Available online at http://www.journalijdr.com

IJDR

ISSN: 2230-9926

International Journal of Development Research
Vol. 08, Issue, 05, pp.20264-20267, May, 2018

ORIGINAL RESEARCH ARTICLE OPEN ACCESS

SECURITY ASPECTS IN SOCIAL NETWORK - A ROUGH SET APPROACH

*Dr. Panda, B.S. Alok Kumar Jena and Ashalata Nayak

Department of Computer Science & Engg., MITS, Rayagada, Odisha, India

ARTICLE INFO

Article History:
Received 24th February, 2018
Received in revised form
20th March, 2018
Accepted 27th April, 2018
Published online 28th May, 2018

Key Words:
Social Network,
Privacy, Rough Set,
Attack Detection.

ABSTRACT

Social networks come in many different facets. Some are strong in a particular geographic location like Orkut in Brazil, VKontakte in Russia, or Mixi in Japan. Others are well known globally, like Facebook and Twitter. Depending on the user base, there are specialized or focused groups LinkedIn and Xing have a business-oriented focus enabling people to share business contacts and job offerings. Other networks specialize in keeping in touch with your old friends from high school.The fast development of interconnections among computer systems, network-basedcomputer systems are playing increasingly vital roles in modem society. They becomethe targets of security and privacy issues of modern technology. Network security is becoming amajor challenge. In order to meet this challenge, the rough set technique (RST) to protect network information systems. The notion of rough sets as a model to capture impreciseness in data was introduced by Pawlak(1). Scientific study of social network data can reveal many important behaviors of the elements involved and social trends and provides insight for suitable changes in the social structure and roles of individuals in it. As more and more rich social media, popular online social networking sites and various kinds of social network privacy in social networks becomes a serious concern. When social network data is made public in one way or other, it is far from sufficient to protect privacy by simply replacing the identifying attributes.

Citation: Dr. Panda, B.S. Alok Kumar Jena and Ashalata Nayak, 2018. "Security aspects in social network - A rough set approach", *International Journal of Development Research*, 8, (05), 20264-20267.

INTRODUCTION

Social Network Security is a perception to preserve network and data transmission over wireless network. Data Security is a challenging affair of data communications today that touches many areas including defend communication channel, strong data encryption technique and trusted third party to control the database. The rapid development in information technology, the protected transmission of confidential data herewith gets a great accord of attention. The conventional methods of encryption can only manage the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is crucial to apply effective encryption/decryption methods to enhance data security. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. User's choice is assigned ID and password or other authenticating information that al lows them access to information and programs within their authority.

Network security includes a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It guards the network, as well as defends and overseas operations being done. The most common and simple way of insulating a network resource is by assigning it a unique name and a corresponding password. Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name i.e. the password, which is something the user 'knows this is sometimes termed as one-factor authentication. Communication between two hosts uses a network that may be encrypted to manage Social privacy (Pawlak, 1991). Rough set theory is a major mathematical procedure developed by Pawlak in 1982.

Corresponding author: Dr. Panda, B.S.,
Department of Computer Science & Engg. MITS, Rayagada, Odisha, India.

This rule has been developed to manage uncertainties from information that presents some inexactitude, incompleteness and noises. When the available information is insufficient to determine the exact value of a given set, lower and upper approximations can be used by rough set for the representation of the concerned set. The approximation synthesis of approach from the acquired data is the main objective of the rough set analysis. RST has been applied in several fields including image processing, data mining, pattern recognition, medical informatics, knowledge discovery and expert systems. In the current literature, several research works have been combined to the rough set theory with other artificial intelligence methods such as neural networks, fuzzy logic, additionally to other methods resulting in some good results. The use of rough set theory to solve a specific complex problem has attracted world-wide attention of further research and development.

Related Works

Pawlak, 2004 proposed the operations on sets, approximate equality sets, and approximate inclusion of sets. Wang, *et al.,* 2005 firstly discussed the complications of network security and intrusion, and then some data –mining-based processes were disinterred to settle these dilemmas. Rough set based new techniques such as data reduction, incremental mining, uncertain data mining, and initiative data mining were recommended for intrusion detection systems. Zhao and Zhu 2005 described the effects of spam on network. It proposed a new scheme based on decision theoretic rough sets to classify emails into three categories – spam, no-spam, and suspicious. By comparing the anti-spam filter model reduced the error ratio that a non-spam is discriminated to spam and the potential security problems of some email systems. Li and Yang 2009 proposed a model of network security assessment based fuzzy sets and rough sets. The rough sets and the fuzzy sets were combined to find out the association rules in network security. In this the connection degree in set pair analysis was applied into rough sets. The data were done fuzzy clustering firstly and then the assessment rules in network security were extracted based on fuzzy sets and rough sets. Liu, *et al.,* 2012 proposed a network security events correlation scheme based on rough set, build database of network security events and knowledge base, gives rule generation rule and rule matcher. This technique solved the simplification and correlation of massive security events through combining data discretization, attribute reduction, value reduction and rule generation. Wang and Gui 2012 innovated a process to improve the computation accuracy and the efficiency of the classification computation by using Rough set combined with SVM classifier. Chowdhuri, *et al.,* (2014) proposed the ad hoc routing protocol's design was used in order to detect the unpredictable and rapid mobility of a node. It was created dynamically without any infrastructure. In ad hoc each node was responsible for routing the information between them. Roy *et al.,* 2014 proposed that how rough-set theory helped in very fast convergence and in avoiding local minima problem, thereby enhancing the performance of the EM. During rough-set-theoretic rule generation, each band was individualized by using the fuzzy-correlation-based thresh holding.

Types Attacks in Social Media

Scams; Scams are everywhere - you get them in the mail, through email, and now also on social media sites. It doesn't really matter if you're using Facebook, Twitter, or any other social media site, you'll eventually run into a scammer (Markus Huber and Martin Mulazzani, 2010).

Malicious Apps: Malicious apps, spyware, and viruses have made their way onto social media and into related apps as well. While it's not easy to pass viruses through Facebook or LinkedIn, it's easier for hackers to compromise the apps your employees may have on their smartphones that allow them to post to these sites. This is especially true if employees are using third-part apps.

Social Network Issues: Social networking sites themselves still have a way to go with security. While these sites have certainly improved their security over the years, none of them are perfect or locked down so tight that no one can hack them (Michael Lang *et al.,* 2009).

Untrained Employees: All of the above vulnerabilities aren't as significant an issue if your employees how, and how not, to use social media for business. This is why social media training is so important your employees need to know about the dangers of using social media for anything confidential.

A Lack of Social Media Policies: Training employees leads into the need for strong social media policies. If you don't have any policies regarding how Facebook, Google+, and other sites can be used in the office, you can't effectively train your employees in how to avoid potential security breaches. These policies should cover a number of things: employee use of personal social media at the office, smartphone app use, and use of the company's social media site for publicity and customer engagement (EsmaAimeur *et al.,* 2010). Rough set theory is a technique deals with uncertainty. In this section we reintroduce some basic notations of Rough set theory (Pawlak and Skowron, 2007).

- $U\ (\neq \phi)$ is the universe and be a finite set of objects.
- R is the indiscernibility relation, or equivalence relation over U.
- Indiscernibility is the inability to distinguish between two or more values.
- A= (U, R) an ordered pair is called an approximation space.
- $[x]_R$ denotes the equivalence class or R containing an element $x \in U$.
- For any subset $\mathrm{P}(\neq \phi) \subseteq \Re$, the intersection of all equivalence relations in P is denoted by $IND(\mathrm{P})$ and is called the indiscernibility relation over P.
- Elementary sets in A – the equivalence classes of R.
- Definable set in A–Any finite union of elementary sets in A.
- For any $X \subseteq U$ and an equivalence relation $R \in IND(K)$, there associate two subsets:
- Lower approximation of X in A is the set $\underline{R}X = \bigcup\{Y \in U/R : Y \subseteq X\}$

The elements of $\underline{R}X$ are those elements of U which can be certainly classified as elements of X with the knowledge of R.

- Upper approximation of X in A is the set $\bar{R}X = \bigcup\{Y \in U / R : Y \bigcap X \neq \phi\}$

$\bar{R}X$ is the set of elements of X which can be possibly classified as elements of X employing knowledge of R

- The boundary of X is, $\bar{R}X - \underline{R}X$.

The elements of $\underline{R}X$ are those elements of U,

Rank	Network	Number of Users (in millions)	Monthly Visits (in millions)
1	facebook	901	7012.9
2	twitter	555	182.1
3	Google+	170	61
4	LinkedIn	150	85.7
5	Pinterest	11.7	104.4

Fig. 1. Five biggest social networking sites

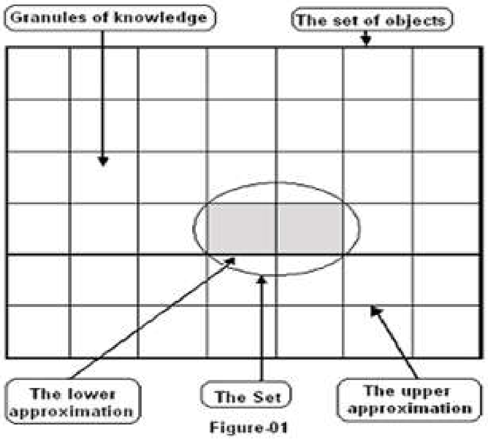

Fig. 2. Rough Set Approach

Junk email detection using RST

It is very essential to eliminate unsolicited emails or junk emails. Rough set based filters can be utilized to perceive junk emails on the Internet. One major procedure is to construct filters in email reassign route. Numerous junk email filters hadn't finished exercise of the entire security information in an email, which subsisted mostly in the junk email header not in the text and attachment. Below are certain guidelines for email headers which are helpful for judging whether an email is junk or not condition attributes and one decision attribute are described as follows.

Condition Attribute

- Amount of "Received" fields which is the times of email relaying. One "Received" per relay.
- Amount of addressees.
- Amount of email route disruption. For example, it's a route disruption when the IP address in the former "Received" field and receiver's domain name are dissimilar from those in the concluding "Received" field;
- Amount of divergence between the domain name and its consequent IP address. This attribute is quite significant.
- Amount of no domain name of the sending host after "from" in the "Received" field.
- Amount of no domain name of receiving host after "by" in the "Received" field.
- Amount of no IP address of sending host after "from" in the "Received" field.
- Whether the original sender address in the "From" field is accordant with that in the "Received" field the original sender address is given in the previous "Received" field after the "from" or "by".
- Whether the target address in "To" field is accordant with that in the "Received" field the final is the actual receiver.
- If "Delivered-To" field subsists, whether it is accordant with the "To" field its default value is 1 that is yes.
- If "Return-Path" field subsists, whether it is accordant with the "From" field its default value is 1 that is yes.

Decision Attribute

Legitimate emails value is denoted by 1 and junk emails value is denoted by 2 irrespective of its type. There are several processes to mine knowledge from a decision table, such as Preprocessing of data, including dealing with values of missing attributes, discretization of data. Attribute reduction. Value reduction. Some useful knowledge about detection of junk email can be obtained from email headers. Our simulation results demonstrate that when mining on selected baleful email corpus, the filter has high efficiency and high identification rate.

Other rough-set-related methods for network security

Another procedure was represented for anomaly intrusion detection with reduced cost and high efficiency (Cai *et al.,* 2003). It extracts detection rules using rough set algorithm from the system call sequences generated during the normal execution of a process and considered as the normal behavior model. It is capable of detecting the abnormal operating status of a process and thus reporting a possible intrusion. Compared with other methods, it requires a smaller size of training data set and less effort to collect training data and is more suitable for real-time detection. Empirical results show that this method is promising in terms of detection accuracy, required training data set and efficiency. Not only rule generation based on rough set theory can be used for network security, but other perception may also be useful. For example, rough inclusion is used for matching of normal behaviors and abnormal behaviors (Li *et al.,* 2003). We conclude that rough set method is suitable and promising for network security.

Misuse Detection

- Misuse detection sets up the attack behaviours based on known attack behaviours during thedevelopment stage. The misuse detection is similar to antivirus software. The antivirus software.
- Compares the scanned data with known virus code. If system finds un-normal attributes, thevirus is existence and removes it. Hence, misuse detection collects the known attack behaviours.

- If the attack behaviour is similar to the one in database, the misusedetection can defend it before the intruder destroys our system.

Anomaly Detection

- Anomaly detection (Simmonds *et al.,* 2004) is different from misuse detection. The system constructs user modelbased on normal users have behaviours. When user has misbehaviours, the system.
- Notifies users that has an intruder. The main drawback of anomaly detection is that thedetection is depended on the latest attack models, so it can't identify new attack behaviours. The intruder attack methods will be changed, so anomaly detection system collects normal behaviours and detects intruding using normal behaviours. The anomaly detection system has a party with clearly defined correct user behaviours. The problemis intruder uses normal behaviours to attack the system.

Conclusion

Social networking communities are an inherent part of today's Internet (Panda *et al.,* 2009). People love using them to stay in contact with friends, exchange pictures, or just to pass the time when bored. Companies have also discovered social media as a new way of targeting their customers with relevant information. With user groups with hundreds of millions of members, there are always some black sheep with malicious intent. We have seen many worms spread through social networks. In most cases they have used social engineering tricks to post enticing messages on behalf of an infected user. Social networks (Wang *et al.,* 2006) definitely can be fun, but users should be aware of the risks and behave with the needed level of skepticism, just like anywhere else.

REFERENCES

Pawlak, Z. 1991. Rough sets, in: Theoretical Aspects of Reasoning about Data, Kluwer Academic Publishers, Dordrecht, 1991.

Panda, G. K. and Panda, B. S. 2009. "Preserving privacy in social network with covering based approximations of classifications" In: Proceedings of NCACNIT-09, *GJ University of Sc. & Tech.,* Hissar, India, pp. 525-530.

Pawlak, Z. 2004. Some Issues on Rough Sets. Transactions on Rough Sets, vol. 1, pp. 1-58.

Wang G., Chen L. and Wu, Y. 2005. Rough Set Based Solutions for Network Security. Monitoring security and Rescue Techniques in Multiagent Systems Advance in Soft Computing Volume 28, pp 455 -0465.

Zhao, W. and Zhu, Y. 2005. An Email classification scheme based on decision –Theoretic Rough Set theory and Analysis of Email Security.

Li, R. and Yang, Y. 2009. Network Security Assesement Based on Fuzzy stes and rough sets.Wireless Communications , *Networking and Mobile Computing*, WiCom '09. 5th International Conference.

Liu, J., Gu, L., Xu, G. and Niu, X. 2012. A Correlation Analysis Method of Network Security events based on rough Set Theory. Network Infrastructure and Digital Content (IC – NIDC), 3rd IEEE International Conference.

Wang H.S. and Gui X.-L. 2012. A Network Security Model Based on Machine Learning. Control Engineering and Communication Technology (ICCECT), International Conference.

Chowdhuri, S., Roy, P., Goswami, S., Azar, A. T. and Dey N. 2014. Rough Set Based Ad Hoc Network : A Review. 66 *International Journal of Service Science, Management, Engineering, and Technology,* 5(4), 66-76.

Roy, P., Goswami, S., Chakraborty, S., Azar, A. T. and Dey, N. 2014. Image Segmentation Using Rough Set Theory:A Review. *International Journal of Rough Sets and Data Analysis,* 1(2), 62-74.

Markus Huber, Martin Mulazzani, Edgar Weippl 2010. "Social Networking Sites Security: Quo Vadis" IEEE International Conference on Privacy, Security, Risk and Trust.

Michael Lang, Jonathan Devitt, Sean Kelly, Andrew Kinneen, John O'Malley, Darren Prunty, 2009. "Social Networking and personal Data Security: A Study of Attitudes and Public Awareness in Ireland" 2009 International Conference on Management of e-Commerce and e-Government.

EsmaAimeur, SebastienGambas, 2010. Ai Ho "Towards a Privacy-enhanced Social Networking Site" 2010 International Conference On Availability, Reliability and Security.

Pawlak, Z. and Skowron, A. 2007. Rough sets some extensions. *J. Information Sciences*, 177(1), 28-40.

Cai Z. M., Guan X. H., Shao P., Peng Q. K., Sun G. J. (2003) A rough set theory based method for anomaly intrusion detection in computer network systems. Expert Systems Vol.20 (5), pp251–259.MATHView Article.

Li, X. J., Huang, Y. and Huang, H. K. 2003. An Computing Immune Model based on Poisson Procedure and Rough Inclusion. *Chinese Journal of Computers,* Vol.26(1), pp.71–76.

Simmonds, A., Sandilands, P. and Van Ekert, L. 2004. Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.

A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

Wang, D. and Liau, C. and Hsu, T. 2006. Privacy Protection in Social Network Data Disclosure Based On Granular Computing. In: Proceedings of IEEE International Conference on Fuzzy Systems, Vancouver, BC, Canada. 2006.

****