# A Novel Technique to Protect Wireless Network against accidental Association

Geetha Manchi Reddy
B.Tech - Student
Department of CSE
JNIT, Hyderabad

Keerthi Priya Nallan Chakravarthula
B.Tech - Student
Department of CSE
JNIT, Hyderabad

Abhilash Reddy Kantu
1st author's affiliation
B.Tech - Student
Department of CSE
JNIT, Hyderabad

G. Manjunath
PhD, Head
Dept. of CSE &IT
JNIT, Hyderabad.

## ABSTRACT
With increasing numbers of corporate and organizations deploying wireless network and allowing the company personnel to access the internet or the wired backbone through wireless access points are increasingly getting exposed to hacking attacks. Due to easy hacking tools and less concerns about the security threats of the deployed, various crucial data of the private network is hacked. One of the important forms of a security loophole in the wireless network is accidental association. In this paper we propose a novel technique to secure the wireless signal to prevent accidental association. Layer 2 of each device is assigned with a unique time bound key and non time bound primary key. As soon as a new device is detected in the proximity by any node, it requests for the time independent primary key from the device. If the device fails to respond with the key then the network connection is withdrawn with immediate effect after the node propagates an alert message encrypted with time bound session key through which it is communicating securely with other wireless peers. A periodic search for checking new devices which may get associated with the existing network accidently is avoided with utmost efficiency. The protocol is tested with Omnet++ simulator and results shows that the proposed technique performs much better than basic protection against such an attack offered by WEP.

## Keywords
WEP, Accidental Association, Wireless Network Security, Dual Key Protection Scheme.

## 1. INTRODUCTION
A wireless network essentially operates the same way as it's wired equivalence but with a difference that such a network is vulnerable to signal leak as the signal and the information is not propagated through closed and secured digital data carrier like ISDN lines or Ethernet connection. Rather data is transmitted in the open air with suitable addressing scheme which enables only the desired destination node to get access to the data. The fundamental can be understood from figure 1.

It is quite clear from figure 1 that in any wireless communication when a node attempts to communicate with any other node, the signal may reach to other devices that are not intended to be communicated. This is called accidental association. Many network deplorers are ignorant about the vulnerabilities of such systems.

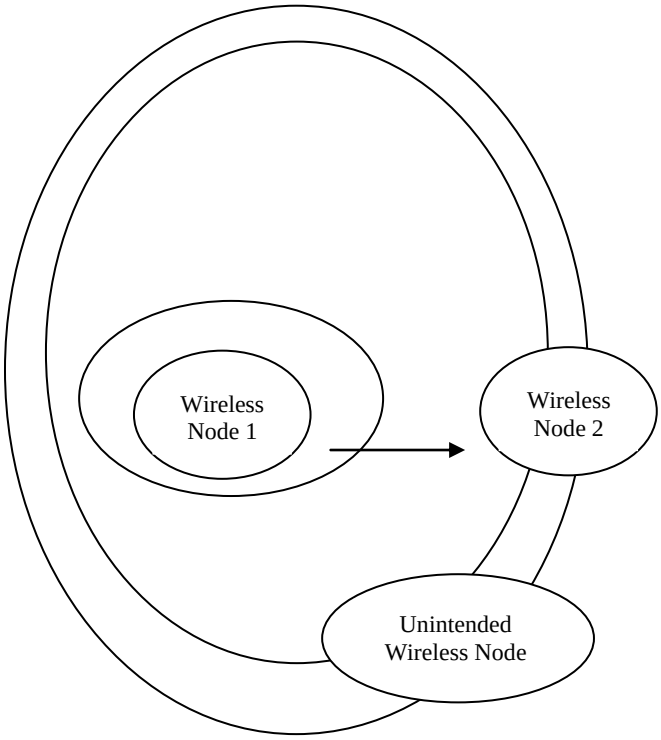


**Fig 1. Accidental Association**

Let us assume that the network deploys a secured communication with the help of key exchange. Therefore for any communication to take place between two nodes, the data needs to be encrypted with keys mutually agreed by two nodes. This key is exchanged at the beginning of the session. Now consider that there is an accidental association and the associated node is able to read the signal at the beginning of the session, then the exchanged key is also exposed to this node. Thus the associated node once gets hold of the key will be able to decrypt any further message being exchanged between the valid nodes as this node also has the authentic key for decryption. Therefore checking the network for any such association and protecting it against such an association is an important aspect.

Now let us discuss about the conventional security offered by WEP against such an association. Once the network is

initiated, as soon as any new device using the same wireless protocol like ieee802.11 comes in the proximity of the devices, it's Mac address or the IP address or high level device name is fetched by the neighboring node. If the node is not authenticated or trusted, then different preventive measures can be taken which includes disassociation even from the existing and ongoing sessions.

Now, assume a simple case of hacking where the hacker manages to stream off device discovery. In such scenarios, the untrusted device will not be discoverable by the other peers but the signal will reach to this device none the less. MAC address of the incoming packets is checked at the MAC layer and the layer discards the packets that are not intended for this node. But if the MAC layer of a device is ticked to push all received packets to higher layers then the accidental association can be used as the first step for hacking the data.

Assuming that the accidentally associated node is not exposed to the genuine keys that are used for encryption of the data, still important information like the amount of packet exchanged between source and destination node, their delay and other information's can be leaked.

## 2. RELATED WORK

Threats and vulnerabilities are associated with each of the three basic technology components of wireless networks (clients, access points, and the transmission medium). There are commonly available countermeasures that can decrease these risks [1]. DoS attacks can be performed easily on WLAN which reduces throughput of communication considerably to make inaccessible wireless connection for its authorized members [2]. Different methods exists that hackers are exploiting weaknesses in 802.11 LANs and different hacking tools [3] which gives rise security issues and possible attacks [4]. Rogue wireless devices are an ongoing threat to corporate wireless networks. Network owners need to do more than just scan for unknown devices: they must be able to detect, disable, locate and manage rogue/intruder threats automatically and in real time.[5]

The use of GSE methodology to analyze the incompleteness and uncertainties in specifications is proposed and the IEEE 802.11i security protocol is used to compare the effectiveness of the GSE and UML models [6].

The management and maintenance of modern communication networks have posed many grand challenges to both industrial and academic communication communities. To overcome these challenges, it is very necessary to find new levels of autonomy and intelligence in designing, deploying, managing, and maintaining communication networks. Embedded software and systems are closely related to our daily life, which reside from smart appliances to unmanned trains. The Protection of data for unauthorized access in Wireless Networks -security Aspects is of major concern [7]. A security protocol for wireless computer virtual laboratory has been presented. The primary motive for this paper has been achieved through the use of fingerprints authentication and intermittent pop-up screen for user verification [8]. WLAN is deployed as an extension of already existed wired LAN. Therefore it is necessary to provide the security of WLAN equals to Wired LAN[9].[10]describes some of the common attacks which can be performed against IEEE 802.11 based networks..

## 3. PROBLEM FORMATION

Before we understand the security essential being proposed by this paper, let us first understand the real time threat or the attack model on the basis of accidental association. The principle threat model is depicted by figure 2.

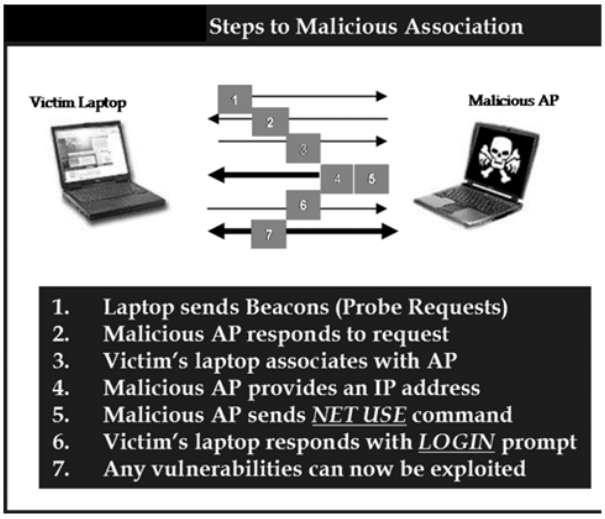


**Fig 2. Practical attack model of accidental association**

As the victim's node sends out a probe to get associated with an AP, the hacker's access point responds to the victim's request. After providing an IP address to the victim's workstation, the Hackers AP can begin its attacks. In such a situation, the hacker can use the vulnerabilities on the victim's node. This can include installing the Host AP software or hardware or any other node configuration techniques.

Such an association attack demonstrates that WLAN are subjected to diversion and nodes do not know which network or AP they are connecting to. Nodes can be tricked or enforced to connect to a malicious AP. Even WLANs that have deployed VPNs are vulnerable to malicious associations. Such an attack does not try to break the VPN. Rather, it takes over the insecure client. Therefore it is quite a fact that t the first and most important step towards securing a wireless network is to prevent the hacked or the malicious node from responding to the beacon packets. One of the alternatives to protect against such an attack is to deploy authentication depending on an authenticated set of MAC addresses. While this gives a low level security for miniature deployments, MAC addresses were never thought to be used in the manner described to exploit vulnerabilities. A user can change the MAC address of a node to change its "identity" and defeat MAC based authentication. This threat model is called MAC spoofing. Hence though authorization based association is a preferred alternative, even such a model comes with a huge security threat as depicted by figure 3.

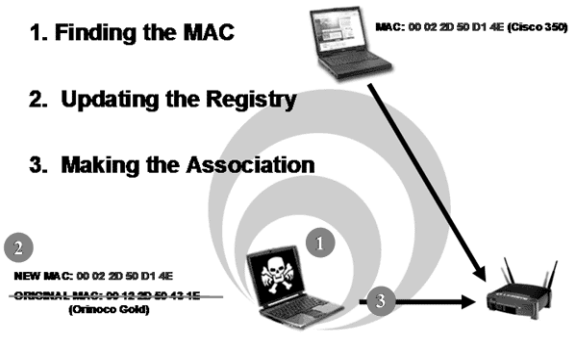


**Fig 3. MAC Spoofing**

Therefore it is quite significant to secure the first stage of the wireless communication, i.e. the association itself. Next section elaborates the model in detail.

## 4. PROPOSED SYSTEM

Let there be a secured key Tp which is time independently distributed across all the wireless nodes that intent to be part of the current communication. Whenever the device broadcasts its beacon, it is encrypted with Tp. Therefore there is no key exchange at the beginning. There is a possibility that the malicious node get hold of the secured key and able to respond to the encrypted beacon. Once a node discovers a neighbor ( assume the neighbor to be an attacker), it needs to mutually exchange a key which is used for the authorization rather than any encryption. This key is time bound and is generated with a random function generator before accepting a connection from a node. The key generated at node 1 is requested to be sent from node 2. Now if the user of node 2 is not known to node 1, it will not be able to send the exact key. Assuming that in such a situation the attacking node may attempt to generate the key multiple times and try to break into the session, number of valid attempts is limited. This key can be exchanged by the user of the systems using vocal exchange or any other form of communication other than the underneath wireless network. As soon as the failed attempt is tracked and traced, appropriate measure is taken for prevention. Which includes the nodes going into sleeping mode withdrawing all form of communication for certain sleep period. Before the node detecting a security threat goes into sleep, withdrawing its wireless interface, it exchanges a alarm message by broadcasting the message. This message triggers switching off of the wireless interface by all neighboring nodes. Such a system is event driven and triggers an alarm only incase a security breach is detected. Now there could be an alternative attack where the attacker does not respond to the beacon message and it's intention is to just read the wireless data rather than accessing any resources of a client. In such a system the model fails to provide enough security. Therefore we extend the technique with a monitoring phase where the every active device preemptively look for the presence of the other wireless interfaces and request every present interface with an encrypted dummy beacon. The technique expects each node to respond to this preemptive beacon. Once beacons are exchanged the nodes keeps track of the total number of communicating entity. Any entity that is detected through beacon exchange but does not participate for long time also triggers the alarm.

## 5. METHODOLOGY

For simulating the Technique we used Omnet++ discrete event simulator. Three types of nodes are randomly placed at random distances over the network of 500 meters such that the radio range of different nodes is overlapped. The types of nodes are Access point, valid client and other nodes which we call intrusive nodes. Though these nodes may not always start an association attack they have a high probability of getting associated with a valid session accidently. Below the algorithm is presented in detail.

Let N be number of nodes, S be the source and D be the destination. Let P packets are to be transmitted between source destination pair of a session.

K=0;

For i=1:1:N

Transmit Advertising packet along with time stamp.

K++;

End

handleHello:

for i=1:1:K

for j=1:1:N

Store Tj at i

Prepare neighbor table

end

end

for each node n in neighbor table

if(n is new)

request n the session key

if(!IsValid(SessionKey(n)))

NOTIFY_BROADCAST

WITHDRAW_NETWORK_INTERFACE(t)// t is the time for passive mode

Else

ExchangeKey(n)

end

end

//Data Transmission

For(i=1:P) // where P is number of packets

AtSender:

C=EN(MSG,Ti+1) where Ti is the TimeBound exchanged key

Send C

AtReceiver:

D=DC(C,Ti)

end

where EN and DC are encryption and decryption function.

## 6. RESULTS

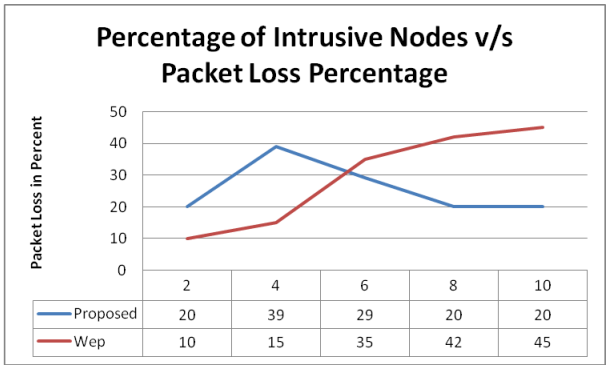


**Fig 4. Plot of % of Intrusive Nodes versus Packet Loss%**

The Figure 4 shows that as number of Intrusive or non non-communicating node increases in a wireless network, Packet loss percentage increases with WEP enabled interfaces. The loss is due to excessive packet exchange and interference

from other nodes. But as the proposed technique withdraws network interface as soon as an accidental association is detected, the losses are minimum.

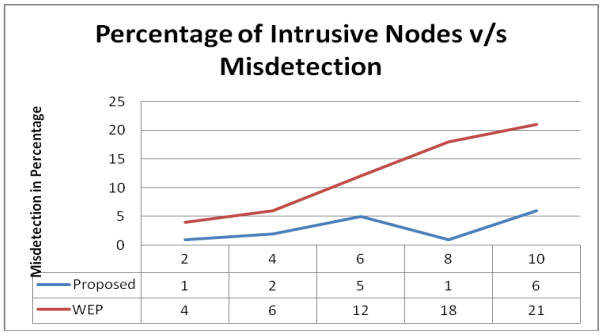


**Fig 5. Plot of % of Intrusive Nodes versus Misdetection**

Misdetection of WEP increases with increase in number of nodes. This is due to the fact that there are no active probing in WEP which makes the protocol vulnerable when there are several other nodes in the vicinity of the communicating nodes. Proposed technique on the other hand depends upon secret session key and relies on a second layer key for communication. Therefore losses are minimum even when number of intrusive nodes increases.

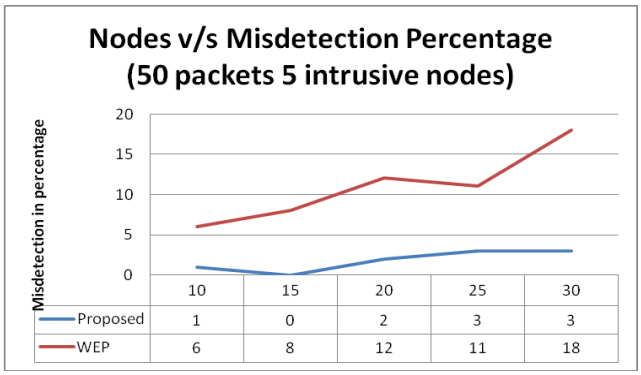


**Fig 6. Plot of Nodes versus % of misdetection**

As number of nodes increases, (Here we also increase the number of sessions), number of overlapping sessions also increases. This results in reception of many packets that belongs to other session. In terms of security loophole even the nodes communicating in other valid sessions are intrusive to any other authenticated session. Therefore accidental association must be avoided even with those sessions. The performance graph in figure 5 and 6 clearly shows that the proposed technique performs better in this aspect than WEP due to separate key for each session which is refreshed periodically even in the middle of a session.

## 7. CONCLUSION

Accidental association is one of the primitive and common modes of wireless attack. Very little research is dedicated to solve the problem. It is considered that even with a Weak WEP, accidental association can be avoided. But through our research we show that WEP is vulnerable in a bigger network and overlapping sessions. In order to avoid packets from one session to reach the other or to avoid intentional and non intentional eavesdropping, stronger mechanism must be developed. The proposed work offers not only a secured communication by secret exchange of key but also protects the process of key exchange through mutually agreed session key which is derived from a function known only to valid nodes of the network. Results show significant efficiency in detection and avoidance of accidental association. The technique can further be improved by adding a piggyback layer where a node can notify the other peer of it's session about the status of wireless interface and number of other devices being listen by the interface. Such a technique can help reduce the misdetection rate further.

## 8. REFERENCES

[1] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.

[2] Mina Malekzadeh, Abdul Azim Abdul Ghani, Jalil Desa, and Shamala Subramaniam,"An Experimental Evaluation of DoS Attack and Its Impact on Throughput of IEEE 802.11 Wireless Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.8, August 2008.

[3] Wireless LAN Security – What Hackers Know That You Don't, White Paper.

[4] http://homepage.ntlworld.com/leon.stringer/cs/FCC/Detecting_and_Investigating_Wireless_LAN_Security_Breaches.pdf

[5] Best Practices for Rogue Detection and Annihilation, A Technical Whitepaper, November, 2004.

[6] Sithirasenan E., Muthukkumarasamy V., and Powell D. 2005. IEEE 802.11i WLAN Security Protocol – A Software Engineer's Model. Proceedings of the 4th Asia Pacific Information Technology Security Conference. pp. 39–50.

[7] Ravneet Kaur, "Protection of Data for Unauthorized Access in Wireless Netwoks Security Aspects", IJCEM International Journal of Computational Engineering & Management, Vol. 15, Issue 1, January 2012.

[8] Edward N. Udo, Imo J. Eyo, Ini J. Umoeka, "Developing a Security Protocol For a Wireless Computer Virtual Laboratory (WCVLAB)", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2 No. 6 Dec 2011-Jan 2012.

[9] D. M. Gharge and S. V. Halse, "WI-FI (802.11) SECURITY ISSUES AND ITS SOLUTION", International Journal of Computer Science and Communication Vol. 2, No. 2, July-December 2011, pp. 587-591.

[10] www.ja.net/documents/services/wtas/known-wireless-attacks.pdf