International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(1), pp.390-393
DOI: http://dx.doi.org/10.21172/1.101.71
e-ISSN:2278-621X

COMPREHENSIVE ANALYSIS OF TECHNIQUES USED TO DETECT ATTACKS IN WIRELESS SENSOR NETWORK

Sumandip Kaur[1], Meenakshi Sharma[2]

Abstract- Complex network deals with uncovering hidden information and links affecting the performance of the network. Complex network like WSN includes large amount of users with varying set of intentions. Frauds with such network degrade the performance of network due to link and node failure. Various kinds of major attacks have been documented in wireless sensor network, till now by many researchers. Wireless sensor network used to transfer the information in terms of packets from source towards destination by the application of malicious users, content transfer is at stakes. Attacks such as clone attack are common in such situations. Clone attacks are very harmful attacks against the wireless network. In order to tackle the issue graph based and overlapping community detection mechanisms are used. The techniques both iterative and direct approaches are researched over for the detection and prevention of such failures. This paper present the analysis of techniques used to detect and prevent such failures. The qualitative comparison between techniques is also present to select the optimal technique for future enhancement.

Keywords – Complex Network, Wireless sensor network, Frauds, Link, node

1. INTRODUCTION

A wireless sensor network (WSN) is an interconnected arrangement of a vast set of physically small, ease, low power sensors that give ubiquitous detecting and processing abilities. The sensors can detect the environment in different modalities, process the data and scatter information wirelessly. Along these lines if the capacity of the wireless sensor network is appropriately harnessed, it is imagined that the wireless sensor network can diminish or even kill the requirement for human association in data assembling in broad civilian and military applications, for example, national security, social insurance, condition assurance, vitality protection, nourishment preservation, movement administration and so on. Since sensor hubs are conveyed in threatening situations, attackers can without much of a stretch infuse pernicious information or can change the substance of honest to goodness messages during multi-hop sending inferable from the idea of wireless correspondence in sensor networks. Along these lines WSN is helpless against numerous dangers, among which hub clone attack is unsafe one. An enemy can catch couple of hubs, extract the codes and every single mystery certification and utilize those materials to clone numerous hubs out of off-the-rack sensor equipment. At that point those hubs that appear to be authentic can join the system and cause extreme harms. It can even dispatch denial-of-service (DoS) attacks to real hubs by diminishing their offer of the resources and giving the attackers more resources to perform different attacks.

Complex network like social media is critically analysed for detection any malicious activity.[1] Users of social media continuously growing. Network behaviour analysis depends greatly upon the size of the user clusters. [2]As the users of the network grows, so does the chances of frauds. Fraud detection thus becomes need of the hour for efficient and effective working of the system. [3]Social media is great way to make people interact with each other which are remote in nature. As more and more users interact with the social media, frauds become common due to indifferent behaviour of users. [4]To examine the frauds, frauds detection techniques are devised. Techniques corresponding to natural language processing is used commonly for fraud detection.

[5]Fraud detection is critical in complex network since it may lead to spreading of infection among community leading to epidemics. [6]In case of electrical networks, the problems within the electricity flow can be determined be examining community structure of electricity system. Today information explosion causing the size of network grows beyond bars. In order to tackle frauds, community overlapping detection within social media is required.

Some of the more common attacks against sensor network privacy are:

1.1 Monitor and Eavesdropping:

This is the most widely recognized attack to security. By intruding to the information, the adversary could without much of a stretch find the correspondence hub substance. At the point when the routing passes on the control data about the sensor

[1] Student Department of computer science engineering, Global institute of management emerging and technology, Amritsar, Punjab, India

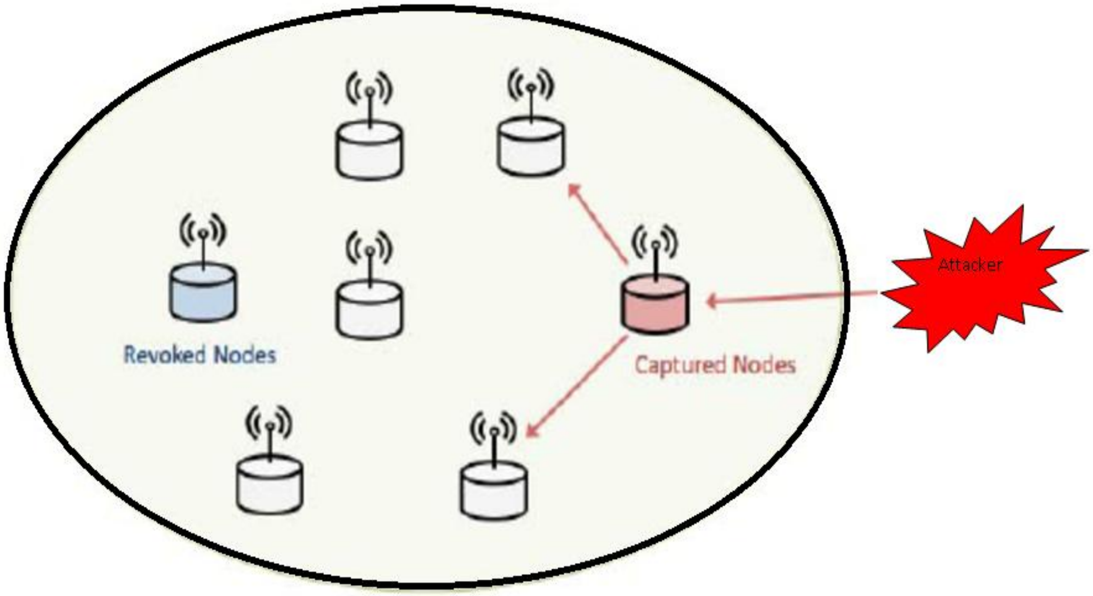
[2] Prof. Department of computer science engineering, Global institute of management emerging and technology, Amritsar, Punjab, India

network configuration, which contains likely more definite data than available through the area server, the listening in can act against the security approach successfully.[7]

1.2 Traffic Analysis:
Even when the messages exchanged are secured, regardless it leaves a high probability examination of the correspondence designs. Sensor exercises can possibly uncover enough data to empower a intruder to make malicious damage to the sensor network.

1.3 Camouflage Adversaries:
Intruders can embed their hub or compromise the hubs to hide the sensor network. After that these hubs can duplicate as an ordinary hub to get data from the bundles, at that point change the path of the packets, leading the security examination. The intruder’s monitoring, listens to and modifies the data stream in the communication[8]

1.4. Clone Attack
An adversary can catch a sensor hub and take out its key materials. Once a hub is caught, the attacker can reinvent it and create a clone of a caught hub. These clones (or) reproductions can be sent in all system zones. These copy hub attacks are exceptionally hazardous to the activities of sensor networks. With a solitary caught sensor hub, the attacker can make the same number of reproduction hubs as he needs. The copy hubs are illegal by the enemy, however have keying materials that enable them to appear like approved members in the system. So it is especially difficult to distinguish a clone attack.[9]



1.5. Clone Attack Detection
Wireless sensor network can be either static or portable .In static wireless sensor network, sensor hubs are conveyed randomly and after deployment their positions don't change.[10] In versatile WSN, the sensor hubs can move their own after deployment. Two kinds of detection techniques are accessible in static WSN are centralized and distributed. In a centralized approach for identifying hub replication, when another hub joins the system, it communicates an area assert containing its area and character to its neighbours. At least one of its neighbours at that point forward this area claim to the base station. With area data for every one of the hubs in the system, the base station can easily distinguish any combine of hubs with a similar character yet at various areas. The principle impediment of this approach is that if the base station is compromised or the way to the base station is blocked, enemies can include any number of copies in the system. Circulated approaches for recognizing clone hubs depends on area data for a hub being put away at least one witness hubs in the system. At the point when another hub joins the system, its area asserts is sent to the relating witness hubs. If any witness hub gets two distinctive area claims for a similar hub ID, at that point the presence of clone is identified.[11]
This paper present the comprehensive analysis of various techniques used to detect frauds within the complex networks. Next section present the literature survey of the techniques used to detect frauds within the complex networks

2. PROPOSED WORK

S. J. Ahuja Mini Singh proposed a Hybrid optimization algorithm including fruit fly algorithm for community overlapping detection and fraud detection is performed by the use of contingency table terminology with multi link metrics. The simulation is performed on five distinct areas and result obtained in terms of normalised information metrics is considerably better. [12]A. Wibisono, W. Jatmiko, H. A. Wisesa, B. Hardjono, and P. Mursanto proposed a technique, a model is speculated for each group to locate the best attack of information for a given model. This strategy finds bunches by grouping the thickness work. It reflects spatial conveyance of the information focuses. This strategy additionally gives an approach to consequently decide the quantity of bunches in light of standard insights, considering exception or commotion. It accordingly yields hearty bunching strategies.[13]J. Zhao, K. Yang, X. Wei, Y. Ding, L. Hu, and G. Xu discussed mechanism to perform clustering that is performed by the consolidation of client or application-arranged imperatives. A requirement alludes to the client desire or the properties of craved bunching come about. Requirements furnish us with an intuitive method for correspondence with the bunching procedure. Limitations can be indicated by the client or the application necessity.[14]S. Kiruthiga proposed profile clone attack mechanism used to detect and prevent the similarity in profile using graph based algorithms. Graph used to detect such attacks is acyclic in nature. In case cycle exists within the graph then that indicates presence of clone and required to be resolve by eliminating extra edge causing cycle within the graph. 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. [15]To detect the profile cloning attacks from such a network technique has been proposed by M. Kharaji and F. Rizi. Entire social media is divided into two 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.[16] To detect the clone attack a new approach for clone attack detection is proposed by F. S. Rizi, M. R. Khayyambashi, and M. Y. Kharaji. 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. [17] A.Fahad, N. Alshatri, Z. Tari, A. Alamri, I. Khalil, A. Zomaya, S. Foufou, and A. Bouras proposed strategy depends on the idea of thickness. The fundamental thought is to keep developing the given bunch or cluster length regards to thickness in the area surpasses some edge, i.e., for every information point inside a given group, the sweep of a given group needs to contain no less than a base number of observations.[18]

3. COMPARATIVE RESULT

Research	Fraud Investigated	Method investigated	Accuracy%
S.J.Ahuja Mini Singh [12]	link and node failure	fruit fly contingency metric	88.8% with maximum of 1.8 nmi out of which 1.6 score is obtained
F.H.Glancy and S. B. Yadav[19]	Credit card frauds	Regression SVM Random Forest	96.7% 95% 97%
E. Duman and M.H.Ozcelik,.[20]	financial statement frauds	Decision Tree Neural Network Bayssian Belief Network	73% 80% 90%
Jarrod West, Maumita Bhattacharya,[21]	financial statement fraud from chinese company	support vector machine genetic programming neural network (feed forward) group method of data handling logistic model (regression) neural network (probabilistic)	70% 89% 75% 88% 66% 95%
Jarrod West, Maumita Bhattacharya, and R. Islam,[22]	managerial statement financial fraud	text mining	95.54%
S. Bhattacharyya, S.Jha,K. Tharakunnel, and J. C. Westland, [23]	financial fraud detection	text mining text mining with svm	45% 50%

4. CONCLUSION

The techniques required for social media fraud detection are critical for preserving the security of data. The information retrieval rate is massive and preserving mechanisms are limited. To handle clone attacks different techniques can be used for the security purpose. Some modification to existing techniques is required to improve the accuracy described in table.

The confusion metric parameters can be evaluated for detecting performance and positive node obtained from fruit fly and contingency metric can be used for fraud detection for better performance and also for security purposes to secure the data in future work.

5. REFERENCES

[1] Michael T. Schaub, J. Delvenne, M. Rosvall, and R. Lambiotte,"The many facets of community detection in complex networks," (2017), Applied Network Science Vol. 2(1), pp. 4.

[2] B. S. Rees, K. B. Gallagher, B. S. Rees, and K. B. Gallagher, "in Complex Networks Using Swarm Intelligence for Multi-threaded Label Propagation," pp. 111–119.

[3] Lei-Lei-Shi, Lu Liu, Yan Wu, Liang Jiang, and James Hardy, "Event Detection and User Interest Discovering in Social Media Data Streams," vol. 3536, no. c, 2017.

[4] S. Li, D. C. Yen, W. Lu, and C. Wang, "Computers in Human Behavior Identifying the signs of fraudulent accounts using data mining techniques," Comput. Human Behav., vol. 28, no. 3, pp. 1002–1013, 2012.

[5] S. Sivagowry, M. Durairaj, and a. Persia, "An empirical study on applying data mining techniques for the analysis and prediction of heart disease," 2013 Int. Conf. Inf. Commun. Embed. Syst., pp. 265–270, 2013.

[6] T. Chalermarrewong, T. Achalakul, and S. C. W. See, "The Design of a Fault Management Framework for Cloud," 2012 9th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol., pp. 1–4, 2012.

[7] P. Uma Maheswari and P. Ganesh Kumar, "Dynamic Detection and Prevention of Clone Attack in Wireless Sensor Networks," Wirel. Pers. Commun., 2016,published by springer US

[8] M. Pulivarthi, S. Shaik, and M. L. Bai, "Detection of Clone attacks in Wireless Sensor Networks Using RED (Randomized , efficient , and distributed) Protocol," vol. 4, no. 7, pp. 30–44, 2012.

[9] H. W. J. L. L. Zhou, "Lightweight and effective detection scheme for node clone attack in wireless sensor networks," no. December 2010, pp. 137–143, 2011.

[10] J. Anthoniraj and T. A. Razak, "Clone Attack Detection Protocols in Wireless Sensor Networks : A Survey," vol. 98, no. 5, pp. 43–49, 2014.

[11] M. Conti, R. Di Pietro, L. V Mancini, and A. Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks," pp. 1–14, 2010.

[12] S. J. Ahuja Mini Singh, "Hybrid Optimization Algorithm for Community and Fraud Detection in Complex Networks for High Immunity Towards Link and Node Failures," vol. 11, no. 1, pp. 211–220, 2018.

[13] A. Wibisono, W. Jatmiko, H. A. Wisesa, B. Hardjono, and P. Mursanto, "Knowledge-Based Systems Traffic big data prediction and visualization using Fast Incremental Model Trees-Drift Detection (FIMT-DD)," Knowledge-Based Syst., vol. 93, pp. 33–46, 2016.

[14] J. Zhao, K. Yang, X. Wei, Y. Ding, L. Hu, and G. Xu, "A Heuristic Clustering-Based Task Deployment Approach for Load Balancing Using Bayes Theorem in Cloud Environment," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 305–316, Feb. 2016.

[15] S. Kiruthiga, "Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques," IEEE, 2014,published in Recent Trends in Information Technology (ICRTIT), 2014 International Conference in Chennai.

[16] M. Kharaji and F. Rizi, "An IAC Approach for Detecting Profile Cloning in Online Social Networks," vol. 6, no. 1, pp. 75–90, 2014.

[17] F. S. Rizi, M. R. Khayyambashi, and M. Y. Kharaji, "A New Approach for Finding Cloned Profiles in Online Social Networks," vol. 6, no. April, pp. 25–37, 2014.

[18] Adi Fahad, Najlaa Alshatri, Zahir Tari, Abdullah Alamri, Ibrahim Khalil, Albert Y Zomaya, Sebti Foufou, Abdelaziz Bouras,"A Survey of Clustering Algorithms for Big Data : Taxonomy & Empirical Analysis," IEEE Access, september 2014.

[19] F. H. Glancy and S. B. Yadav, "A computational model for financial reporting fraud detection," vol. 50, pp. 595–597, 2011.

[20] E. Duman and M. H. Ozcelik, "Expert Systems with Applications Detecting credit card fraud by genetic algorithm and scatter search," vol. 38, pp. 13057–13059, 2011.

[21] Jarrod West and Maumita Bhattacharya, "Title of the paper : Intelligent Financial Fraud Detection : A Comprehensive Review Authors : Corresponding author :," Comput. Secur., 2015.

[22] Jarrod West, Maumita Bhattacharya, and R. Islam, "Intelligent Financial Fraud Detection Practices : An Investigation."published in journal computer and security volume 57 issue c march 2016

[23] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud : A comparative study," vol. 50, pp. 602–604, 2011.