privacy,” Proc. IEEE Int’l Conf. Distributed Computing Systems (ICDCS), **2005**.

[10] M. Gruteser and D. Grunwald, “Anonymous Usage of Location- Based Services through Spatial and Temporal Cloaking,” Proc. ACM MobiSys, **2003**.

[11] Guohong Cao, and Zhichao Zhu, “Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System”, IEEE Transactions on Mobile Computing, **2013**, Vol 12, no.1, pp.**51-64**.

[12] R. Herring, J. Ban B. Hoh , M. Gruteser, D. Work, J.C. Herrera, A.M. Bayen, M. Annavaram, and Q. Jacobson, “Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring,” Proc. ACM MobiSys, **2008**.

[13] Jiang T, H.J. Wang, and Y.C. Hu, “Location Privacy in Wireless Networks,” Proc. ACM MobiSys, **2007**.

[14] Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, “Location-Based Trust for Mobile User-Generated Content: Applications Challenges and Implementations,” Proc. Ninth Workshop Mobile Computing Systems and Applications, **2008**.

[15] Y. Li and J. Ren, “Source-Location Privacy Through Dynamic Routing in Wireless Sensor Networks,” Proc. IEEE INFOCOM, **2010**.

[16] W. Luo and U. Hengartner,” Providing Your Location Without Giving Up Your Privacy,” Proc. ACM 11th Workshop Mobile Computing Systems and Applications (HotMobile ’10), **2010**.

[17] J. Manweiler, R. Scudellari, Z. Cancio, and L.P. Cox, “We Saw Each Other on the Subway: Secure Anonymous Proximity-Based Missed Connections,” Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile ’09), **2009**.

[18] J. Manweiler, R. Scudellari, and L.P. Cox, “SMILE: Encounter- Based Trust for Mobile Social Services,” Proc. ACM Conf. Computer and Comm. Security (CCS), **2009**.

[19] S.Saroiu and A. Wolman, “Enabling New Mobile Applications with Location Proofs,’ Proc.ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile ’09), **2009**.

[20] M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards Statistically Strong Source Anonymity for Sensor Networks,” Proc. IEEE INFOCOM, **2008**.

[21] Shih-Hau Fang, Chung-Chih Chung, and Chiapin Wang,”Attack-Resistant Wireless Localization Using an Inclusive Disjunction Model”. IEEE Transactions on Communications, **2012**, vol.60, no.5, pp.**1209-1218**.

[22] T. Xu and Y. Cai, “Feeling-Based Location Privacy Protection for Location-Based Services,” Proc. 16th ACM Conf. Computer Comm.Security (CCS), **2009**.

[23] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, “Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks,” Proc. First ACM Conf. Wireless Network Security (WiSec), **2008**.

[24] Y. Zhang, W. Liu, and W. Lou, “Anonymous Communications in Mobile Ad Hoc Networks,” Proc. IEEE INFOCOM, **2005**.

[25] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci,’ A Social Network Based Patching Sheme for WORM Containment in cellular Networks”, Proc. IEEE INFOCOM, **2009**.

AUTHORS PROFILE

Vinolia A

Vinolia originates from Thanjavur, Tamil Nadu, India. She received her Bachelor of Technology degree in 2012 from Periyar Maniammai University and is currently studying towards her Master of Technology in Software Engineering degree at the same institution.