International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 6 1673 – 1678

Detection and Elimination of Fake Access Points in WLAN using Multi Agents Sourcing Methodology

Priyanka G. Sasane
Dept. of Computer Engi.
SKNCOE, Vadgaon
University of Pune, India
pdpatil.sae@sinhgad.edu

Prof. S. K. Pathan
Dept. of Computer Engi.
SKNCOE, Vadgaon
University of Pune, India

***Abstract*—** The major security issue in the Wireless LAN is, the presence of access points which are not approved by the administrator. If this issue is not detected on time, them it may lead to serious network damage and may result into major data loss or data impact. Many researchers have already proposed various solutions to overcome the above mentioned situation, but either most of them are limited in techniques or they are not automated to absorb the frequency alterations in WLAN. This is the proposed research paper in which the new approach is presented which is based on Master and Slave Topology. This is specially designed approach which is not only working on ―Fast Detection of Rough Access Points (FDRAP) but also includes the solutions of mitigating these Rough Access Points. In the overview, this new framework will be handling the Detection as well Elimination of Rough Access Points in the network. This Master and Slave agents will automatically scan the network and detect the unauthorized access points using various skew intervals. We have attempted to focus on following methodologies for making it successful – 1) this specially designed approach does not require any special hardware 2) Algorithm is designed to work on both – Detection as well as Elimination 3) As no special hardware is involved, it becomes a very cost effective solution 4) Due to multiple Master agents in action, possibility of network congestion or delay in packet signaling is also reduced. This algorithm is proposed to block the RAPs and also to remove them from the network with covering both aspects like – unauthorized APs or Rough Clients acting as Ap's.

Keywords- *Intrusion Detection System; Manet; Master; Rogue/Fake Access Point; Slave; WLAN*

*****

I. INTRODUCTION

Wireless LAN System (WLANs) is one of the fastest growing technologies in the Communication world. With the fastest growing & communicating world, the demand of devices which can work or communicate without cables are increasing day by day. Primarily Wireless networks are predominantly used by mobile or nomadic computing devices to provide them the network access without cables. It serves its own attractive purposes likes – mobility, greater flexibility in device handling and operating, portability, and more importantly freedom of access with significant security.

There is possibility that snooping of the wireless communication, because the signals from wireless networks are usually unidirectional and due to its variety in range projections it may get reach beyond the intended coverage area. Here this situation it becomes primary alert to secure the network physically because even anyone with wireless receiver can attempt to snoop the network and many times this type of intrusion is virtually undetectable. To overcome this type of security threat, many researchers have proposed various papers, discussing about most common security protocols; also it has been observed that Wired Equivalent Privacy (WEP) also faces breakdowns if it is configured improperly.

One of the most impressive security challenges for the network administrator among rest all is the, designing preventive majors to block the Rough Access Points (RAPs) [10- 12]. This attack of RAP is considered as Serious Threat to the network because, many other threats are either based on very high-level of technical knowledge representations or to breakdown the security very sophisticated & costly instruments are required, but this type of RAPs could be easily accomplished even by people with limited knowledge related with network security.

In the literature the Rough Access Points are referred as Unauthorized AP. In description, it can be described as, a wireless point which is either installed on secure network without taking into consideration the explicit authorization from local administrator [15], or maybe it has been falsely configured which may allow cracker to conduct a man-in-middle attack, or in worst situation, it can be used by adversaries for committing snooping and executing various attacks.

The Rough APs can be classified broadly into various categories based on levels like – Unauthorized Rough APs, Improperly Configured Rough APs, and Compromised Rough APs and used for Phishing Rough APs. To get more information about them along with possible scenarios, readers are advised to refer [5] for in-depth taxonomy of all mentioned categories. Considering the fact that many commercial products are available readily in the market for detecting the RAPs [10-12], and also studies proved that extensive research work has not been carried out, here in this area and moreover many are performing only RAP detection and very few among them are focusing on eliminating / blocking of these RAPs. So to fill this gap, this paper we are proposing a completely new & novel approach with Multi – Agent – Sourcing – Methodology for detection and elimination of RAPs.

The project flow of this paper will be like – Section (II) – will discuss the related work and Current Approaches. And

in next Section (III) – we are discussing about the System Architecture. Mathematical model at section (IV) followed by result at (V). At the conclusion portion the Section (VI) is dedicated followed by References in Section (VII).

II. RELATED WORK

Mobile Ad-hoc Networks abbreviated as MANETs are infamous for their infrastructural support and transient or short-lived nature. These characteristics of MANETs are really providing challenging platform for IDS executions. The major fact of MANETs is , even frequent changes in topology and communication patterns requires the use of specialized protocols and specially designed strategies for successful routing, transporting and securities.

The researches in MANET are majorly focused on Private – Public Key Management, Routing Protocols and Intrusion Detection Systems, but past experiments and researches have proved that the designed intrusion prevention algorithms and encryption techniques are not sufficient, and if we attempt to complex it, it will lead to more complex security problems.

On the contrary, the intrusion techniques used in wired networks are cannot be directly applied as it is to Mobile Ad Hoc Networks, based on special characteristics possessed by this type of networks. To take research one step ahead, most current MANET IDS are still in pre-mature stage, which directly implies huge scope and aggressive development in the program of making Ad Hoc Network more secure which can be achieved by designing more advanced and intelligent intrusion detection systems.

When we make comparison with wired networks and wireless ad hoc networks, we need to consider the important differences while designing an intelligent intrusion detection system. To summarize, we are suggesting few major differences between wired and wireless networks – wired networks are using variety of devices like gateways, routers, and switches for traffic monitoring purposes, but wireless ad hoc networks are purely lacking traffic management aspect. In result the IDS in wireless networks are based on local security audit data. We can suggest to take following aspect into consideration in using IDS in wireless networks – because of limited resources, one should emphasis on securing it with keeping in mind the resource consumption characteristics, which means it is most preferred to use periodic intrusion detection system instead of an "Always – ON" preventive configurations.

A. Introduction to Mobile Agents

Mobile Agents (MA) is basically software entities which can physically travel across the network and perform various assigned tasks on targeted machines which provide the hosting capacity for this agent. This allows processes to migrate from one computer to other, or sometimes base on requirements processes gets spilt into multiple instances that will get executed on different machines and will return to their point of origins. Here term migrations of mobile agents essentially implies that, some code with required set of data in transferred to another node for remote execution of that code.

B. Rogue Access Point

The Rogue Access Point can be defined as:

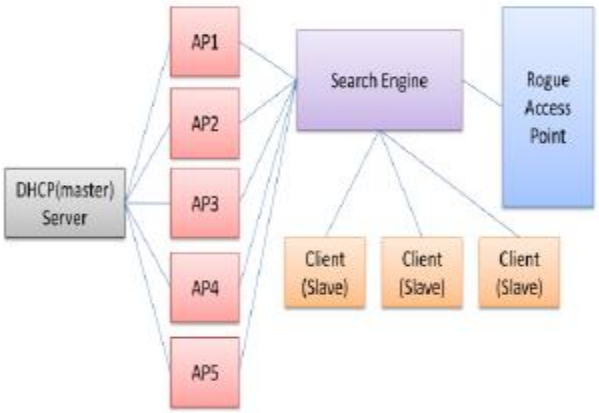

Fig 1. System Architecture [6]

- Rough Access Points are usually installed over the network without authenticating itself and also it will violate the security policies.
- Basically these Rough Access Points are installed to the network with the major intention to attack on the confidential information.

Based on above two definitions we can easily identify the Rough Access Points.

In above figure we have attempted to show the approaches we have taken for this paper.

While designing this proposed approach, we have taken into consideration following elements which will be the limitation for this work –

- Due to use of Multi-Agent System, the performance of this proposed system along with overall network may get impacted like – overall throughput or wireless network, packet drop ratio, end to end delay etc.

- While authenticating the new the access point for its validity, Heavy load on one Master Agent may involve unnecessarily extra time, which will result into increment in extra network overhead and may decrease the overall network throughput.

III. ADVANCEMENT IN THE PROJECT

There are few researches that have already performed in the field of detecting and blocking these Rough Access Points, but none of them is able to provide the really fruitful solution on this. Most of the developments are done on the base of need of dedicated piece of software and hardware, or even some special qualified employees for performing different types of network scans also sometimes it is like using current employees for regular scanning of their vicinity for cross checking any unauthorized access points active around them.

To overcome this type of dependencies on specially customized hardware or dependencies on manual efforts which are most of the time subjected to be error prone, here we are proposing the fully automated concept of detecting the eliminating RAPs by applying the Mobile Multi-Agents effectively on to the network. Here we are using new approach with using two different levels of Mobile Agents under new classifications – Master & Slave Mobile Agents.

To achieve this we extended the system architecture with addition of skew intervals to periodically scan the networks

instead of scanning in an Always ON mode. The executions process will be like –

- Initially a master agent is generated on the DHCP-M Server, which will be responsible for all regulating all the authorization procedures for the wireless network.
- In later stages, the Master Agent will generate the Slave Agent based on number of Active Access Point connected to the server at that moment of time.
- Based on the supplied data, these Slave Agents are dispatched to the respective APs connected.
- Now, all these Slave Agents will be cloned on every Access Point and being dispatched to the every connected clients over that Access Point.
- Now this newly Cloned Slave Agents will constantly monitor the client systems and detects new Access Points if any
- If these newly Clone Slave Agents detect new Access Point, it will automatically build information packets INFO containing following information about detected Unauthorized APs – SSID of Unauthorized APs, MAC-Address of Unauthorized APs, Vendors Name used for Unauthorized APs, Channel Used by Unauthorized APs, etc
- This INFO packets are then transferred to main Slave Agent and this Slave Agent will deliver this packet safely to the Master Agent on the sever.
- At server, this newly arrived information is compared with the stored repositories of all valid Access Points.
- If found that AP is authorized, then new Slave Agent will be generated and sent over the respective AP to monitor it again for next attempt of intrusions.
- But if AP is found unauthorized, then Disassociation Frame is sent to all APs informing them not to connect with this unauthorized AP
- Else if details doesn't match with the repository, then the MAC- Address of the AP will be fetched from the INFO, and the port at which the MAC-Address is connected will be get searched and then it will be blocked for any sort of LAN Traffic.
- This will automatically deactivate the RAP and also prevents clients (if any) from dropping the active connection and allows clients to get associate with the nearest AP which is authorized.

- This is a very simple and most effective technique for completely routing out the RAP from the network [1].

Please find the next steps from algorithm designed for the Skew Intervals

A. Steps to implement

1. First create – Master Agent on the DHCP server
2 From Master Agent – Generate the Slave Agent based on number of access points
3. Once Slave Agents are generated, transfer them to all access points
4. When Slave Agents are arrived at all the Access Points, clone all the Slave Agents again.
5. Now, by generating Clock Skews at each Slave Agent, scan all the Access Points. And it will create first Genuine Database.
6. If new Access Point is detected, the cloned agent will build the INFO Packet automatically containing important information about newly detected Access Point.
7. This INFO packet is handed over to the related Slave Agent
8. Now, Slave Agent will hand over this INFO packet to the Master Agent and then Master Agent will transfer this entire packet to the DHCP Server for testing Authenticity of the Information contained in the INFO Packet
9. If the DHCP server does NOT found any match of new information in the firstly created Genuine Database, then it will declare it as Rough Access Point.
10. Now to block or deactivate this Rough Access Point, following steps are performed, ensuring no mistakes
    a. First to get highest accuracy, the INFO packet is extracted properly to get the correct MAC address
    b. Based on this MAC address, the exact Network Switch Address is identified.
    c. After successfully identifying the Network Switch, the next target is to locate the exact port number.
    d. Once the accurate port number is calculated, then the final task will be blocking it from any other wireless network traffic.

B. *Clock Skew*

The Clock Skew can be defined as the variances between the times publicized by the clocks at various nodes at the same time interval. As this Clock Skew indicating the time differences between nodes, so we can use it to identify and categories various network devices falling into similar or different time intervals.Studies have shown that we can implement the usability of these clock skews to isolate more than 512 unique access points.

a. Linear Programming Method (LPM)

In this LP Method, first we need to minimize or reduce following function carefully by entering appropriate values in the function.

$$\frac{1}{n}\sum_{i=1}^{n}(\delta(xi)-\varphi-oi)$$

The major drawback of this method is –it indicates High tolerance inclining towards the outliers.

b. Least Square Fit (LSF)

In this method, we have to focus on minimizing the following equation, by submitting the exact figures from the calculated inputs.

$$\sum_{i=1}^{n}[oi-(\delta xi+\varphi)]^2$$

The master advantage of this methodology is, it allows low tolerance towards outliers which is really important element in this proposed architecture.

As an outcome, we can distinguish between two Access Points, even if their Clock Skew values are very closely located alongside each other's. Indicating, we can use this methodology to identify the Fake Access Points, by taking

 ISSN: 2321-8169
1673 – 1678

accurate judgment on the Access Points which are engineered very close to the Clock Skew of the Authorized Access Points.

c. Implementation of LSF:
We have already defined a function

$$f = \sum_{i=1}^{n} [yi - (\delta xi + \varphi)]^2$$

Applying standard procedure to find minima, we differentiate it partially with respect to δ and equate it to zero.

A. $\partial f/\partial\delta = 0$ and $\partial f / \partial = 0$

Solving them simultaneously, we get estimated value of δ as

$$\delta = \frac{n\sum xy - \sum x \sum y}{n\sum x^2 - \sum x^2}$$

C. Major Components of System:

- DHCP-M: This is central repository responsible for monitoring authentication process of active wireless networks.
- Master Agent: Generated at DHCP Server.
- Slave Agent: Generated at every access point in network
- Clone Agent: Resided at client side.
- Access Point: Connected with DHCP sever
- Client: Connected with AP.

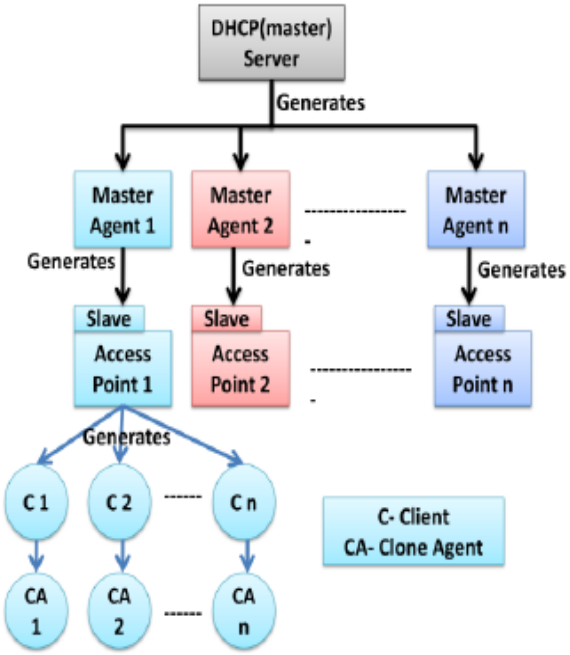

Fig 2. RAP Detection and Elimination System architecture

IV. UML DIAGRAMS

1. USE case diagram

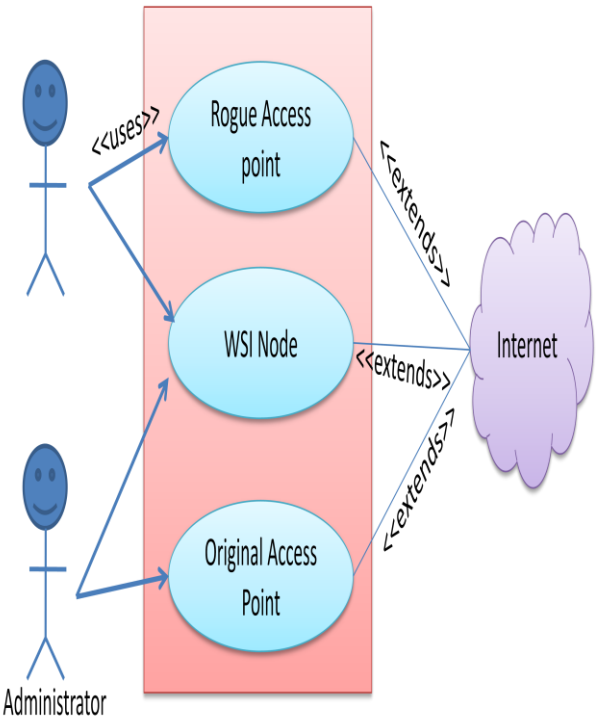

Fig 3. USE case Diagram

2. Sequence diagram

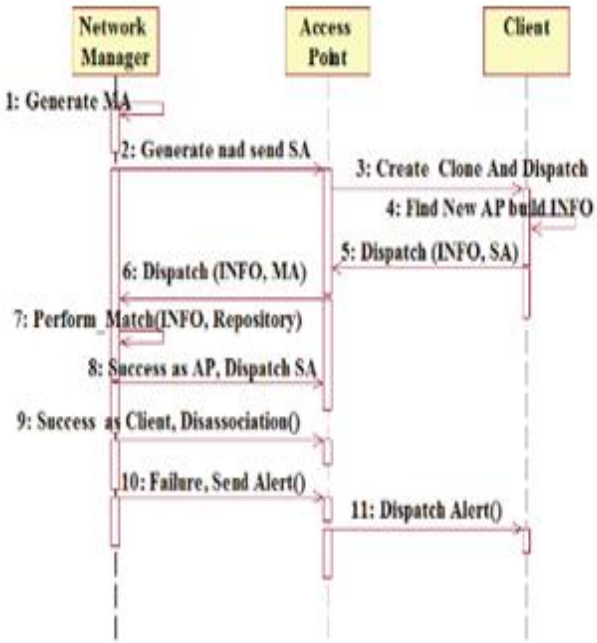

Fig 4. Sequence Diagram

3. Flowchart

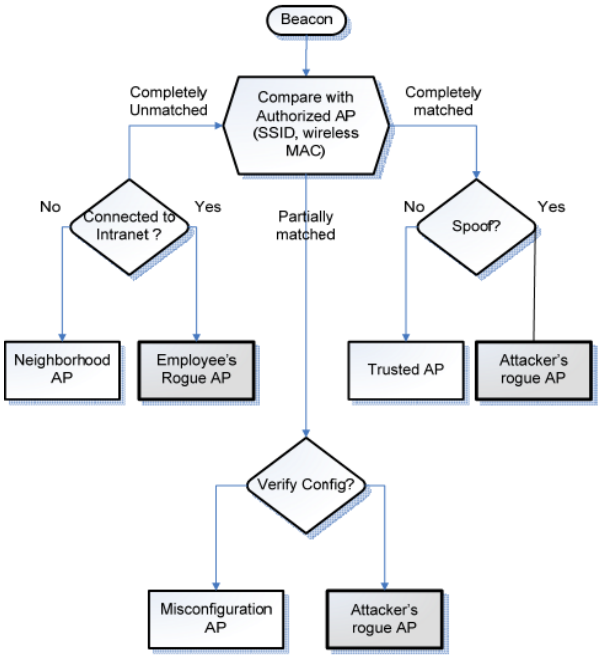

Fig 5 RAP Detection Algorithm

V. RESULT

As described, the practical evaluations can be expressed by considering following – while developing this application, we have developed a small desktop application using C#.net and making this code act like a Rogue Access Point. Also similarly we will develop another application which will check the data provided by the Access Points. The main achievable from all this is – to detect the Rogue Access Points present in the network. In the simulation we will activate both above mentioned modules and on execution we will check for Original and Rogue Access Points, and if we locate the Rogue Access Points, then block that port from transferring data using our application.

The major modules of this application can be summarized as –

1. Detection of access points.
2. Checking of access point. Rogue (Fake)/original
3. Blocking the access point from transferring data.

The first module will need Wi-Fi connection and some access points which we will be detecting. (Laptop devices have the Wi-Fi hardware inbuilt, so we can use laptop here). Now once the second module gets initiated, it will collect the valuable data about access points like – MAC Address, SSID, RSI etc. and this data will be reported to the server. Now at server level, this data is processed on the skew intervals along with estimating second skew intervals for some equation and will be checked for equality – if both the results are indicating identical information, if they are same, then we can declare that the mentioned Access Point is Original, otherwise if results are not similar we can declare that Access Point as Fake.

Once this Access Point judgment is done, the final module will get involved and it will block the data communication from the Fake Access Points, by blocking the port numbers of those Rogue Access Points. (The port number is calculated from the MAC Address)

To evaluate the performance we can produce the graphs like Time Graph and Channel Graph and also we can provide filtering mechanisms for filtering the Access Points based on APs Age, Channel Number etc.

Please see following representation for the results acquired

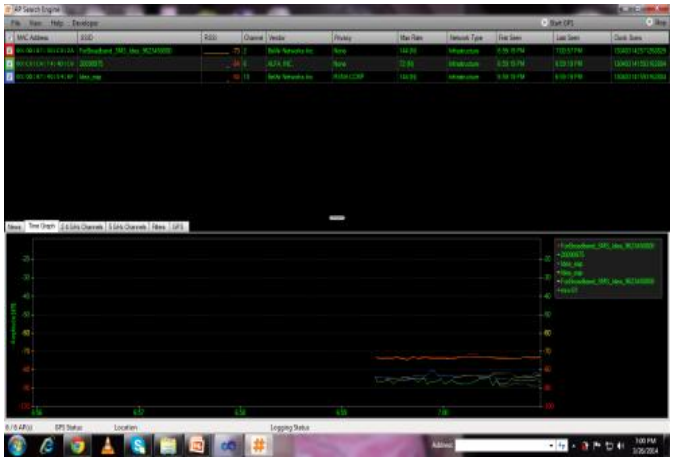

Fig. 3 Main screen of proposed architecture

Above figure showing that access point scanning windows is ready to capture all the available access points in networks in your area.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, we proposed a new methodology of using Multi- Agent as an integrated solution for both detecting and eliminating the Rogue Access Points from the network. Clear and easy to implement algorithm makes this architecture robust. This multi agent based architecture proved to not only identify but also eliminate the rogue access points completely. Our proposed technique is very reliable and cost effective, as it deals with multiple level of detection and doesn't require any specialized hardware device; implementation performed also supports our belief and results in a very effective methodology of complete removal of RAPs.

ACKNOWLEDGMENT

I feel happiness in forwarding this paper as an image of sincere efforts. The successful project design reflects my work, effort of my guide in giving me good information.

My sincere thanks to my guide Prof. S.K. Pathan who has been a constant source of inspiration and guiding star in achieving my goal. I express my deep gratitude to all staff members who lend me their valuable support and cooperation to enable me to complete my project design paper successfully.

REFERENCES

[1] V. S. Shankar Sriram, G. Sahoo, Ashish P. Singh, Abhishek Kumar Maurya "Securing IEEE 802.11 Wireless LANs - A Mobile Agent Based Architecture" 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[2] Prof.S.B.Vanjale (Ph.D Student), J.A.Dave(M.Tech. Student), "Unapproved Access Point Elimination In

Wlan Using Multiple Agents And Skew Intervals", Department of Computer Engg Bharati Vidyapeeth Deemed University College of Engineering Pune, International Journal of Engineering Science and Technology (IJEST), Feb. 2012.

[3] V. S. Shankar Sriram, G. Sahoo "A Mobile Agent Based Architecture for Securing WLANs" International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[4] Songrit Srilasak, Kitti Wongthavarawat and Anan Phonphoem, Intelligent Wireless Network Group (IWING) "Integrated Wireless Rogue Access Point Detection and Counterattack System" published in 2008 International Conference on Information Security and Assurance.

[5] Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng "A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks" published in the IEEE INFOCOM 2008.

[6] Ahmed Ayad Abdalhameed, "Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN Based on Agents Terminology and Skew Intervals: A Proposal", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013

[7] Lanier Watkins, Raheem Beyah, Cherita Corbett "A Passive Approach to Rogue Access Point Detection" 1930-529X/07/$25.00 © 2007 IEEE.

[8] Songrit Srilasak, Kitti Wongthavarawat, Anan Phonphoem "Integrated Wireless Rogue Access Point Detection and Counterattack System" 2008 International Conference