ISSN 2348 – 9928
IJAICT Volume 5, Issue 7, July 2018 Doi:01.0401/ijaict.2015.11.17 Published on 05 (7) 2018

REAL-TIME UNAUTHORIZED ACCESS DETECTION IN WIRED OR WIRELESS NETWORKS: USING DOMINO CONCEPT

Mr. S. SheikAbdulla ***UG Student***
Mr. N. ArunKumar ***UG Student***
Mr. B. lokeshAravind ***UG Student***
Mr. S. Thivaharan ***Assistant Professor***

Information Technology,
Kalaignar Karunanidhi Institute of Technology,
Coimbatore, Tamilnadu, India

Abstract—We find interprets with the security and the misbehavior threat within the 802.11 connections. Whereas the connection are used worldwide with the level of integration of the devices, within some of its relational devices which provide connections .The misbehavior achieved with their connections are the real time misbehavior,back-off misbehavior , distribution co-ordination misbehavior and MAC protocol misbehaviors. Due to these a large number of a data loss and the missing of the important information's,losses are achieved by the hackers. This wireless medium does not contain the facility of detecting the things happening around but, where it has happened and what has happened and what has been done can be detected. To avoid such conditional behavior, the introduction of the DOMINO detector is used within the connections to make them secure

Keywords— IEEE 802.11, MAC, DOMINO.

I. INTRODUCTION

In these recent years, the internet is a very essential thing found common for the people. This plays an important role among worldwide. For the easy access and the transfer of the file we use IEEE 802.11 wireless connection .Where they are even comfortable but are loaded with various threats and encryption misbehavior. Many malicious users are approaching for the distractions of the connection, for the stealing of the information and ending up of the transactions. Still for this, the sequential test and ratio test is used in order to detect those misbehaviors in the network configuration .Later on this method of detecting such as fair share detector and non-parametric CUSUM tests are done for back off detections.

The user 1 is the actual transporter of the data and the data must be received by the user 2, but the malicious user interacts between users. Therefore the data loss and ending up of the transaction occurs.

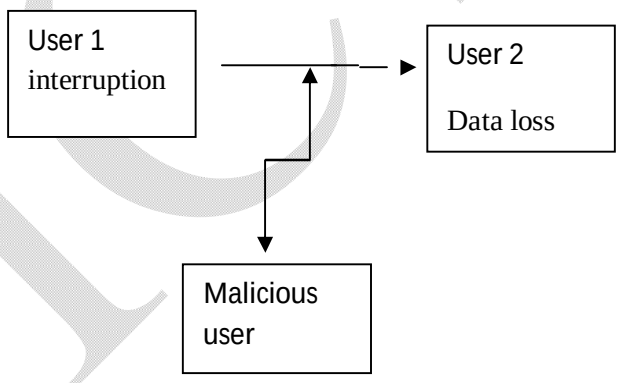

Fig 1 : Data Interruption

II. PROBLEM DEFINITION

2.1 Data Interruption

The data sent to the WIFI are captured by some of the unauthorized user and the data are stored as information's.
The change of actual data and detection of some data could be done by them.

2. 2. Denial of services

The same frequencies are passed for all the connections established within the device so that the services provided could cause a change of service or no service response.

2.3. Rogue Access points (AP's)

The unauthorized AP's are found in all type of IEEE 802.11 connections, thus if the interactions of an unauthorized person are found, in case of detections the connection will be shut down.

2.4. Wireless intruders

These are done by the malicious intruders within the connection provider's. Whereas they could change the data's during the data transactions that causes a larger amount of the problem.

2.5. AP's Misconfiguration

When some of the individual AP's are handled, the significant security threats within the wireless LAN'S are found. As there are centralized connection promoters.

2. 6. AdHoc and soft AP's

The WIFI connection provided laptops have AdHoc's where they arehard to configure so it makes some sense for using them literally. These soft AP's measures could provide some unauthorized connections of clients and can interact towards them.

2.7. Misbehaving clients

`The actual client may also form some of the unauthorized WIFI connections of any type. These cause the end user change. That requires usage of the WIPS to monitor WIFI client activity.

2.8. End point attack

As the connections and the transactions are somehow secure now-a-day .The attackers focuses on the end points. They use the buggy WIFI devices to perform these threats. The WIFI end point exploits are made in ordered.

2.9. Twin AP's

The AP's with same adjacent names are found, they are called the twin AP's, where the AP's form by the malicious users with the adjacent name of the original AP.

2.10. Wireless phishing

There are done by the hackers, where the phishing is done for the WIFI actual user. They are done within the middle of the transaction to route this kind of phishing, the hotspot traffic and cleaning of the caches.

III. TO OVERCOME THESE ISSUES DOMINO

The domino is the kind of the detection technique which in this indicates the spot clearly of misbehavior or some unnatural conditions. This domino deals with the wide range of 802.11 MAC misbehaviors' .This nature of the domino is applicable within some of the scenarios in IEEE 802.11 for the detection of their backoff misbehavior .The domino observes about the whole node of the connections with the ratio detection. This has a capability of quick accessing, detecting and making decision. This easily differentiates the normal behavior and abnormal behavior of a backoff node, and quickly react the intrusion of the malicious nodes.

IV. ASSUMPTION OF DOMINO INTO 802.11

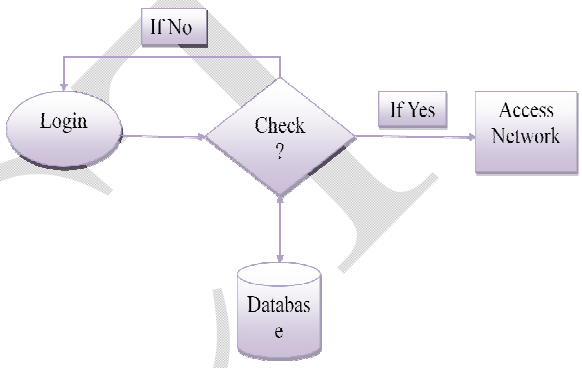

Fig 1 : Ordinary processing

In this the connection of 802.11 is introduced within two users just using some scenarios that is the login of the actual users and then encryption of the user is done with various scenarios, along with this is the regular base of the connection provided by 802.11.

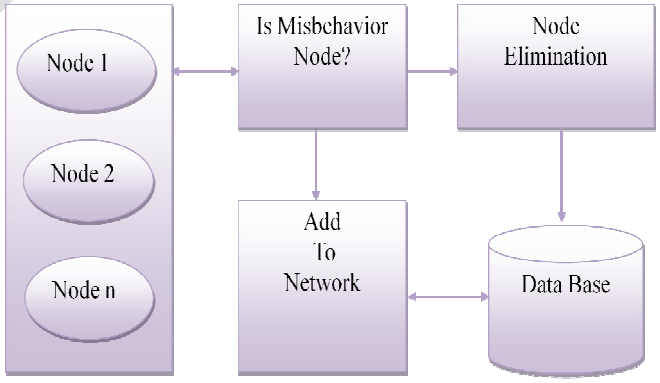

Fig 2 : Domino Behavioral Processing

Thus when an domino is accessed within an AP, if there is any misbehavior activities. Domino detects them and quickly responds towards the threat, where the cheater is denoted and the transmission towards them is stopped immediately. The

domino provides information about which device or medium thatmisbehaves within the larger area connections of 802.11. The domino attached to the access point provided stops such threat.

V. CONCLUSION

In this paper we have proposed an usage of the domino detector within the 802.11 connections. The advantage of this method is that it detects the misbehavior as well as spots the device that involves in such misbehavior. This method of the usage of the domino is that the setup of the domino is attached with the access point providers. Whereas all the nodes those which are provided with the access are monitored by the domino, in case of that which are provided connection with the acknowledgement of the domino. The domino performs the detection over the each node which is accessed and the connection is provided on the basis of strategy of the domino. The comparisons of the working of the domino with other existing technique such a chi-square test, Markova chain process and the ratio test is considered to be an updated and ease of modular technique for back-off detection and the detection of misbehaving connections provided.

References

[1] J. Tang, Y. Cheng, and W. Zhuang, "An Analytical Approach to Real-Time Misbehavior Detection in IEEE 802.11 Based Wireless Networks," Proc. IEEE INFOCOM, 2011.

[2] S. Szott, M. Natkaniec, and R. Canonico, "Detecting Backoff Misbehaviour in IEEE 802.11 EDCA," European Trans. Telecomm., vol. 22, no. 1, pp. 31-34, Jan. 2011.

[3] S. Radosavac, J.S. Baras, and I. Koutsopoulos, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks," Proc. ACM Workshop Wireless Security, pp. 33-42, 2005.

[4] P. Serrano, A. Banchs, V. Targon, and J. Kukielka, "Detecting Selfish Configurations in 802.11 WLANs," IEEE Comm. Lett rs, vol. 14, no. 2, pp. 142-144, Feb. 2010.

[5] S. Radosavac, G. Moustakides, J. Baras, and I. Koutsopoulos, "An Analytic Framework for Modeling and Detecting Access Layer Misbehavior in Wireless Networks," ACM Trans. Information ad Systems Security, vol. 11, no. 4, article 19, July 2008.

[6] M. Raya, J. Hubaux, and I. Aad, "DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots," Proc. ACM MobiSy , 2004.