A Comprehensive Review: Trust and Location Based Security in Mobile Social Networks

[1]A.Srinivasan, [2]Dr Shaik Naseera

[1]Research Scholar, [2]Associate Professor, [1,2]School of Computer Science and Engineering, VIT University, Vellore, India.

[1]*sreenivasan.phd@gmail.com*

Abstract: - Mobile social network (MSN) has increased momentous improvement with the fast advancement of cell phones, the gigantic reception of mobile phones and the enormous development in social networks. Such network can give an assortment of systems to clients to impart information to different clients. Additionally, it can look for clients with comparative interests and to set up and keep up correspondence between them. However most MSN applications see portable terminals similarly as passage focuses to existing social networks, in which concentrated servers and persistent Internet availability are essentials for versatile clients to misuse MSN administrations, despite the fact that they are inside closeness range, and can straightforwardly trade information through different remote advances. In this paper we have displayed an entire survey on different security issues on mobile social networks and the current arrangements in light of the two viewpoints, namely, trust and area. To acquire exact answers for every one of the issues an expansive number of structure, have been utilized, however it is exceptionally testing to discover the ideal and effective one which can be utilized comprehensively.

Keywords —Location Identification, Mobile Social Network, Network Attacks, Privacy, Security, Trust Evaluation

I. INTRODUCTION

The data communication technology has profoundly enhanced the lives of current society through mobiles, for example, publicizing, advancement, marking, data seek, building client relations and numerous more [1]. Communication in Social network is a perfect situation for building brand groups [2].The rapid increment of social networks and boundless utilization of the web in associations have make ready in number of unauthorized activities [3]. Mobile social networks associated between mobile users and other potential users communicate with them and benefit from their information [4].Personal data is essential for the improvement of online relationships [5].Online clients are at the hazard because of they might not have any information about others [6].

Keeping in mind the end goal to ensure clients it is imperative to keep up an abnormal state security for sheltered and trusted correspondence of data between different organizations [7]. To construct secure social network it is fundamental to investigate the accessibility, security and protection among the clients [8].The security strategy of online social networks lays on the rule that a client's contact a man by method for trust [9]. Appropriate trust models ought to be characterized with security strategy to give secure transmission in portable networks [10].The security arrangement addresses limitations on capacities and stream among them, imperatives on access by outer frameworks and adversaries including projects and access to information by individuals [11].

The mobile nodes normally have requirements like limited energy, bandwidth and computational power [12]. Evaluation of interactions between mobile nodes is critical for the advancement of trust instruments [13]. Trust is the metric that portrays the real status of the mobile nodes display in the network amid transmission [14]. Trust is likewise generally acknowledged as a noteworthy part to distinguish and approve the social connections between the portable nodes [15]. Certain level of trust is basic for fruitful transmission and trust based structure is used to evaluate delivery competency of the mobile nodes more accurately [16]. Several trust management protocols are also used for the purpose of bias minimization and performance maximization in the network [17].

Our contributions: In this paper we attempt to fill the gap in the existing literature surveys by providing a clear knowledge about mobile social networks and a focused survey on various trust and location based security in such networks.

 DOI : 10.18231/2454-9150.2017.0001

II. NETWORK & ISSUES

A. Social Networks

Social networks (SNSs) give electronic administrations that permit people to (1) develop an open or semi-open profile inside a limited system, (2) explain a list of different clients with whom they share an association, and (3) view and cross their list of associations and those made by others inside the framework [18]. While SNSs have actualized a wide assortment of specialized components, their spine comprises of obvious profiles that show an enunciated list of friends who are also users of the system. The visibility of a profile shifts by site and as per client circumspection. Of course, profiles on Friendster and Tribe.net are slithered via web crawlers, making them obvious to anybody, paying little mind to regardless of whether the watcher has a record [19]. Subsequent to joining a social network site, clients are incited to distinguish others in the system with whom they have a relationship [20].

B. Mobile Social Networks

Mobile Social Networks is a method for transmitting data utilizing a combination of voice and information gadgets over networks including cell innovation and components of private and public IP infrastructure [21]. 'Mobile Social Networking' (MSN) alludes to the majority of the empowering components important for the commitment and utilization of social media over a portable network [22].

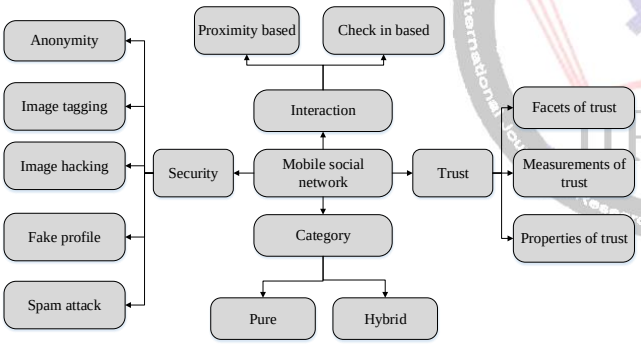

Figure 1: Classification Aspects of Mobile Social Networks

C. Security Issues in MSN

Users' Anonymity [23]: Almost all the users of online social network applications make use their real name as the profile name. Hence, users' name is publicly available on social media and all the social media are indexed in the search engines. Hacker can obtain all the possible information of the victim through the social networking websites.

Profile and Personal Information [24]: Social network users almost provide their real name and sensitive information on their profile such as full name, contact information, date of birth, relationship status, education details, present and previous work locations. These kind of sensitive information available on social network provides all the needed information to the hackers. These basic and sensitive information available as public to all the users of social networking web applications.

Image Tagging [25]: Users of online social network can tag the images with full name, E-Mail address and even they can provide the link to their OSN profile. This tagged image can be accessible to the friends of friends and even to public. Hence, this image tagging provides the information about the particular user to others users which can be used by the hackers for nuisance activities.

Image Hacking [26]: Every day many real images are posted in each user's profile. Some of the photos are available as public because unawareness of the privacy settings. Most of the real images are viewable to the friends and friends of friends. Hence there is no security to the images posted on the social networking websites. Hackers can easily hack the real images of the particular user and those photos can be misused widely for nuisance activities.

Fake Profile [27]: When the particular user's entire personal information as well as real image is available in social media, it is easily for the hackers to obtain those details. Once the sensitive information as well as photos are hacked the attacker will create the fake profile with those details. The name of the particular original user can be damaged completely the victim will be under trouble forever because of fake profile. Through this fake profile the attacker can add the friends of the victim to his/her circle and their personal information also can be hacked.

Social Phishing [28]: Social Phishing is the method for attack utilized by the attackers to acquire the delicate data of the casualty. In this attack the hacker will give a fake site which will resemble a genuine site. Aggressor will send the message to the casualty that you need to confirm your profile generally your profile will be erased. At the point when the casualty visits the specific fake site it will incite the client to enter the touchy data and username and secret word of the casualty. More often than not the aggressor is fruitful on account of unawareness of the users.

E-Mail Spam Attack [29]: In this attack the programmer will get the E-mail address of the casualty and forward the spam sends to the clients. The greater part of the clients keep their E-Mail is accessible open in social media and the aggressor can undoubtedly recognize it. On the off chance that the client keep their email id as private the email id can be speculated with the casualty first and last name. The majority of the social networking sites offer companion look through email. The aggressor can without much of a stretch acquire the subtle

 DOI : 10.18231/2454-9150.2017.0001

elements effectively from these components offered by the social networking destinations.

Malware Attack [30]: Malware attack get to be distinctly popular among social networking clients. Attacker will send the malware infused code to the casualty profile. Once the client tap the malware URL false data will be posted on the casualty divider. Other kind of malware is, when the casualty tap on the URL the client will be diverted to the fake site where the casualty will be made a request to enter his/her touchy data. So also by tapping the malware the URL a customer side code will be introduced on the casualty framework to take the data put away on the machine.

Sharing Day to Day activities [31]: Users of online social networking have the habit of sharing their day to day activities among their friends. For instance consider the following post. "Hi I am moving the beauty parlor alone". These kind of posting gives the clue to the kidnappers. Then the kidnapper is very well aware where the victim is going and who are all with the victim. These kind of sharing present ongoing activities online will lead to a security threat to the users especially to women.

Gathering Social Data [32]: Monitoring the casualty in social media the attacker can come to know, in which thing the casualty is intrigued and what does the casualty like. In light of the data accumulated on the casualty profile, the casualty will get the showcasing notice and shopping offers. Here the client protection is totally corrupted.

Deleting the User Account [33]: When the client needs to erase his/her profile everlastingly, he/she can't erase the record totally. In spite of the fact that the record is erased, the substance posted by the client on another client's profile will be accessible on social networking sites until the end of time. Client can't erase his/her correspondence on the social media until the end of time.

Physical Threat [34]: A dynamic client of online social network gives the delicate data online, for example, E-Mail, Contact telephone number, and place of residence. These kind of giving the physical identify to the attackers, they may ring up a call to the victim and send unwanted e-mails to the victim mail account. This will be a physical threat to the victim forever.

III. SECURITY IN MSN

Social network information is now being used in ways for which it may have not been originally intended. In particular, increased use of smart phones capable of running applications which access social network information enable applications to be aware of a user's location and preferences. However, current models for exchange of this information require users to compromise security [35]. This brings security in mobile social networks as an essential one. Since there exist a security gap in the various works which are carried out to provide security in mobile social network in the past decades. This section presents a broad review on trust and location based security in mobile social networks.

A. Review on Trust based Security in MSN

Fenye Bao *et al.* [36] have proposed a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. They considered multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. By means of a novel probability model, they described a heterogeneous WSN comprising a large number of sensor nodes with vastly different social and quality of service (QoS) behaviours with the objective to yield "ground truth" node status. That served as a basis for validating the protocol design by comparing subjective trust generated as a result of protocol execution at runtime against objective trust obtained from actual node status. To demonstrate the utility of the hierarchical trust management protocol, they applied it to trust-based geographic routing and trust-based intrusion detection. For each application, they identified the best trust composition and formation to maximize application performance. The results indicate that trust-based geographic routing approaches the ideal performance level achievable by flooding-based routing in message delivery ratio and message delay without incurring substantial message overhead. For trust-based intrusion detection, they discovered that there exists an optimal trust threshold for minimizing false positives and false negatives.

Mawloudomar *et al.* [37] have aimed to provide a fully distributed trust model for mobile ad hoc networks. A fully distributed public key certificate management system based on trust graphs and threshold cryptography was proposed. It permits users to issue public key certificates, and to performed authentication via certificates' chains without any centralized management or trusted authorities. Moreover, thanks to the use of threshold cryptography; our system resists against false public keys certification. They performed an overall evaluation of the proposed approach through simulations.

Jin Hee Cho *et al.* [38] identified the optimal length of a trust chain among peers in a trust web that generates the most accurate trust levels without revealing risk based on a tradeoff between trust availability and path reliability over trust space. They defined a trust metric for mission-driven group communication systems in mobile ad hoc networks to properly reflect unique characteristics of trust concepts and

 DOI : 10.18231/2454-9150.2017.0001

demonstrated that an optimal trust chain length exists for generating the most accurate trust levels for trust-based collaboration among peers in mobile ad hoc networks while meeting trust availability and path reliability requirements.

Joseph domingo *et al*. [39] have described a new protocol which offered private relationships allowing resource access through indirect relationships without requiring a mediating trusted third party (although an optimistic trusted third party was used which only acts in case of conflict). Thanks to homomorphic encryption, the scheme prevented the resource owner from learning the relationships and trust levels between the users who collaborate in the resource access. In this way, the number of users who might refuse collaboration due to privacy concerns was minimized. That resulted in increased resource availability, as the chances that certain nodes become isolated at a given period of time were reduced.

FeiHao *et al.* [40] have proposed a new fuzzy inference mechanism, namely MobiFuzzy Trust, for inferring trust semantically from one mobile user to another that may not be directly connected in the trust graph of MSNs. Firstly, a mobile context including an intersection of prestige of users, location, time and social context was constructed. Secondly, a mobile context aware trust model was devised to evaluate the trust value between two mobile users efficiently. Finally, the fuzzy linguistic technique was utilized to express the trust between two mobile users and enhance the human's understanding of trust. Real-world mobile dataset was adopted to evaluate the performance of the MobiFuzzy Trust inference mechanism.

XiaoHui Liang *et al*. [41] proposed a Trustworthy Service Evaluation (TSE) system to enable users to share service reviews in service-oriented mobile social networks (S-MSNs). Each service provider independently maintains a TSE for itself, which collects and stores users' reviews about its services without requiring any third trusted authority. The service reviews can then be made available to interested users in making wise service selection decisions. They identified three unique service review attacks, i.e., linkability, rejection, and modification attacks, and develop sophisticated security mechanisms for the TSE to deal with these attacks. Specifically, the basic TSE (bTSE) enables users to distributedly and cooperatively submit their reviews in an integrated chain form by using hierarchical and aggregate signature techniques. It restricted the service providers to reject, modify, or delete the reviews. Thus, the integrity and authenticity of reviews were improved. Further, they extend the bTSE to a Sybil-resisted TSE (SrTSE) to enable the detection of two typical sybil attacks. In the SrTSE, if a user generates multiple reviews toward a vendor in a predefined time slot with different pseudonyms, the real identity of that user was revealed.

MariosKoufaris *et al*. [42] proposed a model to explain how new customers of a web-based company develop initial trust in the company after their first visit. The model was empirically tested using a questionnaire-based field study. The results indicated that perceived company reputation and willingness to customize products and services can significantly affect initial trust. Perceived web site usefulness, ease of use, and security control are also significant antecedents of initial trust. Finally, they found no support for the hypothesized effect of individual customer trust propensity on initial trust.

JunhaiLuo *et al*. [43] have proposed RFSTrust, a trust model based on fuzzy recommendation similarity, to quantify and to evaluate the trustworthiness of nodes, which includes five types of fuzzy trust recommendation relationships based on the fuzzy relation theory and a mathematical description for MANETs. Fuzzy logic provides a natural framework to deal with uncertainty and the tolerance of imprecise data inputs for the subjective tasks of trust evaluation, packet forwarding review and credibility adjustment. Theoretical analysis and experimental results showed that RFSTrust was still robust under more general conditions where selfish nodes cooperate in an attempt to deliberately subvert the system, end-to-end packet delivery ratio more quickly, and decreases the average energy consumes more effectively.

Jin wang *et al.* [44] have presented a contextual social network model that takes into account both participants' personal characteristics and mutual relations (referred to as the dependent social context, including the trust, social intimacy, and interaction context between two participants). In addition, they proposed a new probabilistic approach, SocialTrust, as the first solution in the literature, to social context-aware trust inference in social networks.

Shin and Dong-Hee [45] examined security, trust, and privacy concerns with regard to social networking Websites among consumers using both reliable scales and measures. It proposed an SNS acceptance model by integrating cognitive as well as affective attitudes as primary influencing factors, which were driven by underlying beliefs, perceived security, perceived privacy, trust, attitude, and intention. Results from a survey of SNS users validate that the proposed theoretical model explained and predicted user acceptance of SNS substantially well. The model showed excellent measurement properties and establishes perceived privacy and perceived security of SNS as distinct constructs.

B. Review on Location based Security in MSN

Muyuan Li *et al.* [46] have developed an automated user location tracking system and tested it on leading LBSNs

 DOI : 10.18231/2454-9150.2017.0001

including Wechat, Skout, and Momo. They demonstrated its effectiveness and efficiency via a 3 week real world experiment on 30 volunteers and shown that we could geolocate any target with high accuracy and readily recover his/her top 5 locations. Finally, they also developed a framework that explored a grid reference system and location classifications to mitigate the attacks. The result served as a critical security reminder of the current LBSNs pertaining to a vast number of users.

Wei Wei *et al.* [47] have presented MobiShare, a system that provides flexible privacy-preserving location sharing in mOSNs. MobiShare was flexible to support a variety of location-based applications, in that it enables location sharing between both trusted social relations and untrusted strangers, and it supports range query and user-defined access control. In MobiShare, neither the social network server nor the location server has a complete knowledge of the users' identities and locations. The users' location privacy was protected even if either of the entities colludes with malicious users.

Wei Cherng Chenga and Masayoshi Aritsugi [48] have proposed a user sensitive privacy-preserving location sharing system to avoid leaking. Users define sensitivity profiles to transform the public available geographic data into personal obfuscate region maps. Shared locations from obfuscate region maps provide close enough coordinates for application to use, but disconnected correlation between exact public available geographic data and user's actual location to prevent malicious tracking.

Pravin Shankar *et al.* [49] have presented Social Telescope, a location-based service that automatically compiles, indexes and ranks locations, based on user interactions with locations in mobile social networks. They implemented the system as a location-based search engine that uses geo-tweets by Twitter users to learn about places. They evaluated the coverage and relevance of the system by comparing it against current state-of-the-art approaches including page-rank (Google Local Search), expert-based (Zagat) and user-review based (Yelp). The results show that a crowd-sourced location-based service returns results that are at least as relevant as those returned by current approaches, at a substantially lower cost.

Chi-Yin Chow *et al.* [50] have focused on the ubiquity of mobile devices with global positioning functionality (e.g., GPS and AGPS) and Internet connectivity (e.g., 3G and Wi-Fi). In general, there are two types of Location based Services (LBS), namely, snapshot and continuous LBS. For snapshot LBS, a mobile user only needs to report its current location to a service provider once to get its desired information. On the other hand, a mobile user has to report its location to a service provider in a periodic or on-demand manner to obtain its desired continuous LBS. Protecting user location privacy for continuous LBS is more challenging than snapshot LBS because adversaries may use the spatial and temporal correlations in the user's location samples to infer the user's location information with higher certainty. An overview of the state-of-the-art privacy-preserving techniques in these two problems was presented in that paper.

Raz Schwartz and Germaine R. Halegoua [51] have provided an encompassing interdisciplinary survey of research that investigates the relationships between location, information technology, and identity performance. Then they identified and characterize the spatial self as well as examined its occurrences through three case studies of popular social media sites: Instagram, Facebook, and Foursquare. Finally, they offered possible research directions and methodological considerations for the analysis of geocoded social media data.

Ling Zhao *et al.* [52] have created a privacy calculus model to investigate the factors that influence LBSN users' intention to disclose location-related information in China. In addition, the study applied justice theory to investigate the role of privacy intervention approaches used by LBSN Web sites in enhancing users' perception of justice, including incentives provision, interaction promotion, privacy control, and privacy policy. Model testing using structural equation modelling reveals that perceived cost (users' privacy concerns) and perceived benefits (personalization and connectedness) influence intention to disclose location-related information.

Zhichao Zhu and Guohong Cao [53] have proposed a Privacy-Preserving Location proof Updating System (APPLAUS) in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and update to a location proof server. Periodically changed pseudonyms were used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. They also developed user-centric location privacy model in which individual users evaluate their location privacy levels in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels. APPLAUS can be implemented with the existing network infrastructure and the current mobile devices, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost.

AnastasiosNoulas *et al.* [54] have examined how venue discovery behaviour characterizes the large check-in datasets from two different location-based social services, Foursquare and Gowalla: by using large-scale datasets containing both user check-ins and social ties, the analysis reveals that, across 11 cities, between 60% and 80% of users' visits are in venues that were not visited in the previous 30 days. They then show

 DOI : 10.18231/2454-9150.2017.0001

that, by making constraining assumptions about user mobility, state-of-the-art filtering algorithms, including latent space models, do not produce high quality recommendations. Finally, they proposed a new model based on personalized Marco Anisetti *et al.* [55] have presented a technique that provides geo-location and mobility prediction both at network and service level, does not require any change to the existing mobile network infrastructure, and is entirely performed on the mobile network side, making it more robust than other positioning systems with respect to location spoofing and other terminal-based security threats. The approach was based on a novel database correlation technique over Received Signal Strength Indication (RSSI) data, and provides a geolocation and tracking technique based on advanced map- and mobility-based filtering. The performance of the geolocation algorithm has been carefully validated by an extensive experimentation, carried out on real data collected from the mobile network antennas of a complex urban environment.

random walks over a user-place graph that, by seamlessly combining social network and venue visit frequency data, obtains between 5 and 18% improvement over other models.

IV. COMPARITIVE ANALYSIS

This section provides a detailed comparison and performance analysis of trust and location based security in mobile social networks process and the various techniques within each category in which security is provided. In this review, we have compared different techniques based on the parameters like the technology used, Advantages, and Disadvantages.

Table 1: Comparitive Analysis for Trust based Security in Mobile Social Networks

S. No	Study	Techniques Used	Strengths	Limitations
1.	[36]	Cluster-based hierarchical trust management protocol.	Highly scalable, Inexpensive, access sensitive data, collect multidimensional attributes.	Computational complexity and computation time is high.
2.	[37]	Fully distributed public key certificate management system based on trust graphs and threshold cryptography.	High security.	Used only for limited application areas.
3.	[38]	Trust management Protocol using hierarchical modeling techniques based on stochastic Petri nets.	Highly trustable and reliable.	Limited in the selection of samples
4.	[39]	A new protocol based on homomorphic encryption.	Offers private relationships allowing resource access through indirect relationships without requiring a mediating trusted third party which is also scalable and deployable.	Complexity is high.
5.	[40]	A new fuzzy inference mechanism, namely MobiFuzzyTrust.	Efficiently infer trust with a high precision.	Time consumption is high.
6.	[41]	Trustworthy Service Evaluation (TSE) system.	Better performance in terms of submission rate and delay.	Since some special type of network attacks exist.
7.	[42]	A novel model to evaluate initial trust.	Ease of use, and security control.	No support for the hypothesized effect of individual customer trust propensity on initial trust.
8.	[43]	RFS Trust, a trust model based on fuzzy recommendation similarity.	End-to-end packet delivery ratio was high, and decreases the average energy consumption. The effect of node rating data's sparsity can be greatly reduced.	Clear knowledge about the output is required.
9.	[44]	Context-aware trust inference for trust enhancement in social network.	Deliver more reasonable and trustworthy results, efficient and applicable to real social networks.	More data samples required.
10.	[45]	SNS acceptance model for examination of trust, security in mobile networks.	Provides high security and privacy.	Requires integrating cognitive as well as affective attitudes which are driven by underlying beliefs, perceived security, perceived privacy, trust, attitude, and intention.

 DOI : 10.18231/2454-9150.2017.0001

Table 1 shows the Comparitive analysis of the methods used for trust based security in mobile social networks. New techniques and trust protocols were developed to provide security, for example, MobiFuzzy Trust a new fuzzy inference mechanism, RFSTrust a trust model based on fuzzy recommendation similarity, etc. are displayed about. Using these techniques the security issues have been solved and also improves the performance of the network in terms of end- to end delay, packet delivery ratio, etc. From table 1 we observed that by various detection mechanism we can evaluate the trust metric which identifies the malicious behavior of the networks and able to provide high security to the networks efficiently with its own advantages and disadvantages.

Table 2: Comparitive Analysis for Location Identification based Security in Mobile Social Networks

S. No	Study	Techniques Used	Strengths	Limitations
1.	[46]	An automated user location tracking system	Provide high security with accuracy.	Limited safeguards.
2.	[47]	MobiShare, a system that provides flexible privacy-preserving location sharing in MSNs	The users' location privacy is protected even if either of the entities colludes with malicious users.	System performance is low.
3.	[48]	User sensitive privacy-preserving location sharing system.	Prevent from malicious tracking	Used only in limited distance.
4.	[49]	Location-based search engine.	Low cost.	Security is limited due to leaking.
5.	[50]	Privacy-preserving techniques	Establish social relationships	Time consuming.
6.	[51]	Spatial self: a theoretical framework encapsulating the process of online self-presentation based on the display of offline physical activities.	Evaluate the value of social networks	Doesn't explain the security gap in the network.
7.	[52]	Privacy preserving in social networks.	Provides practical implications for service providers and policy makers to develop better LBSNs.	Tracking is complex in nature.
8.	[53]	A Privacy-Preserving Location proof Updating System.	Can significantly preserve the source location privacy.	Expensive.
9.	[54]	A new model based on personalized random walks.	Mediate and enhance informations effectively.	Limited security.
10.	[55]	Novel database correlation technique.	Effective tracking based on RSSI.	More data samples required.

Table 2 shows the Comparitive analysis of the methods used for location based security in mobile social networks. New techniques and systems were developed to provide security in the network via tracking the locations, for example, Location-based search engine, privacy-preserving location sharing system and a privacy-Preserving Location proof updating System etc. are displayed about. Using these techniques several security issues in the network can be solved. From table 2 it is observed that to provide security in social networks each of the above specified methods can able to detect malicious behaviour of network based on location accurately and efficiently with its own advantages and disadvantages.

V. FUTURE ENHANCEMENT

This paper presents a broad review on security on mobile social networks based on two different aspects such as trust and location. We also presented an overview of the various techniques, systems, protocols and frameworks which are utilized for solving the security issues in mobile social networks. From the review we have observed that the existing systems concentrated on neither trust nor location to provide security. Since there exists some security gap due to the presence of malicious behavior of mobile nodes. In order to overcome such issue and to provide better security several security aspects can be integrated or utilized simultaneously in future which enhances the network security and can provide better transmission on mobile social networks.

VI. CONCLUSION

In this paper, we have discussed about the work done by various researchers, with the attempt made to include as many references as possible from recent years. Based on this paper, we beat out some of the problems occurred during security in mobile social networks which malicious node identification, selective packet drop etc. We indicating on the role of

 DOI : 10.18231/2454-9150.2017.0001

existing security on mobile social networks based on trust and location with the reliance that it would serve as a reference to both old and new, incoming researchers in this field, to support their understanding of current trends and assist their future research perspectives and directions. Further, we compared the techniques in terms of their advantages and disadvantages and from the analysis we observed that each of the solutions has its own advantages and disadvantages thus indicates that still there remains a security gap in the existing solutions.

REFERENCES

[1] Habibi, Mohammad Reza, Michel Laroche, and Marie-Odile Richard. "*The roles of brand community and community engagement in building brand trust on social media*." Computers in Human Behavior vol.37, pp.152-161, 2014.

[2] Rayman-Bacchus, L., and A. Molina. "*Internet-based tourism services: business issues and trends*." Futures, no. 7, vol.33, pp.589-605, 2003.

[3] Burt, Ronald S. "*Network items and the general social survey*." Social networks no. 4, vol.3, pp.293-339, 2000.

[4] Bryce, Jo, and James Fraser. "*The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions*." Computers in Human Behavior vol.30, pp.299-306, 2014.

[5] De Jonge, Janneke, J. C. M. Van Trijp, Ivo A. van der Lans, Reint Jan Renes, and Lynn J. Frewer. "*How trust in institutions and organizations builds general consumer confidence in the safety of food: A decomposition of effects*." Appetite, no. 2, vol.51, pp.311-317, 2008.

[6] Mohaien, Abedelaziz, Denis Foo Kune, Eugene Y. Vasserman, Myungsun Kim, and Yongdae Kim. "*Secure encounter-based mobile social networks: Requirements, designs, and tradeoffs*." IEEE Transactions on Dependable and Secure Computing no. 6, vol.10, pp. 380-393, 2013.

[7] Shin, Dong-Hee. "*The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption*." Interacting with computers no. 5, vol.10, pp.428-438, 2010.

[8] Perez, Charles, BabigaBirregah, and Marc Lemercier. "*A smartphone-based online social network trust evaluation system*." Social Network Analysis and Mining no. 4, vol.3, pp. 1293-1310, 2013.

[9] Blaze, Matt, Joan Feigenbaum, and Angelos D. Keromytis. "*KeyNote: Trust management for public-key infrastructures*." In International Workshop on Security ProtocolsSpringer Berlin Heidelberg, pp.59-63, 1998.

[10] Omar, Mawloud, YacineChallal, and AbdelmadjidBouabdallah. "*Certification-based trust models in mobile ad hoc networks: A survey and taxonomy*." Journal of Network and Computer Applications no. 1, vol.35, pp.268-286, 2012.

[11] Karlof, Chris, and David Wagner. "*Secure routing in wireless sensor networks: Attacks and countermeasures*." Ad hoc networks no. 2, vol.5, pp.293-315, 2003.

[12] Han, Guangjie, Jinfang Jiang, Lei Shu, JianweiNiu, and Han-Chieh Chao. "*Management and applications of trust in Wireless Sensor Networks: A survey*." Journal of Computer and System Sciences no. 3, vol.80, pp.602-617, 2014.

[13] Cho, Jin-Hee, Ananthram Swami, and Ray Chen. "*Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks*." Journal of Network and Computer Applications no. 3, vol.35, pp.1001-1012, 2012.

[14] Li, Na, and Sajal K. Das. "*A trust-based framework for data forwarding in opportunistic networks*." Ad Hoc Networks no. 4, vol.11, pp.1497-1509, 2013.

[15] Chen, Ray, JiaGuo, FenyeBao, and Jin-Hee Cho. "*Trust management in mobile ad hoc networks for bias minimization and application performance maximization.*" Ad Hoc Networks vol.19, pp.59-74, 2014.

[16] Velloso, Pedro B., Rafael P. Laufer, Daniel De OO Cunha, Otto Carlos MB Duarte, and Guy Pujolle. "*Trust management in mobile ad hoc networks using a scalable maturity-based model*." IEEE transactions on network and service management no. 3, vol.7, pp.172-185, 2007.

[17] Cao, Yang, Tao Jiang, Xu Chen, and Junshan Zhang. "*Social-aware video multicast based on device-to-device communications*." IEEE Transactions on Mobile Computing no. 6, vol.15, pp.1528-1539, 2016.

[18] Liu, Yan, Kun Wang, Huang Guo, Qing Lu, and Yanfei Sun. "*Social-Aware Computing based Congestion Control in Delay Tolerant Networks*." Mobile Networks and Applications pp.1-12, 2016.

 DOI : 10.18231/2454-9150.2017.0001

[19] Habibi, Mohammad Reza, Michel Laroche, and Marie-Odile Richard. "*The roles of brand community and community engagement in building brand trust on social media*." Computers in Human Behavior vol.37, pp.152-161, 2017.

[20] Jiang, Wenjun, Guojun Wang, and Jie Wu. "*Generating trusted graphs for trust evaluation in online social networks*." Future generation computer systems vol.31, pp.48-58, 2014.

[21] Carter, Michelle, Ryan Wright, Jason Bennett Thatcher, and Richard Klein. "*Understanding online customers' ties to merchants: the moderating influence of trust on the relationship between switching costs and e-loyalty*." European Journal of Information Systems no. 2, vol.23, pp.185-204, 2014.

[22] Leong, Lai-Ying, Teck-Soon Hew, Garry Wei-Han Tan, and Keng-Boon Ooi. "*Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach*." Expert Systems with Applications no. 14, vol.40, pp.5604-5620, 2013.

[23] Li, Na, and Sajal K. Das. "*A trust-based framework for data forwarding in opportunistic networks*." Ad Hoc Networks no. 4, vol.11, pp.1497-1509, 2013.

[24] Bellavista, Paolo, Rebecca Montanari, and Sajal K. Das. "*Mobile social networking middleware: A survey*." Pervasive and Mobile Computing no. 4, vol.9, pp.437-453, 2013.

[25] Jung, Jason J. "*Ubiquitous conference management system for mobile recommendation services based on mobilizing social networks: A case study of u-conference*." Expert Systems with Applications no. 10, vol.38, pp.12786-12790, 2011.

[26] Hui, Pan, Jon Crowcroft, and EikoYoneki. "*Bubble rap: Social-based forwarding in delay-tolerant networks*." IEEE Transactions on Mobile Computing no. 11, vol.10, pp.1576-1589, 2011.

[27] Yang, Shuiqing, Yaobin Lu, Sumeet Gupta, Yuzhi Cao, and Rui Zhang. "*Mobile payment services adoption across time: An empirical study of the effects of behavioural beliefs, social influences, and personal traits*." Computers in Human Behaviour no. 1, vol.28, pp.129-142, 2012.

[28] .Michael, Katina, and Roger Clarke. "*Location and tracking of mobile devices: Überveillance stalks the streets*." Computer Law & Security Review no. 3, vol.29, pp.216-228, 2013.

[29] Incel, OzlemDurmaz, Mustafa Kose, and CemErsoy. "*A review and taxonomy of activity recognition on mobile phones.*" BioNanoScience no. 2, vol.3, pp.145-171, 2013.

[30] Mejia, Marcela, Néstor Peña, Jose L. Muñoz, Oscar Esparza, and Marco A. Alzate. "*A game theoretic trust model for on-line distributed evolution of cooperation inMANETs*." Journal of Network and Computer Applications no. 1, vol.34, pp.39-51, 2011.

[31] Sadeh, Norman, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, MadhuPrabaker, and Jinghai Rao. "*Understanding and capturing people's privacy policies in a mobile social networking application*." Personal and Ubiquitous Computing no. 6, vol.13, pp.401-412, 2009.

[32] Parveen, Farzana, Noor IsmawatiJaafar, and SulaimanAinin. "*Social media usage and organizational performance: Reflections of Malaysian social media managers*." Telematics and Informatics no. 1, vol.32, pp.67-78, 2015.

[33] De Jonge, Janneke, J. C. M. Van Trijp, Ivo A. van der Lans, Reint Jan Renes, and Lynn J. Frewer. "*How trust in institutions and organizations builds general consumer confidence in the safety of food: A decomposition of effects*." Appetite no. 2, vol.51, pp.311-317, 2008.

[34] Guo, Linke, Chi Zhang, and Yuguang Fang. "*A trust-based privacy-preserving friend recommendation scheme for online social networks*." IEEE Transactions on Dependable and Secure Computing no. 4, vol.12, pp.13-427, 2015.

[35] Fogel, Joshua, and ElhamNehmad. "*Internet social network communities: Risk taking, trust, and privacy concerns*." Computers in human behavior no. 1,vol.25,pp.153-160,2009.

[36] Bao, Fenye, Ray Chen, MoonJeong Chang, and Jin-Hee Cho. "*Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection.*" IEEE transactions on network and service management no. 2,vol.9,pp.169-183,2010.

[37] Omar, Mawloud, YacineChallal, and AbdelmadjidBouabdallah. "Reliable and fully distributed trust model for mobile ad hoc networks." Computers & Security no. 3,vol.28,pp. 199-214,2009.

[38] Cho, Jin-Hee, Ananthram Swami, and Ray Chen. "Modeling and analysis of trust management with trust chain

 DOI : 10.18231/2454-9150.2017.0001

optimization in mobile ad hoc networks." Journal of Network and Computer Applications no. 3,vol.35,pp.1001-1012,2012.

[39] Domingo-Ferrer, Josep, Alexandre Viejo, FrancescSebé, and Úrsula González-Nicolás. "Privacy homomorphisms for social networks with private relationships." Computer Networks no. 15,vol.52,pp.3007-3016,2008.

[40] Hao, Fei, Geyong Min, Man Lin, ChangqingLuo, and Laurence T. Yang. "*MobiFuzzyTrust: an efficient fuzzy trust inference mechanism in mobile social networks*." IEEE Transactions on Parallel and Distributed Systems no. 11,vol.25,pp.2944-2955,2014.

[41] Liang, Xiaohui, Xiaodong Lin, and Xuemin Sherman Shen. "*Enabling trustworthy service evaluation in service-oriented mobile social networks*." IEEE Transactions on Parallel and Distributed Systems no. 2 ,vol.25,pp.310-320,2014.

[42] Koufaris, Marios, and William Hampton-Sosa. "*The development of initial trust in an online company by new customers*." Information & management no. 3,vol.41,pp.377-397,2014.

[43] Luo, Junhai, Xue Liu, and Mingyu Fan. "*A trust model based on fuzzy recommendation for mobile ad-hoc networks*." Computer Networks no. 14,vol.53,pp.2396-2407,2003.

[44] Wang, Yan, Lei Li, and Guanfeng Liu. "*Social context-aware trust inference for trust enhancement in social network based recommendations on service providers*." World Wide Web no. 1,vol.18, pp.159-184,2014.

[45] Shin, Dong-Hee. "*The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption*." Interacting with computers Vol.22, no. 5, pp.428-438, 2010.

[46] Li, Muyuan, et al. "*All your location are belong to us: Breaking mobile social networks for automated user location tracking*." Proceedings of the 15th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2014.

[47] Wei Wei, FengyuanXu and Qun Li,"*MobiShare: Flexible privacy preserving location sharing in mobile nonline social networks*", In proceedings of the 31stAnnual IEEE International conference on computer communications: Mini –Conference, 2012.

[48] Wei Cherng and Masayoshi Aritsugi, "*A user sensitive privacy preserving location sharing system in mobile social network*", In Proceedings of 18th International conference on Knowledge Based and Intelligent Information & Engineering Systems – KES2014.

[49] Shankar, Pravin, Yun-Wu Huang, Paul Castro, BadriNath, and LiviuIftode. "*Crowds replace experts: Building better location-based services using mobile social network interactions*." In Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on, pp. 20-29. IEEE, 2012.

[50] Chow, Chi-Yin, and Mohamed F. Mokbel. "*Trajectory privacy in location-based services and data publication*." ACM Sigkdd Explorations Newsletter 13.1 (2011): 19-29.

[51] Schwartz, Raz, and Germaine R. Halegoua. "*The spatial self: Location-based identity performance on social media*." New Media & Society 17, no. 10 (2015): 1643-1660.

[52] Zhao, Ling, Yaobin Lu, and Sumeet Gupta. "*Disclosure intention of location-related information in location-based social network services*." International Journal of Electronic Commerce 16, no. 4 (2012): 53-90.

[53] Zhu, Zhichao, and Guohong Cao. "*Applaus: A privacy-preserving location proof updating system for location-based services*." INFOCOM, 2011 Proceedings IEEE. IEEE, 2011.

[54] Noulas, Anastasios, Salvatore Scellato, Neal Lathia, and Cecilia Mascolo. "*A random walk around the city: New venue recommendation in location-based social networks*." In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom), pp. 144-153. Ieee, 2012.

[55] Anisetti, Marco, Claudio A. Ardagna, Valerio Bellandi, Ernesto Damiani, and Salvatore Reale. "*Map-based location and tracking in multipath outdoor mobile networks*." IEEE Transactions on Wireless Communications 10, no. 3 (2011): 814-824.

 DOI : 10.18231/2454-9150.2017.0001