International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 24th December 2017. Link :

http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-13

Title: A Novel Solitude Preserving Localization System Based On Authentication For Mobile User Rigorous Networks.

Volume 06, Issue 13, Page No: 200 - 205.

Paper Authors

*** YARAMACHU SRIKANTH, MEDIDA NAGARJU.**

* Benaiah Institute of Technology and Science.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A NOVEL SOLITUDE PRESERVING LOCALIZATION SYSTEM BASED ON AUTHENTICATION FOR MOBILE USER RIGOROUS NETWORKS

***YARAMACHU SRIKANTH, **MEDIDA NAGARJU**

*PG Scholar, Benaiah Institute of Technology and Science,Rajhamundary,East Godavari(Dt),AP,India

**Assistant Professor, Benaiah Institute of Technology and Science, Rajhamundary,East Godhavri(Dt),AP,India

ABSTRACT

Location tracking and preserving in wireless networks are tedious as the network consists of infrastructure less devices that change their position more frequently due to acquired mobile patterns. In such networks, malicious users may prevail to snatch information by hiding their location and other spoofing other user information. STAMP is designed for adhoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. But STAMP does not ensure localization accuracy and time for switching user location. A new Lateration based Privacy preserving and Transmission Scheme (LPTS) is proposed for wireless networks to improve localization accuracy. Besides, trust group based verification improves secure transmission over the network minimizing errors in communication.

Keywords: - Lateration, Localization, Temporal provenance, Trusted Authority, User Privacy

I. INTRODUCTION

Location based services are emerging as a popular technology in mobile devices that support extensive applications, these days. The aim of the service is to locate and to share user position through a common intermediate like servers. The mobile devices at the user end identify its own position and broadcast the same to its neighbours through service providers. The major challenge in localization is its accuracy and trust ability.

Unknown or illegitimate users share false information to trusted users in the aim of spoofing or acquiring information through false locations. Location information spoofed or acquired in an unauthorized manner reveals tracking of user activity [1, 2].

Therefore preserving location of a user becomes vital to ensure security and authorized access in a global network. The process of securing location information starts from the end user by sharing their proof to a third-party verification agent. The user needs to share their location history and digital authentication metrics to the third party. The third party authenticates user through time slotted spatialtemporal provenance (STP) metrics [3,4]. In this paper, we propose novel light weight localization and secure sharing scheme through lateration and privacy preserving schemes. Unlike the other methods, rather than deploying a Certificate Authority (CA), we provide user dependent authentication scheme for localization and trusted group verification. In this scheme, the process is considered as the user need not rely on third party but it can achieve secure localization through self and neighbour verification process. Our contributions are

as follows:

a) We propose a dual state location preserving scheme that works in an autonomous manner.

b) The first phase of the process aims at locating user with minimum errors.

c) The second phase is developed for securing location sharing and to improve privacy preserving factors through a global network.

d) Simulation results validate the proposed approach in terms of location accuracy, overhead and success ratio. The rest of the paper is organized as follows: Section II briefs about the survey of the previous approaches. Section III explains the proposed LPTS method, phases of LPTS with its results and discussion. Finally, in section V we provide conclusion and future scope of our work.

II. RELATED WORK

Waters et al., [5] proposed a localization scheme aided by location manager for verification. The location manager distinguishes between forged and trusted information through location proofs provided, the end users must be aware of the verifying manager. Luo and Hengartner [3] proposed a three tier localization architecture called VeriPlace that ensures privacy and prevents collusion. VeriPlace is a three tier architecture that identifies user through their location or identity. VeriPlace fails when the number of requests generated by the user is more frequent. A two way location verification scheme is proposed by Hasan and Burns [6], in which location information is verified using WAPs and peer to peer devices. This method is centralized and supports limited user information.

A decentralized approach for user location information and sharing has been proposed by Davis et. Al [7]. The decentralized system achieves security and privacy using cryptography. This methods is not devised to handle attacks. Zhu et. al [4] proposed a tri-element verification scheme called APPLAUS. In APPLAUS, the mobile devices change their identity and update the same to a location server, CA and a verifying agent. Any of the three verification elements serve better in collusion and privacy preserving state of the end user. The drawback is that, this method consumes higher energy. Wang [8] et. al. Proposed a STP based mutual proof verification system called STAMP. Different from the previous approach, STAMP requires one CA with STP time slotted proofs for location information verification. STAMP aims atimproving user anonymity, being collusion defiant and support heterogeneous mobile network.

III. LATERATION BASED PRIVACY PRESERVING AND TRANSMISSION SCHEME (LPTS)

A. Problem Formulation

Privacy preserving and improving anonymity of users in a wide spread network is vital to protect user information to be accessed by unauthorized or illegitimate users. Security and verification schemes so far provided aim at improving the fore discussed metrics by compromising control message generation that leads to overhead and the post location services are affected by drop in accuracy. Accuracy drops increases localization errors. Providing multi level granularity and supporting heterogeneous network are considered to be the positive part of location sharing applications. For ensuring collusion resistance and to support external networks, the number of control messages generated at the time of verification holds user communication with delay or localization error in a growing mobile network. To retain the previous betterment and to minimize overhead in a scaling network, we propose a novel location and information sharing method called LPTS.

B. Network Model

We consider a wireless network with ‘N’ users reliable to communicate with their neighbours. Each user has different transmission range ( ) and possesses different mobility speed (m). The network is distributed in either sparse or dense manner. Higher the mobility, higher is the collusion rate. Our assumptions are as follows:
(i) Each user is aware of its own position
(ii) User must share their position for each communication they initiate.

(iii) Users can share location information based on either tri-angulation or multi lateration.

C. Proposed LPTS

The proposed Lateration based Privacy preserving and Transmission Scheme is of two-fold process:
(i) Lateration based Localization
(ii) Group Verification

(i) Lateration based Localization

Lateration is an effective technique [9,10] for locating mobile users with multi level location proof verification. Lateration is either tri or multi based on the available users in raange of the communicating user. The process of lateration in LPTS is illustrated in Figure 1.

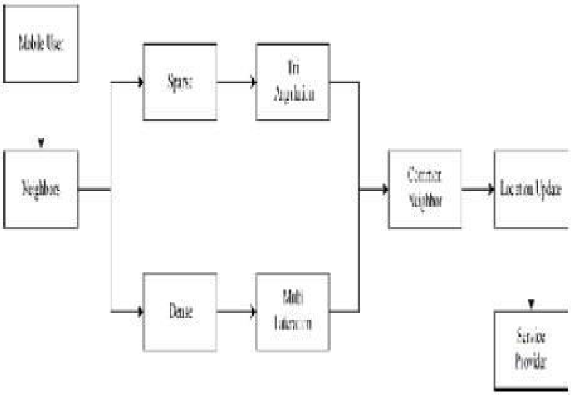

Figure 1. Lateration in LP TS

Tri lateration comes into existence when the number of users in a network region is less. In a tri lateration, the location proof of the user is determined using three reference p oint in the network. The process of triangulation is illustrated in figure 2.

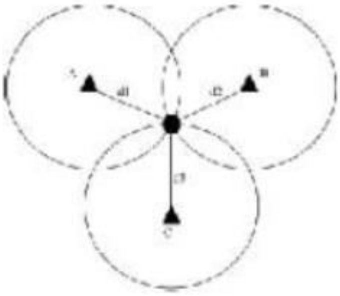

Figure 2. Triangulation

Figure 3. A and B point analysis

Let A(x , y) and B(x , y) represent the coordinates of the users A and B respectively, then the Euclidean distance (d) between A and B is given by equation given by equation (1)

$$d_{AB} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

For a mobile user, d contains some distortion and therefore, the new distance (d′) is given by equation (2)

$$d_{AB} = d'_{AB} + v_i$$

Where, v is the correction ind′ . v varies as mobility of the user varies and v is 0 if the user is static. The correction can be computed using equation (3)

$$v_i = \sqrt{(B_{x\_curr} - B_{x\_prev})^2 + (B_{y\_curr} - B_{y\_prev})^2}$$

Where, (B _ , B _) and (B _ , B _) are the current and previous positions of the user B. Multilateration [11, 12] comes into existence when the network is dense with more users. Multi lateration avoids collision by pre-determining the verifying users at the time of broadcast. Multi lateration (Figure 4.) can be employed for both range dependent and non-range dependent protocols in locating ser position. In multi lateration, a reference anchor user is selected based on heuristic optimal approach. An anchor must possess higher accuracy that is given by equation (4)
A^ = argmin ^ ∈ C |mul(A^ − P)| (4)

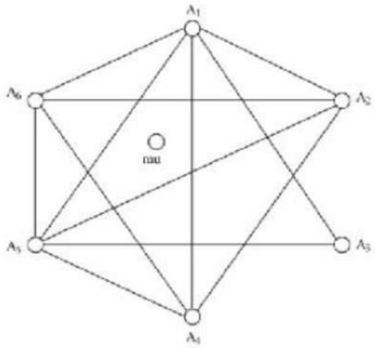

Figure 4. Multilateration

Where, P is the current position of the user considered for anchoring, C is the set of users present in of the mobile user. In a multi lateration, Geometric Dilution of Precision (GDOP) is used to measure localization errors. An mobile user to be selected as an anchor must be possess lesser GDOP. The GDOP of a mobile node is computed using equation (5)

$$\mathrm{GDOP} = \sqrt{(R^T R)^{-1}}$$

Where, R is the matrix that is represented as m × 2, ‘m’ is the set of nodes within the of the mobile user. The matrix R is represented as in (5)

$$R = \begin{matrix} \frac{\cdot d_1}{\cdot d(x,y)} \\ \\ \frac{\cdot d_m}{\cdot d(x,y)} \end{matrix}$$

The GDOP of all users are computed and the original Distance is computed using (2). A user possessing higher accuracy is selected as next anchor node. The location proof is verified by the new anchor for verification by the other in range users. Handling multiple requests in the previous studies increased the complexity by increasing the number of request messages and thereby leading to collusion. In multi lateration, the in-range neighbours are selected for location verification and peer to peer verification is avoided to minimize the additional requests being generated in lesser frequency.

(ii) Group Verification

This phase intends to provide security for existing users and their location information at the time of sharing through global network. For location information authentication, both the user and anchor must sign the broadcast at the time of verification. Mobile user verifies its neighbour and anchor verifies the mobile user with its adversary update from anywhere in the global network. For an unauthorized user to access location information, the anchor in its transmission range must attach a group ID to the broadcast information along with the authenticated user request. Let h() be a hash cryptographic function, AID be the identification unit of the anchor and *lm* be the location message of the mobile user. The pre authentication is given by the mobile user as represented

$$\Phi_M(lm) = [H_1 \quad H_2 \quad \cdots \quad H_k]$$

$$H_i - h(A_{ID} \quad lm \quad k_j)$$

Where, H = h(,M) and k is the transmission sequence key generated by the mobile user. The anchor node generates a session ID for authenticating the location message generated by the mobile user. After verifying the mobile user ID, the anchor integrates the ession ID for further security while sharing the information across the network. The ID generated by the anchor node is time dependant and expires after the slot time (T). The ID is not reusable and therefore a new ID needs to be generated at the time of next location sharing. This ID is common for users in the transmission range of a fixed anchor. Anchors exchange their ID periodically to ensure correctness of verification. The authentication of anchor is expressed as follows

$$'_A \quad \Phi_M(lm) - H(s_{ID};\ T_{slot};\ lm) \qquad (9)$$

Where, s is the session ID generated by the anchor. At the receiving end, the neighbour or another mobile user extract the authentication in (9) as follows

Where, s is the session ID generated by the anchor. At the receiving end, the neighbour or another mobile user extract the authentication in (9) as follows

$$\Phi_A(lm) - \mathrm{H}(\mathrm{M}_{\mathrm{ID}}, \mathrm{T}_{\mathrm{slot}}) \qquad (10)$$

Conditions for verification
Condition1: If T is greater than the broadcast time, the message will be discarded.
Condition2: If Φ ( ) − Φ ≠ then report M to neighbour anchor.
Procedure for authentication
Step1: The anchor identifies its in-range mobile users and shares theirP .
Step2: Anchor generates a series of random time slots (T) for *lm* sharing.
Step3: Anchor generates A ‖ T where, A is known to all {A , A ,…, A } ∈ (A)
Step4: The authenticated *lm* i.e. Φ ( )is broadcasted to the neighbour for location proof.
Step5: if T ≫ BCST_Time(A)then A discards the information.

IV. Results and Discussion

In order to prove the efficiency of the proposed LPTS method, we implement the method using Network Simulation Tool and analyze the performance of the method with a comparison to the previous approach STAMP.

1) *Simulation Setup*: We deploy 20, 40, 60, 80 and100 users who are aware of their position at the time of communication. A few nodes that satisfy (4) are selected as anchors that verify location of the mobile users and authenticate their transmission using a 32-byte authentication message. The network scenario is considered as a 1000mx1000m region. The broadcast time interval is 10s and the mean pause time for transmission is set as 0.25ms.

(2) Performance Metrics: We consider location accuracy, success ratio and localization overhead as our performance metrics. We plot location accuracy, success ratio and localization overhead with respect to number of mobile users.

(3) Analysis of Location Accuracy

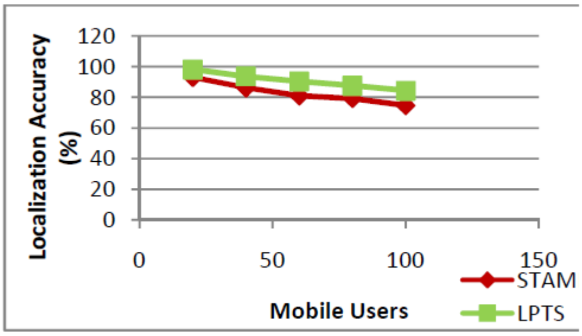

Figure 7. Overhead Comparison Graph

We compare the performance of overhead compared between STAMP and LPTS. As the number of users increases, control messages generated by the users increases and thereby retards location information exchange, increasing the overhead. LPTS prevents periodic broadcast of location information minimizing the number of control messages generated. Therefore the location overhead is less in the proposed LPTS.

IV. CONCLUSION

In this paper we propose a novel localization and privacy preserving algorithm called Lateration based Privacy preserving and Transmission Scheme (LPTS). LPTS overwhelms the major drawback of overhead observed in the existing approaches by minimizing the frequency of location update and location request. To retain control over privacy the non-periodic updates, a global verification scheme based on trusted anchor points is integrated with the localization scheme to ensure secure information sharing. Moreover the process is light weight as it requires lesser control messages to be broadcasted at the time of location sharing. This work can further be integrated with on-demand location services with handoff management and extend its support for heterogeneous network.

V. REFERENCES

[1] S. Saroiu and A. Wolman, “Enabling new mobile applications with location proofs,” in *Proc. ACM HotMobile*, 2009.
[2] I. Krontiris, F. Freiling, and T. Dimitriou,

"Location privacy in urban sensing networks: Research challenges and directions," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 30–35, Oct. 2010.

[3] W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture," in *Proc. ACM GIS*, 2010, pp. 23–32.

[4] Z. Zhu and G. Cao, "Towards privacypreserving and colluding-resistance in location proof updating system," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 51–64, Jan. 2011.

[5] B. Waters and E. Felten, "Secure, private proofs of location," Department of Computer Science, Princeton University, Princeton, NJ, USA, Tech. Rep., 2003.

[6] R. Hasan and R. Burns, "Where have you been? Secure location provenance for mobile devices," *CoRR* 2011.

[7] B. Davis, H. Chen, and M. Franklin, "Privacy preserving alibi systems," in *Proc. ACM ASIACCS*, pp. 34– 35, 2012.

[8] X. Wang, A. Pande, J. Zhu, and P. Mohapatra, "STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users," *IEEE/ACM Transactions on Networking*, vol. 24, no. 6, pp. 3276–3289, 2016.

[9] Z. Yang, Y. Liu, and X.-Y. Li, "Beyond Trilateration: On the Localizability of Wireless Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, vol. 18, no. 6, pp. 1806–1814, 2010.

[10] C.-Y. Shih and P. J. Marrón, "COLA: Complexity-Reduced Trilateration Approach for 3D Localization in Wireless Sensor Networks," *2010 Fourth International Conference on Sensor Technologies and Applications*, 2010.