Security Loopholes Of 802.11 Wireless LANs And Their Solutions

#1 Shikha Goswami
M.tech Student (CDLU, Sirsa)

+91-9996969646
#2 Mrs. Sangeeta Thakral
A.P,CSA Deptt. (CDLU, sirsa)

Abstract- **The major concern in Wireless LANs is security.**

So in this Paper to fix security loopholes a public key authentication and key-establishment procedure has been proposed which fixes security loopholes in current standard. The public key cryptosystem is used to establish a session key securely between the client and Access point. A client -Agent based Rouge Access point detection system was developed to counter the threat of Rouge Access points in wireless LANs and are difficult to handle at the protocol level. Hence a centralized RAP was developed for organization where the area is quite large to cover manually or form a single location. An algorithm was also developed to detect Evil-Twin Access points, which cannot be detected by traditional methods. The algorithm works on fact that the evil-twin is placed at a distance from the good-twin to prevent direct detection.

Keywords- **802.11, wireless LANs, threats, loopholes**

I. INTRODUCTION

Wireless LANs are becoming popular day-by-day. They are being used as replacement technology to Wired LANs to connect end users. The reason behind this that wireless LANs to connect end users. The reason behind this is that wireless LANs Provide users with ubiquity and mobility. The speed of Wireless LANs has also become comparable to wired LANs. The major concern in Wireless LANs is security. Since they operate in broadcast medium it is very difficult to ensure confidentiality and availability.

The IEEE 802.11 standard for WLANs is one of the most widely adopted standards for broadband wireless Internet access. The first 802.11 standard came out in 1997. It featured data transfer speed of a maximum of 2 Mbps. The second version came out in 1999 and was called 802.11b. data transfer speed of 11mbps. At the same time IEEE 802.11t was also released which allowed 802.11 to run outside the crowded 2.4-Ghz industrial, scientific and medical band and in the 5-GHz Unlicensed National Information Infrastructure band. It could support maximum data transfer rate of 54 Mbps then in 2003, they released another speed boost, 802.11g, which brought 54 Mbps, while also utilizing the 2.4-GHz band. The next speed increase is 802.11n, which allows speeds of 100Mbps.

The IEEE 802.11 standard has defined the following two basic security mechanisms for secure access to IEEE 802.11 networks:

- Entity authentication, including open system and shared key authentication
- Wired Equivalent Privacy

II. MOTIVATION

Various researchers have found out vulnerabilities in the protocol that can cripple the availability and the confidentiality of Wireless LANs. Securing wireless networks is much more difficult than securing wired networks. Securing wireless networks is much more difficult as in addition to the challenges faced in wired networks wireless networks pose other unique challenges as well. i.e

1. Open air as the medium
2. Man- in -the middle attacks

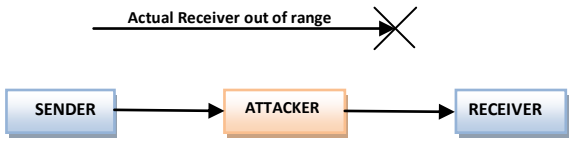

Fig Man-in-the-middle attacks in wireless network

3. Availability issues
4. Detection

Some scenarios even require the wireless network to be open to all users and still be able to protect data of one user from another. Airports or hotels for example provide free Jut met services to visitors. It is still a necessity to protect data transmitted by one user from

another otherwise an attacker can sniff and obtain confidential information about other users in the network.
After the security amendment the Wireless LANs have become a lot more secure than they used to be. But a vast majority of organizations have already deployed wireless equipment using older hardware which is not compatible with the newer standard. So it is necessary to device methods to protect these networks till it is possible to migrate them to the newer standard.

III. PROBLEM STATEMENT

To find various security loopholes in IEEE 802.11 Wireless LAN protocol and provide measures to improve its security at protocol and physical level.
This problem can be divided into following sub-problems:
(i) To design a more secure authentication and key-establishment mechanism.
(ii) To design a centralized Rogue Access Point detection system.
(iii) To design an algorithm this can detect Evil-Twin Access Points.

IV BACKGROUND STUDIES & RESEARCH GAPS

A lot of work has already been done to counter the security problems present in 802.11i. 802.11w amendment provides security for unicast as well as multicast management frames. To counter the problem of DOS attacks on the 4-way handshake various alternatives have been provided to the 4-way handshake

Although 802.11i has made wireless LANs more secure, many vulnerabilities still exist in the protocol. DOS attacks can be performed on wireless LANs either by sending a continuous stream of de-Authentication packets to wireless clients. This is possible since the management frames are not protected by any kind of encryption. Also DOS attacks can be done during the 4-way handshake as explained earlier.
In case a Pre-Shared Key (PSK) is used then all STAs use the same PSK as the Pair-Wise Master Key (PMK) during the 4-way handshake. As shown in figure 2.2 the session key used is generated from Snonce, Anonce and the PMK. Hence if any node with the knowledge of the PMK snoops on the 4-way handshake of another node then it can calculate lie session key of that node and decipher all communication between the node and the AP. This is undesirable and is known as insider attack.

The problem of Rogue Access Points still exists in Wireless LANs. Rogue Access Points can cause serious problems like back-door entry to the corporate network to phishing attacks on wireless users. Evil-twin Rogue access Points make the threat even more serious since they are extremely difficult to detect.
From the above research gaps the following are required in a proposed scheme to mitigate security threats in Wireless LANs.

1. An authentication and key-establishment scheme, which can prevent denial of service attacks and insider attacks on wireless LANs.
2. A mechanism to provide protection to both uni-cast as well as multi-cast management frames.
3. A centralized Rogue Access Point Detection and counter-attack system, which can be easily deployed on existing corporate networks.
4. A method to detect Evil-Twin access points.

V PROPOSED MECHANISM

1. Proposed Authentication and Encryption Mechanism

A symmetric key cryptosystem is a fast and efficient way to encrypt data.
The authentication scheme proposed by us is shown ii figure The Access Point has a public and a private key. The public key can be distributed to the client's offline or can be provided with a certificate. The clients then use this public key to establish a Session Key with the AP as shown in MESSAGE-2. The Session-Key is chosen by the AP. This is done in order to prevent replay attacks in ease a previous session key has been compromised. Since the session key is chosen by the AP, it is guaranteed to be fresh and confidential. The client sends a Pre-Session Key to the AP by encrypting it with the Public Key of the AP. The AP then sends an ID and the Session-Key back to the client. The ID and the Session-Key is encrypted with the Pre-Session key previously received by the AP. The client then has to authenticate itself before it can avail any service from the network. If the number of unauthenticated clients increases, the Access Point has to store the Session keys of all the clients and this may increase the load on it. Such situation might 1 ad to denial of service attacks. To prevent attackers from launching denial of service attacks on the AP unauthenticated clients have to keep sending KEPALIVE messages to the AP at regular intervals till they are authenticated.

This will ensure that all session keys belong to actual clients that exist in the network. To authenticate clients the Extensible Authentication Protocol can be used. The result of the authentication along With the knowledge of the Session-Key will determine if the client is given access to the network or not.

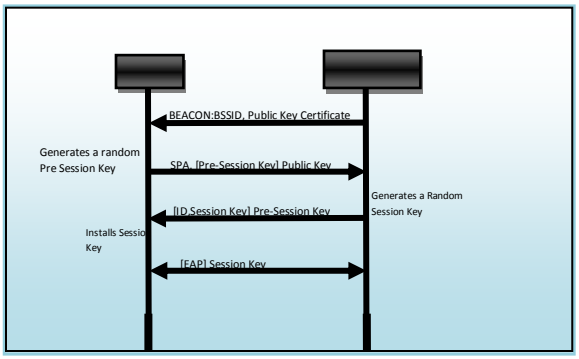

Fig Asymmetric-Key Authentication Mechanism

The access point can broadcast its public key in its BEACON frame and in the probe e frame. The public key can either be accompanied by a certificate or its authenticity can be verified offline. It is also possible to use organization-wide public keys for wireless LANs and broadcast the public key through an offline means. In public places such as airports and restaurants the public keys can be provided to users via notices. In case different Access Points use different Public-keys a certificate authority is required to verity's the authenticity of each public key. In case the authenticity of the public-key cannot be verified then the authenticity of the Access Point is in question since it may be a Rogue Access Point. But the threat of Rogue Access Point can be countered by the two-way authentication of EAP. Thus even if public key cannot be verified it will not result in a major problem. Once the public key of the Access Point is known to the client rest of the authentication procedure is autonomous and secure. The messages exchanged are as follows:
[Frame 1: AP-> STA] BEACON
BSS1D, Public Key, Certificate

[Frame 2:STA-> AP] Association
[Pre-Session Key]Public Key

[Frame :3: AP -> STA] ACK
[ID, Session Key]Pre-Session Key

[AP -> STA] EAP
[EAP] Session Key

Once a session key has been established the station can then follow the EAP authentication procedure to gain access to the services from the network. The public-key of the access point is also used to sign the management frames. The complete procedure ensures that clients first establish a secure Session-Key and then authenticate themselves to the server. Attackers can neither sniff the session key nor launch DOS attacks by blocking the authentication procedure.

2. Mitigation of Attacks

The proposed asymmetric authentication procedure mitigates most of the attacks as follows:

- Protection for Management Frames

In 802.11i there is no provision for protection of management frames. But using asymmetric authentication scheme all management frames that are sent before any session key is established are signed by the public key of the AP and thus protected from any modification. The public-key of the Access Point is known to all clients. Hence the clients can easily verify the signature of management frames. Unicast management frames can be signed by the Session-key to reduce the verification time. But to protect multi-cast management frames the public-key should be used. De-authentication frames are sent by attackers during the open authentication or 4-way handshake. In the asymmetric authentication method both the open system authentication as well as the 4-way handshake methods are not present and all management frames are signed by either the private key of the AP or by the session key. Hence de-authentication attacks are not possible.

- More Key Exchange Mechanism Secure

The proposed key-exchange mechanism is more secure than the earlier 4-way handshake. The vulnerable 4-way handshake is completely removed, so DOS attacks on it will not be possible. In the proposed mechanism all messages are protected.

FRAME-l is protected by the certificate. This protects it against modification.
FRAME-2 is protected by the public-key of the Access Point. Hence only the Access Point can read it.
FRAME-3 is protected by the pre-session key, which only the client knows. Thus only the concerned client can decrypt it.

- Protection Against Insider Attacks

Insider attacks were possible in 802.lli because the session key could be known if the Pres-Shared Key is known and the attacker monitors the 4-way handshake. Since the PSK was same for all the clients, one client could know the session key of other clients. Once the session key is known all

communication between the victim and the AP in that session can be decrypted by the attacker.

But in the asymmetric-key mechanism proposed all clients get a random session key chosen and securely sent to the clients by the AP. Hence all session keys are secure. Even if PSK is used each client will have its separate and secure Session-key making it impossible for other clients to decrypt their communication. Thus the proposed mechanism mitigates insider attacks.

- Mitigation of Denial of Service Attacks

In 802.lli Denial-of service attacks were possible on wireless LANs since management frames were not protected and could be easily forged. The asymmetric-key authentication mechanism protects the network from de-authentication attacks by protecting management frames. The protection of management frames has been described earlier. Now attackers cannot send forged de-Authentication frames. Hence de-Authentication denial-of-service attacks are not possible. , DOS attacks were also possible since FRAME-I of the 4-way handshake was not protected. This enabled attackers to continuously send forged FRAME-I blocking a client from authentication procedure. In the proposed mechanism the 4-way Handshake is replaced y an asymmetric-key session key establishment mechanism h which all messages are authenticated. This mitigates denial of service attacks on the 4-way handshake.

VI COUNTERING THE THREATS

Threat of Rogue Access Points in Wireless LANs

1. Client based RAP detection

The RAP Detector can be deployed in an organization with a large number of wireless users, which are scattered all over the organization

The RAP Detector will be useful for such organizations as it will require little additional infrastructure and can be easily deployed as most organizations already have a DHCP server on which the RAP Detector can be deployed. The RAP detector can be configured to notify the system administrator about suspicious Access Points, which can be investigated to confirm their purpose. As shown in figure wireless nodes are scattered all over the organization. The shaded region depicts the area that can be scanned for rogue Access Points. The details of all the Access Points present in the area will be available at a central location (DHCP Server). Periodic scans can be scheduled that a more comprehensive coverage can be established. This can be done without manual intervention hence enhancing the security of the organization.

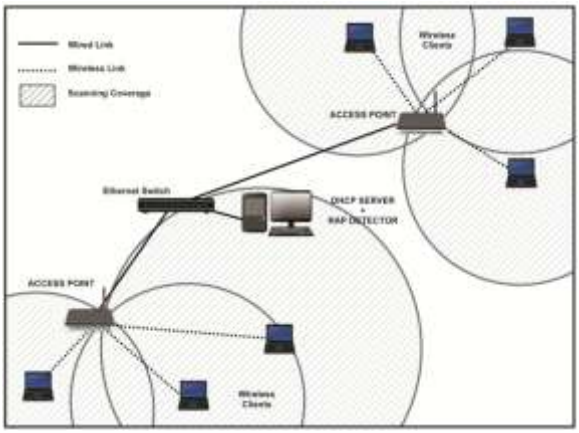

Fig Deployement Senerio Client Based RAP Detector

2. Basic system archrtecture

As shown in figure the complete system consists of three major components; a DHCP server, a Master Agent program having the database of all authentic APs and many wireless nodes (Laptops used by the members of the organization). These Laptops act as client agents. They will execute a small program it all times which will listen for a query from the Master Agent and then send a list of Access Points in its vicinity to the Master Agent. These lists are then consolidated and a list of all detected Access point is generated. This list of detected Access Points is then analyzed for anomalies. It is compared with the database of known Access Points. Also an algorithm to detect Evil-Twin Access Points is run to detect Evil-Twins in the list of detected Access Points.

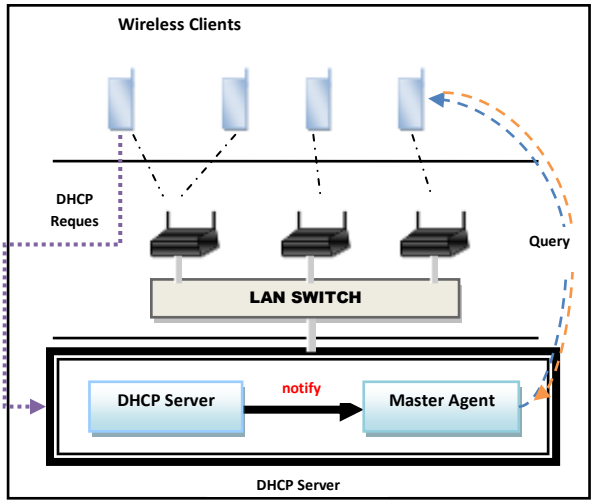

Fig Architecture of RAP detection system

3. Algorithm for Detecting Evil Twin Access Points

Evil Twin Access points are access points that have the MAC address of a legitimate Access Point installed by the organization. They spoof the MAC

address to masquerade as a legitimate Access Point. These Access points are very difficult to detect. Most commercial Access points have methods to detect Evil twin Access Points if they are in the range of the Access Point they are trying to masquerade. This is easy as an Access point can detect if another Access Point in its range has the same MAC address. Hence most Evil Twin access points are placed outside the range of their authentic twin. This fact is used to detect the Evil Twin Access Point. To detect twin the algorithm analyzes the context of each Access Point. It checks that all the clients that detect a particular Access Point are located in the same locality. This is to be expected since two clients that are located far-off should not detect an Access Point. Two clients located far-off can detect the same Access Point only if the Access Point has a twin located at a distance.

The pseudo-code for the algorithm is given in figure

1. For each AP in AP List[]
2. For each CLIENTi that detected A
3. For each CLIENTj that detected AP (i != j)
4. Compare APs detected by CLIENT i and CLIENT j
5. If both lists completely mismatch Flag CLIENTi and CLIENTj as ABNORMAL.
6. IF ABNORMAL clients for AP> Threshold
   i. AP has twins
7. END

4. The Experimental Scenario

To test the RAP detection system, it was tested in a hostel LAN with two clients and a master agent.

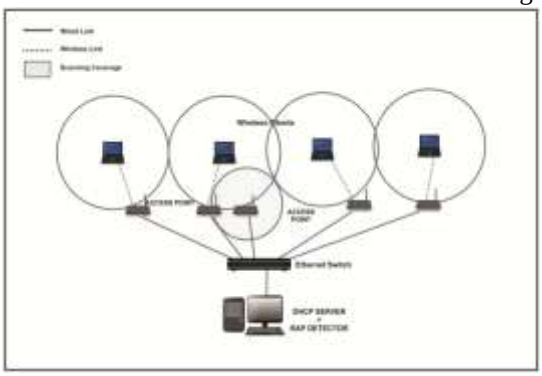

Fig Experimental Setup used to test RAP detector

The experimental setup used is shown in figure For experimental purposes the two clients were located at opposite ends of the building to provide maximum coverage. The IP addresses of the clients were manually entered in the database. Some of the Access Points were manually entered into the database of known APs. The two clients were placed at a distance to provide maximum coverage. Query packets were sent to the clients at regular intervals to the clients. The Master-Agent gathered and processed the response front the different clients and built a list of Access Points in the building. The Access Points entered manually were flagged as Authentic Access Point whereas the Access Points that were not present in the database were flagged as Rogue Access Points. The System was kept running for a period of 30 minutes during which it provided real-time information about all the Access Points in the building. The following parameters were collected about the Access Points in the building:

• MAC ID of the Access Point
• List of clients that detected the Access Point
• Last time when the Access Point was detected.

VII RESULTS

1. Results of RAP Detector

The RAP detector was test in a building with 25 Access points and only two client agents. The two client agents were able to provide information about almost all the access points in the building. Only one Access Point was outside the range of both the clients. 17 Access points were added to the database of known Access Points and hence were detected as authentic APs whereas the rest were flagged as Rogue Access Points. The list of all detected access points was built within a time period of 1 minute. The clients were queried at an interval of 10 seconds and the replies were received almost instantly. In comparison the manual auditing took 30 minutes to scan the building and compare the results with the list of known Access points. Table shows the various results obtained from the experiment.

Result of RAP detection in the Experimental setup

Parameter	Value
Total Access points	25
Known Access points	16
Total Access points Detected	24
Rogue Access points Detected	8

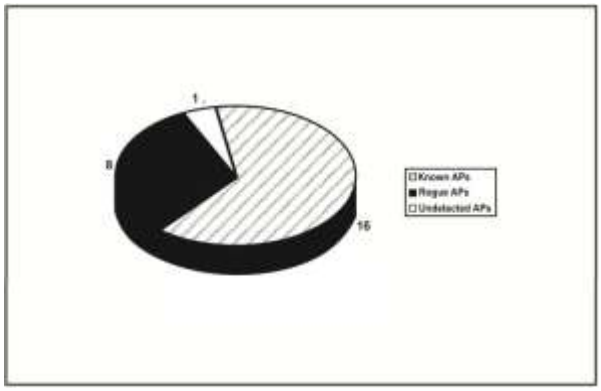

Figure RAP Detection Results

It was very clear from the experiment that in organizations where manual scanning for Rogue Access Points is time consuming, such a centralized client-based RAP detector is very useful. As our system requires almost no additional hardware installation, it can be easily installed in organizations and can provide with real-time, centralized RAP detection.

2. Simulation Results for detection of Evil Twin Access Points

To simulate the performance of the Evil-Twin Access point detection algorithm it was tested in a virtual environment. Since it was not feasible to deploy such a large number of clients and access points the algorithm was tested on a virtual grid of l000xl000. Although Access Points operate in a 3-D space, a 2-D space was used instead for simplicity. The positions of 20 Access Points were randomly generated in a coordinate grid of 1000x1000. Various numbers of client positions were generated. The number of clients varied from 20 to 100.Out of the 20 Access Points two was twins. The algorithm was then used to detect the twins.

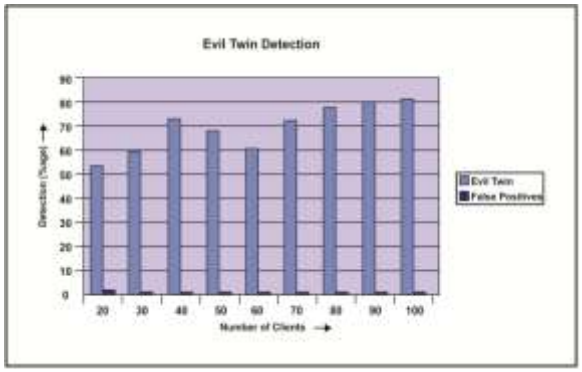

Fig Accuracy of Evil –Twin detection algorithm

For each client-set size the simulation was performed 100 times and the results were noted. The accuracy was calculated as follows:

Accuracy = (Number of Times Evil-twins were correctlydetected)x100
Total number of simulations

False Positive Rate = (Number of times other Access Points were wrongly detected) x 100
Total number of Simulations

A very high rate of success was observed. The algorithm detected the Access Point with twins with a high success rate. The results for various client-set sizes are shown in figure It was observed that accuracy increased with increasing number of wireless client- agents. With 20 clients the accuracy was 54% while with 100 clients it increased to 81%. Although some false positives were detected it was very low and always remained under 2%.

As is clear from the results the accuracy for the algorithm is quite high whereas the false positive rate remained very low throughout all client-set sizes.

VIII CONCLUSIONS

Security is very important in Wireless LANs since they operate in a broadcast medium.

From the obtained results the following can be concluded about the public-key based authentication scheme:

1. The authentication scheme will successfully stop DOS attacks by providing a secure key-establishment mechanism.

2. Both unicast and multicast management frames will be protected from eavesdropping and modification since they will be signed with the public key of the Access Point.

3. Insider Attacks will be stopped by providing each client with a secure session key.

4. Public-key based authentication mechanisms are feasible in wireless LANs without introducing much delay in the authentication procedure. It was seen from the results that while EAP (Extended Authentication Procedure) takes about 2.5 ms, a session key establishment will take around .4 ms with 10 concurrent clients.

The Client-Agent based Rogue Access Point detection system was tested and the following conclusions can be drawn from the results:

1. The client-agent based RAP detection system will be able to provide real time RAP detection capabilities in organizations that have a set of trusted wireless clients.

2. As the results show using the proposed system, even with a small number of trusted clients a very large area can be covered and monitored. In our experiment with only 2 wireless clients an area of 100 sq meters was covered.

3.The Evil-Twin detection algorithm also performed well under the simulation environment. It showed 81% accuracy when the number of clients is 100. The false-positive rate was as low as 1%.

IX FUTURE SCOPE

There is obviously scope for improvement and future work. The possible improvements to our work can be:

1. Although the proposed authentication scheme has been shown to mitigate existing attacks, it should be evaluated by formal evaluation method and predicate logic for the sake of completeness.

2. It was shown that public-key cryptosystem is feasible in Wireless LANs by simulating it on machine with CPU speed comparable to Access Points. As future work the mechanism should be implemented on an actual Access Point and tested for feasibility.

3. The RAP detection system only detects Rogue Access Points. A counter attack system can be incorporated into the Rogue Access Point system to block detected RAPs in the future. This can be done using SNMP to block the port where the Rogue Access Points are connected.

REFERENCES

[1] William A. Arbaugh, "Wireless security is different*" Computer,* Vol.1, pp.99-101, April 2003.

[2] William A. Arbaugh and Shankar, "Your 802.11 Wireless Network has No Cloths," *Wireless Communication, IEEE,* vol.9, pp.44-51, December 2002.

[3] B.Brown,"802.11: the security differences between band I,"IEEE *Potentials*,vol22, pp.22-27,April 2003.

[4] Branch, J., Petroni Jr., N,Van Doorn, L and Safford, D. "Autonomic 802.11 Wireless LAN Security Auditing." IEEE Security & Privacy, May/June 2004, pp56-65.

[5] Wei, W.; Jaiswal, S. ; Kurose, J ; Towsley, D. "Identifying 802.11 Traffic from passive Measurement Using Iterative Bayesian Inference." In Proceedings of INFOCOM, 2006

[6] Shetty, Sachin ; Song, Min ; Ma Larin., "Rogue Access Point Detection by Analyzing Network traffic Characteristics," *Military Communication Conference, 2007*. MILCOM 2007. IEEE, vol.,1. Pp.1-7,29-31, Oct.2007

[7] Wireless LAN Medium Across Control (MAC) AND Physical Layer (PHY) Specification, ANSI/IEEE Std 802.11, 2007.

[8] Johnny Cache and Vincent Liu, Hacking Exposed Wireless:Wireless Security Secrets Solutions, Osborne, McGraw-Hill, 2007.

[9] Sriram, V.S.S.; Sahoo, G.; Agrawal, K.K., "Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN-a multi-agent sourcing Methodology,"*Advance Computing Conference 2010 IEEE 2nd International*, pp.256-260, 19-20 Feb 2010.

[10] Li Wang ; Sriniwasan, B ;Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard," *Networks Security Wireless Communications and Trusted Computing (NSWCTC),* 2010 *Second International Conference, vol no-2*, pp.109-113, 24-25 April 2010.