Design and Analysis of Fabrication Threat Management in Peer-to-Peer Collaborative Location Privacy

Balaso Jagdale†*, Shounak Sugave, and Kishor Kolhe

*Corresponding author E-mail: *balaso.jagdale@mitwpu.edu.in*
†Faculty at School of CET, Dr. Vishwanath Karad MIT World Peace University, Pune, India

Summary

Information security reports four types of basic attacks on information. One of the attacks is named as fabrication. Even though mobile devices and applications are showing its maturity in terms of performance, security and ubiquity, location-based applications still faces challenges of quality of service, privacy, integrity, authentication among mobile devices and hence mobile users associated with the devices. There is always a continued fear as how location information of users or IoT appliances is used by third party LB Service providers. Even adversary or malicious attackers get hold of location information in transit or fraudulently hold this information.

In this paper, location information fabrication scenarios are presented after knowing basic model of information attacks. Peer-to-Peer broadcast model of location privacy is proposed. This document contains introduction to fabrication, solutions to such threats, management of fabrication mitigation in collaborative or peer to peer location privacy and its cost analysis. There are various infrastructure components in Location Based Services such as Governance Server, Point of interest POI repository, POI service, End users, Intruders etc. Various algorithms are presented and analyzed for fabrication management, integrity, and authentication. Moreover, anti-fabrication mechanism is devised in the presence of trust. Over cost analysis is done for anti-fabrication management due to nature of various cryptographic combinations.

Keywords: *Location Privacy, Fabrication Management, Cryptography Applications, Peer-to-Peer, Authentication*

1 Introduction

Fabrication is the basic type of attack in information where adversary generates or fabricates malicious information and sends it to targets, either for monetary benefits or to hog down the targets or for playing fun with the system.

Formally, fabrication process creates packets or frames of information wherein headers, Meta data and payload data is created maliciously. That means source address or identity is changed by the adversary or malicious mobile user. Fabrication attack can be launched by any entity in the system that is application, transport, network or data-link layer entity. Even networking element such as switches, routers or gateways can also launch this attack.

Figure 1 shows threat classification.

Fig 1: Basic types of threats

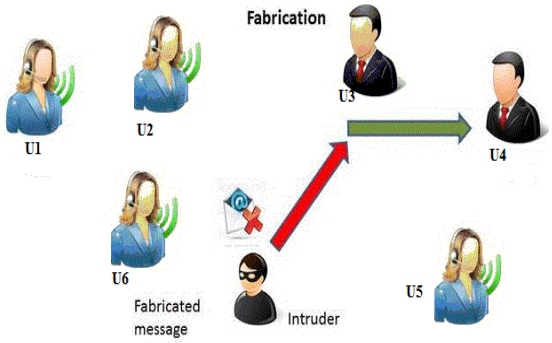

Fig 2: Fabrication scenario

As shown in figure 2, even if U6 do not send any information to U4, an adversary or intruder fabricates entire packet along with header, address and sends to U4, as if packet is sent from U6. Or even payload can also be fabricated and sent to U4.

2 Related work

Yuwen Pu and other [7], have proposed location privacy scheme that introduces idea of integrity and collusion protections, however detailed fabrication management algorithms are required further in vehicular or collaborative adhoc networks. Jun Jhou et al. [8], explored secured and light weight privacy protocols for authentication in VANET and demonstrated reduction of redundancy of

Manuscript revised December 20, 2021

https://doi.org/10.22937/IJCSNS.2021.21.12.55

messages, however integrity issue is not addressed in the protocol. Levent Ertaul and Nitu Chavan [9], brought forward investigation of location proximity protocols, where without exact location sharing with third party, users can shared their whereabouts. Author has claimed performance and trust benefits in location privacy, but not mentioned how fabrication attacks can be mitigated. GUANHUA CHEN and Others in [10], presented certificates less interaction between mobile users, where authentication between users is assured but not revealed to third party service providers in the process. Authors have upheld good performance and better communication efficiency but there is a lack of integrity and signatures. CAO SHOUQI and his research team, [11] reviewed Memon's protocol of authentication protocol with enhanced anonymous authentication, with protection of context information from adversaries and claimed higher secrecy with moderate computational overhead. Philip Asuquo and others [12], have examined location privacy obligations in VANETs and used cryptographic techniques are employed which needs more attentions in terms of development of algorithms. Xiong Li et al., [13] suggested light weight technique of authentication in multiparty mobile user nodes and indicated its usefulness in new high-speed networks and Vehicle to everything applications. Lili Yu [14] and others, focuses in personalized anonymity and location anonymity techniques with randomness, where protocol provides faster processing in real time environment, for location privacy, mechanism of anti-fabrication is very much anticipated as future work. Lijuan Zheng [15] and others have anticipated use of K-anonymity clustering to balance the location privacy and quality of service. It used centroid of group to mix end users location, however integrity need to be explored. Mahesh Kumar et al., [16] have used new technology of blockchain to expliot inherent benefits of blockchain, for providing anonymity and integrity issues of location of mobile users in location-based services. Further they have proposed Hyperledger fabric, but need to be verified with adversary models, its success for security and performance. Elbasher Elmahdi et al., [17] have studied compression-based scheme to isolate adversary nodes after detecting malicious data integrity by rode side units, showing good communication speed in applications. Balaso Jagdale et al., [18] have proposed location privacy protection in mobile object monitoring systems, thus balancing privacy and effective monitoring, however authors have hinted for fabrication management thus specifying need of integrity and authentication of mobile users. Turki Kordy et al [19] suggested Hyperelliptic Curve Cryptosystem and claimed better performance as compared to public key system such as RSA. Signature is achieved with hyperelliptic curve with multifactor authentication. It is reviewed good for light weight devices, but assuming enough power in mobile devices, we can have better multiprotocol hybrid algorithms to achieve integrity and authentication goals for better anti fabrication of location sharing.

3. Fabrication in Peer-to-Peer cooperative systems for Location Privacy

As stated in peer-to-peer LBS system or in collaborative cloaking, decisions are to be taken based on peer user's information regarding cloaking computation, query formation and shortlisting of required POIs. Authentic information is required for decision making. Otherwise, it will have adverse effect on quality of POIs and privacy strength. Member users who are not cooperating or some adversary users may send fabricated identity and LBS information to peers which may cause wrong calculations of cloaking regions and thus hampering the privacy achieved. Fabrication attacks deals mainly with authentication. Authentication is mainly addressed by public key cryptography and digital signatures. If it has to happen in commercial and social domain applications, IT law is also associated for the acts committed by different users of the system. It always happens in crowdsourcing application where information fabrication chances are there by service providers, software operators and end users [1]. Following diagrams illustrates example scenarios in collaborative and peer to peer cloaking system.

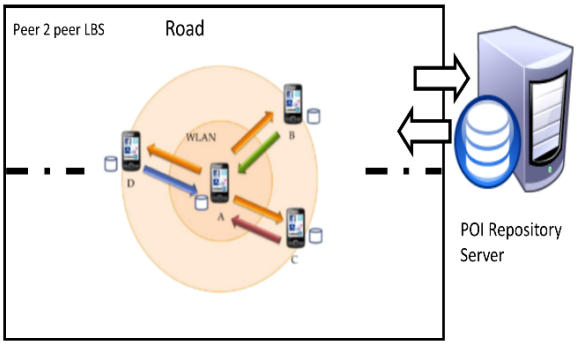

Fig 3: a) Peer to Peer LBS

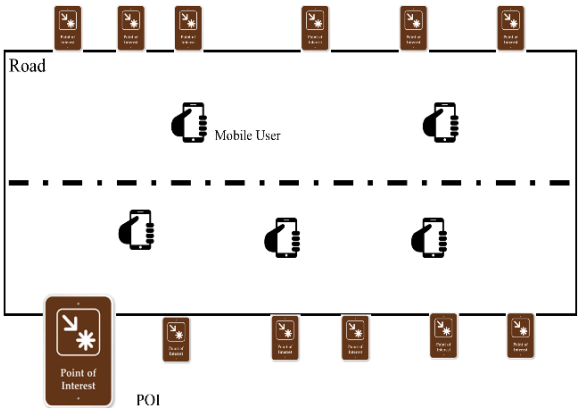

Fig 3: b) Controlled POI Broadcasting

Figure 3a shows the peer-to-peer local database scheme, which populates its POI database based of its locality persistency. But users' needs cooperative exchange of POI information to each other. Fabrication problem is in the form of adversary and /or malicious member users.
Figure 3b shows the peer-to-peer scheme, where POI keeps on broadcasting with some interval, about its presence. Meanwhile user sets his preference in mobile and keeps moving around. It there is match, mobile client gets alert of POI availability. POI devices fitted in shops or adversary POIs are possible threats for fabrication.

Public key systems and digital signatures
Digital signatures are the general population key primitives of message confirmation. In the physical world, it is basic to utilize manually written signatures on transcribed or wrote messages.
Essentially, a digital signature is a system that ties a man/substance to the digital information. This coupling can be autonomously confirmed by collector and in addition any outsider. Digital signature is a cryptographic esteem that is ascertained from the information and a mystery key known just by the underwriter. In business, the collector of message needs confirmation that the message has a place with the sender, and he ought not to have the capacity to revoke the agreement of that message. This necessity is extremely urgent in business applications, since probability of an argument about traded information is high.
As specified before, the digital signature plot depends on open key cryptography. The model of digital signature process is portrayed in the accompanying representation in figure 4.

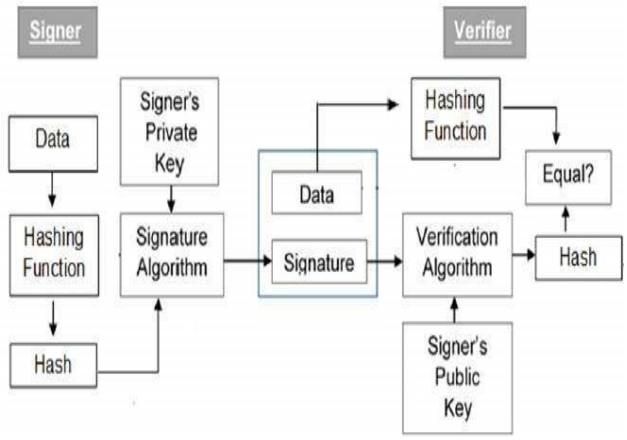

Fig 4: Digital Authentication Process

Figure 4 shows the process of digital signatures and verification process. Signature process achieves Responsibility, Integrity and Message verification Goals in the secured networked applications

4 Proposed Anti Fabrication solution with Public key cryptography and Digital signature

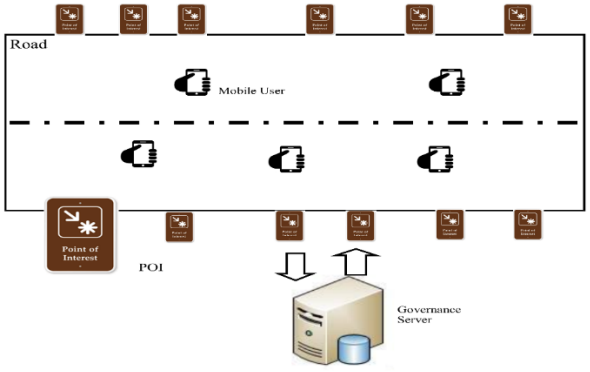

Fig 5: Peer 2 Peer - POI broadcasting location privacy

As shown in figure 5, Governance server (GS) is introduced to mitigate fabrication done by malicious users and adversaries. Every user has to register with GS, with mandatory information pertaining to identity, such as Public id (Uid), Name, address, email id, phone etc. During registration user has to sign digitally and it is stored on server as Uid and Signature USid.

Similarly POI owner has to register his POI mandatory data with GS server with POI ID, Owner ID, POI location, POI address, POI search data, phone etc. During registration POI owner has to sign digitally and it is stored on server as Pid and Signature PSid.

4.1 Registration of POI with Governance Server

Registration of POI with GS server

1. Pre-conditions: PKI infrastructure is in place and public certificate are distributed
   Let own_k1 and own_k2 are private key and public key of POI owner
   Let gs_k1 and gs_k2 are private key and public key of GS server
   Let Gid is GS server ID,
2. Let the mandatory POI information document be *poi_doc* { POI ID, Owner ID, POI_long, POI_latt, POI address, POI search data, Email, Phone }
3. Signature of POI is
   $$PSid <- Encr_{own\_k1}\{Hash\{poi\_doc\}\}$$
4. Owner of POI sends tuple to GS database entry as { *Pid, OiD, PSid, poi_doc* }

5. GS server verifies the record received from Owner of POI as

$$t1_{hash} = Decr_{own\_k2}\{PSid\}$$
$$t2_{hash} = Hash\{poi\_doc\}$$

If ($t1_{hash} == t2_{hash}$) verification status is true else return status is false

6. Owner gets registration acknowledgement gs_ack as

$$gs\_ack <- Encr_{gs\_k1}\{Hash\{Gid + Pid + Oid + poi\_doc + status\}\}$$
$$reg\_doc <- \{\{Gid + Pid + Oid + poi\_doc + status\}\}$$

GS sends tuple to POI device as {Gid, gs_ack, reg_doc}

7. POI device verifies the record received from GS server as

$$t1_{hash} = Decr_{gs\_k2}\{gs\_ack\}$$
$$t2_{hash} = Hash\{reg\_doc\}$$

If ($t1_{hash} == t2_{hash}$) verification status is true else return status is false

8. Registration process ends here

POI Fabrication check by LBS user

1. All Users and POIs gets the Public key certificates (PKI). Public ids of mobile user and POI device are used to retrieve the public keys from different sources.
2. Ui sets his search in his mobile application with keywords on his way.
3. POIj (shop) broadcasts its information on regular interval say Tt
4. Ui gets match and alert on the way for required POI say POIj. It's from Pid. Alert is AnsPj
5. Now, user UI needs to verify POI, he requests the server GS to send PSid of Pid
6. Server Sends PSid to user Ui.
7. Ui verifies identity of Pid by decrypting process (Pid, AnsPj, PSid, Pidkey2)
   Pidkey1 is assumed as Private Key, Pidkey2 as public Key, and thus protection of fabrication.
8. Ui utilizes information as per his requirements.
   Ho is original hash of POI data, Hc is current hash

$$Ho = Decr_{Pidkey2}(PSid)$$
$$Hc = Hash(AnsPj)$$

If (Ho == Hc) no fabrication of identity and information of POI

4.2 Mobile Users Fabrication Verification

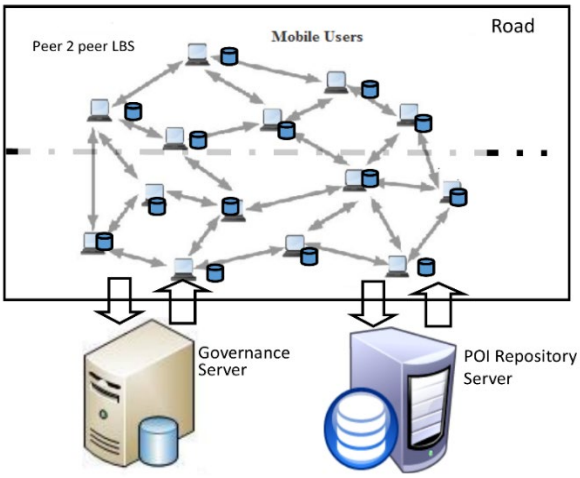

Fig 6: Governance Server for fabrication protection using digital signature

As shown in figure 6, mobile users maintains database of local POIs based on their locality or persistency. Mobile users cooperatively pledge to help each other for POI answers and privacy. Mobile devices populates their database from POI repository server maintained by national regulatory authority.

Terminology:

1. POI- Point of Interest device
2. USid- Signature of mobile user
3. upid- Users public Identity
4. Gid- GS server Unique Identity
5. GS server name- gs_name
6. user_doc – user registration information in format
7. ureg_doc – User registration document received from GS server

a. POI repository server registration
POIs are registered as explained in section 4.1

b. Registration of Mobile User with Governance Server

Registration of Mobile User with Governance server

1. Pre-conditions: PKI infrastructure is in place and public certificate are distributed
   Let user_k1 and user_k2 are "private key and public key" of mobile user
   Let gs_k1 and gs_k2 are "private key and public key" of GS server
   Let Gid is GS server ID,
2. Let the mandatory POI information document be *user_doc* { upid, nick_name, user_address, email, phone, remarks }
3. Signature of mobile user is
   $$USid <- Encr_{user\_k1}\{Hash\{user\_doc\}\}$$
4. Mobile user sends tuple to GS database entry as { *upid, USid, user_doc* }
5. GS server verifies the record received from mobile user as
   $$t1_{hash} = Decr_{own\_k2}\{USid\}$$
   $$t2_{hash} = Hash\{user\_doc\}$$
   If ($t1_{hash} == t2_{hash}$) verification status is true else return status is false
6. User gets registration acknowledgement *gs_ack* as
   $$gs\_ack <- Encr_{gs\_k1}\{Hash\{Gid + gs\_name + upid + user\_doc + status\}\}$$
   $$ureg\_doc <- \{\{Gid + gs_{name} + upid + user\_doc + status\}\}$$
   $$user\_hash\_1 <- \{Hash\{Gid + gs\_name + upid + user\_doc + status\}\}$$
   user_hash_2 = user_hash_1
   GS sends tuple to mobile user as {*Gid, gs_name, gs_ack, user_hash, ureg_doc*}
7. User verifies the record received from GS server as
   $$t1_{hash} = Decr_{gs\_k2}\{gs\_ack\}$$
   $$t2_{hash} = Hash\{ureg\_doc\}$$
   If ($t1_{hash} == t2_{hash}$) verification status is true else return status is false
   Store in GS database { *upid, nick_name, user_address, email, phone, remarks, USid, gs_ack, user_doc, ureg_doc, user_hash_2* }
8. User registration process ends here

c. Verification of peer mobile users with the help Governance Server

Identity fabrication check of one user by other peer mobile user

1. All system users gets the public key certificates (PKI). Public ids of mobile user are used to retrieve the public keys of other users for verification.
2. User *i* forms and broadcasts his query Q = { upid_*i*, search keywords }
3. Nearby user *j* broadcasts reply to user *i*
   ans = {*upid_j, user_hash_1, answer array of tuples*[*pid, PSid, poi_doc*]}
4. Now, user *i* needs to verify identity of j, he sends upid_*j* to GS server
5. $Server\ Computes\ _{gs\_sig\_j} = Encr_{gs\_k1}\{upid_j + user\_hash\_2\}$
6. GS Server sends { *upidj*, *gs_sig_j* } to user U*i*.
7. **USER *verification***
   $User\_hash\_2 = retrive(\ Decr_{gs\_k2}\{gs\_sig\_j\}$
   If (*user_hash_1 == user_hash_2*) no fabrication of identity else return false

   POI *verification*
   For (all POIs in ans List 1…n)
   {
   Ho is original hash of POI data, Hc is current hash
   $Ho = Decr_{Pidkey2}(PSid)$
   $Hc = Hash(poi\_doc)$
   If (Ho == Hc) no fabrication of identity and information of POI
   }
8. U*i* utilizes ans information as per his requirements.

d. Fabrication proof communication (Authentication, Integrity) for collaborative cloaking.

Following process describes how mobile users exchange cloaking information in collaborative way and sends request through agent nodes or through trusted third party servers to LBS server.

Fabrication proof communication (Authentication, Integrity) for collaborative cloaking

1. Precondition: Let us have *uid* per user
2. Precondition: Let *user_k1* and *user_k2* are private key and public key of mobile user.
3. Msig_j is a signature of cloaking information from user *j* and Smsg_j is secured cloaking information from user *j*.

4. Suppose user *j* is sending cloaking communicating to user *i*
5. $Msig\_j < -Encr_{user\_k1\_j}\ (Hash(uid_j + User\ j\ cloaking\ information))$
6. $Smsg\_j < -\ Encr_{user\_k2\_i}\ \{\ Encr_{user\_k1\_j}\ (uid_j + User\ j\ cloaking\ information)\}$
7. U*j* sends its cloaking information to *i* as { *uid, Msig_j, Smsg_j* }
8. // Double encryption ensures authentication & secrecy and hash ensures integrity.
9. User *i* retrieves cloaking information as follows

$$info = Decr_{user\_k2\_j}\left\{Decr_{user\_k1\_i}\{Smsg\_j\}\right\}$$

$$hasht1 = hash\ (info)$$

$$hasht2 = Decr_{user\_k2\_j}\{Msig\_j\}$$

$$if\ hasht1 == hasht2, verified\ information\ of\ j\ by\ i$$

10. End of fabrication proof communication between two user *i* and *j*

Note: For non-repudiation purpose i.e. *i* must not deny message from *j*

$$ack = Encr_{user\_k2\_j}\left\{Encr_{user\_k1\_i}\{info\}\right\}$$

User *i* send this ack to *j* for confirmation

5 Proposed Anti Fabrication solution with Trust Management

Xheng [2] has discussed trust management in collaborative systems and also given challenges of trust management.

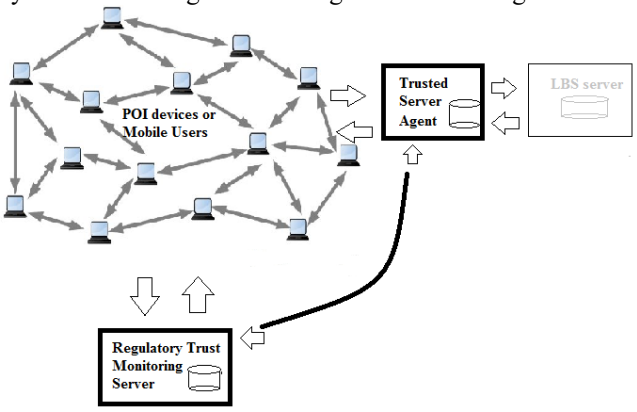

Fig 7: Regulatory Trust measurement server

As shown in figure 7, Mobile users or POI nodes need to register with regulatory authority for identity and trust management. Later database of trust is deployed indicating the different trust parameters on the Regulatory Trust Monitoring Server (RTMS). Trust measurement is mostly related with application domain of location based services. For example, if it's about OLA taxi, then taxi (POI) drivers trust is measured by parameters such as vehicle conditions, delays, driving skills, interactions, ambience etc. Similarly mobile user who is availing service, trust is also measured for him, like user's cooperation, punctuality, interaction, payment, luggage, etc.

In LBS system, mobile users who are exchanging cloaking information with other users in a collaborative way, trust is measured by other mobile users as well as trusted third party agents. This is done by introducing RTMS component, where users and POIs trust is stored in database system and it is used to take cloaking decisions.

5.1 Database Design at RTMS

POI_trust_DB

POI_id	POI_Category	Sub_Category	Longitude	Latitude	User_id	Date & Time	Trust value

USER_trust_DB

User_id	Name	Email	Phone	User_id	Date & Time	Appl Domain	Appl Sub_Domain	Trust Value

1. Trust database is accumulated and maintained at every user mobile device database.
2. Trust database is accumulated and maintained at every POI device database.
3. Trusted Server agent also report about user's feedback to RTMS.

Thus the trust value increases as the user is cooperating with the system to form the cloaking for other mobile users or if users are acting as carriers for other users to protect the privacy from TTP server or from LBS centralized server. Similarly POI trust will be improved like many system operating today such as OLA car booking system or shops experience to the user. Users' gives high ranking to the POI's if POI is performing well and not fabricating the data to attract the customers.

User Trust

Ui stores Uj's trust value if Uj is cooperating for LBS cloaking and LBS query system. As the times goes on Ui will accumulate the trust of Uj and gives priority to Uj if Uj has high trust with Ui. This priority means, involving Uj for cloaking, or query formation or query execution

operations. Participating nodes are rewarded like OLA system, which we are keeping out of scope of this discussion.

POI Trust

POI are shops or actual service components of LBS system. POI gives its information to various servers such as LBS servers, Government servers, Other Peer users in case of peer systems. But trust improves over the period of time, if POI service is satisfied. If an adversary POI is present in the system, its trust value is automatically decreases thus protection of tampering. Trust does not give full formal satisfaction of fabrication but digital signatures with law binding ensures full satisfaction for tampering from malicious users.

5.2 Collaborative privacy is based on user trust parameters

1. Based on User –Reliability (tp1, 0.2), Locality (tp2, 0.2), Quality (tp3, 0.2), Cooperative Nature (tp4, 0.2), Delay (tp5, 0.2)
2. Feedback stars– 10, 20, 30, 40, 50 .. 100 (100 being maximum)
3. No of participating users for user i, say N

1. $Trust(t) = \left(\sum_{i=1}^{N}\{(tp1_i * 0.2)+(tp2_i * 0.2)+(tp3_i * 0.2)+(tp4_i * 0.2)+(tp5_i * 0.2)\}\right)/$ N
2. If (trust ($user_i$) > 85) user i is excellent for cloaking association
3. If (trust ($user_i$) < 85 && > 60) user i is ok for cloaking association
4. If (trust ($user_i$) > 40 && < 60) user is i can be considered for cloaking association
5. If (trust ($user_i$) < 40) user is i is not considered for cloaking association

Use of fabrication protection for following methods of location privacy

Both the techniques of fabrication protection described above are applicable to collaborative location privacy such as persistency and broadcast based Message exchange protocol, collaborative cloaking method of location Privacy.

6 Overhead cost analysis of anti-fabrication mechanism

To mitigate the fabrication attacks, digital signatures are the prime solutions other that trust management. Adversaries or even mobile elements of the system will not be able to fake identities and information send for collaborative cloaking. To use digital signatures, we need to use encryption algorithms such as public key cryptography, symmetric key cryptography and digest algorithms. Use of RSA, ECC, AES 128, AES 256, Sha1, Sha256 algorithms will suffice for the purpose of digital signatures. Public key algorithms are costly in terms of time, and hence more power consumption in mobile phone. But today's mobile hardware and technology encourages to use complex cryptography algorithms in mobile phones. It is important to understand the performance of these algorithms to study the overhead of anti-fabrication management in peer to peer location privacy.

6.1 Estimates of cost for digital signatures

It is important to understand the cost in mobile client rather than sever side as power is not a big issue at stationary site of server and POI device if stationary (ex. shop). So more stress is given to study the cost if registration and verification in user mobile device.

A) Registration by mobile user

1. Cost over head registration without digital signatures

Under normal process, without digital signatures

$$Trsimple = t1 + t2 + t3 + wt$$

(Let us assume wt as 0 for simplicity)

Where *t1* is Communication time to send query

t2 is the time required to process registration at server

t3 is the round trip time required to get reply

wt is the variable waiting time due to networking parameters

2. Cost over head for registration process with digital signatures

Registration process is only in the beginning.

$$trsign = hasht1 + signt1 + trsimple$$

hasht1 = time to computer hash of user information or POI information

signt1 = time to compute signature

3. Cost with Authentication and Integrity & Non repudiation

$$Treg = tsign2 + trsign$$

tsign2 is the time for double encryption

4. Verification of registration after receiving registration docs from server

$$Tr\_verification = tdecr + thash + Treg$$

tdecr is the time of decryption of communication from server after registration

thash is the fresh has computation of doc received from server

***Tr_verification* is the total time of registration and its verification**

B) Cost of Verification of mobile user by another user

1. Cost over head of verification without digital signatures

Under normal process, without digital signatures

$$tsimple = t1 + t2 + t3 + wt$$

(Let us assume wt as 0 for simplicity)

Where *t1* is Communication time to send query

t2 is the time required to process query at other mobile device

t3 is the round trip time required to get reply

wt is the variable waiting time due to networking parameters

2. Cost over head of verification process with digital signatures

$$Tu\_verification = decrt + tsimple$$

decrt = time to decrypt with server public key

***Tu_verification* is the time required for user verification**

C) Cost of Verification of POI answers by Querying user

When user gets poi reply list from other user, additional verification goes as follows

$$poi\_verficiation = decrt + hasht$$

decrt is the time for decryption of answer received

hasht is the time for hash of poi_doc for verification

Assuming final POI list of N POI

Tpoi_verfication = $poi\_verficiation$ * N

***Tpoi_verification* is the time required for poi verification**

6.2 Experimental results of cryptographic algorithms in android platforms.

For 20 KB file Sha1 is fastest, Next to that is AES 128 shows more time than digest but less than RSA1024. RSA has got least performance that is 1000msec for small file. Experiments are carried out with android phone for various cryptographic algorithms to know the cost of cryptography. These results are used as reference to analyze the cost of fabrication management impact. This analysis is shown in figure 8.

6.3 Generalization of time required for SHA, AES, & RSA used in digital signature

Many authors [3, 4, 5, and 6] have presented the benchmarking of cryptographic algorithms in various platforms, different operating systems, using different libraries such as open SSL, java, Cryptpp etc. Timing recorded are relative in terms of hardware and libraries.

Practically there is a variation in time required, if we change libraries, hardware platforms etc. For analysis we have generalize the time of algorithms in terms of ref x unit. Let us say x milliseconds is the time standard time slice unit for reference, as shown in table 1.

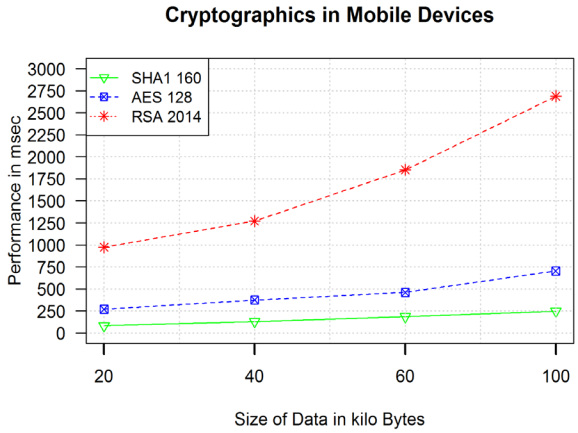

Fig 8: Cryptographic cost in msec in android phone

Table 1: Relative cryptography cost

Sr.	Name of Algorithm	Process	Key bits	Time x units
1.	SHA1	Encryption	-	1x
2.	SHA-256	Encryption	-	1.2x
3.	AES	Encryption	128	4x
4.	AES	Decryption	128	4x
5.	AES	Encryption	256	5.6x
6.	RSA	Encryption	1024	10x
7.	RSA	Decryption	1024	50x
8.	ECC	Encryption	160	5x
9.	ECC	Decryption	160	5x

6.4 Computing cost overhead for various anti-fabrication operations

Chart in figure 9 shows various security operations required to protect from fabrication attacks. Nonrepudiation implementation add maximum cost, while as POI and user verification cause medium overhead issues. However communication security, tamperproof communication and authenticated interactions requires very less overhead.

7. Conclusions:

Various anti fabrication algorithms are devised such as registration of POI and LBS users, Fabrication Verification and Communication integrity check verification. Location privacy with trusted server and non-trusted peer-to-peer algorithms are presented in this paper.

Also, various cryptographic combinations and its impact-overhead for anti-fabrication is presented.
In a peer-to-peer broadcast systems of LBS or peer to peer information based cloaking systems, location information should be private or in the form of predefined format, but participation must be correct without disclosing personal data.

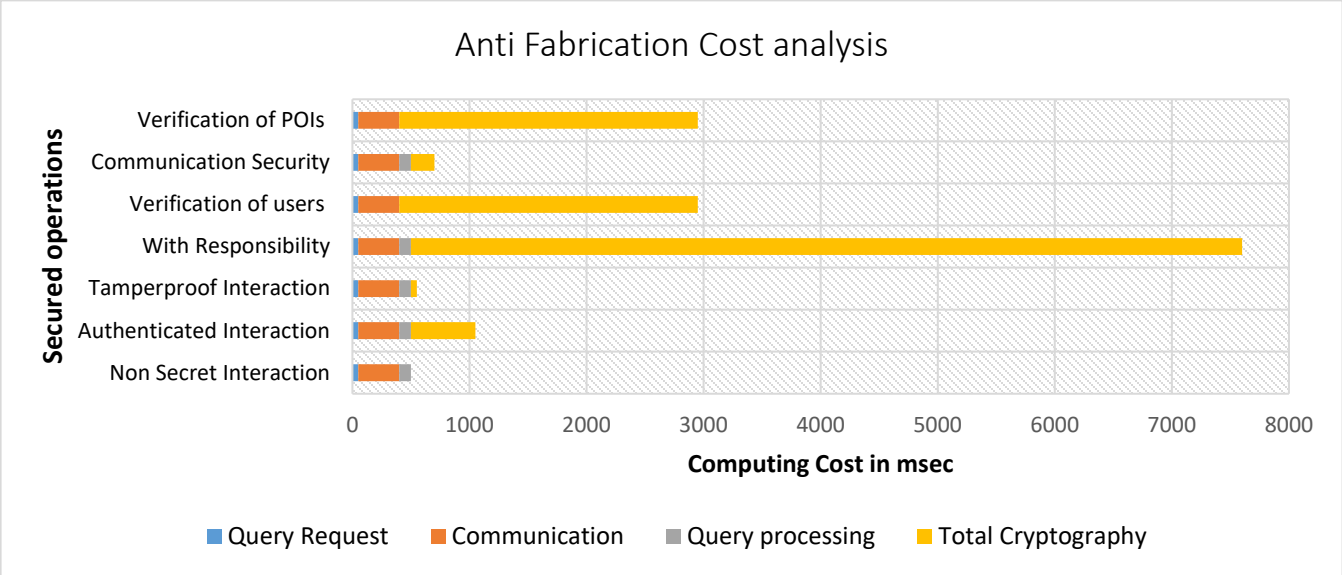

Fig 9: Cost analysis for anti-fabrication operations

Similarly, POI's should not make false claims of its services by fabricating data. We have suggested two mechanisms which mitigates the attacks from fabrications of user data, POI data, Meta data, and payload data. Signature based protection is better coupled with IT law and trust-based mechanisms are also performs well in collaborative privacy protection.

References

1. S. Shafiee, H. Shafiee and F. Mortazavi, "Security of crowd sourcing," 2016 10th International Conference on e-Commerce in Developing Countries: with focus on e-Tourism (ECDC), Isfahan, 2016, pp. 1-6.doi: 10.1109/ECDC.2016.7492978
2. X. Zheng, P. Maille, C. T. P. Le and S. M. Swid, "Trust Mechanisms for Efficiency Improvement in Collaborative Working Environments," 2010 IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, Miami Beach, FL, 2010, pp. 465-467.
3. Nidhi Singhal and JPS Raina, "Comparative analysis of AES and RC4 for better utilization, International journal on computer trends and technology, ISSN 2231, 2011
4. Simar Preet Singh, and Raman Maini, "COMPARISON OF DATA ENCRYPTION ALGORITHMS", International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127
5. Guillermo A. Francia III MCIS & Rahjima R. Francia "An Empirical Study on the Performance of Java/.Net Cryptographic APIs", Information Systems Security, 16:6, 344-354, DOI: 10.1080/10658980701784602
6. B. N. Jagdale, J. W. Bakal, "Issues of Cryptographic Performance in Resource Constrained Devices Experimental Study", International Conference on Intelligent Computing & Communication -2017, ISBN 978-981-10-7245-1, publication by Advances in Intelligent Systems & Computing (AISC), Springer, August 2017. https://doi.org/10.1007/978-981-10-7245-1_44
7. Y. Pu, J. Luo, Y. Wang, C. Hu, Y. Huo and J. Zhang, "Privacy Preserving Scheme for Location Based Services Using Cryptographic Approach," 2018 IEEE Symposium on Privacy-Aware Computing (PAC), 2018, pp. 125-126, doi: 10.1109/PAC.2018.00022.
8. J. Zhou, Z. Cao, Z. Qin, X. Dong and K. Ren, "LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 420-434, 2020, doi: 10.1109/TIFS.2019.2923156.
9. Levent Ertaul, Nitu J. Chavan, "Privacy in Location Based Services (LBS) via Composite Functions: The L4NE Protocol", IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.3, March 2017
10. G. Chen et al., "Certificateless Deniable Authenticated Encryption for Location-Based Privacy Protection," in IEEE Access, vol. 7, pp. 101704-101717, 2019, doi: 10.1109/ACCESS.2019.2931056.
11. C. Shouqi, L. Wanrong, C. Liling, S. Qing and H. Xin, "An Improved Anonymous Authentication Protocol for Location-Based Service," in IEEE Access, vol. 7, pp. 114203-114212, 2019, doi: 10.1109/ACCESS.2019.2930740.
12. P. Asuquo et al., "Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges, and Countermeasures," in IEEE

Internet of Things Journal, vol. 5, no. 6, pp. 4778-4802, Dec. 2018, doi: 10.1109/JIOT.2018.2820039.
13 X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar and N. Kumar, "A Lightweight Privacy-Preserving Authentication Protocol for VANETs," in IEEE Systems Journal, vol. 14, no. 3, pp. 3547-3557, Sept. 2020, doi: 10.1109/JSYST.2020.2991168.
14 L. Yu, X. Su and L. Zhang, "Collaboration-Based Location Privacy Protection Method," 2019 IEEE 2nd International Conference on Electronics Technology (ICET), 2019, pp. 639-643, doi: 10.1109/ELTECH.2019.8839605.
15 L. Zheng, H. Yue, L. Zhang and X. Pan, "A New Location Privacy Protection Algorithm," 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 2017, pp. 364-367, doi: 10.1109/CSE-EUC.2017.253.
16 K. M. Mahesh Kumar and N. R. Sunitha, "Preserving Location Data Integrity in Location Based Servers using Blockchain Technology," 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT), 2017, pp. 1-6, doi: 10.1109/ICECIT.2017.8453286.
17 E. Elmahdi and S. -M. Yoo, "Secure Data Integrity in VANETs based on CS-DC Scheme," 2020 IEEE Latin-American Conference on Communications (LATINCOM), 2020, pp. 1-5, doi: 10.1109/LATINCOM50620.2020.9282267.
18. B. N. Jagdale, J. W. Bakal, "Privacy Aware Monitoring of Mobile Users in Sensor Networks Environment", iJIM International Journal: Interactive Mobile Technologies DOI:10.3991/ijim.v13i02.10023, eISSN: 1865-7923, iJIM Vol. 13, No. 2, Pages 127-140, 2019
19 Turki Kordy, Fazal Noor and Oussama Benrhouma, "Security Analysis of Authentication Protocol for Mobile Devices Using Hyperelliptic Curve Cryptography", IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.10, October 2021

Balaso Jagdale received Diploma in Industrial Electronics from Govt. Polytechnic Latur and BE Computer Engineering degree from Pune University in 1992 . He received ME in Computer Engineering, from VJTI, under Mumbai University in 1999. He has been awarded Ph.D. in the field of Computer Science and Technology from G H Raisoni College of Engineering affiliated to RTM Nagpur University, India. He is presently working as Associate Professor, School of Computer Engineering and Technology at Dr. Vishwanath Karad MIT World Peace University, Pune. He has more than 28 years of academics experience including head of computer department at Sardar Patel College of Engineering, Mumbai. He has publications in journals, conference proceedings, and books. He has research interests in Computer Network Security and Intelligence in Internet of Things. He has also a Certified Ethical Hacker certification from EC Council in his credit. He is also associated with Govt. and University committees as subject expert. He is a Member of IET Pune LN and life member of CSI, IETE, ISTE INDIA.

Shounak Rushikesh Sugave received BE Computer Science & Engineering degree from Dr Babasaheb Ambedekar Marathavada University, Arangabad India in 1992. He received MTech in Network & Internet Engineering from SJCE Mysore under VTU University in 2005. He has been awarded Ph.D. in the field of Software Testing from JNTU Anantapur, Anantapuram, Andra Pradesh, India. He is presently working as an Associate Professor in the School of computer Engineering and Technology at Dr. Vishwanath Karad MIT World Peace University, Pune India. He has more than 13 years of academics and industrial experience. He has publications in referred journals and conference proceedings. His has research interests in the field of software testing and more specifically, test suite minimization in Software Engineering.

Dr. Kishor Kolhe obtained PhD from Shri JJT University, Jhunjhunu (Rajasthan), India in 2013, M. Tech. in Information Technology from the Bharati Vidyapeeth Deemed University, Pune [M.S.] in year 2010 and B.E (Hons) Electronics Engineering from S.G.G.S. Institute of Engineering & Technology, Nanded [M.S.] in year 1996. He is currently working as Associate Professor in School of Computer Engineering and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India. He has more than 14 years teaching and 11 years of industry experience. His areas of interest are Network and Security, Software Engineering, Artificial Intelligence, Internet of Things. He has published more than fifty research papers in reputed journals and conferences. He has also guided more than 56 undergraduate students, Thirteen post graduate students and presently guiding Three Ph.D. research scholar. He is working as CEO (Examination) for the Institute. He has also worked as Head, I.T. Department, System In-charge of Center for Professional Courses and Member of various committees. He has reviewed research papers in national and international conferences and journals. He is a life member of CSI, ISTE and Fellow member of IETE etc