DETECTING ROGUE BRIDGE ACCESS POINT USING THRESHOLD CRYPTOGRAPHY

Bhale Pradeepkumar.G, T.S. Ravi Chandra, Kolla Raja Sekhar
Indian Institute of Information Technology, Gwalior, India

ABSTRACT
Installing wireless LANs (WLAN) on a broad scale is influenced by performance, availability, reliability and security. The security vulnerability has become the prime factor in wireless LAN design. In the present paper an Effective and low cost wireless LAN security solution has been proposed. It is based on eliminating Rogue Bridge access point and prevents their access to the WLAN by deploying the ID based cryptography and threshold secret sharing. The proposed authentication mechanism gives end-to-end security with less resource consumption and communication overhead. In (m, N) threshold cryptography, the master key is generated from m out of N shares. No one can figure out the key using (m-1) shares. This approach maximizes the overall security of the wireless networks.

KEYWORDS: *Rogue Access Point, Rogue Bridge Access point, Wireless local Area Network, Threshold Key Distribution, identity-based Encryption*.

Notation	Description
$(\varepsilon\, \chi)$	**Key Generation**
H_1, H_2	**Couple of Hash function for some k ε Z**
$F_i(Z)$	**A polynomial over Z_q of degree m-1**
$SS_{ij} = F_i(j)$	**The node P_i generates the sub share for node P_j**
$K_{sj} = \sum_{k=1}^{n} SS_{ij}$	**Master secret key of node P_j**
$K_s = \sum_{k=1}^{m} S_i \lambda_i(Z) \bmod q$	**Master secret key**
$\lambda_i(Z) = \prod_{j=1, j\neq i}^{m} \frac{Z-j}{i-j} \bmod q$	**Lagrange coefficient**
$(K_s) = \sum_{i=1}^{n} \chi_i$	**The mutually created master secret key**
SSID	**Name of the Network**
$\varepsilon\, \chi\, P_{TM}$	**Time stamp of the private key**
$F_{extract}(S_i, SSID)$	**The share of the master secret key of the serving node**

I. INTRODUCTION

As Wireless LAN is becoming more widely deployed, organizations and companies are heavily investing in such networks to take the advantages of mobility, reducing complexity and risk. Also, it should be possible to install wireless networks very swiftly and without the need of expensive, tedious site surveys. Normally, the security needs for a WLAN incorporate availability, integrity, data confidentiality and mutual authentication. A Wireless Distribution System (WDS) expands the range

of wireless networks using Bridge Access Point without the requirement of the wired connection. It is very useful for companies, organizations, universities, offices, shops and public places. The reason behind the popularity and exponential growth is the easy internet access anywhere in the range, without wires. The growth in WLANs also has security threats involved. Numerous associations use the WLAN to give fast and easy access to the intranet and internet enabling workforce. Workers have the freedom to roam in association. At the same time, connection with internet and intranet should always be maintained. It has been indicated that using WLAN helps to boost the productivity of an organization. However the wireless security is all the time an issue which is to be taken care off. The data transferred by the client is broadcast over-the-air. Every one inside the radio coverage can tune easily and extract information. In organizations, wireless implementations commonly involve the wireless security measure like WPA (Wireless Protected Access). WPA gives the authentication and encryption methods to protect clients from illegal access over the WLAN. Still, such security measures cannot defend against the illegal installation of the bridge access point. The staff can connect the illegal bridge AP (generally called rogue bridge access point). Most of the staff ignores the security guidelines that arrive along with this act. The Assailant can bypass the organization network defenses (i.e., access control, firewall) as a result of the rogue bridge AP and pose a major vulnerability to the company. In this paper, the proposed scheme is based on detection and termination of the rouge bridge access point in wireless networks utilizing ID-based encryption [1] and Shamir's (k, n)-threshold scheme [2]. Compared with the PKI-based network authentication approaches, which rely on a trusted third-party server, our approach takes a self-organized group key management without assuming the existence of any centralized trusted third party in the WLAN. Moreover, the proposed authentication mechanism gives end-to-end security with less resource consumption and communication overhead.

II. RELATED WORK

A wireless network is most vulnerable network since everything in this network is broadcast in open media "air". Many approaches for detecting Rouge Wireless Access points (RWAPs) and Rouge Bridge access point (RBAPs) are easily evaded by dark-side hackers. Some organizations equipped Information Security team with Radio frequency monitoring tools (e.g., Air Magnet [3] and Net Stumbler [4]), requiring the security team to walk the campus and enterprise for rogue APs. This type of approach is normally unproductive because manual scanning are time-consuming, tedious and costly. So, to deal with the security issues in the wireless network against rogue (RWAP), Proxim [5] used for monitoring the wired as well as wireless network. They recommended integrated RWAP detection and counter-attack system in ORiNOCO wireless access point (WAP) where wireless rogue/ unauthorized access point detection is capable of using low-level 802.11 active / passive scanning schemes in its coverage area. A strategy to detect (RWAP) in a Heterogeneous Networks (Het Nets) incorporate wireless and wired network. This strategy is applied by analyzing wireless traffic analysis contains two phases:

Phase I: wired LAN and wireless LAN traffic patterns [6]. These traffic patterns assist to find WLAN hosts.

Phase II: this phase have couple of configurable parameters rest on crossing-access and straight-access attempts. Inter arrival time is the best criterion to differentiate wireless and wired traffic. To detect illegitimate mobile hosts link to a (RWAP) [7].

The rogue wireless access point detection systems utilize existing APs. No committed wireless sensor is needed. The proposed system consists of three main components [8]:

2.1 Access Point:

It supports two operating modes:

I. Normal,

II. Sniffer

In Normal Mode the AP (access point) execute as a regular AP and in sniffer Mode it acts like the AP execute as the wireless sniffer gathering surrounding wireless data. New generation access points incorporate such a characteristic.

2.2 Switch:

It is a part of the counter attack process. The switch can down the port to which the RWAP is connected. Normally the administratively down switch port can be managed by SNMP (Simple Network Management Protocol) command. As a result the proposed approach needs the switch with SNMP ability.

2.3 Central System:

It contains intelligent functions such as gathering sniffed information, rogue access point determination, localization and switch port blocking.

III. BACKGROUND

In the last few years, the proliferation of wireless enabled device has caused an increase in the range of places where people perform computing. Simultaneously, network connectivity is becoming an increasingly essential part of computing environments therefore, wireless networks of different kinds have achieved abundant popularity [9].Wireless LAN ingredient includes a radio network interface controller (NIC), access points, repeaters, routers, and antennae that enable wireless applications in buildings and campus areas. These ingredients are elementary unit for effectuate wireless LANs in enterprises, small offices, enterprises, homes and public hotspots.

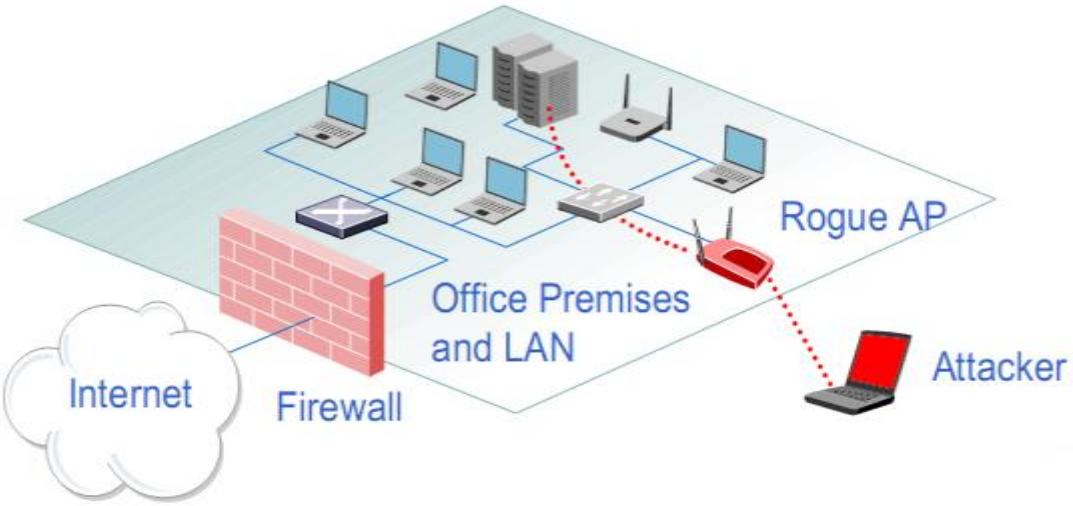

Figure1. Rogue Wireless Access Point (RWAP) [8].

The illicit access point (RWAP for short; sometimes called rogue hotspots) is the "Wi-Fi Hotspots which is setup by an attacker for the purpose of sniffing wireless network traffic" [8]. In this paper we encapsulate the RWAP with two definitions:

Definition 1:

"Rogue wireless access point is the access point that is setup to the network without permission and does not follow the organization's security guidelines" [10].

Definition 2:

"Rogue wireless access point is the access point that is installed for the evil intention to compromise the organizations information system i.e., sniffing information moving across the rogue wireless access point" [10].

The wireless access point with the feature that exhibit either definition is evaluated as a RWAP as shown in Figure 1.

3.1 Rogue access points are classified into four types which are discussed below:

1) Staff rogue wireless access point:

Installed by employees for flexibility and scalability. This is very common because of lack of wireless network security guideline and security awareness practice for staff.

2) Assailant's external rogue wireless access point:

Deployed outdoors of the organization and intents to attract the target staff to join the rogue AP (access point).

3) Assailant's internal rogue wireless access point:

Deployed inner side of the organization and join to the organization's WLAN.

4) Neighborhood rogue wireless access point:

Deployed by the organization which is established in the close vicinity [2].

3.2 Wireless bridge:

A wireless bridge is used to link, two or more LANs or parts of a LAN which are logically and physically isolated is shown in Figure 2. Conventional access points do not always satisfy an organization's necessity for providing coverage, availability, extend the range, and functionality of the existing WLAN by using bridges [7] [11].

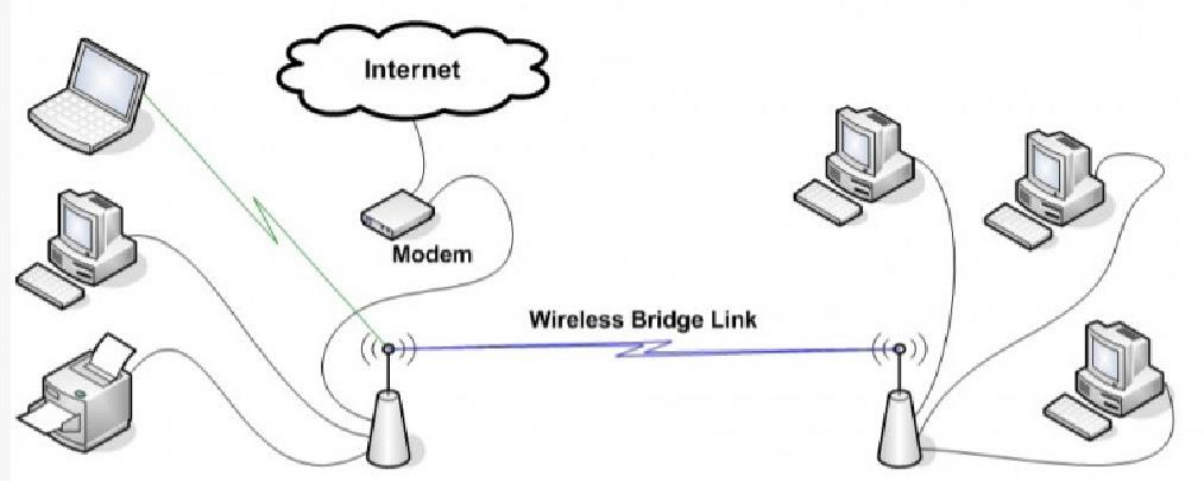

Figure2. Wireless Bridge Access Point [12].

3.2.1 Types of WLAN Bridges:

Basic Ethernet-to-Wireless Bridges: This type of bridge joins to a device through an Ethernet port, and then gives a wireless connection to AP.

Workgroup Bridges: It joins WLAN to wired LAN networks. Substantially a Workgroup bridge serves as a wireless client on the WLAN and then interfaces to an Ethernet. Normally, a Workgroup bridge provides high-end management.

Access Point/Wireless Bridge Combos: The access points (APs) that can be configured as a bridge, but not both at one time. This AP can operate in point-to-multipoint and point-to-point bridge mode.

Rouge Bridge Access Point: Security at the wireless local area network (WLAN) can be gained using Wired Equivalent Privacy (WEP) and Wi-Fi protected Access (WPA) protocol. In spite of utilizing the above security methods, attack surface still exist in WLAN. This attack surface can be correlated to Denial of Service attack (DoS).

3.3 Identity-Based Encryption (IBE):

The idea of ID-based Encryption (IBE) is suggested with the initial purpose of IBE to its simplicity. By using well known identifiers, like email addresses avoid the expensive cost of the PKI (public-key infrastructure) in PKI enabled cryptography. IBE is encoded directly into encryption and authentication methods, exclude the need for heavy certificates and Certification Authorities [1] [2]. Working model of ID based encryption is shown in Figure 3.

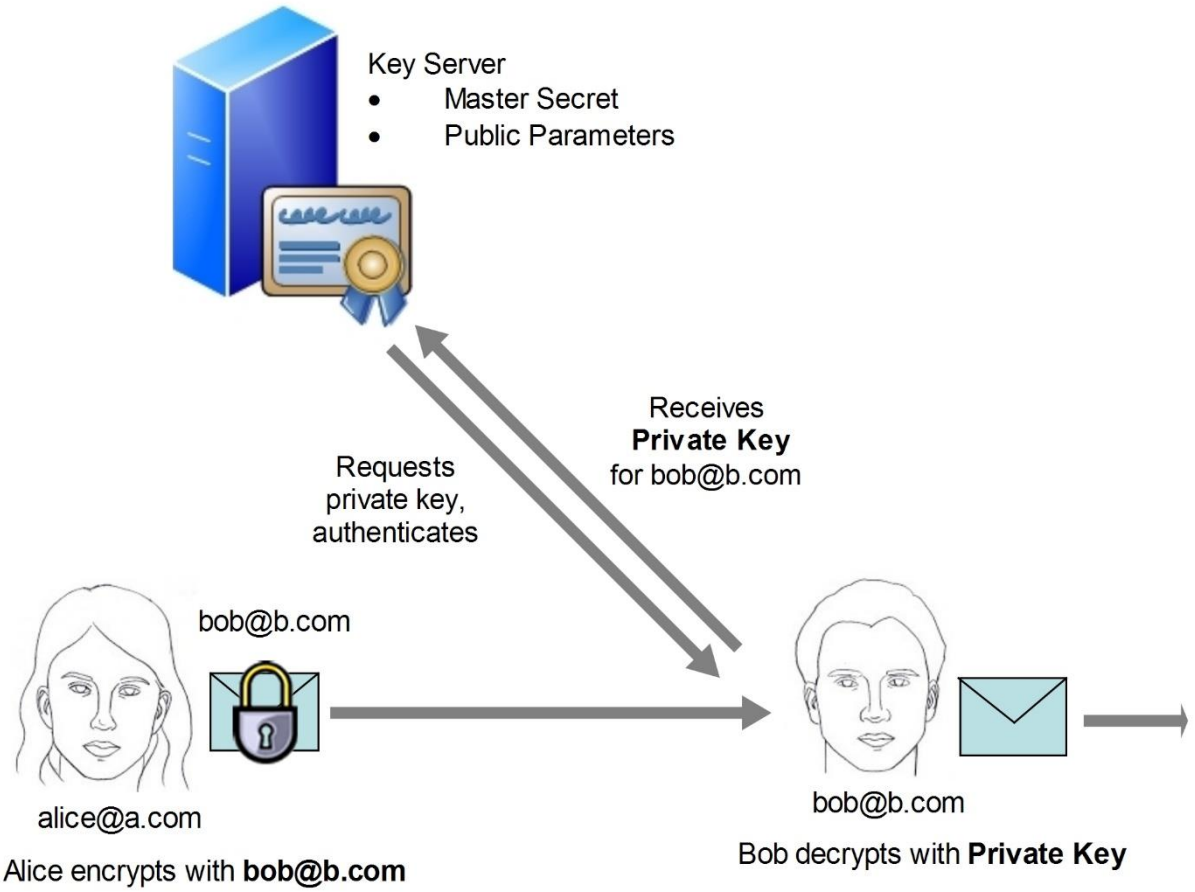

Figure3. Identity Based Encryption (IBE).

An identity based Encryption strategy (IBE) is described by a 4 tuple of algorithms [1]
1. Setup
2. Key Generation
3. Encryption
4. Decryption

1. Set-up: Setup algorithm produces the public parameters denoted by params of the strategy and a master private key.

2. Key Generation: In key generation (k_m) and a public unique id UID $\in\{0, 1\}^*$ and EX (k_m, UID) computes the equivalent private key k_s.

3. Encryption: In Encryption algorithm public unique identity UID and a message MSG, E (UID, MSG) computes a cipher text C.

4. Decryption:

In Decryption algorithm private key K_s and cipher text C, D (K_s, C) returns the plaintext.

3.4 Example:

Let G_1 and G_2 are two cyclic groups with order q, where q is prime .Now we consider the Bilinear mapping f as follows

f: $G_1 * G_2 \Rightarrow G_2$

where A group G is cyclic if $G=\langle b\rangle$ for some $b \in G$ and $\langle b\rangle = \{b^k | k \in Z\}$

Let HF_1 and HF_2 are couple of hash function defined as follows

$HF_1:\{0,1\}^* \rightarrow G_1^+$

$HF_2: G \rightarrow \{0,1\}^m$, where $m \in Z$

An identity-based encryption strategy (IBE) groups is elucidated by the subsequent algorithm

Set-up(η):

$P \leftarrow G_1^+$; b $\leftarrow Z_q^+$;
$P_{pub} \leftarrow bP$; return $((P,P_{pub}),b)$

E X(b,UID):
$Q_{id} \leftarrow HF_1(UID)$; return bQ_{id}

E(UID,MSG):
$Q_{UID} \leftarrow HF_1(UID)$; c $\leftarrow Z_q^+$;
MSG $\leftarrow HF(e(Q_{UID},P_{pub})^c)$;
Return $(cP, MSG \oplus MSG^i)$

D(K_s,(u,v)):
Return $v \oplus HF_2(e^{\wedge}(K_s,u))$

IV. PROPOSED APPROACH

In this section, first the assumption is being described about the wireless LAN and an overview of the proposed approach which integrates the idea of the manageable APs list and distributed key management approach is discussed. The distributed key generation mechanism has been discussed in detail.

4.1 Assumptions

For the generation and distribution of public (K_p) /private (K_s) keys there is no trusted authority, means all keys are created self-perpetuating way and there is no trust among the nodes in the WLAN.2.6.1. Further Subsections are the general assumptions on securing WLAN. The additional assumption that all wireless connections are bidirectional. The WLAN requires (bi-directional) links for evading collisions. This implies that X and Y are two wireless nodes with certain transmission ranges. The transmission range of X is intersecting with the transmission range of Y.

4.2 Threshold Based Cryptography

Consider a wireless local area network (WLAN) which consists of N number of Access Points (APs) in the early phase. The WLAN has secret key k_s it is also named master key, which is utilize to supply key generation service to all existing nodes. The master secret key K_s is shared among the nodes in m out of n threshold scheme. Every node in the network holds secret share of the K_s, and nobody can rebuild the master secret key using their own information. Any m nodes among the network can rebuild the master secret key mutually, because it is impracticable for completely m-1 nodes to do so, even a more chance of a collision is a big deal. The threshold parameter m (1 <= m <= n) modulate the tradeoffs between service availability and security. Taking value (m = 1) result the minimum wireless security with ultimate service availability. Moreover, value (m = n) causes a maximal security but bad quality service availability. The proposed scheme illustrates the fundamental operations of key management approach which is discussed below:

1) Secret key Generation
2) Secret key generation service
3) Master secret key share creation (K_s)

4.2.1 Master Key Generation:

Distributed key generation (DKG) scheme is different from the fundamental **m** out of **n threshold** secret sharing in which it does not require a CA (certification authority) and trusted third party to generate a master key K_s. The K_s is generated cooperatively. The proposed approach is an extension to Shamir's secret sharing [6][13][14] independent from a trusted authority.

The proposed approach is implemented as follows

Distribution Phase - The steps for distribution phase are as follows:

Step 1 - A set P = { P_1 ……. P_n } // P is the no of nodes in wireless environment

Step 2 - Chooses a polynomial $F_i(Z)$ over Z_q of degree m-1 and a secret X_i, such that $F_i(0) = X_i$.

Step 3 - The P_i node generate the sub-share for P_j node like $SS_{ij} = F_i(j)$ for j = 1…….n

Step 4 - Send generated sub-share S_{ij} to P_j // A set {S_1……S_i} of shares for each P_i

4.2.2 Reconstruction Phase:

The reconstruction algorithm accumulates each share Si from share holder P_i and utilizes those shares to build the master secret key as $K_{sj} = \sum_{k=1}^{n} SS_{ij} = \sum_{k=1}^{n} F_i(j)$ =Master secret key of node P_j:

Similarly, to build the master secret key Ks the following steps are used:

Step 1 - Minimum shares are needed to build master secret // A set N $\subset\{P_1\ldots\ldots\ldots P_m\}$ of size m nodes // In order to regenerate the secret key

Step 2 - A set of shares S_i from each $N_i \in$ N // we have taken the shares (m) value from the set to reconstruct the secret key.

Step 3 – Master secret key $K_s = \sum_{k=1}^{m} S_i \lambda_i(Z) \bmod q$

// where $\lambda_i(Z)$ = The Lagrange coefficient

// $\lambda_i(Z) = \prod_{j=1, j\neq i}^{m} \frac{Z-j}{i-j} \bmod q$

Step 4 – The mutually created master secret key is $(K_s) = \sum_{i=1}^{n} \chi_i = \sum_{i=1}^{n} F_i(0)$

Distributed Private Key Generation:

Adopting the concept of ID-Based Encryption (IBE), is a system where any random string may assist as a public key, a user's email address, a date, an IP address, a location are all potential public keys.

Example:

Alice's public key is her e-mail address, "alis@iiit.com".

After authenticating Alice, the key server then returns his private key corresponding to this id.

Bob encrypts the massage using "alis@iiit.com", as the public key.

Alice can decrypt the message using her private key.

No CA (certification authority); no certificates; no CRLs (Certificate Revocation Lists).

In proposed proposal, the public key is generated as K_p = HF(SSID||IPADD||EXPTM)

where:

HF () = A hash function described in (IBE)[2]

SSID = Name of network // (e.g., Secured Comp Lab, Info Security Lab, etc.)

IPADD = An Internet Protocol address (IP Address) // an unique numerical label is used to each device (e.g. Laptop, Access point, etc) participating in a wireless network

EXP_{TM} = the expiration time is protecting from the private key (k_s) is compromised or lost.

When the "private/public key" expired, the AP (Access point) requires its fresh key pair. The best approach to achieve the private key (k_s) is to communicate with the minimum neighbor APs, and appeal key-generation authority (known as PKG) service. The AP that grasps the master key share could be the PKG service AP. In the proposed design, every AP share the master secret key K_s Subsequently all of them could be the PKG service AP. Any of the mPKG service APs produces a secret share of a novel private key k_s and redirect to the requesting AP. To verify the produced shares are safely transferred, the requesting AP additionally it produce temporary public key $(k_p)_{temp}$ while sending request. Every PKG service AP sends shares with encrypted manner to the demanding AP using the demanding APs temporary public key $(k_p)_{temp}$. The methodology of creation of a share of the fresh secret key k_s could be served as a function $(K_s)_i = FUNC_{extract}(S_i; SSID) = S_i k_p$, where S_i(i = 1,……k) is the share of the master secret key of the serving node, SSID is the ID of the demanding AP, k_s, k_p are private key and public key of the demanding AP. In the end this public key information becomes familiar with the entire network. By gathering the m sub-shares of its fresh private key (k_s), the demanding AP can compute its fresh private key $(k_s)_{i=1} S_i k$. Beside this key construction process, the demanding AP gets its fresh private key k_s.

4.3 Proposed security Framework:

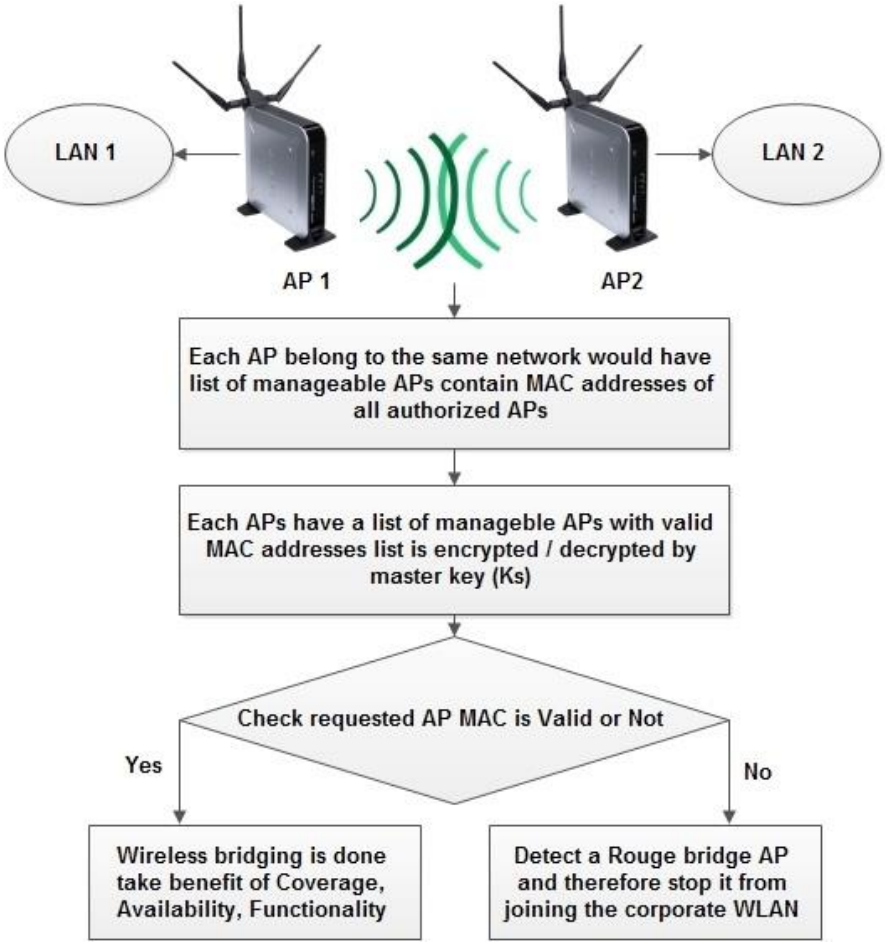

Figure4. Detect Rogue bridge access points.

Wireless Access Point offers the security as (WEP, WPA, WPA2, etc). Even though, security threats can still exist in WLAN.

1. One wireless access point (AP1) request for bridging the other wireless access point (AP2).
2. Each access point (AP) belongs to the same subnet would have a list of managed APs that incorporate MAC addresses of every legitimate APs and list is encrypted by a master key (K_s).
3. Compute a master key on the basic m out of n threshold secret sharing approach in that it does not require a trusted third party (TTP).
4. Identity-based cryptosystem evade the high cost of Public key authentication and management.
5. Any time an access point AP1 attempt to connect the existing subnet by a manageable AP, then decrypt the MAC address list. Check requested access point (AP) MAC address is Valid or Not.
6. Valid MAC address establishes a bridge connection to access point AP2.
7. Invalid MAC address cannot establish a bridge connection to AP2.

This will improve the system availability and WLAN security to prevent unauthorized wireless access points from accessing the wireless LAN illegally.

V. SECURITY EXPERIMENT

In identity-based encryption (IBE), the notions of security for IBE are used by introducing the in distinguish ability under chosen cipher text attack (IND-Id-CCA) [13]. The game for IBE is an IND-Id-CCA, having two parts an adversary (A) and challenger (C). ID contain associated text like SSID, IP address, expiry time that is dealing with Identity Based Encryption schemes (IBE).

The challenger (C) capture as input the security parameter, execute the Setup algorithm. It gives the adversary A the resulting K_p. It keeps master key K_s to itself. Adversary a then execute in two phases (A and B):

Phase A: "A" issues secret key extraction queries< QRI_i , ….., QRI_m> where query QRI_k is one of :

- Extraction query < Id_k> where $Id_k \neq <Id_{challeng}>$.The "C" reply by operational algorithm obtain to generate the secret key $(K_s)_k$ correlative to the identity Id_k.It transmits K_{sk} to the "A"
- Decryption Query <Id_k.CT_k>. "C" reply by operational algorithm obtain to generate the secret key $(K_s)_k$ correlative to Id_k. It then execute the decrypt algorithm to decrypt the cipher-text (CT_i) utilizing the secret key $(K_s)_k$. It transfers the deriving plain-text to the "A".

Above queries may communicate adaptively, every query QRI_k may be based on the responds to <QRI_i,……,QRI_{m-1}>.

Challenge: When an adversary A come to an end Phase A, it outputs two equal length plain-texts $M_x, M_y \in M$. "C" picks a random bit $x \leftarrow \{0,1\}$ and sets the challenge to $CT=Encrypt(K_p, QRI_k, M_b)$ gives CT to the "A"

Phase B : The private key query <Id_k>≠<Id> "C" reply, similar as in phase A. Decryption algorithm query <Id_k,CT_k>≠<$Id_{challeng}$,CT>.The challenger reply similarity as in phase A.

Guess: Lastly, an adversary outputs a guess bit $x` \in \{0,1\}$ and wins the game if x`=x.

The advantage of the adversary is defined as:

$Adv_A IND – Id – CCA_k$.

$Adv_A IND –Id – CCA_k = |Pr[x`=x]-1/2|$

Now,

$2*Adv_A IND – Id – CCA_k$

$2*|pr[x`=x]-1/2|$

$2*|Pr[x` =1|x=1].Pr[x=1]+Pr[x`=0]|x=0].Pr[x=0]-1/2$

$2*|(1/2)*Pr[x` =1|x=1]+1/2Pr\{x`=0|x=0]-1/2|$

$|Pr[x`=1x=1|] – (1-Pr[x`=0|x=0])|$

$|Pr[x`=1|x=1]– Pr[x`=1|x=0]|$

The last result of the mathematical formula is the benefit of "An" in IND-Id-CCA security experiment

5.1 Security Service Analysis:

Confidentiality:

It guarantees that list of manageable APs is not at all revealed to illegitimate entities. Proposed scheme, takes care of confidentiality and Integrity by an identity-based Encryption scheme (IBE).

Availability:

It guarantees the survivability of network services in the presence of DoS attack. The proposed scheme deal with this issue by making the utilization of m out of n threshold secret sharing algorithm. Any m nodes (wireless access points) work jointly for key production. Consequently, security result is tolerant to compromised m-1 nodes.

Authentication:

Authentication is used by a wireless AP when the wireless AP require to know exactly who is accessing the wireless AP. Proposed scheme, acquires a secure authentication by using an identity-based encryption scheme (IBE).Lastly, non-repudiation guarantees that a party to a communication cannot deny having sent the authenticity of their signature on the sending documents that they originated. Non-repudiation is convenient for identification and separation of compromised APs. In the proposed scheme, the packets are signed and encrypted by an identity-based encryption scheme (IBE).

Communication Costs:

- The PKI (public key infrastructure) supported security approach, the proposed methodology has a minor communication costs.
    - The public key and private key pair is created by the service APs of PKI.
    - The public key is obtained using master public key (K_p), any user can construct a public key associated to the identity ID.

- There's no requirement for certificate creation, propagation, and storage.

- While the conventional PKI (public key infrastructure) approaches contain
  - All APs private key and public key pair is self created, the public key is spread in the whole WLAN.
  - To recognize every AP, the public key has to be signed by a trusted (CA) certification party.
  - The certificates are needed to propagate in the whole network, so every AP may fetch another APs certificate.
  - Spreading these certificates and public keys take a plenty of network bandwidth, and network and connection set-up delay.
- Additional, the public key in the proposed scheme is dependent upon every node's identity, and it is much smaller as comparison with the 1024 bits RSA public keys. The properties of utilizing smaller private key and public key pair, without propagating the long-size certificates minimize the computational utilization and communication costs.
- The communication costs in proposed method are predominantly initiated by the process keys generation. In the network beginning stage, n nodes require to create together the master key K_s pair in self-organizing patterns that raise the network setup time. Furthermore, several wireless access points requires to broadcast a key generation demand to its neighborhood, and every PKG service node respond by forwarding the sub-share of the secret key k_s of the requesting node is shown in Figure 4.
- We utilize Shamir's (m, n) -Threshold Scheme to improve the fault-tolerance of the wireless LAN, at the same time initiates additional communication costs to the WLAN. One appealing point is that if same system is implemented using traditional PKI based scheme, a much bigger communication costs are predicted.

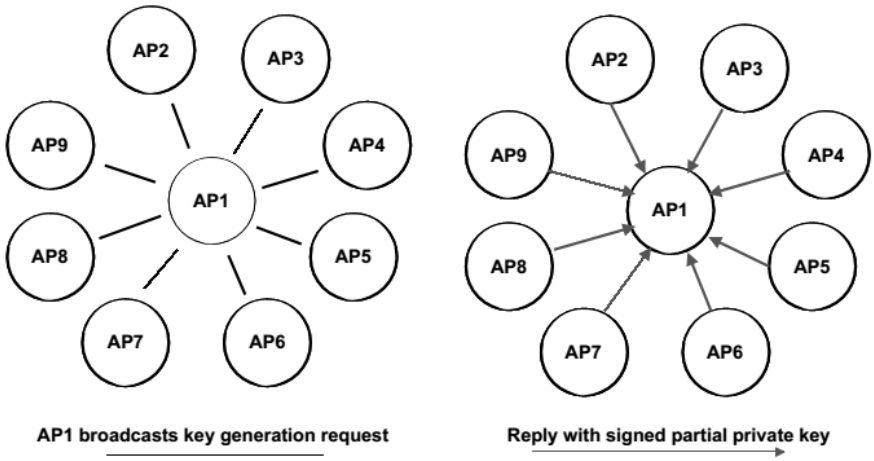

Figure5. Key generation request and PKG service node reply.

Computational Complexity:

The major computations in proposed method are listed as follows:

1. Key generation
2. Key operations

In key generation and key operations for example encryption, decryption and verification. The master key generator uses threshold secret sharing, and the computational complexity depends on the number of share holders. The computational complexity of identity-based signature generation and verification is the same as the traditional schemes, and the identity-based encryption is analogous to the traditional schemes, with just somewhat variance. As we mentioned prior, utilizing shorter size keys within our identity-based methodology results less resource utilization.

VI. CONCLUSION

Wireless LAN is an emerging research field with plenty of productive applications. Still, the security issue in the WLAN is not trivial to look for a proper solution. In this paper, various security procedures for WLAN have been defined. Mainly the security issues at bridge access points as well as access points have been considered. The paper proposes a new efficient security solution; threshold master key based encryption on the manageable APs list so that no one (outside the network) can alter it, and evades some common attacks against wireless access point. The principal contribution of the proposed wireless LAN security solution depends on the subsequent aspects:

1. A new security scheme for WLAN installing the concept of distributed master key encryption.
2. Detecting rogue wireless bridge AP as well as RWAP and denying their access to the wireless LAN. Minimize communication overhead and computational cost than the traditional schemes.
3. Totally avoid a trusted third party.
4. Finally the existing WAP (wireless access point) to identify a rogue wireless bridge access point and as a result prevent it from connecting to the corporate wireless LAN. This will stop unauthorized wireless access points from accessing the wireless LAN illegally.

The most notable advantage of the proposed strategy has a minor communication overhead and computational cost while amplifying the Wireless LAN Security. Since the threshold master key based encryption with a cost significantly smaller than the traditional public-key cryptosystems.

REFERENCES

[1] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology CRYPTO 2001.Springer Berlin Heidelberg, 2001, pp. 213–229.
[2] H. Deng and D. P. Agrawa, "Tids: threshold and identity-based security scheme for wireless ad hoc networks," in Ad HocNetworks, vol. 2, 2012, pp. 291 – 307.
[3] Airwave., "The most powerful rf management for wireless lans," in http://www.airwave.com.
[4] NetStumbler., "Wi-fi security," in http://www.netstumbler.com.
[5] P. W. network, "Rogue access point detection: Automatically detect and manage wireless threats to your network," in Whitepaper Tech Republic, CNET Networks, 2004.
[6] D. Galindo, "Boneh-franklin identity based encryption revisited," in Automata, Languages and Programming, vol. 3580, 2005, pp.791–802.
[7] G. Kbar and W. Mansoor, "Securing the wireless lans against internal attacks," in Mobile Ad-Hoc and Sensor Networks, vol.4864. Springer Berlin Heidelberg, 2007, pp. 814–821.
[8] S. A. P. Ganesh B. Bandal, Vidya S. Dhamdhere, "Rogue access point detection system in wireless lan," vol. 2, Issue 5.International Journal of Computer Technology and Electronics Engineering (IJCTEE), 2012.
[9] http://www.ons.gov.uk, "Securing the wireless lans against internal attacks," in People using wireless hotspots, GB, 2011.
[10] S. Srilasak, K. Wongthavarawat, and A. Phonphoem, "Integrated wireless rogue access point detection and counterattack system," in Information Security and Assurance, 2008. ISA 2008. International Conference on, April 2008, pp. 326–331.
[11] A. Hills, "Large-scale wireless lan design," in Communications Magazine, IEEE, vol. 39, 2001, pp. 98–107.
[12] W. Bridge., "Wireless bridge access point and types of wlan bridges," in howto.cnet.com.
[13] G. Barthe, B. Grgoire, Y. Lakhnech, and S. Zanella Bguelin, "Beyond provable security verifiable ind-cca security of oaep" in Topics in Cryptology CT-RSA 2011, vol. 6558. Springer Berlin Heidelberg, 2011, pp. 180–196.
[14] A. Shamir, "How to share a secret," vol. 22. ACM, 1979, pp. 612–613.

AUTHOR'S BIOGRAPHY

Bhale Pradeep Kumar.G received his M.Tech. degree in Information Systems from Indian Institute of Information Technology & Management, Gwalior, India in 2014. His research interests include Wireless Networks, Information Security and privacy, ad hoc networks, and wireless communications.

T.S. Ravi Chandra is currently pursuing his Integrated post graduation course in Information and Communication Technology at Indian Institute of Information Technology & Management, Gwalior, India. His research interests include wireless networking, network security, vehicular networks, sensor networks, network simulation and modeling.

Kolla Raja Sekhar is currently pursuing his Integrated post graduation course in Information and Communication Technology at Indian Institute of Information Technology & Management, Gwalior, India. His research interests include vehicular networks, mobile ad-hoc networks, intelligent systems and wireless networking.