ATTACK DETECTION STRATEGIES IN WIRELESS SENSOR NETWORK

Manbir kaur[1], Tejinderdeep singh[2], Sapinder kaur[3]

[1]Student, Dept of Computer Science Engineering, GIMET Amritsar, Punjab, India
[2,3] Assistant Professor, Dept of Computer Science Engineering, GIMET Amritsar, Punjab, India

Abstract - *Today WSN play very important role in the communication process. With the help of WSN number of tasks is being accomplished. Normally social media is used to sell products, Career Consultancy, Communication, sharing resources etc. Along with the advantages there are number of disadvantages of the social media also. WSN uses number of mechanisms to create users. And increase their database. But they do not ensure validity of information provided by the user. This will cause the deception or attacks. Attacks or Deception will cause number of problems. There are number of types of deceptions or attacks which exist over the internet. Deception model is prepared in order to analyze these problems. Some of the deceptions are difficult to detect than the others. Some of the challenges which WSN must address are considered in this paper.*

***Key Words*: Deception, wsn, Internet**

1. INTRODUCTION

With the growth of the internet social media growth is increased. (Bu et al. 2015)[1]The social media is used for wide variety of purposes. WSN is used to share user generated contents to large number of other users. With that the number of services provided by the social media also increases. With the advent of technology the deception also has been increased. Deception is caused due to falsifying information provided by the user. (Aprem & Krishnamurthy 2016)[2]WSN provide new environment for the deceivers to perform illegal tasks over the internet. The main cause of deception is that it is very easy to create account over the social media like Facebook, Twitter etc. No verification of records is done in case of the social media. They are just consider the increase of database and do not consider deception.

In this paper we consider or attack deception as the deliberate attempt to provide falsifying information to conduct harm over the network. (Zhou 2011)[3]The problem is extravagated since receiver does not know about the deception. Because of which receiver privacy will be on the stakes. The private information of the receiver will be determined by the deceiver. These false beliefs are transferred through verbal and non verbal communications.(Kiruthiga 2014)[4] Clone attacks are common source of deception over the social media. Rest of the paper is focused on determining clone attack detection strategies which result in redundant information or users over the social media.

2. BACKGROUND ANALYSIS

Techniques are devised to check the falsifying information provided by the user in order to achieve desired goals. These techniques are discussed in detail in this section.

2.1 Centralized Detection Techniques

(Grewal & Scholar 2015) Central authority is established in detection and prevention of clone attack in social media. Mainly this application is deployed in sensor networks but due to heavy traffic associated with the social media need for centralized detection comes into place. Under centralized detection following techniques appear

A1: Straightforward approach[5]

(Khabbazian et al. n.d.) In this approach every node in the network send the information towards the neighbor and neighbor in turns send the information towards the base station. The base station scan all the relevant information from the recived report and if conflicting position information is spotted then message is conveyed to all the nodes in the network.[6]

A2: Set operations

(Solanki 2016) Another method of detection is the set operations. this mechanism reduces the number of transmitted packets hence overhead is considerably reduced by the use of set operations. in this mechanism duplicity from the subset is detected and removed. This technique is cost effective but also disallow some of the critical packet transmission. [7]

A3: Cluster based approach

(Wang & Zhang 2007) Cluster based approach is based on attribute similarity. The data being transmitted is analysed for similarity based on properties they have. In case of similar attributes disclosure, the information is packed in a common group known as cluster. Cluster contains information of similar sort hence these are homogeneous clusters. Threshold value upon the number of attributes similarity is maintained. In case similarity index exceeds threshold value, clone attack is detected. Heterogeneous cluster is not worked upon in existing literatures as yet. [8]
A4: Replicated Key Detection

(Ren et al. n.d.) This is the process in which key generated through cryptography process is analyzed for redundancy. The data transmitted in such fashion is secured and difficult to analyze. In order to detect replicated keys, extra storage is required at data centers. The upcoming key is compared against the incoming keys. The incoming keys if similar, replication is detected so does clone attack. [9]

2.2 Distributed Detection techniques

These are the techniques which do not rely on the centralized authority to check for the abnormality. Watcher nosed are established in order to check for the anomalies. Under distributed techniques following mechanisms appear B1: Content Based Filtering.

(Devi & Poovammal 2016) Content based filtering mechanism is used to detect the abnormal material among the transmitted contents. The social media is prone to large number of users having large number of data associated with them. Content filtering mechanism maintains a word count register, containing the total number of words to be transmitted. After transferring the word, word count register is decremented by one. After word count register reaches 0, words to be transmitted still pending is analyzed. In case any word is still left, that indicates malicious entry. Some work towards saving time is still required to be accomplished. [10] B2: Attributes Based Filtering Mechanism.

(Dave et al. n.d.) Attributes are the properties associated with the content being transmitted. Attributes of use must be transmitted with integrity check. Primary key is implied over the attributes being transmitted. The attributes values cannot be redundant and also it cannot be null. Problem with the attribute based approach is attribute similarity is checked but content is not purified. [11]

Both content based and attribute based approaches commonly used with the applications of recommender system.

3. Comparison Of Various Techniques for clone attack detection

The comparison table for detection of clone attack is given as under

Authors and Year	Techniques	Attack Detected	Merit and Demerits
(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 attack detection strategies

4. CONCLUSION AND FUTURE SCOPE

From the analysis conducted we conclude that the deception is a common problem in the field of online social media. The steps must be taken in order to prevent the deception. The causes of deception 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 deception.

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 background check mechanisms to prevent clone attacks.

REFERENCES

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

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

[3] Aprem, A. & Krishnamurthy, V., 2016. Utility Change Point Detection in Online WSN : A Revealed Preference Framework. , (c), pp.1–12.

[4] Bu, K. et al., 2015. Deterministic Detection of Cloning Attacks for Anonymous RFID Systems. , 11(6), pp.1255–1266.

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

[6] Devi, J.C. & Poovammal, E., 2016. An Analysis of Overlapping Community Detection Algorithms in Social Networks. Procedia - Procedia Computer Science, 89, pp.349–358. Available at: http://dx.doi.org/10.1016/j.procs.2016.06.082..

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

[8] Grewal, R. & Scholar, P.G., 2015. A Survey on Proficient Techniques to Mitigate Clone Attack in Wireless Sensor Networks. , pp.1148–1152.

[9] Khabbazian, M., Mercier, H. & Bhargava, V.K., Wormhole Attack in Wireless Ad Hoc Networks : Analysis and Countermeasure.

[10] Kiruthiga, S., 2014. Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques.

[11] Ren, Y., Chen, Y. & Chuah, M.C., Social Closeness Based Clone Attack Detection for Mobile Healthcare System.

[12] Shi, L. et al., 2017. Event Detection and User Interest Discovering in WSN Data Streams. , 3536(c).

[13] Solanki, S., 2016. Related Study of Soft Set and Its Application A Review. , 7(4), pp.15–22.

[14] Tsikerdekis, M. & Zeadally, S., 2014. Multiple Account Identity Deception Detection in WSN 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].

[15] Wang, W. & Zhang, Y., 2007. On fuzzy cluster validity indices. Fuzzy Sets and Systems, 158(19), pp.2095–2117.

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

[17] Zhou, H.W.J.L.L., 2011. Lightweight and effective detection scheme for node clone attack in wireless sensor networks. , (December 2010), pp.137–143.