Print ISSN: 2321-6379
Online ISSN: 2321-595X
DOI: 10.17354/ijssl/2017/115

Original Article

Investigation of the Wireless Networks and Private Security

Mona Azadmanesh

Master of Telecommunication Technology (M.Sc T.T), Manipal University of Technology, Pune, India

Abstract

Wireless network is considered as important element in internet and web activities and is also one of the most influential media. Wireless networks with unlimited physical distance supply new and interesting instruments to web users to communicate and interact with each other. However, these networks provide conditions repetitively to share data and enable communications of users immediately. There are many issues in field of privacy, which are revealed here. One of these issues is how to prevent privacy attacks when there is a lot of personal information available. In this study, the issues related to privacy of people in wireless networks are discussed. Using wireless network analysis and link mining methods, this purpose is realized. Moreover, basic common representations of wireless network are described. After that, this study shows that how privacy attacks can affect analysis of wireless networks and link mining technique to disclose sensitive user information.

Key words: Wireless networks, Private security, Privacy threats

INTRODUCTION

According to the development of information technology (IT) and various needs in life scopes, wireless have lots of manifestations in their users and are available in many devices. Many wireless networks like Facebook, LinkedIn and Twitter supply new interesting tools for users to communicate each other and share information. With the development of wireless networks, sharing data in these networks has been changed into their increasing importance. Clearly, wireless networks have found the innovative way to collect data through communicating users. Not surprisingly, social users are in interaction with each other and have tendency to disclose their information freely. To control access to this personal information and to implement the protection, wireless networks have used some constructed controlling mechanisms and has prevailed them [1]. However, wireless network users are not mostly successful to protect their profiles completely and personal data have undesirable access problems. Online social networks may suffer from problems such as private security against capability and sociability and they may disclose information of users for unauthorized or third parties intentionally or accidently [2]. In the continue, this study will discuss on privacy in wireless networks and explains that how network analysis and data mining methods can be useful in understanding behavior of users and networks and a source can be changed into the risk of protecting privacy.

Access this article online

IJSS
www.ijss-sn.com

Month of Submission : 01-2017
Month of Peer Review : 03-2017
Month of Acceptance : 05-2017
Month of Publishing : 07-2017

WIRELESS NETWORKS

A wireless network is a social structure formed of nodes (generally individual or organizational) linked by one or more special types of attachment. In other words, a wireless network is a collection of tools referring to users who tend to share their interests, thoughts and activities with each other and also use shared media by others. These networks are used by many systems such as worldwide web (www), computer networks, biochemical networks, display networks and social networks. Each network is a structure including some actors as a representative of the network. For example, web pages in the www or people in a wireless network are in interaction with each other as a representative of links of web pages or friendship among people. In addition to these structural features (actors and relations),

Corresponding Author: Mona Azadmanesh, Master of Telecommunication Technology (M.Sc T.T), Manipal University of Technology, Pune, India. E-mail: Monaazad64@gmail.com

they include some fundamental concepts including relationships, couple, subgroups and groups.

The most important goal of wireless networks is expansion of interpersonal relations.

Generally, wireless networks are web-based services.

Online service is considered as a platform or site, in which people can create interests and content and share them with their friends or others. Wireless networks, especially those with conventional and noncommercial uses, are places in virtual world where people introduce themselves shortly and provide conditions to make communications between self and others in different interested fields.

Finding a good representative showing efficient and exact facilitation of network data is an important step in field of wireless network researches. Using graph is a powerful visual instrument and official instrument to show wireless networks.

There are abundant symbols to represent wireless networks: algebra symbol, matrix and graph. Wireless networks maintain value relations and user-related features, which can't be managed by algebraic symbols. Matrixes are mainly efficient for small networks. As a result, according to large size of social networks, matrix is not the best option to show the networks. To show a wireless network using matrix, two-way matrix called sociomatrix could be used. Sociomatrix includes row and column, which refer to social actors. In Figure 1, wireless network is noted through 3 methods.

Therefore, representation based on graph is more common than other methods to model wireless networks [3]. Graphical notation of wireless networks can facilitate perception, labeling and modeling properties of these networks. Hence, graphs can show different properties of social data and their features.

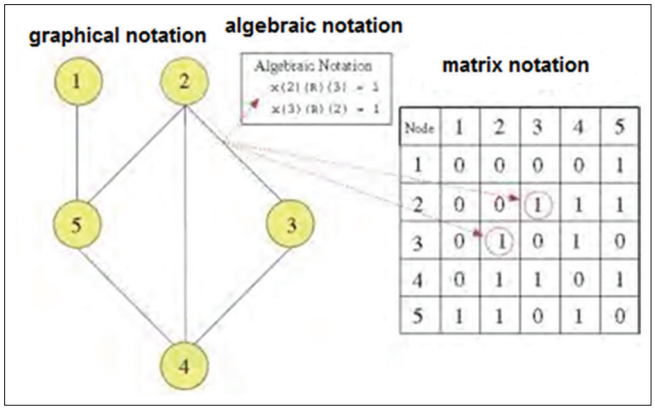

Figure 1: Notation of wireless networks

CAPABILITIES OF WIRELESS NETWORKS

In cable networks, as each client should be abled from the location of relevant switch, problems such as making holes, ducting and installing sockets are created. In addition, if physical location of the station is changed, again cabling and other steps should be done.

Wireless networks use waves and have high moving capability. Hence, changes in physical location of clients are also possible easily and following methods could be applied to mount it:

Ad hoc that can provide direct peer to peer link of equipment with each other

Infrastructure system that can link all devices to central device

Therefore, it could be found that installation of cabled networks or changing them is more difficult than similar case (wireless networks).

Cost

Equipment such as hub, switch or cable of network are more cost-effective than similar cases in wireless networks; although considering installation costs and probable environmental changes is also considered. It should be mentioned that with the increasing growth of wireless networks, their cost is also being increased.

Reliability

Cabled devices are also highly reliable and the reason for investment of constructors since about 20 years ago has been same reason; although they should be controlled carefully while installation or displacing and moving the cables and joints. Wireless equipment such as Boardband Router has problems such as continuous blackouts, intervention to adjacent electromagnetic waves and so on; although the developing process compared to past times (e.g. 11.802g) has improved reliability.

Efficiency

Cabled networks have highest efficiency. At the first, bandwidth of 10Mbps and then, they have been enhanced to higher bandwidths (100 and 1000Mbps) and even some switches with bandwidth of 1Gbps have been also provided. Wireless networks with standard of 11.802b support maximum bandwidth of 11Mbps and the wireless networks with standard of 11.802g support bandwidth of 54Mbps. Even in modern technologies, the process has been increased in a price relatively higher than 108Mbps. Moreover, efficiency of Wi-Fi is sensitive to distance; it means that maximum efficiency is declined with the

increased distance to Access Point. The bandwidth is enough to share internet or files; although it is inefficient for programs that need exchange of types of data between server and client (client server).

Security

As in cabled networks connected to internet existence of firewall is required and equipment such as hub or switch can't take the responsibility of firewall, separate firewall should be installed in these systems. In wireless networks devices like boardband router, firewall is available in form of software and just needed settings should be done. On the other hand, as air is used as transfer media in wireless networks, data security can't be realized completely without implementation of special techniques such as encryption. Using WEP (Wired Equivalent Privacy) encryption can enhance security in these devices.

Wireless Networks Data

Wireless networks have been changed into an important platform to connect users, sharing information and also a valuable source of wireless network data. Therefore, availability of such data shows an opportunity to study people and analysis of these networks. However, different data sources in wireless networks are not only considered as perception of a series of values and knowledge reservoirs, but also availability of them is changed into a form of threat and the different types of information could disclosed through using them and through the hackers.

Traditionally, many data in wireless networks are collected using questionnaires, these surveys can be in form of face to face interview, call survey or computer-based questionnaire. The conventional methods have many restrictions in terms of scalability, subjectivity and inconsistency. Nowadays, use of electronic data extraction for purpose of data collection of relevant networks is useful and it has shown its success to extension of different scopes [5]. Many advanced wireless network systems are made to collect and analyze data. Currently, wireless networks help users to exchange types of information such as messages, photos and texts.

Development and Measures Taken in Wireless Networks

Analysis of wireless networks in field of different programs has been used mostly as communicative networks like email, learning network, terrorist networks and wireless networks [6]. This is the result of trying to respond to a few numbers of questions such as the way that an actor can connect to a network; who are the most influencing actors within the network? What center an actor has in a network? Centrality includes the direction of ranking actors from a graph or use of self-connection inside the network. Several structure-based criteria have been presented to calculate centrality of an actor un a network like degree of closeness and degree of centrality.

SECURITY IN WIRELESS NETWORKS

3 security methods in wireless networks are as follows:

- Wired Equivalent Privacy (WEP)
  In this method, hears of unauthorized users in network is prevented and this is appropriate to small networks, since it needs manual settings of relevant KEY of each client. The basis of WEP encryption is on RC4 algorithm by RSA.
- Service Set Identifier (SSID)
  WLAN networks have several local networks and each local network has an identifier. These identifiers are located in several access points. Each user should enter the settings of SSID to have access to the desired web.
- Media Access Control (MAC)
  A list of MAC of previously used addresses in a network is entered to the relevant Access Point (AP) and hence, only computers with this MAC addresses are authorized to have access. In other words, when a computer sends a request, MAC address compares it with MAC address list in relevant AP and the permission of access or lack of access is analyzed. This security method is appropriate to small size networks, since it is hardly possible to enter these addresses to AP in large networks.

PRIVACY THREATS

Availability of wireless network data has gained attention of academic community, third party ads and governmental services for purpose of data analysis. Anonymity of these networks before making them free is required to implement privacy protection. A hacker can disclose the actual identity of users through referring to targeting network structure and using background knowledge. Anonymizing wireless network information is more challenging than Anonymization of relational data [7].

As it was mentioned, wireless networks can be noted in form of graphs and as a result, wireless network can be preprocessed and can be analyzed through wireless network analysis measures. Various attacks are existed in these networks. In first type of these attacks, attacks are active and the attackers can change the network before releasing the information and can potentially make identifiable sub-graph through putting the nodes and edges into the network.

Passive attack is another type of attack, which can be released after anonymizing the network and without

placing new nodes and edges. Particularly, they are structural information related to nearest degrees of nodes and neighbors in a network. It could be mentioned that degree of a node on a graph among other structural features can result in distinguishing a node from others. As a result, the attacks can take benefit of structural properties of the network, which can be changed into identification properties. Every wireless network that does the best to implement privacy of users should pay special attention to reduction of vulnerability by those relations through lack of notation of exact number of links of each user. In short, analysis of wireless networks refer to a series of measures widely used to study properties of networks and users' behaviors. Privacy attacks of users can be advantages of wireless networks to find out more about the users of wireless networks using structural information. Moreover, extension of wireless networks can lead to production of high volume of available data in the networks. An important necessity implemented by wireless networks is protection of personal data and privacy of users and the relations between users [8].

TASKS AND THREATS

According to popularity of www, increased calculative power and performance and higher capacity to collection and analyze data in large scale of wireless networks are being developed. Link mining studies with the aim of exploration of valuable and innate data from large databases related to privacy protection are efficient [9]. Although the centrality measures are being widely used in analysis of wireless networks, link mining techniques are relied on recent advancements in data mining and have emphasis on the links among actors of wireless networks [10]. In the rest of paper, the tasks related to link mining are described before description of privacy threats related to each task.

Development and Tasks

According to the possibility of links between wireless network actors, different data mining techniques help emergence of a new conventional scope called link mining. Links can show the central rich patterns in exploration of implicit knowledge of available data. Link analysis, relational learning, web mining and graph mining are widely the techniques used in link mining. Through making evaluation models, link mining can be used as applied data mining in wireless networks and plays key role in these networks. Not only network links can be used to explore brilliant actors in a network, but also it can help disclosure of the information discovered related to identity, classes and relations among actors [11].

Privacy Threats

The worries of users about protection of privacy and personal information have been recently considered in type of link mining. In the rest of paper, the tasks of each link mining is described that can be abused by attackers or destructive users.

Relevant Nodes Threats

Wireless network users have many expectations of the privacy. Tracking interactions of users and reconstruction of details based on their behaviors are not usually considered. However, ranking link-based node can be used to measure the effect and importance of wireless network users.

Utilization of the network structure refers to finding the significant relations and determining quantity of users' interactions. Identification of influencing users capable to stimulate other users is very important in many cases [13]. With the increased number of users of social networks, link-based node ranking is used in many fields such as marketing, releasing applied information and governmental data collection tasks.

The consequences of privacy protection through link-based node ranking and cluster link-based node can be related to sensitive information such as membership in a special group or political party. Node and node cluster classification is mainly used in field of computer security. They are beyond a simple case of wireless network and systematic advertisements to achieve sensitive uses such as terrorist networks. In addition to conventional properties of the traits, these activities and interactions of users over the time are the most important databases. These online activities and interactions are available in different forms such as making contacts, messaging and publishing photos [14].

Link-based node clustering technique can be considered as a potential source of privacy threats. They could be used by users of groups with same activity.

Relevant Links Threat

Link prediction can increase privacy concerns and worries when the predicted link is created among users tended to maintain their relationships private. In many cases link can be considered as sensitive information to maintain protected data. The attacks caused by prediction of types of links can be sensitive type of clear existence of two users in privacy that should be protected. Despite to link prediction, link type prediction in protecting privacy is depended on the types of relationship between two users. This kind of attack is identified as link. This happens when an attacker is able to identify the identity of person in the

link between two users [15]. Link can identify accuracy of classified data when the attacker is trying to identify information related to personal interests, physical location and political dependences. For example, friendship links are more important than professional links to find out personal interests; e.g. political dependences and religious beliefs, especially if considerable numbers of friends have displayed such sensitive personal information in their profile.

Graph Dependence Threats

The attack to try to disclose sub-graph to gain new information about unknown network are noted using structural sub-graph.

Sub-graph is effectively useful in similar structures in large wireless networks and could be noted using two main types of attacks: active attacks and passive attacks [16]. In both types of attacks, structural data used to note the actual identity of users are targeted. As a result, attacks of disclosing sub-graph can be used for adjustment of users' privacy and enhancement of identity of audiences and problems with disclosing social links.

CONCLUSION

In this study, a general view of privacy protection in wireless networks is introduced and different concepts of understanding wireless networks are explained. In wireless networks, different analysis methods and link mining techniques are investigated. Among all challenges of social networks, protecting privacy is important for all users. Impossibility of providing good protection of privacy may lead to undesired consequences in popularity of wireless networks and mostly in volume of information shared by users of wireless networks. Therefore, wireless networks' sites have to provide types of supporting and backup instruments to their users.

REFERENCES

1. Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A.: Analyzing facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. IMC '11, pp. 61–70. ACM, New York (2011).
2. Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and security for online social networks: challenges and opportunities. IEEE Netw. 24(4), 13–18 (2010).
3. Newman, M.: The structure and function of complex networks. SIAM Rev. 45(2), 167–256 (2003).
4. Fortunato, S.: Community detection in graphs. Phys. Rep. 486(3–5), 75-174 (2010).
5. Gonzalez-Billon, S.: Opening the black box of link formation: Social factors underlying the structure of the web. Soc. Network 31(4), 271–280 (2009).
6. Mislove, A., Marcon, M., Gummadi, K.P., Druschel, P., Bhattacharjee, B.: Measurement and analysis of online social networks. In: Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement. IMC '07, pp. 29–42. ACM, New York (2007).
7. Zhou, B., Pei, J.: The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks. Knowl. Inform. Syst. 28(1), 47–77 (2011).
8. Liu, K., Terzi, E.: Towards identity anonymization on graphs. In: Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data. SIGMOD '08, pp. 93–106. ACM, New York (2008)
9. Zheleva, E., Getoor, L.: Preserving the privacy of sensitive relationships in graph data. In: Bonchi, F., Ferrari, E., Malin, B., Saygin, Y. (eds.) Privacy, Security, and Trust in KDD.Volume 4890 of Lecture Notes in Computer Science, pp. 53–171. Springer, Berlin.Heidelberg (2008).
10. Getoor, L., Diehl, C.P.: Link mining: a survey. SIGKDD Explor. Newsl. 7(2), 3–12 (2005).
11. Wu, X., Kumar, V., Ross, Q., Ghosh, J., Yang, Q.,Motoda, H.,McLachlan, G., Ng, A., Liu, B., Yu, P., Zhou, Z.H., Steinbach, M., Hand, D., Steinberg, D.: Top algorithms in data mining. Knowl. Inform. Syst. 14(1), 1–37 (2008).
12. Lin, Z., Wang, L., Guo, S.: Recommendations on social network sites: From link mining perspective. In: International Conference on Management and Service Science, 2009. MASS '09, pp. 1–4 (Sept. 2009).
13. Segal, E.,Wang, H., Koller, D.: Discovering molecular pathways from protein interaction Bioinformatics 19(SUPPL. 1), i264–i272 (2003).
14. Adali, S., Sisenda, F., Magdon-Ismail, M.: Actions speak as loud as words: predicting relationships from social behavior data. In: Proceedings of the 21st International Conference on World Wide Web. WWW '12, pp. 689-698. ACM, New York (2012).
15. Zheleva, E., Getoor, L.: Preserving the privacy of sensitive relationships in graph data. In: Bonchi, F., Ferrari, E., Malin, B., Saygin, Y. (eds.) Privacy, Security, and Trust in KDD. Volume 4890 of Lecture Notes in Computer Science, pp. 53–171. Springer, Berlin.Heidelberg (2008).
16. Hay, M., Miklau, G., Jensen, D., Towsley, D., Li, C.: Resisting structural re-identification in anonymized social networks. VLDB J. 19(6), 797-823 (2010).

How to cite this article: Azadmanesh M. Investigation of the Wireless Networks and Private Security. Int J Sci Stud 2017;5(4):849-853.

Source of Support: Nil, **Conflict of Interest:** None declared.