International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Hybrid Approach of KNN and Euclidean Distance to Tackle Sybil Attack in the Network

Yasmeen[1], Parminder Kaur[2]

[1]M Tech Scholar, Department of Computer Science and Engineering, Punjab Technical University, India

[2]Professor, Department of Computer Science and Engineering, Punjab Technical University, India

Abstract: ***The wireless sensor network uses batteries which decay as data is being transmitted from source and destination. This decay in batteries requires to be minimised. Reasons for decay in batteries could be congestion and attacks. The attacks which are common in WSN is Sybil attack which is multiple identity attack. In such a situation, attacker node copies the identities of other nodes and data which is transmitted delivered to the wrong node causing threat to secure data. In order to solve the problem KNN mechanism is used in the proposed system. KNN is used in order to form clusters of the minimum distance nodes. These clusters then can be examined for similarity in terms of identities. In case similarity in terms of identities is found then Sybil attack is detected. The result is presented in terms of classification accuracy and mean square error. Classification accuracy is obtained by subtracting the actual value from the approximate value. The error rate is obtained by subtracting the classification accuracy from 100. The proposed approach uses Euclidean distance to determine the neighboring nodes. The simulation of the proposed system is conducted in MATLAB 2017. The mechanism employed detects the Sybil attack with more precision. The result is improved by the margin of 10% proving worth of the study.***

Keywords: KNN mechanism, MATLAB

1. Introduction

The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder.

A Sybil attack is a Multiple Identity Attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots distributed in different locations to launch a large number of Multiple Identity Attack attacks against a single target or multiple targets. With the rapid development of network technology in recent years, the attack traffic scale caused by Multiple Identity Attack attacks has been increasing, with the targets including not only business servers, but also internet infrastructures such as firewalls, routers and DNS system as well as network bandwidth, the attack influence sphere has also become broader.

WSN (wireless sensor network) provides a wide range of computing resources from servers and storage to enterprise applications. WSN is a hosting environment that is immediate, flexible, scalable, secure and available. The computing resources from cloud can be easily and quickly accessed and released after use with very less management effort. The concept of WSN can be used in mobile applications running on SMDs (surface mounted device) to boost up their performance. With the integration and support of WSN into the complex mobile applications, the term Mobile WSN (MCC) arises.

Issues in WSN

During the last few years, there has been a sharp increase in the number of network-based computer attacks.This has led many researchers to study this field in great depth in order to develop novel methods that are capable of eliminating this threat from today's computer networks. This chapter presents a summary of some of the most recent work on the mitigation techniques of common identity based attacks like Sybil and spoofing. The work that is summarized in this chapter deals primarily with attacks on the transport layer, attacks on the network layer, and a thorough introduction to the concept of the mitigation technique known as client puzzles. It is very difficult to secure data from intruders. Now in our proposed system we detect the malicious nodes as well as correct them.

Popular WSN Services Model

The WSN Is One Of The Most commonly used technologies. The cloud is used in order take a backup of the data which is used in case of mobiles and other devices. As cloud is exposed to more and more users, the security is becoming an issue. There exist data centers in case of the cloud. The data center is the one which is going to provide the resources to the user. The work load is distributed in case of cloud. This is known as Load Balancing. In case of Load Balancing the load will be equally distributed among the large number of data centers. No data center will going to get partial load. If data center goes down it is possible to ensure that work is not going to be stopped. The work will be continuously down through the other centers. In WSN load balancing will ensure that one resource is not overwhelmed or underutilized.

- IaaS (Infrastructure as a service) model
- PaaS (Platform as a service) model
- SaaS (Software as a service)

Research Gap

The literature survey suggests that mobility of nodes causes a problem a problem with most of the strategy suggested. Energy consumption is increased substantially when Sybil attack is encountered. Also packet drop ratio is increased. The techniques used tackles such issues but energy consumption and packet drop ration can be reduced further.

Lifetime of the network is reduced through the application of Sybil attack enhancing lifetime in case of static nodes is tackled in most of the literature studied. Mobility of nodes can be tackled in the future using modified hybrid approach combining optimal features of existing techniques to tackle Sybil attack.

2. Objective of Study

The proposed work deals with the mobility of nodes along with the static nodes to reduce the identity based attacks in the cloud like networks. The objectives are listed as follows

1) Increasing the lifetime of the network.
2) Reduce the energy consumption within the network.
3) Reduce the packet drop ratio.
4) Increase reliability and reduce bandwidth consumption of the network

3. Conclusion and Future Scope

The proposed work efficiently analyses the Sybil attack. Strategy to tackle Sybil attack is suggested. Using the methodology lifetime of the network can be considerably enhanced. Packet drop ratio which is the problem in existing research is also tackled. Static nodes are considered and handled in existing scheme of thing but this approach combines Euclidean distance with KNN approach to handle mobility of nodes.

In future K means clustering technique can be used along with KNN_Euclidean distance approach to further classify and analyses the adverse effects of Sybil attacks.

References

[1] Z. Zhou, C. Du, L. Shu, G. Hancke, J. Niu, and H. Ning, "An Energy-Balanced Heuristic for Mobile Sink Scheduling in Hybrid WSNs," *IEEE Trans. Ind. Informatics*, vol. 12, no. 1, pp. 28–40, 2016.
[2] A. Mateska, L. Gavrilovska, and S. Nikoletseas, "Mobility Aspects in WSN," Springer London, 2011, pp. 119–143.
[3] S.-H. Yang, "WSN Security," pp. 187–215, 2014.
[4] S. Muhammad, S. Hussain, and M. Yousaf, "Neighbor Node Trust Based Intrusion Detection System for WSN," *Procedia - Procedia Comput. Sci.*, vol. 63, pp. 183–188, 2015.
[5] D. Tang, T. Li, J. Ren, and J. Wu, "Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 960–973, Apr. 2015.
[6] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, May 2015.
[7] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks 1," 2003.
[8] C. Wu, Z. Yang, Y. Liu, and W. Xi, "WILL: Wireless Indoor Localization without Site Survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 4, pp. 839–848, Apr. 2013.