Preserving Privacy in Mobile Social Networks by Personalization of Fine Grained Spam Filtering Scheme

Savita Baban Ghatte [1], Prof. Pravin B. Ghewari[2], Prof. Prathmesh Powar[3]
[1,2,3]*Ashokrao Mane Group of Institutions, Vathar*

Abstract — A mobile communication network (MSN) emerges as a promising social network paradigm that enables mobile users to share information closely and facilitate their cyber-physical-social interaction. As ads, rumors, and spam spread across MSN, it is necessary to filter out spam before they reach the recipients to make MSN work properly. In this regard, we propose a well-designed filtering system (PIF) with confidentiality on MSNs. Exactly; begin to develop a community-based filter distribution scheme, in which filters create filters for their social networks (i.e., filter holders). These filters retain filters and decide to block spam or transfer the desired packets through keyword filters with rough and refined characters. At the same time, advanced cryptographic filter schemes protect the privacy of the creator (i.e., keyword) embedded in the filters so that they can be disclosed directly to other users. In addition, we develop the Merkle Hash tree to store filters as leaf nodes where filters creators can check that distributed filters need to be updated by finding the root node value. It is shown that PIF can protect users' passwords that have been filtered from being disclosed to others and detected forged filters.

Keywords: Fine-grained, mobile communication network (MSN), personalized, privacy protection, spam filter

I. INTRODUCTION

A social networking site is a social networking site where people with similar interests meet and interact with their mobile phone and / or tablet. The mobile communication network (MSN) represents a promising cyber-physical system, which connects mobile nodes within a virtual environment using smart phones and wireless communication. To create an opportunity network users use a mobile network to connect to each other via Bluetooth, Wi-Fi and device-to-device communication. In MSNs users can interact anytime and anywhere without accessing the internet and charging wireless data.

Different types of information, such as newsletters, personal posts, rumors, and ads can be accessed by MSN users. In MSN users can quickly exchange useful information but may find part of the useless information i.e. spam. Therefore to make the connection meaningful to MSN, there is a need to filter out spam early and transfer the required information to users.

Most existing spam filtering programs are run by a central server or trusted authorities and require historical information to detect spam. But MSNs do not have Android SDKs and trusted servers and have no history information so when spam senders switch to MSNs; they are more likely to be detected. In the proposed system, distributed filter schemes are used when users of the mobile communication network i.e., the creators of filters create their own personal filters by embedding keywords. The filter creator sends his filters to his social media i.e., filter filters. Filter managers use these filters when they meet a sender who wants to send a package to filter the creator to check if the package is wanted by the filter creator, and to block spam at the start of package delivery.

II. BOOK REVIEW

1. In the app to match the profile of mobile social networks, users need to show their interests to each other in order to find common interests. By knowing personal information, a malicious user may harm the user. Therefore, similar interests need to be explored in a way that maintains privacy. Fizza Abbas, Ubaidullah Rajput, Heekuck OH [1] proposed an effective privacy and interest-sharing service called Interests of Interests and Consistent Privacy (PRISM). The authors have introduced effective privacy

protection and an interest-sharing protocol on mobile social networks. Give them the conditions for a novel attack and their effective solution. PRISM does not require the user to express an interest in a trusted third party and only use it as a proven identity and dispute resolution solution. Proposed use of a different user ID helps prevent Sybil attacks. With the help of implementation, the authors demonstrated the possibility of PRISM. Moreover, with complete security and sophisticated analysis, the authors demonstrate the resilience of PRISM in various attacks and its effectiveness.

2. Haojin Zhu et al. [2] point to a new security threat arising from existing secure acquisition agreements, identified as an illegal attack, which could lead to a serious problem of injustice. To counter this new threat, the authors introduced a blinding conversion process, which could hide the correlation between the original vector and the modified effects. Based on this, the authors proposed a privacy and impartial interest-based and profile-matching profile, which allows one organization to match its interests with another's profile, without expressing its genuine interest and profile and vice versa. The authors have developed a new protocol that will ensure the integrity and confidentiality of popular privacy issues and the process of profile matching on mobile social networks.

3. Lu et al. [4] proposed a keyword-based filtering program (PReFilter). PreFilter allows transfers to have certain filters generated by others. It can detect and block spam before it is transmitted to recipients. Filters with sensitive keywords are encrypted to prevent user privacy leaks. Delay networks (DTNs), using a list of keywords spam packets are matched and available. Filters with sensitive keywords are encrypted to prevent user privacy leaks.

4. Anti-spam, malware and theft of URLs, Thomas et al. [5] developed a real-time system that includes URL compilation, feature collection, feature extraction, and editing. The proposed system visits all URLs and collects its features stored by the central server for removal from the training phase and real-time deck.

5. Lahmadi et al. [6] utilize social network to collaboratively filter the short message services-based spam via the Bloom filters and content hashing filters. Social network, i.e., the social graph formed by users in the network is the methodology used to detect and filter spams. To build the social network among users this collaborative filtering scheme relies on centralized server.

6. Stringhini et al. [8] developed a new approach to detect spams by looking at the way how e-mails are sent instead of content and origin of emails. It can detect the IP address from which the message is sent, and the geographical distance between the sender and the receiver. They investigate the SMTP communication between the e-mail sender and receiving mail server. The introduced concept of SMTP dialects captures small variations in the ways to carry out the SMTP protocol, so that they can distinguish the between normal e-mail senders and spam bots.

III. THE NEED FOR CURRENT WORK

MSN does not have a centralized and reliable servers and a lack of historical information, so when spammers switch to MSNs, they are more likely to be detected. The proposed system uses a distributed filter system where MSN users create their own spam filters, redirect them to others and allow the filters to filter out as soon as possible.

In order to minimize the filtering of the filter and to maintain the filtering accuracy of the proposed system it uses a community-based filter distribution system that allows the filter creator to send filters to his / her potential social media contacts. The creators of the filter make the distributed filters personal and updated periodically. The proposed system protects user passwords from directly identifying curious intruders and detects inaccurate filters. To counter the onslaught of curiosity, the proposed system encrypts the creator filter.

IV OBJECTIVES

The objectives of the proposed project are as follows,

1. Develop a community-based filtering system.
2. Develop a cryptographic filter system to protect the confidential information of the creator.
3. Using the Merkle tree hash to secure the filter.
4. Develop a personal filtering system for privacy protection.

V PROBLEM STATEMENT

Improving a personalized refined spam filter system for mobile users to streamline filters and prevent spam in a way that keeps the privacy of mobile users safe and secure from explicit disclosure.

VI SYSTEM DESIGN

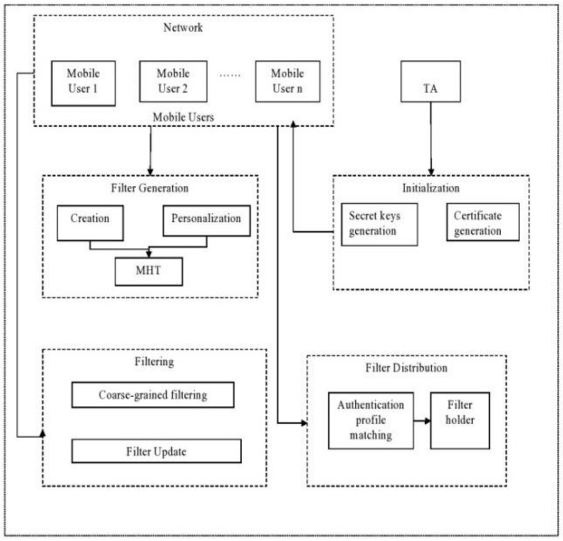

Figure 1: Privacy Policy for Mobile Social Networks

The proposed system provides the following policy management modules:

Getting Started:
In this module, the trust authority (TA) sets up a mobile communication network. TA generates private keys for authorized users and issues certificates to authorized users when they register.

Filter generation:
In this module, users create their own filter by embedding keywords. Users customize their filters to your liking. The filter creator will define his or her interests in a specific keyword, and will allow filter filters to fine-tune the packaging. To verify each filter of the proposed system use the Merkle Hash tree.

Distribution Filter:
In this module, the filter creator distributes their filter to filter filters. When user ui meets another user uj, they first verify authenticity and secretly compare their profiles, determining the number of their normal communities. The proposed system will use a profile matching system that maintains privacy.

Filtering:
In this module, when the filter encounters a sender who wants to send a package to filter the creator, the filter operator uses a filter to check whether the package is required by the filter creator, and to prevent spam. The proposed system will use a filter keyword based on rough keywords that can block part of the package when matching keywords.

VII. PERFORMANCE

The plan is divided into two parts firstly by the Trusted Authority (TA) and the second is for implementation. The following describes the work performed by the Trustees and User.

Getting Started:
Trust authority (TA) connects the system and assigns private keys to individual users. MSN includes N users defined by U = {u1, 2… uN}. Each authorized user first registers on the TA in order to create a user profile and receive important information including private keys.

Filter generation:
User i.e. filter creator creates a filter by embedding keywords. The filter creator selects his keywords Wi, 1… Wi, k, where 1 <= k <= K, and creates a list of Wi keywords. K is the keyword space for every MSN. All keywords are defined by the trust authority.

Distribution Filter:
When user ui meets another user uj, they begin to verify authenticity and privately compare their profiles to determine the number of their normal communities. The privacy profile profile system is used to enable users to read their general communities. If the number of their normal communities is greater than the TH limit, ui can send its Fi filter to uj as a filter holder.

Filtering
Package sender wants to deliver a package that includes keywords (Ws, 1… Ws, x) to ui. When we meet uj, uj helps ui to find out if a package from us can be delivered or not.

Filter Update: The proposed system uses the Merkle Hash (MHT) tree to update the filter. The root of the Merkle Hash tree changes when there is a leaf node varies. There is no need to check the entire leaf node i.e. the keyword of the distributed filter. Ui filter creator checks root root Rui in its filter filter j of FRui filter filter. If the root is the number of existing roots, ui sends the updated filter FR'ui to uj.

VIII. IMPLEMENTATION

Server:
On the server side, the proposed system sets up Mobile Social Network and Trusted Authority.
Trusted authorities trust users, and they activate the entire system during the first phase.
Every user of a mobile network begins to register with a trusted authority.
The trusted administrator maintains a registered mobile user details on the website and generates private keys and a certificate issued to the authorized user.
A trusted authority system is implemented in Java using NetBeans IDE 8.0.2.

Client:
The mobile communication network user is using a mobile app built using android setting and eclipse.

Server:
On the server side, the trusted administrator maintains the website. Trusted authorities keep the entire profile of registered users on the site and the list of keywords of their choice and preferences.
MySQL data is used on the server side. MySQL is an open source SQL database management system.

IX. CONCLUSION

In the proposed project four modules were identified and successfully implemented. Existing spam filtering methods have been researched using an intermediate server or trusted spam management and a new system is proposed, which uses distributed filters to block spam and maintain privacy on the mobile communication network with g fine g.

REFERENCE

[1] Fizza Abbas, Ubaidullah Rajput, Heekuck OH, “PRISM: PRivacy-Aware Interest Sharing and Matching in Mobile Social Networks,” IEEE J., 2016, pp.

[2] Haojin zhu, Suguo du, Muyuan li,and zhaoyu gao, “Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks,” in Proc. IEEE Trans. Comput. Commun, 2013, pp. 192 - 200**.**

[3] H. Shen and Z. Li, “Leveraging social networks for effective spam filtering,” IEEE Trans. Comput., vol. 63, no. 11, pp. 2743–2759, Nov.20142594 - 2603

[4] R. Lu et al., “PReFilter: An efficient privacy-preserving relay filtering scheme for delay tolerant networks,” in Proc. IEEE Conf. Comput.Commun. (INFOCOM’12), 2012, pp. 1395–1403.

[5] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, “Design and evaluation of a real-time URL spam filtering service,” in Proc. IEEE Symp.Secur. Privacy, 2011, pp. 447–462

[6] A. Lahmadi, L. Delosières, and O. Festor, “Hinky: Defending against text-based message spam on smartphones,” in Proc. IEEE Int. Conf.Commun. (ICC’11), 2011, pp. 1–5.

[7] Z. Li and H. Shen, “SOAP: A social network aided personalized and effective spam filter to clean your e-mail box,” in Proc. IEEE Conf.Comput. Commun. (INFOCOM’11), 2011, pp. 1835–1843.

[8] F. Soldo, A. Le, and A. Markopoulou, “Blacklisting recommendation system:Using spatio-temporal patterns to predict future attacks,” IEEE J.Sel. Areas Commun., vol. 29, no. 7, pp. 1423–1437, Aug. 2011.

[9] K. Zhang, X. Liang, R. Lu, K. Yang, and X. Shen, “Exploiting mobile social behaviors for sybil detection,” in Proc. IEEE Conf. Comput.Commun. (INFOCOM’15), 2015, pp. 271–279.