JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DDOS ATTACKS WITHIN COMPLEX NETWORK: A COMPREHENSIVE ANALYSIS OF SOCIAL MEDIA

Sheetu Bala*a , H.O.D. Harjinder kour*b

a* (Email Address – er.sheetudnn@gmail.com)

SSGI Dinanagar G.T.Road Near Dayanand Math, Dinanagar, Punjab 143531

b*(Email Address – harrysaini988@gmail.com)

Head of Department SSIET, Dinanagar

Abstract

Social media nowdays become heart and soul of modern world. Peoples who are far away from each other interact with each other using this medium. Social network forms the complex network as its size grows beyond bar and is exposed to attacks. Most common attack in social media is clone attack. This paper provide in depth analysis of clone attack along with techniques used to tackle this type of attack. Comparative analysis also suggests the best possible mechanism that can be selected for future enhancements.

Keywords

Social Media, Complex Network, Clone Attack, Techniques

1. Introduction

Social media provide mechanism to interact distinct persons that are near and far effectively. People can interact in a manner as if sitting in front of each other and talking. Both online as well as offline communication are supported by the use of social media. Connection between the users in such a network is represented with the help of a graph. The users in this case are termed as nodes and links connecting them are known as edges. The links between the nosed could be multivariate in nature. As the users of the social media increases, so do the attacks. Most common attack present over the social media is clone attack.

Clone attack causes the replication of user profile. This will cause the critical information to be accessible to unauthorised user. Trust is at stake by the application of clone attack. The definition of clone attack is as under

Definition: Clone attack on social media primarily deals with the profile clone where information associated with the single user is copied and used by unauthorised user.

Cloning attack is one of the insidious attacks in facebook. Usually attackers stole the images and personal information about a person and create the fake profile pages. Once the profile gets cloned they started to send a friend request using the cloned profile. In case, if the real users account gets blocked, they used to send a new friend request to their friends. At the same time cloned one also sending the request to the person. At that time it was hard to identify the real one for users.

2. Clone Attack DetectionMechanisms

There are techniques used to detect clone attacks within the social media. Complex network considered as a connected graph which if contains a cycle leads to the cloning. Clone detection becomes critical to enhance trust levels of users. Clone detection techniques analysis is primary objective of this paper which is given as under

2.1 Component Based Clone attack detection

Clone attack detection methodology is proposed by (Kontaxis et al. 2013). The framework employed by Kontaxiset. Al can be used by the users to determine whether they are under clone attack or not. The components employed in this framework involves

a. Information distiller

This component is used in order to extract the information from legitimate social networking site. Information that could be used to identify the user is extracted by this component and maintained within the buffer.

b. Profile Hunter

Profile hunter used to locate the profile of the users. In case multiple records corresponding to single user is fetched then clone attack is detected.

c. Profile verifier

This component verifies the records filtered by profile hunter. The filtered information is compared against the profile of the user to find the nearest matches. In case matches do occur, profile clone attack is detected.

2.2 User Footprint Analysis

User footprint analysis is proposed by (Malhotra n.d.). User may have multiple accounts over the various services over the internet. All the services over the internet uses digital mechanisms. All these digital footprints can be collected together to determine the profiles of the users consuming multiple web services.

2.3 Topological Feature extraction

Topological feature extraction mechanism is proposed by (Bhat & Abulaish 2014)for clone attack detection. In clone attack detection, earliest techniques assume that distinguished keywords are used by malicious users. But this may not be the case all the time. in order to tackle the situations, features like images, topological features etc. must be analysed. Topological analysis allow the user to construct the profile on the basis of heterogeneous features hence producing accurate result associated with the clone attack.

2.4 Attribute Similarity Mechanism

The clone attack detection techniques as proposed by (Dave et al. n.d.) can be considered for such attack resolution. According to Dave et. Al., attack can either be on the access restricted information and anonymous data attacks. To tackle the situations attributes similarity based privacy preservation solutions are proposed. Several techniques corresponding to attribute similarity are used in order to determine the clone attacks.

2.5 Architectural Based Clone Attack Detection

Social networking is one of the most widely used internet activity as proposed by (Kontaxis et al. 2013). it is prone to profile clone attacks and its preservation is compulsory. Kontaxis et al proposed mechasnism for detection of profile clone attacks by the use of archituctural design and prototype system for detecting similarity of attributes in case profile of the user is copied. Experiment result shows better result of clone attack detection hence proving worth of the study.

2.6 Graph Based Clone Attack based Technqiues

Clone attack is a problem over the online social media. Detecting and preserving the state of the online social media is a need of the hour. Online social media plays a role of complex network. **To detect the profile cloning attacks from such**

a network technique has been proposed by (Kharaji & Rizi 2014)**.** Entire social media is diided into tow parts. First part considered and dra the social network as a graph. In the second part, graph is divided into subparts based on the similarity of profile. The modular approach considered ultimatley led to the formation of smaller networks consisting of only those nodes having similar characterstics or properties thus facilitate detection of clone attacks. Online social media is a huge network of users. As the uers of the online social media grows, so does the chances of clone attack. To detect the clone attack a new approach for clone attack detection is proposed by (Rizi et al. 2014). Clone attacks causes the similar profiles from one or more users. In order to determine the similarity, strength of suers profiles matching is determined. The strength determines profile clone attack by the said mechanism. degree of modularity achieved through this technqiue is not perfect and required certain degree of modifications.

3. Comparison Table

Comparison of various techniques is presented in this section corresponding to clone attack detection. This comparison can be used to select the technique that can be used in future for optimised results.

Authors and Year	Techniques	Attack Detected	Merit and Demerits
(Barbera & Mei 2012)	Personal Marks and certificates	Clone Attack	Personal Marks and certificates can accurately detect the clone attack but overall execution speed is low
(Freeman & Hwa n.d.)	Supervised machine Learning	Clone Attack	Multiple fraud accounts by the same user can be identified however modularity could be further improved
(Kharaji & Rizi 2014)	Graph based Approach	Clone Attack	Graph based mechanism to detect clone attack is used. Cycle within graph indicate clone but poor modularity could be an issue
(Kontaxis et al. 2013)	Component based Clone attack Detection	Clone Attacks	Module based approach ensures complexity is reduced in detection process. Modularity and slow rate could be problem in this work
(Malhotra n.d.)	User Foot prints	Clone Attack	Multiple user profiles can be easily analyzed using this approach. Complexity of the

			system increases as the size of profile analyzer increases.
(Tsikerdekis & Zeadally 2014)	Nonverbal Behavior	Multiple Identities Clone attack Detection	Non verbal behavior techniques is implied which gives result faster but it may not be accurate in all situations
(Egele et al. 2015)	Detection using similarity profile check	Clone Attack	Suited only for high profile accounts while low profile attacks are difficult to identify
(Wu et al. 2017)	Social Norm Incentives	Sybil attacks in networks	Suitable for small networks but is not suited for complex networks
(Anjos et al. 2014)	Attack detection using face recognition	Photo Attack detection	Used only for photo attack in social media
(Amerini et al. 2011)	Copy move attack	SIFT Based mechanism for attack detection	Can be implied on large image sets but not tested on textual information
(Shi et al. 2017)	Event attack detection	Event detection in social media	Fixed datasets or static datasets uses produce effective results but dynamic datasets still not checked

Table 1: Comparison of techniques used for clone attack detection

Detection mechanism lacks application of learning mechanisms so to tackle the situation, machine learning can be incorporated within the clone attack detection for better performance.

4. Our Contribution

In future, community overlapping mechanism can be used to determine the clone attacks. the community overlapping is the mechanism in which same communities are liked by multiple distinct users. By the application of community overlapping detection, clusters of same liking communities are formed. Once clusters of similar likings are formed, analysis of clone attack is limited to selected cluster only. Thus reducing time complexity in detection of clone attack.

Thus Community overlapping in the field of clone attack detection could be future course of action for obtaining better results.

5. CONCLUSION AND FUTURE SCOPE

From the analysis conducted we conclude that the attack is a common problem in the field of online social media. The steps must be taken in order to prevent the deception. The cause of clone attack is lack of structure to ensure that only

valid users can enter into the system. The proper validation mechanisms are missing since the OSN is typically concerned about the length of the database rather than security of the system. This is a prime factor which is leading to the profile clone attacks.

In the future some sort of security mechanisms must be enforced to ensure the validity of the user. This can be accomplished by the use of community overlapping along with clone attack detection methodology to prevent clone attacks.

6. REFERENCES

Amerini, I. et al., 2011. A SIFT-Based Forensic Method for Copy – Move Attack Detection and Transformation Recovery. , 6(3), pp.1099–1110.

Anjos, A., Chakka, M.M. & Marcel, S., 2014. Motion-based counter-measures to photo attacks in face recognition. , (November 2012), pp.147–158.

Barbera, M. V & Mei, A., 2012. Personal Marks and Community Certificates : Detecting Clones in Wireless Mobile Social Networks.

Bhat, S.Y. & Abulaish, M., 2014. Communities A gainst Deception in Online Social Networks 1 The Platform 2 The Mischef. , 2014(2), pp.8–16.

Dave, D., Mishra, N. & Sharma, S., Detection Techniques of Clone Attack on Online Social Networks : Survey and Analysis. *Elsevier*, pp.179–186.

Egele, M. et al., 2015. Towards Detecting Compromised Accounts on Social Networks. , 5971(c).

Freeman, D.M. & Hwa, T., Detecting Clusters of Fake Accounts in Online Social Networks Categories and Subject Descriptors.

Kharaji, M. & Rizi, F., 2014. An IAC Approach for Detecting Profile Cloning in Online Social Networks. , 6(1), pp.75–90.

Kontaxis, G. et al., 2013. Detecting Social Network Profile Cloning. *IEEE*.

Malhotra, A., Studying User Footprints in Different Online Social Networks.

Rizi, F.S., Khayyambashi, M.R. & Kharaji, M.Y., 2014. A New Approach for Finding Cloned Profiles in Online Social Networks. , 6(April), pp.25–37.

Shi, L. et al., 2017. Event Detection and User Interest Discovering in Social Media Data Streams. , 3536(c).

Tsikerdekis, M. & Zeadally, S., 2014. Multiple Account Identity Deception Detection in Social Media Using Nonverbal Behavior. *IEEE Transactions on Information Forensics and Security*, 9(8), pp.1311–1321. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6843931 [Accessed February 25, 2016].

Wu, C., Gerla, M. & Schaar, M. Van Der, 2017. Social Norm Incentives for Network Coding in MANETs. , pp.1–14.