STUDY OF PRESERVING PRIVACY IN MOBILE SOCIAL NETWORK BY PERSONALIZATION OF FINE GRAINED SPAM FILTERING SCHEME

S. B. GHATTE
PG Student, Ashokrao Mane group of institutions, Vathar

A. B. RAJMANE
Associate Professor, Ashokrao Mane group of institutions, Vathar

ABSTRACT:

Mobile social-networking is a social networking where people with similar interests connect to their social communities with a mobile device. Mobile users share various types of information, such as newsletters, advertisements, experiences, interests, opinions and personal content through their mobile devices. Because of Mobile social network (MSN) it is possible for mobile users' to share information in the near area and makes their cyber–physical–social interaction easier. It is very important to filter spams before they arrive at the recipients because as the advertisements, rumors, and spams spread in MSNs. The paper presents spam filtering scheme with privacy preservation in MSNs. The mobile users i.e. filter creators will build their personalized filters by embedding keywords. The filter creator sends his filter to his social friends i.e., filter holders. When filter holders meet a sender who is interested to send a packet to the filter creator, filter holders use these filters to check if the packet is desired by the filter creator, if not then such messages will block by filter holder.

KEYWORDS: Fine-grained, mobile social network (MSN), Personalized, privacy preservation, spam filter.

1. INTRODUCTION:

In Mobile social networks users exchange there useful information but they may receive portion of useless information i.e. spams. So to make the communication meaningful in MSN, there is need to filter spams as possible in early stage and transmit desired information to users.

Most of the existing spam filtering schemes are performed by centralized server or trusted authority, and to detect spams historical information is required. But as in MSNs there is no any centralized servers or trusted authority and lacks historical information. So when spammers are shifting to MSNs, they have more chances of going undetected.

The proposed system uses distributed filtering schemes where MSN users i.e., filter creators create their personalized filters by embedding keywords. The filter creator sends his filters to his social friends i.e., filter holders. Filter holders use these filters when they meet a sender who is interested to send a packet to filter creator to check if this packet is desired by filter creator, and block spams in early stage of packet delivery.

In proposed system, the mobile social network users i.e., filter creators will build their personalized filters by embedding keywords. Then the filter creator sends his filter to his social friends i.e., filter holders. When filter holder meet a sender who is interested to send a packet to the filter creator, filter holders use these filters to check if the packet is desired by the filter creator, and block spams.

Malicious users may participate in MSNs and launch attacks in the phases of packet delivery and spam filtering. Proposed system defines two types of attacks. One is inside curious attack (ICA) and second outside forgery attacks (OFA). ICA violates and disclose other user's personal information. OFA forge other user's filters. To resist ICA, proposed system encrypts the creator's filters and detects the forged filter from OFA with Merkle Hash tree.

2. RELATED WORK:

In a profile matchmaking approach of MSN, to find the commonality, users required to show their interests other users. By knowing personal information of user, a spiteful user may harm a user. A privacy preserving is used to find mutual interests.

Fizza Abbas, Ubaidullah Rajput, Heekuck OH [2] proposed an efficient privacy protection and interests sharing protocol called as PRivacy-aware Interest Sharing and Matching (PRISM). Authors presented an efficient privacy protection and interest sharing protocol in mobile social networks. They have provided novel attacks scenarios and their efficient solution. PRISM does not require a user to disclose interests to a trusted third party and only uses it as an identity verifier and conflict resolver which helps user to prevent Sybil attacks. With the help of implementation, authors have shown the viability of PRISM and the robustness of PRISM against various attacks.

Haojin Zhu et al. [3] identified a new security threat which emerging from existing secure friend discovery protocols, termedas runaway attack, which introduces animportant unfairness subject. To prevent this new threat, authors introduced a novel blind vector transformation technique, which hide the association between the original vector and transformed results. Based on this, authors proposed privacy-preserving and fairness-aware interest and profile matching protocol, where one party matches its interest with the profile of another, without disclosing its real interest and profile. Authors developed a novel protocol that guarantees the fairness and the privacy of privacy-preserving interest and profile matching process in mobile social networks.

Lu et al. [4] proposed a decentralized keyword –based filtering scheme (PReFilter).The Pre Filter allows others to generate some filters. Before transmitting filters to the receivers, it detect and block spams. To protect user's privacy leakage the filters with delicate keywords are encrypted. To match and detect spam packets via keyword list in delay tolerant networks (DTNs).To protect user's deliberate disclosure of confidential information, the filters with delicate keywords are encrypted.

To restrict or avoid spam, phishing and malware through URLs, Thomas et al. [5] developed a real-time system which consists URL aggregation, collection of feature, feature extraction, and classification. The proposed system visits every URL and collects its features that are stored in centralized server for taking out in the training phase and real-time decision making.

Lahmadi et al. [6] utilized social network to collaboratively filter the short message services-based spam via the Bloom filters and content hashing filters. To detect and filter spams the social graph is used which is established by user in network. This collaborative filtering scheme based on centralized server to build the social network among users.

Based on how emails are sent, Stringhini et al. [9] developed a new way for detecting spams. It can detect the IP address from which the message is sent, and the geographical distance between the sender and the receiver. They investigated 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 implement SMTP protocol, so that it is distinguished between normal e-mail senders and spam bots.

3. PROPOSED WORK:

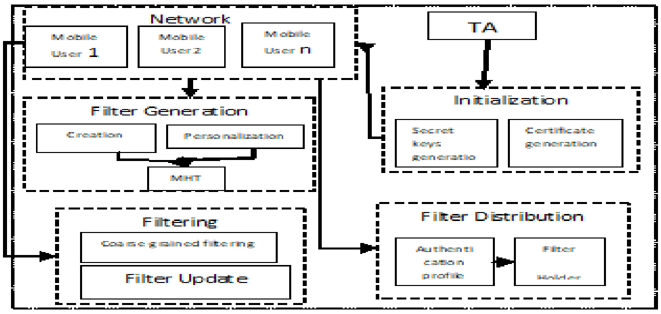

Figure 1 Architecture of Preserving privacy in MSN.

Figure 1 shows the proposed architecture of preserving privacy in mobile social network with fine grained spam filtering schemes.

In proposed system, the system will bootstrapped by the trusted authority (TA) and assigns secret keys to individual users. TA also issues certificates to authorized users when they register.

MSN include N users denoted by U= {u_1, $u_{2…}u_N$}.Each authorized user will first register to TA to build user's profile and obtain key materials which include unique identity, certificate, and secret keys.

The user i.e., filter creator creates filter by embedding keywords. The filter creator u_i selects his keywords $W_{i, 1,}$ … , $W_{i, k}$, where 1<=k<=K , and establishes a keyword list W_i. K is the keyword space of the whole MSN. Every keyword is defined by trust authority.

The filter creator distributes their filter to filter holders. If user u_i meets another user u_j, they first authenticate each other and privately comparing their profiles, determine the number of their common communities. The proposed system uses privacy preserving profile matching scheme.

The proposed system will filter the packets. If packet sender $u_s$is interested to send a packet including keywords ($W_{s, 1, ………}$,Ws, $_x$) to user u_i. When sender u_s meets user u_j, u_j helps u_i to determine if the packet from u_s can be delivered or not.

For filter update, the proposed system uses Merkle Hash tree (MHT). The root of Merkle Hash tree changes if any leaf node varies. So it does not require to check every leaf node i.e. keyword of the distributed filter. The filter creator u_i checks the root value $R_{ui}$from his filter holder u_j for filter tree FR_{ui}. If the root is an existing root value, u_i sends the updated filter tree $FR'_{ui}$to u_j.

The proposed system will use coarse-grained keyword-based filtering scheme which can block a portion of packets when matching keywords. It will also use fine-grained filtering where users personalize their filters on their own preferences. The filter creator defines his interests for specific keyword, and will allow the filter holders to fine grained filter the packets.

The proposed system provides following dynamic policy management modules:

INITIALIZATION:

In initialization module, trust authority (TA) setup mobile social network .TA generates secret keys for authorized users and issues certificates to authorized users when they register.

FILTER GENERATION:

In filter generation module, the users create their filter by embedding keywords. Users personalize their filters on their own preferences. The filter creator will define his interests for specific keyword, and will allow the filter holders to fine grained filter the packets. To authenticate each filter the proposed system use Merkle Hash tree.

FILTER DISTRIBUTION:

In filter distribution module, the filter creator distributes their filter to filter holders. If user u_i meets another user u_j, they first authenticate each other and privately comparing their profiles, determine the number of their common communities. The proposed system will use privacy preserving profile matching scheme.

FILTERING:

In this module, if filter holder meets the sender who is interested to send the packet to filter creator, filter holder use the filter to check if this packet is desired by the filter creator, and block spams.

The proposed system will use coarse-grained keyword-based filtering scheme which can block a portion of packets when matching keywords.

4. SCOPE OF THE WORK:

As there is no any centralized server or trusted authority in mobile social network so there is a lack of historical information. So when spammers shift to MSNs, they have more chances of going undetected. The proposed system uses distributed filtering scheme where users in mobile social network to personalize their spam filters, send them to others and allow filter holders to filter spams as early as possible.

To reduce the filter distribution overhead and maintain filtering accuracy the proposed system uses social-assisted filter distribution scheme which enable filter creator to send filters to his social friends who have high probability to meet him. The distributed filters should be personalized by filter creators and updated timely. The proposed system protects user's private keywords from directly disclosing to inside curious attackers and detects forged filters. To resist inside curious attack, the proposed system encrypts the creator's filter.

5. CONCLUSION:

In this paper, the existing spam filtering techniques have studied which uses centralized server or trusted authority to resist spam and new system is proposed, that uses distributed filtering to block spam and preserve privacy in mobile social network with fine grained spam filtering scheme.

REFERENCES:

1) Kaun Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen,"*PIF:A Personalized Fine-Grained Spam Filtering Scheme with Privacy Preservation in Mobile* Social *Networks*," IEEE transactions on computational social systems, vol.2, No.3, September 2015.
2) Fizza Abbas, Ubaidullah Rajput, Heekuck OH, *"PRISM: Privacy-Aware Interest Sharing and Matching in Mobile Social Networks,"* IEEE J., 2016, pp..
3) Haojinzhu, Suguo du, Muyuanli, and zhaoyugao, *"Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks*," in Proc. IEEE Trans. Comput. Commun, 2013, pp.192 - 200.
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) 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
8) 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.
9) F. Soldo, A. Le, and A. Markopoulou, "*Blacklisting recommendation system: Using patio-temporal patterns to predict future attacks,"* IEEE J.Sel. Areas Commun, vol. 29, no. 7, pp. 1423–1437, Aug. 2011.
10) 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.