International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 14 (2018) pp. 11540-11547

A TTP-Free Location privacy framework for mobile social networks with key agreement protocol

Ahmed Mahmoud Al-Badawy
Teaching Assistant, Computer Science Department,
Faculty of Computers and information, Helwan University
Cairo, Egypt.

Hala M. Abbas
Assis. Prof., Computer Science Department,
Faculty of Computers and information, Helwan University
Cairo, Egypt.

Mohammed Belal
Prof., Computer Science Department,
Faculty of Computers and information, Helwan University
Cairo, Egypt.

Abstract
Location information protection in Location Sharing Services (LSSs) is one of most *important issues* in Mobile Social Networks (MSNs). LSSs enable users to *exchange* their exact locations. Without a strong mechanism for protecting users' privacy, users' location information will be *leaked* which in turn puts' their life in *danger*. Although, a lot of current solutions tried to protect users' location privacy via Trusted Third Party (TTP) utilization- which usually has *access* to full/part of users' location information, they introduced *false* protection mechanism since TTPs, access to user information, is considered *privacy leakage*. Furthermore, they depend on securing *either* users' identities or users' locations in order to achieve users' privacy. In this paper, we introduce a location privacy framework which has the following features: a) Trusted Third Party Free (TTP-Free). b) Complete privacy, which aims to *protect* both users' identities and locations. c) Strong cryptography mechanism. d) Key agreement protocol in order to avoid *limitations* of pre-shared key mechanisms or direct key exchange.

Keywords: Security, Privacy, Location Privacy, Mobile Social Network, Location Sharing Services, Location Protection, TTP-Free.

INTRODUCTION

Recently, evolution of mobile phones including Global Positioning System (**GPS)** and **wireless technologies** [1] led to *emersion* of mobile social communities. Mobile social communities- also known as **Mobile Social Networks** (**MSNs**) – [2] [3] are *social services* offered via mobile phones in order to facilitate *users' daily life* [4] such as: People Communication, Location Sharing Services among friends [5], restaurants, stores recommendations, sharing pictures, videos, traffic information and location based reminders [6]. So that, MSNs become *staple* in users' daily life.

Mobile Social Networks (**MSNs**) are *architected* according to the following [7]:

a) **Web Based MSNs**: Users Communicate with social network providers through the *internet* using their mobile phones. A lot of applications follow that architecture ex: Google latitude [8] and Facebook [9].
b) **Decentralized MSNs**: Users Communicate to each other via *wireless technology* (Bluetooth or WIFI) using their mobile phones in order to exchange/share their data with no need to use servers ex: EyeVibe [10].

Location Sharing Services (LSSs) in Mobile Social Networks (MSNs) enable users to *continuously* share their locations among their friends. Continuous sharing of users' locations without a strong mechanism for protecting users' location information *may put users' life in danger*. Since location information contains users' *sensitive information* such as user's identity, current location, habits, work and home location [11] which in turn leads to users' privacy leakage.

Existing solutions tried to *fulfill* one of the following location privacy objectives:

a) **Identity Based Protection (IDP) objective** aims to *preserve* user's privacy by protecting their identities. Often, it *requires* TTP(s) in order to either replace user real identity with fake one or replace and store identity mapping [12] [13].
b) **Location Based Protection (LBP) objective** aims to *preserve* user's privacy by protecting their locations. LBP can be *either* TTP [14] [15] or TTP-Free [16].

c) **Complete Privacy Protection (CPP) objective** which aims to protect both users' identities and their locations. CPP can be *either* TTP [17] or TTP-Free [18].

In this paper we introduce *a TTP-Free Complete Privacy framework*. This framework *employs* key agreement protocol in order to create *secure channel* between users which has ability to *Mutual authentication* of users, *key establishment* and *key confirmation* which in turn *overcome limitations* of key exchange, pre-key *establishment* and *resistant* for active attacks.

The rest of this paper is organized as follows: Section 2 gives a brief description of related work. Section 3 introduces an overview of proposed framework. Section 4 discuss security of proposed framework by both threat model and it's analysis. Section 5 discusses experiment and the results followed by conclusion.

RELATED WORK

Location based services with continuous sharing of users' location information in mobile social networks led to **Users' Locations Privacy Leakage** (**ULPL**) Problem. A lot of techniques tried to solve ULPL problem.

K-anonimity [19] is one of techniques tried to solve ULPL problem by making user *unidentifiable* from (K-1) users. Usually, it achieves location based protection objective and relies *completely* on **Trusted Third Party** (**TTP**) [14][15][16][20] which has *full access* to *either* users' locations or identities or both which in turn considered a *privacy leakage*.

MixZones technique [12] tried to solve ULPL problem by *replacing* users' identities with new one and *stop sending* their locations in some zones-called **silent zones**- so that users' location information could not be easily *revealed* which in turn protects user's location privacy. One of Mixzones issues that must be *carefully addressed* is *placement* of mixzones which is *precisely* solved in optimal placement of mixzones [21].Usually, Mixzones technique achieves identity based protection objective that *follows* TTP structure [12] [21] [22] [23] which is responsible for changing users' *pseudonyms* in silent zones in order to *fulfill* users' location privacy.

Location Dummies technique tried to protect users' location privacy by *masquerading* location. **Location masquerading** is accomplished by generating and sending *false* location updates combined with real one [25] in order to solve ULPL problem. Usually location dummies achieves *either* complete privacy protection [26][27] or location based [28] with TTP structure in order to *generate false locations update*.

Obfuscation technique tried to solve ULPL problem by *degrading* location quality which means instead of sending exact users' location, *disguised location* will be sent in order to preserve users' privacy [29]. It can be either TTP which obfuscation is achieved through [14] or TTP-Free which obfuscation area is determined by users [30].

Cryptography Technique tried to fulfill users' location privacy *via encryption / decryption techniques*. Here, users' locations are sent to the servers in an encrypted form which later can be decrypted by his friends. It achieves *either* location based [31] or complete privacy protection [32]. Often, it can be TTP structure which is *commonly* used [33] or TTP-Free [34].

One of frameworks that followed *complete* privacy based cryptography technique is MobiShare [32]. It is a *TTP* framework that *utilizes* **cellular towers** in order to be responsible for *anonymizing* users' location information by replacing real user identity with fake one and applying location *dummy queries* to users' locations then *sending* identity mapping to social server to be *stored* and location updates with dummies to location server.

MobiShare has some limitations, **firstly** usage of cellular tower as TTP impose *TTP limitations and Impracticality*. **Secondly**, location can be easily *leaked* since the encryption decryption algorithm used is *AES-128* which can be *easily* identified [35] [36]. After *detection* of algorithm type, a key *recovery process* is accomplished by using **cipher text only attack** [37] [38] which in turn leads to users' locations leakage. **Thirdly**, weakness of threat model assumptions which stated that two servers cannot be attacked *simultaneously*. Moreover, no obvious mechanism for *key exchange* which is significant issue that must be *addressed*.

As an *extension* to MobiShare, N-MobiShare [33]. N-MobiShare tried to *overcome* MobiShare's limitations. Instead of using cellular towers, which made MobiShare impractical, social server is used. Although, *eliminating* usage of cellular towers solved *impracticality* problems, still *TTP limitations*, encryption/decryption algorithm identification , key recovery process using **cipher text only** attack, *absence* of key exchange mechanism and threat model assumptions *weakness*.

PROPOSED FRAMEWORK:

Proposed framework is a *TTP-Free Complete Privacy* framework based *cryptography* which aims to protect both users' identities and users' locations. As being TTP-Free, it *overcomes* TTP limitations. Identity protection mechanism is accomplished through usage of fake identity generated on users' mobile phones. Moreover, it *employs* key agreement protocol for *securing* channel between users. Employed key agreement protocol has ability to users' *mutual authentication*, *key establishment* and *key confirmation* which overcome *limitation* of key exchange or pre-key establishment and *resistant* for active attacks.

Notations used in proposed framework are summarized in table 1.

The proposed framework consists of *three* entities as in Figure 1:

1. **User**: is denoted by U_i, uses his mobile phone in order to *generate* fake identity, communicate with Social networks to connect with his friends and share his location information among them.

Table 1: Notation Summary

Notation	Description
U_i	User i
S_{OSN}	Social network server
L_S	Location Server
FID_i	User i Fake Identity
RID_i	User i real Identity
SG	Social Graph
SGK_i	Social Group Key for User i
K_{ij}	Key between user U_i and his friend U_j

2. **Online Social network Server**: is *denoted* by S_{OSN} which is responsible for storing user information to be *authenticated*, connecting users with each other and also storing users' encrypted fake identities in user's information table.
3. **Location Server**: is denoted by L_S, is responsible for receiving users' locations from S_{OSN} and *storing* them in order to be retrieved later by users' friends.

A. Proposed Framework consists of five stages:

1. **Registration***:* Is the stage that user U_i tries to *join* mobile social network. U_i firstly sends the required information to S_{OSN} in order to be *authorized* to create his social network profile. Once accepted, user immediately creates his own *Social Group Key* (SGK_i) and safely stores it in his mobile phone in order to be used later in *encrypting and decrypting* his locations.

2. **Authentication***:* Is the stage accomplished on S_{OSN} , responsible for *verifying* user identity via comparison between user's *provided information* and *pre-stored one* - in registration stage- to gain access to his mobile social network profile which in turn minimize NO of *unauthorized access* to social networks which in turn helps in protecting users' privacy.

3. **Friendship and Key Exchange:** Is considered to be one of our framework important stages. In this stage, *exchange* of user SGK is accomplished according to users' social graphs. **User Social Graph** (**SG**) is a *graph* that depicts relations between user and his friends. So to be part of user's social graph, a friendship *request* must be issued in order to be added to his social graph and vice versa.

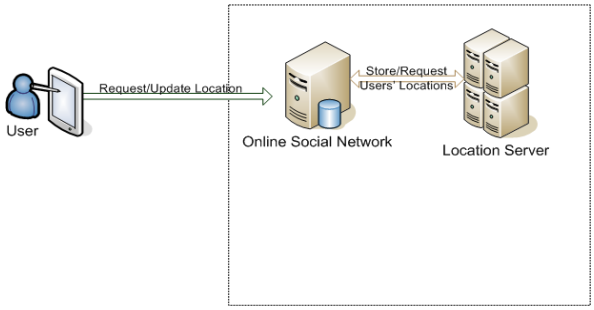


Figure 1: Proposed Framework

After that, immediately friendship requester tries with requested friend to create their own key (K_{ij}) via Key Agreement Protocol [39] in order to *securely* transfer SGK_i. Once SGK_i is transferred, any user's friend can *decrypt* users' locations.

4. **Update Location***:* Is considered to be core stage in this framework. each user updates his location *securely* according to the following:
   - The user U_i *generates* his fake identity on his mobile phone in order to obtain FID_i to be used on location update.
   - The user U_i *encrypts* his location with SGK_i and then sends a *tuple* consists of (FID_i , Encryption of location with SGK , timestamp) to S_{OSN}.
   - S_{OSN} *stores* FID_i and timestamp then *forwards* the whole tuple to L_S to be stored there for later retrieval.
   - U_i then updates his information table with the latest fake identity (FID_i) used *encrypted* with SGK.

5. **Query Location:** Is the stage responsible for retrieving users' locations, the user U_1 can retrieve his friend (U_2) latest location according to the following:
   - The user U_1 *retrieves* friend (U_2) latest FID_2 from U_2's information table and then *decrypt* it using U_2's SGK.
   - U_1 *generates* fake identity FID_1 on his mobile phone.
   - U_1 *communicates* with social network using FID_1 and requests FID_2's location.
   - Social network server *retrieves* FID_2's location from location Server and returned it to FID_1.
   - Using U_2's SGK, U_1 *decrypts* U_2's location.

B. Fake Identity Generation on users' mobile:

According to our model, fake identity (FID) is *generated* by users themselves on their mobile phones. Fake identity generation mechanism *consists* of the following phases:

1. **Fake Identity Generation**: responsible for generating user fake identity according to algorithm 1.
2. **Check Uniqueness**: aims to *validate* uniqueness of generated fake identity. After generation, user will request social server for his table information then compare the generated FID with the saved identities to confirm uniqueness.

C. Key Agreement Protocol [39]:

Establish a *secure* communication channel between communication parties using elliptic curve cryptography - algorithm 2 - which is proved to be secured [39] in order to securely *exchange* SGK_i . This protocol consists of three phases:

- **Mutual Authentication**: responsible for authenticating communication sides which means two sides must be authenticated by each other before key establishment.
- **Key Establishment**: responsible for sharing key between communication parties without exchanging it.
- **Key Confirmation**: responsible for confirming key after establishment between communication parties.

Algorithm 1: Fake Identity Generation by User U_i

1: generate identity with length K as part 1.
2: generate identity with length M as part 2.
3: X<-integration of part 1 and part 2 with salting mechanism.
4: FID<-Hash (X)
5: **EFID**<-Encrypt With SGK
5: List <-Request Social Network Server for U_i table information.
6: For each Fake_identity **in** List
7: **IF** (Fake_identity==EFID) **Then**
8: **GOTO 1**
9: **End IF**
10: Return FID

These phases resulted in secure channel establishment. This protocol is *proved* to be *resistant* for *passive* attacks which mean data cannot be decoded or understood by any intruder. Also *resistant* for *man in the middle* and *active attacks* which means information sent through cannot be *altered* or any communication party cannot be *simulated*.

SECURITY ANALYSIS:

A. Threat Model:

According to proposed framework, social network server, location server and users' mobile phones are *communicated* through the internet. Current users' locations and fake identities are *obtained* via users' mobile phones which can connect directly to social network server but for *more* security cannot connect to location server. *Only* social server can connect directly to location server. Furthermore, the social server and location server are assumed to be dishonest.

Up to our knowledge, attackers which can be server operators aim to *reveal* users' location information which includes users' identities, mapping between users FIDs and real ones, locations and timestamps. Assume that any attacker has *ability* to gain access to social server and location server individually or simultaneously. This assumption is considered the *worst case* since attacker has ability to control *all servers simultaneously*. Our Objective is to *minimize* attacker knowledge in order to protect uses' location privacy.

Attacker knowledge is categorized into:

- Revealing users' fake identities and their relations with real ones.
- Revealing users' Social group key.
- Detecting encryption decryption algorithm type.
- Revealing Users' exact location.

Assume that, key agreement protocol here is *secured* [39] and also assume that security of mobile phones by using *trustworthy mobile platform* [40].

Algorithm 2: Key Agreement Protocol between Ui and Uj

1: U_i selects elliptic curve $\mathbf{E}(Z_P)$ defined over Z_P .
2: U_i Chooses (**P**) random point with large order (**n**) on elliptic curve- n is large prime number-.
3: U_i generates strong numbers p and q where p=2*q+1.
4: U_i transfer (E,Q,P,n) to U_j
5: U_j chooses (b) where $1 \le b \le n-1$ then calculates B=b*P+Q then send B to U_i
6: U_i chooses (a) where $1 \le a \le n-1$ then Computes $A=a*P=(x_A,y_A)$ and calculates $\alpha=a(B-Q)$ and $K=Q+\alpha$.
7: U_i calculates $r=(x_A)$ Mod (n) and calculates $i=a^{-1}(h(\alpha)+x*r) \bmod(n)$ then U_i transfers (A,i) to U_j as his signature.
8: U_j computes $\beta = b*A$. then computes $K=Q+\beta$, $W=i^{-1} \bmod(n)$.
9: U_j Computes $u_1 = (h(\beta)*W) \bmod(n)$, $u_2 = (X_A*W) \bmod(n)$, $u_1*P + u_2*Q=(x_0,y_0)$ then Calculates $v= x_0 \bmod(n)$.
10: U_j check if($v== x_A$) then U_j authenticates U_i and confirmed that U_i has reestablished the same shared key then U_j computes $Y_B=h(\beta)$ then send it to U_i
11: So U_i tries to authenticate U_j by computing $Y_A=h(\alpha)$ then check if ($Y_A == Y_B$) so if matched then the key is confirmed to be the same on both sides.
12: ESGK <-U_i encrypt SGK with new established key.
13: U_i Send ESGK to U_j .
14: U_j Receives ESGK and Decrypt it using new established key.

B. Threat Model Analysis:

Recall that from our threat model, our goal is to *minimize* attacker knowledge in order to protect users' location privacy. According to our framework, attacker knowledge is minimized according to the following:

For user identities privacy: according to our proposed framework, fake identities are *generated* –algorithm 1 - in mobile phones which according to our threat model are secured. After generation and location update, user updates his information table with latest fake identity used in an encrypted form using SGK. So that, users' identities are *protected*.

For Encryption/Decryption Key: our key agreement protocol consists of three stages:

- **Mutual Authentication**: provides an authentication mechanism for each user in order to *authenticate* each other before establish key which in turn protect key establishment from *man in the middle attack* [41] *and identity theft attack* [42].
- **Key Establishment:** tries to create a key *without* exchanging it which latterly used to *exchange* SGK Key. So that, SGK exchange is *secured* since key establishment stage *create* a secure channel used to be a communication channel between communication parties.
- **Key Confirmation:** after key establishment, a key confirmation mechanism is carried out in order to *ensure* that the *same* key is established between two communication parties which in turn protects from *active attacks*.

For Encryption Decryption Mechanism: According to our proposed framework, the encryption decryption mechanism used is *Elliptic curve cryptography* [43] *which is proved to be secured.*

Location Privacy: According to our proposed framework, location cannot be attacked since it is sent and stored in an *encrypted* form using SGK and Elliptic curve cryptography which is protected from *passive* attacks which in turn protect users' location privacy
So the proposed framework aims to *minimize* attacker knowledge in order to protect users' location privacy.

EXPERIMENT AND RESULTS:

Recall from our threat model, our goal is to *minimize* attacker- or server operator- knowledge in order to *preserve* users' location privacy. In order to fulfill this goal, an attack model has been designed according to proposed framework, mobishare and n-mobishare to simulate all possible attacks. This attack model helps in determining attacker knowledge after applying each attack which in turn helps in proving frameworks security. *Simulation* was carried out according to attack model parameters table 2.

Attack model has been designed according the following:

- If the attacker or server operator *gained access* to parameter, it is marked with *one*.
- If the attacker or server operator *failed to control* parameter, it is marked with *zero*.

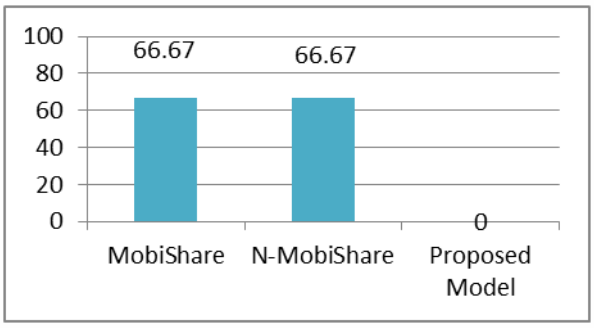
This simulation model generates attacks up to *15 attacks* for attacker and *3 attacks* for server operator using **combinations theory**. This simulation model is applied to proposed framework, mobishare and n-mobishare and results are shown in Fig. 2 for server operators' attacks and Fig. 3 for attackers' attacks.

Table 2: Attack Model

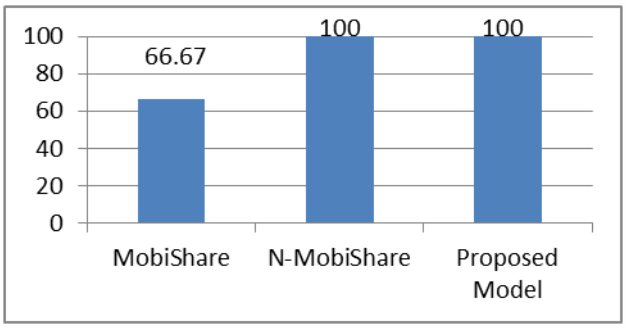
Parameter	Attack Description and Attacker Type		
	Description	Server Operator	Attacker
Control Social Server	Ability of attacker or server operator to gain access to social server.	(0 or 1)	(0 or 1)
Control Location Server	Ability of attacker or server operator to gain access to Location server.	(0 or 1)	(0 or 1)
Connection Between User, Social Server	Ability of attacker to gain access to connection between user and social server (Man in the Middle Attack).	___	(0 or 1)
Connection Between Social Server, Location Server	Ability of attacker to gain access to connection between user and social server(Man in the Middle Attack).	___	(0 or 1)

CONCLUION:

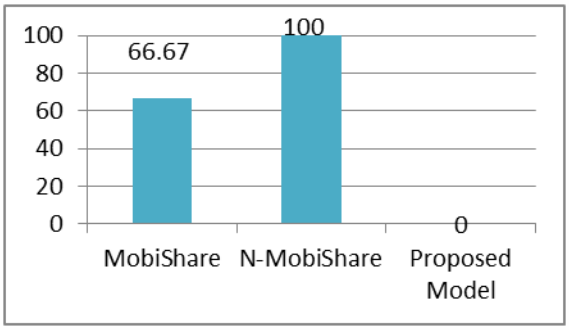
In this paper, a Location privacy protection framework is introduced. Unlike other solutions, proposed framework does not require trusted third party in order to provide users' location privacy. It also introduced fake identity mechanism which is carried on mobile phones in order to add extra level of security. Moreover, it solved key exchange problems and defending a lot of known attacks by employing a strong key agreement protocol which allows users to establish key between them without need for exchanging it. In brief, proposed framework tried to minimize attacker knowledge in order to preserve users' location privacy.



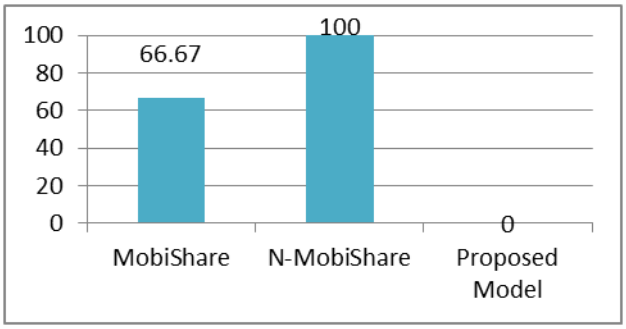
(a) Identity Knowledge after Attack



(b) Encryption Decryption Type Knowledge after Attack

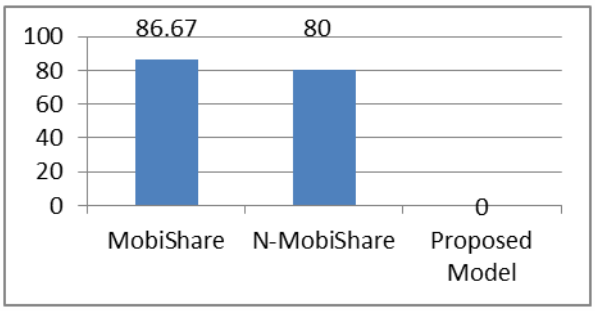


(c) Key Knowledge after Attack

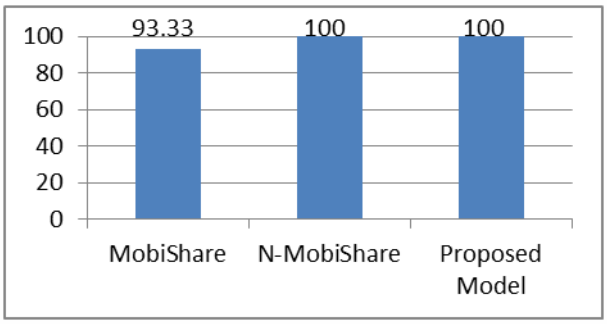


(d) Location Knowledge after Attack

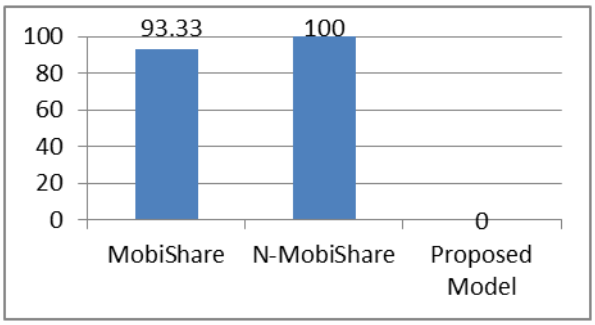
Fig.2. Server operator Knowledge After running attack machine



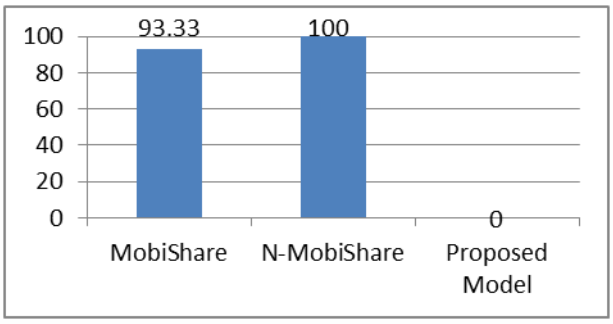
(a) Identity Knowledge after Attack



(b) Encryption Decryption Type Knowledge after Attack



(c) Key Knowledge after Attack



(d) Location Knowledge after Attack

Fig.3. Server operator Knowledge After running attack machine

REFRENCES

[1] P. A. Zandbergen, "Accuracy of iphone locations: A comparison of assisted gps, wifi and cellular positioning," Transactions in GIS, vol. 13,no. s1, pp. 5–25, 2009

[2] L Humphreys ,"Mobile Social Networks and Social Practice:A Case Study of Dodgeball" - Journal of Computer Mediated Communication, 2007 - Wiley Online Library

[3] Yao-Jen Chang , Hung-Huan Liu , Li-Der Chou, Yen-Wen Chen, Haw-Yun Shin "A General Architecture of Mobile Social Network Service" 2007

[4] A. Beach, M. Gartrell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan, B. Surendar,M. Terada, and R. Han. WhozThat? Evolving an Ecosystem for Context-Aware Mobile Social Networks. IEEE Network, 22(4):50–55, July-Aug. 2008.

[5] E. Miluzzo , "Sensing meets Mobile Social Networks: The Design, Implementation, and Evaluation of the CenceMe Application" , Proc. 6th ACM SenSys , pp.337 -350 , 2008

[6] SOHN, T., ET AL. Place-its: "A study of location-based reminders on mobile phones". In Proc. of Ubicomp (2005).

[7] N. Kayastha, D. Niyato, P. Wang, and E. Hossain. Applications, architectures, and protocol design issues for mobile social networks: A survey. Proceedings of the IEEE, 99(12):2130--2158, 2011.

[8] "Google Latitude. [Online]. Available: http://www.google.com/latitude"

[9] "Facebook Applications. [Online]. Available for Iphone on : https://itunes.apple.com/en/app/facebook/id284882215?mt=8

[10] Information about EyeVibe: http://www.o2.co.uk/termsandconditions/archive/other-products-and-services/eye-vibe-terms-and-conditions [accessed online 20/12/2015]

[11] Golle and K. Partridge. On the anonymity of home/work location pairs. InPervasive '09: Proceedings of the 7th International Conference on Pervasive Computing, pages 390–397,Berlin, Heidelberg, 2009. Springer-Verlag.

[12] Beresford, Alastair R., and Frank Stajano. "Location privacy in pervasive computing." IEEE Pervasive computing 2.1 (2003): 46-55.

[13] Beresford, Alastair R., and Frank Stajano. "Mix zones: User privacy in location-aware services." Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on. IEEE, 2004.

[14] Gruteser, Marco, and Dirk Grunwald. "Anonymous usage of location-based services through spatial and temporal cloaking." Proceedings of the 1st international conference on Mobile systems, applications and services. ACM, 2003.

[15] Gedik, Bugra, and Ling Liu. "A customizable k-anonymity model for protecting location privacy." (2004).

[16] Takabi, Hassan, James BD Joshi, and Hassan A. Karimi. "A collaborative k-anonymity approach for location privacy in location-based services." Collaborative Computing: Networking, Applications and Worksharing, 2009. CollaborateCom 2009. 5th International Conference on. IEEE, 2009

[17] Gedik, Bugra, and Ling Liu. "Protecting location privacy with personalized k-anonymity: Architecture and algorithms." IEEE Transactions on Mobile Computing 7.1 (2008): 1-18.

[18] Schlegel, Roman, et al. "Privacy-preserving location sharing services for social networks." IEEE Transactions on Services Computing 10.5 (2017): 811-825.

[19] Sweeney, Latanya. "k-anonymity: A model for protecting privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.05 (2002): 557-570.

[20] Mokbel, Mohamed F., Chi-Yin Chow, and Walid G. Aref. "The new Casper: query processing for location services without compromising privacy." *Proceedings of the 32nd international conference on Very large data bases*. VLDB Endowment, 2006.

[21] Freudiger, Julien, Reza Shokri, and Jean-Pierre Hubaux. "On the optimal placement of mix zones." *International Symposium on Privacy Enhancing Technologies Symposium*. Springer Berlin Heidelberg, 2009.

[22] Beresford, Alastair R., and Frank Stajano. "Mix Zones: User Privacy in Location-aware Services." *PerCom Workshops*. 2004.

[23] Palanisamy, Balaji, et al. "Location privacy with road network mix-zones." *Mobile Ad-hoc and Sensor Networks (MSN), 2012 Eighth International Conference on*. IEEE, 2012.

[24] Kido, Hidetoshi, Yutaka Yanagisawa, and Tetsuji Satoh. "An anonymous communication technique using dummies for location-based services." *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on*. IEEE, 2005.

[25] Kido, Hidetoshi, Yutaka Yanagisawa, and Tetsuji Satoh. "An anonymous communication technique using dummies for location-based services." *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on*. IEEE, 2005.

[26] Shen, Nan, et al. "B-mobishare: Privacy-preserving location sharing mechanism in mobile online social networks." *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2014 Ninth International Conference on*. IEEE, 2014.

[27] Li, Jingwei, et al. "{MobiShare}+: Security Improved System for Location Sharing in Mobile Online Social Networks." *J. Internet Serv. Inf. Secur.* 4.1 (2014): 25-36.

[28] Kido, Hidetoshi, Yutaka Yanagisawa, and Tetsuji Satoh. "Protection of location privacy using dummies for location-based services." *Data Engineering Workshops, 2005. 21st International Conference on*. IEEE, 2005.

[29] Duckham, Matt, and Lars Kulik. "A formal model of obfuscation and negotiation for location privacy." *International conference on pervasive computing*. Springer, Berlin, Heidelberg, 2005.

[30] Ardagna, Claudio Agostino, et al. "Location privacy protection through obfuscation-based techniques." *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, Berlin, Heidelberg, 2007

[31] Mascetti, Sergio, et al. "Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies." *The VLDB Journal—The International Journal on Very Large Data Bases* 20.4 (2011): 541-566.

[32] Wei, Wei, Fengyuan Xu, and Qun Li. "Mobishare: Flexible privacy-preserving location sharing in mobile online social networks." *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012.

[33] Liu, Zheli, et al. "New privacy-preserving location sharing system for mobile online social networks." *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on*. IEEE, 2013.

[34] Schlegel, Roman, et al. "Privacy-preserving location sharing services for social networks." *IEEE Transactions on Services Computing* 10.5 (2017): 811-825.

[35] Tan, Cheng, and Qingbing Ji. "An approach to identifying cryptographic algorithm from ciphertext." *Communication Software and Networks (ICCSN), 2016 8th IEEE International Conference on*. IEEE, 2016.

[36] Manjula, R., and R. Anitha. "Identification of Encryption Algorithm Using Decision Tree." *Advanced Computing* (2011): 237-246.

[37] Bahrak, Behnam, and Mohammad Reza Aref. "Impossible differential attack on seven-round AES-128." *IET Information Security* 2.2 (2008): 28-32.

[38] Fuhr, Thomas, et al. "Fault attacks on AES with faulty ciphertexts only." *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*. IEEE, 2013.

[39] Abi-Char, Pierre E., Abdallah Mhamed, and Bachar El-Hassan. "A secure authenticated key agreement protocol based on elliptic curve cryptography." *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on*. IEEE, 2007.

[40] Gilbert, Peter, et al. "Toward trustworthy mobile sensing." *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*. ACM, 2010.

[41] Bhushan, Bharat, G. Sahoo, and Amit Kumar Rai. "*Man-in-the-middle attack in wireless and computer networking—A review*." Advances in Computing, Communication & Automation (ICACCA)(Fall), 2017 3rd International Conference on. IEEE, 2017.

[42] Lorimer, Philip AK, Victor Ming-Fai Diec, and Burak Kantarci. "*Participatory detection of identity theft on mobile social platforms*." in IEEE Global Information and Signal Processing Conference (GlobalSIP). 2017.

[43] Jana, Bappaditya, and Jayanta Poray. *"A performance analysis on elliptic curve cryptography in network security." Computer, Electrical & Communication Engineering (ICCECE), 2016 International Conference on. IEEE, 2016.*