Cloned Access Point Detection and Prevention Mechanism in IEEE 802.11 Wireless Mesh Networks

Shafiullah Khan[1,2], Noor Mast[1,2] and Kok Keong Loo[1], Ayesha Salahuddin[3]

[1]School of Engineering and Design, Brunel University, United Kingdom
[2]Kohat University of Science and Technology (KUST), Pakistan
[3]Allama Iqbal University Computer Science Department Islamabad, Pakistan

***Abstract*:** IEEE 802.11 Wireless Mesh Network (WMN) is an emerging low cost, decentralized community-based broadband technology, which is based on self-healing and multi-hop deployment of Access Points (APs), so that to increase the coverage area with maximum freedom to end-users to join or leave the network from anywhere anytime having low deployment and maintenance cost. Such kind of decentralized structure and multi-hop architecture increases its security vulnerabilities especially against the APs. One of such possible security attack is the placement of cloned AP to create serious performance degradation in IEEE 802.11 WMN. In this paper, we discuss the different security vulnerabilities of AP in IEEE 802.11 WMN along with possible research directions. We also propose a mutual cooperation mechanism between the multi-hop APs and serving gateway so that to detect and prevent the possibility of cloned AP. In this way the large scale exploitation of IEEE 802.11 WMN can be eliminated.

.

Keywords: Wireless Mesh Network, Denial of Service (DoS), Security, Multi-hop, Cloned Access Point

1. Introduction

Wireless broadband networks are the hot topic. The industries and the researchers are trying for such a broadband technology which ensures high bandwidth internet provision to a large geographical area with minimum deployment and maintenance cost having maximum flexibility for end users to connect from anywhere anytime. The broadband wireless technologies like IEEE 802.11 WLAN and IEEE 802.16 WMAN are making progress rapidly.

Now, the emerging 4th generation broadband technology of WMN, which is decentralized, self-healing, self-configuring and facilitates the integration of other wireline and wireless networks such as WLAN, WMAN, Cellular, Sensor and LANs. Both IEEE 802.11 WLAN and WMN use APs as backbone devices. Being single-hop in nature, WLAN's AP directly connects each node with the internet. In IEEE 802.11 WMN, the APs serve in multi-hop manners, and the end-user nodes may be one-hop, two-hop, three-hop and so on away depending on the distance between the client nodes and gateway. Normally, there is one gateway, and all the APs in WMN are directly or indirectly (forming hops) connected with the gateway for broadband access.

Furthermore, IEEE WMN is self-healing and self-configuring in nature. Unlike, WLAN, WMN conducts three levels of operations. At the lower level, the mesh nodes operate which are either static or mobile. APs or mesh routers form the multi-hop structure at middle level by connecting the mesh nodes directly with gateway or indirectly (through another AP). At top level, mesh gateways are in operations, which are connected with the Internet. The traffic flow in WMN is between the mesh nodes and the gateways through the multi-hop backbone of APs. The multi-hop architecture and self-healing nature of WMN greatly reduce the maintenance and deployment cost as compared to WLAN, however increases security vulnerabilities to many potential attacks against network devices like APs.

Being a key component of WMN, APs may be the key targets of the attackers. In the current setup of WMN, APs are not fully secured, and the attackers not only conduct physical damage but also can easily compromised it by launching passive, active and Denial of Service (DoS) attacks. In passive attack, the attackers only analyze the network traffic passing through the APs to get valuable information without harming the traffic or APs. In active attack, the attackers may create serious routing disruptions by altering or dropping the packets or selectively forward the packets toward the destination. In DoS attack [5], the attacker makes the services of AP unavailable to the legitimate users by flooding to overflow the AP's resources such as memory, computational or bandwidth. One of such attack in the multi-hop architecture and self-healing nature of WMN is the placement of cloned AP at the desired location.

Cloned AP can be used for passive traffic analysis as well as active packets dropping or selective forwarding. However, the severe type of attack using cloned AP would be DoS attack, in which the cloned AP may be used to isolate the particular location from the rest of the network, and hence the legitimate users will not be able to access the broadband services. Keeping in view the importance of IEEE 802.11 WMN and the severity of cloned AP attack, we proposed a mechanism which is based on the mutual cooperation amongst the backbone APs and the serving gateway so that to detect and prevent such kind of attack, which may result in a large scale exploitation of the broadband services.

This paper presents two principal findings. First, all possible security vulnerabilities of AP in IEEE 802.11 WMN are described with possible research directions. Second, we elaborate the possibility and severity of cloned AP attack in the multi-hop architecture and self-healing nature of IEEE 802.11 WMN, and propose a mutual cooperation mechanism

Received September 23, 2008

between the multi-hop backbone APs and serving gateway to eliminate the possibility of cloned AP attack. The remaining of the paper continues by giving an overview of the AP mechanism in IEEE 802.11 WMN along with features, specifications and encryption weaknesses. Then the possible vulnerabilities of APs in IEEE 802.11 WMN and some future research and mitigation techniques are discussed. Next, the cloned AP attack and its consequences in IEEE 802.11 WMN are described. Finally a mutual cooperation mechanism is proposed between backbone APs and the serving gateway so that to avoid the possible large scale exploitation due to the cloned AP attack.

2. AP Mechanism in WMN

In IEEE 802.11 WMN, the APs are the backbone devices that operate in many modes such as single-radio wireless mesh, dual-radio wireless mesh and multi-radio wireless mesh at physical layer [10]. In single-radio mesh also known as first generation mesh, each node acts as an AP, and relay traffic for other nodes. The same radio is used for nodes as well as backhaul access, which is the inexpensive form of wireless mesh network, but may result in traffic congestion due to the heavy load, and will not deliver efficient broadband services to large coverage area.

The scalability of WMN can be improved by using dual-radio mesh which is also called second generation of mesh, in which the APs having two separate radios for client access and the backhaul connectivity, and this technology separated the user traffic form backhaul traffic. This offers significant performance improvement, However, in dual-radio; the backhaul shared medium contention may decrease the capacity and increase the latency.

To overcome the problems of dual-radio architecture, third generation multi-radio solution was proposed, which uses separate radio for client access and multiple radios for backhaul so that to improve the capacity and to decrease the latency, as in multi-radio scheme, multiple radios are dedicated to backhaul. Regardless of the radios scheme used in WMN, APs form the backbone multi-hop architecture to reduce the cost and to increase the coverage area. These are used to connect the mesh nodes with the gateways to access the broadband services. In Fig. 1, it is shown that node C is two-hop away from the internet, while node D is three-hop away. Nodes I and H are four-hop away. It should be noted that in IEEE 802.11, the clients can also relay traffic for each other, as node D is relaying traffic for nodes H and I, where both these nodes are not in the direct communication range of any AP or mesh router. There may be some confusion over the Wireless Mesh Router (WMR) and AP. The main difference is that, an AP allows a client to access a single network, while the WMR allows a client to access multiple networks. One AP can communicate with 30 nodes located within the transmission range of 100 meters. However, factors such as placement, height, obstacles, weather, operating radio frequency and the power output can significantly decrease the actual communication range.

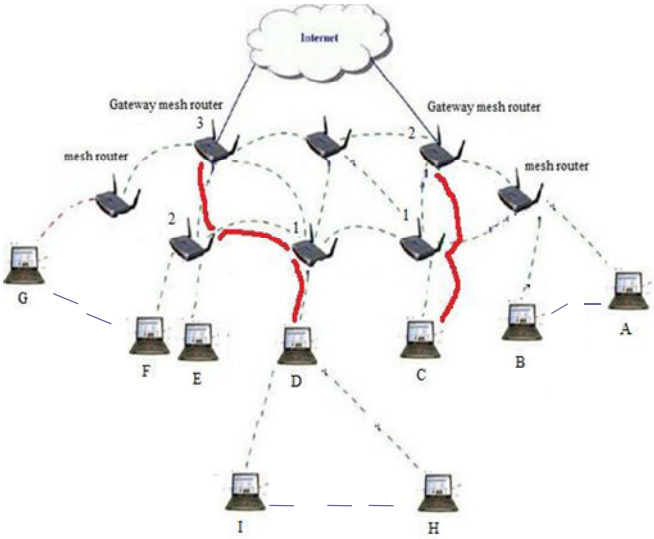

Fig. 1. WMN Architecture

The current standards of IEEE has made significant progress as

- IEEE 802.11b standard provides 11 Mbps bandwidth
- IEEE 802.11a and IEEE 802.11g provide 54 Mbps bandwidth
- IEEE 802.11n ensures 540 Mbps bandwidth

However, if all the overheads are considered such as interference, MAC contention, 802.11 headers, ACK and packet errors, the actual goodput available is almost half [5]. In IEEE 802.11 WLANs and WMN, *Probe request* frames are used by client nodes to discover and scan the AP of a wireless network. If a wireless network exists then the client node gets *Probe response* frame from all the available APs. The information about the AP is stored in the Information Base (IB) of the client's wireless adaptor. Now the client sends an association request to the AP on the basis of the strongest signal.

The important specifications of an AP are given in the Table 1. WMN and WLAN use Wired Equivalent Privacy (WEP), WEP1, Wi-Fi Protected Access (WPA1) and WPA2 for authentication and encryption between the AP and the client nodes [8]. The WEP and WEP1 mechanisms have some built-in limitations which can easily be compromised by the adversary to gain access to the AP. The shared secret keys of WEP are almost static and remain the same for long period. This provides enough time to hackers to analyze and hack into WEP enabled wireless networks using passive eavesdropping attack, in which the attacker can analyze the communication between a legitimate node and AP. Furthermore WAP uses a 64-bit encryption (40-bit encryption key and 24-bit initialization vector (IV)) for both client and AP [3] which can easily be compromised by the adversary by mean of Brute Force attack [4]. The WEP protocol uses RC4 cipher symmetrical cryptographic algorithm with either 40-bit or 128-bit key. In this symmetric key cryptographic algorithm, the secret key always remains the same, and the change in the key sequence is due to the change in IV every time. Since the length of IV in WEP is 24-bit, and can only produce maximum of 2^{24} possible combinations [9], which are not sufficient, and can be compromised for the key-reuse attack.

Received September 23, 2008

Table 1. Specification of an AP

Features	Specification
Standards	IEEE 802.11b, IEEE 802.11g, IEEE 802.11a, IEEE 802.11n
Operating modes	AP mode, Repeater mode, Bridge mode, Client mode
Data rates	Normally, 11 Mbps and 54 Mbps
MAC	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Power supply	DC 5V-9V, 700mA-2A, 10W
Modulation	DSSS (IEEE 802.11b), OFDM (IEEE 802.11g)
Frequency Band	2.4 GHz
Security	WEP, WPA

WPA is much better mechanism which provides encryption via the Temporary Key Integrity Protocol (TKIP) and addresses the weaknesses of WEP by providing some enhancements. However, it is needs firmware upgrade of the existing hardware or it is enabled in new hardware. WPA2 uses more powerful method of encryption known as Advanced Encryption Standard (AES). AES supports key sizes of 128 bits, 192 bits, and 256 bits. It is backward compatible with WPA and uses a fresh set of keys for every session; hence every packet that sent over the wireless medium is encrypted with a unique key. As WPA needs firmware upgrade, otherwise cannot be enabled in the existing hardware, that is why, still WAP is widely used. These weaknesses in encryption mechanisms increase the AP vulnerabilities to many active, passive and DoS security attacks.

3. Possible attacks against AP in WMN

As early discussed, In IEEE 802.11 WMNs, the large scale dense and multi-hop deployment of APs having the capabilities of self-healing and self-configuring are such characteristics which not only facilitate the end-users but also open many doors for the attackers to execute large scale exploitation. Some of the possible security attacks against APs in IEEE 802.11 WMN are given below and are summarized in Table 2.

- Jamming attack
- Fairness attack
- Flooding attack
- De-authentication attack
- Flash crowd
- Cloned AP attack

Jamming [1] the broadband services is an easy way to zero-services, where zero-service is a situation where a network is down for legitimate users after a severe attack. In WLAN, the attacker needs to be near the premises of target organization to launch jamming attack against the APs. On the other hand, WMN is a large scale broadband network in which the APs are deployed city-wide for community-based broadband services, which facilitates the attacker to conduct jamming from anywhere anytime. The communication between AP and the nodes in the range can easily be jammed by introducing a source of strong noise so that to interfere the physical channel. Jamming a single AP would make the services unavailable to the nodes in direct communication range of that AP. The more severe form of this attack is the distributed jamming, in which many attackers at the same time target many APs in WMN, and makes the zero-service for a large coverage area. However, jamming attack on the gateways would even result in the total failure of the WMN, as all the APs are connected with the gateway in WMN. There is a need to consider the implementation of spread spectrum techniques or cognitive radio mechanism [2] at Physical layer so that to reduce the signal interference and to improve the goodput at user end.

In WMN, the bandwidth share decreases as the number of hops increases from the gateway i.e. an AP which is one hop away from the gateway will get more share of bandwidth as compared to an AP which is two hops away. The attackers can exploit this feature of WMN for bandwidth fairness attack. The attackers who manage to increase the number of hops between gateway and APs by exploiting the network protocols would cause the bandwidth of the users connected to the APs to reduce in great extent. The purpose behind this attack is, the attacker has the desire to increase its own share of bandwidth and QoS at the cost of other nodes. In [7], it is described that a DoS attack on gateway by a nearby mesh client is a serious threat to a longer hop communications which already receive low bandwidth due to the poor performance of multi-hop network. One of the experiment in [13], shown that if the number of hops are more than four, then it is not feasible for any multi-media application. A user who is more than four hops away from the gateway will not be able to smoothly access the bandwidth hungry applications such as IP-TV, Video on Demand (VoD), video conferencing etc. There is a need for such scheduling and bandwidth allocation mechanisms which ensure relatively smooth distribution of bandwidth to all the APs. Packet priority mechanisms can also be investigated so that to assign higher priority to a multi-media packet over the WMN.

In single node flooding, an attacker transmits a flood of packets toward a target node to consume its resources or congest the network and degrade its performance. Such type of flooding can be conducted by smurf attack in which a target node is flooded via spoofed broadcast ping messages. In Smurf attack, ICMP echo is used for flooding, while Fraggle flooding, an UDP echo is used to overload the network as well as the target node. An active cache based defence against the flooding style of DoS attacks is proposed for WMN in [7]; however this mechanism may not be able to handle Distributed DoS (DDoS) attack.

DoS is mostly launched by a single person or single host, however in DDoS attacks, multiple infected system flood to break or completely block the services of any of the three important elements of wireless networks [12], such as

- Bandwidth
- Access Points (APs), gateways or any server
- Target user's system

The attackers usually try to overflow the resources of these three elements to bring serious performance degradation in the wireless network to reduce the bandwidth, prevent access to the services or particular service, or to stop the services to

Received September 23, 2008

a specific system. Such security mechanisms need to be investigated at these backbone devices which can distinguish the normal flow and flooding from malicious node as well as distributive flooding from many zombies, and has the ability to block or isolate the malicious node or zombies from the network by sending block signal, also the security mechanism keep the record of MAC addresses of all the malicious nodes so that not to allow them to take part in network operations. Another flooding type attack is *Probe request* frames flooding, which are used by client nodes to discover a wireless network. If a wireless network exist then the AP or WMR respond with *Probe response* frame. The attacker can send a flood of probe request frames using MAC spoofing to represent large number of wireless nodes scanning for the wireless network heavily overloading and consuming the computation power, memory resources and bandwidth resources of the AP [12]. The more harsh form of probe-request flooding would be distributed probe-request flooding, in which large number of nodes with the ability of MAC spoofing may overflow the AP memory or computational resources, and hence zero-service situation.

Another problem in the AP which may result in the DoS attack is the *deauthentication attack.* The 802.11 client first authenticate with the AP before the start of communications. When the client finishes its communication and wants to leave the network, then it needs to send deauthentication message to the AP to stop the communication. This deauthentication message is itself not authenticated. The attacker may spoof this message on behalf of the target node, and the AP will stop its communication with the target node until the authentication is re-established [11]. As the attackers use spoofing mechanism to conduct de-authentication and probe-request flooding sort of attacks. A location-based detection mechanism can be investigated for preventing these attacks, in which the AP has the capability to locate the exact location of the node. Once, the location is accurately determined, then the AP can detect the malicious node even if it is spoofing, as the location will be the same. Furthermore, the de-authentication attack can be mitigated by improving the encryption and authentication mechanisms in IEEE 802.11 WMN.

The operations of WMN need dense multi-hop APs for broadband coverage and some may overlap to provide better bandwidth in heavily loaded geographic area. The WMN support roaming feature, as each node is equipped with a wireless card that implements the roaming algorithm. Generally up to 30 legitimate users with normal traffic flow can access the AP on the basis of the strongest signal received. When the number of users exceed the certain limit may result in bandwidth as well as throughput reduction. In flash crowd also termed as innocent DoS attack, no attacker is involved, instead when legitimate users requests exceed the certain threshold may overflow the memory, computation and bandwidth resources of the AP, which may bring down the network services. Currently, the nodes access the AP on the basis of the strongest signals. An area having more broadband users may overload the AP resources, and can result in Innocent DoS attack. Here, there is a need to investigate the possibility of load balancing amongst the APs.

Table 2. Possible attacks and defences against APs in WMN

Attack	Purpose	Possible Research directions
Jamming	Denial of Services	Cognitive radios, spread spectrum
Fairness reduction	Improve own bandwidth share at the cost of innocent node bandwidth	Improved scheduling and bandwidth allocation mechanisms
Flooding	Congest the network	Traffic monitoring and controlling mechanisms
Probe-request flood	Exhaust the resources of AP	Location based detection mechanism
De-authentication	Isolate an innocent node from the network operations	Enhanced authentication and encryption mechanisms

4. Cloned Access Point

As early discussed, WMN is a large scale city-wide, community-based broadband network; it needs a lot of APs to be deployed for the broadband services. In cloned AP attack, first, an attacker gains illegal access to the internal configuration of an AP either with the help of brute-force mechanism by testing all the possible passwords periodically or using sniffer, which are applications used to capture and read the ongoing packets. Once, the attacker gains an access to the internal configuration of the AP, and then a duplicate copy of that compromised AP is created and places it at some important strategic location to offer connectivity to legitimate nodes. The purpose of duplicate AP attack is to

- Capture and analyse all the packets passing through it
- Bring routing disruption by misdirecting the packets
- Offer only connectivity to legitimate users without offering any broadband services (zero-service situation).
- Isolate a particular location from the rest of the network.

One solution to this kind of attack is the periodic erasure and reprogramming of the access point [6]. However this is not the perfect solution as during the reprogramming and erasure process, the end-users will not be able to access the network.

4.1 Mutual Cooperation Mechanism

The utmost priority for the research community is to protect this multi-hop broadband wireless network from security attacks, in particularly DoS attacks against the APs, because they are operating in the middle level. If the APs are protected, it means there are less chances of severe attacks and exploitations at the top gateway level. As gateways are serving many APs and are directly connected with the wired internet infrastructure, if the attacker successfully target the gateways, its consequences will be more severe and may even result in the Zero-Service of the broadband network. Thus to keep the WMN broadband services functional

Received September 23, 2008

without any disruption, and to avoid the zero-service situation, there is indeed necessary to protect the AP from security attacks especially DoS.

The cloned AP attack can be easily launched due to the self-healing and self-configuring nature of IEEE 802.11 WMN. The proposed solution to overcome the cloned AP attack is based on the mutual cooperation between the multi-hop APs and the serving gateway in WMN. The proposed mechanism is given in Fig. 2.

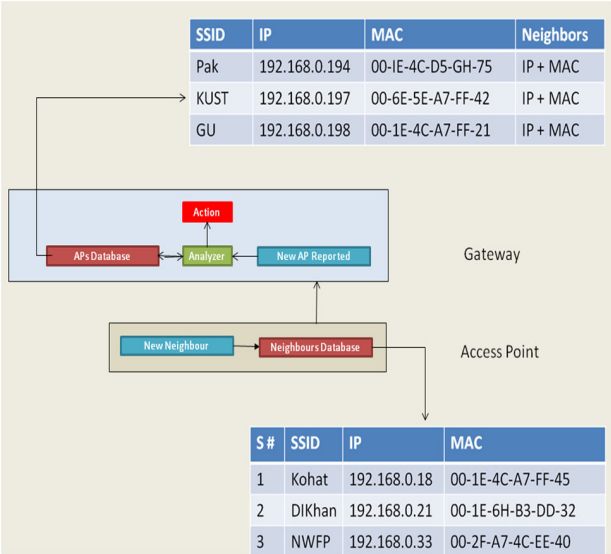

Fig. 2. Mutual Cooperation Mechanism

When a new AP will join the IEEE 802.11 WMN, it will send a friendly packet to all those neighbours which are in its direct communication range. When the existing APs receive the friendly packet, the AP performs two steps.

- The new AP information is stored in the neighbour database. The information contains the Service Set Identifier (SSID), IP and MAC address.
- A report is send to the gateway, that a new AP has been added to the network. The report contains the SSID, MAC and IP address of the newly joined AP.

The SSID is a unique identifier that client devices use to associate with an AP. It is case-sensitive, and the normal length is 2-32 characters.

Once, the gateway receives the information about a new AP, the information is analysed with the help of APs database which contains the information such as SSIDs, IP addresses, MAC addresses and the neighbours of that AP. If an AP already exist having the same information, then the new AP is treated as cloned AP, otherwise normal. Once the gateway makes the decision that the new AP is normal, an acknowledgement message is send to all its neighbours that they can route the traffic, if the newly added AP is cloned, then the gateway informs all its neighbours not to route the traffic through it. The algorithm of the proposed mechanism is given in flow chat in Fig. 3.

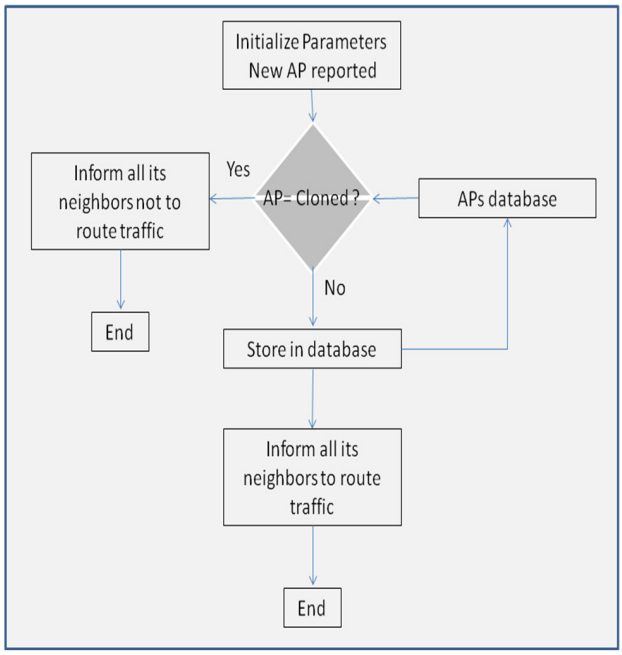

Fig. 3. Complete operation of the proposed algorithm

For instance, an IEEE 802.11 WMN consists of six APs which are providing broadband services to the clients. In first case, a normal AP is added in WMN as shown in Fig. 4 (a), while in second case, a cloned AP is added as shown in Fig. 4 (b). When a normal AP is added in the IEEE 802.11 WMN, the neighbours AP2 and AP3 send a report to the gateway. The gateway analyzer analyses, and store the information in AP database as shown in Table 3.

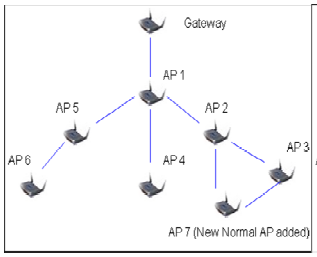

Fig. 4 (a) Normal AP is added

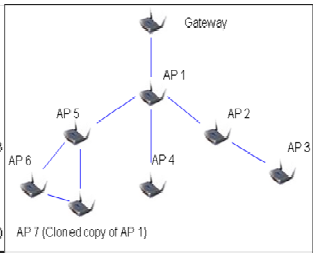

Fig. 4 (b) Cloned AP is added

Table 3. Information of AP 7 in APs database of gateway.

SSID	IP	MAC	Neighbours
AP7	192.168.0.124	00-1E-4C-A7-FF-32	AP2 + AP3 (IPs + MACs)

As this information does not already exist in the gateway APs database, so the AP7 is treated as a normal AP.

In Fig. 4 (b), the attacker gets access to the internal configuration of AP1, and a cloned AP7 is placed at a desired location to degrade the normal network operation. The information of AP1 already exists in the APs table of gateway as shown in Table 4.

Table 4. Information of AP 1 in APs database of gateway.

SSID	IP	MAC	Neighbours
AP1	192.168.0.154	00-1E-4E-A9-FF-82	AP2 + AP4 + AP5 (IPs + MACs)

As soon as the cloned AP7 is placed, the neighbours AP5 and AP6 send a report to the gateway. The information are analyzed and compared with the APs database. The gateway detects that such an entry already exist in the APs database,

Received September 23, 2008

and hence the newly added AP is treated as cloned. The gateway sends a message to all the neighbours of the cloned AP not to route traffic through it. Hence the cloned AP is isolated from taking part in the network operations.

5. Conclusion

The multi-hop architecture and self-healing nature of WMN not only increase the freedom to join and leave the network from anywhere anytime, but also decrease the deployment and maintenance cost. Both these factors depend on the dense deployment of APs. The APs are vulnerable to many DoS attacks such as jamming, fairness, distributed flooding, de-authentication, flash crowd, probe-request flooding and cloned AP. Cloned AP is a severe attack against the IEEE 802.11 WMN, which can result in passive traffic analysis, misdirecting network packets, and even can isolate a portion of network which may result in zero-services to the legitimate end-users. The proposed mechanism is based on the mutual cooperation between the backbone APs and the serving gateway to detect and prevent the possibility of placing cloned AP anywhere in IEEE 802.11 WMN. When a new AP is added to the network, the neighbours APs immediately send a report to the serving gateway. The gateway analyzes and decides on the basis of the received information, that whether the newly added AP is normal or cloned, and acknowledge accordingly. The security of such a city-wide community-based wireless network is highly important, as only secure IEEE 802.11 WMN is necessary for world-wide acceptance and commercial deployment.

References

[1] S. Khan, K-k. Loo, T. Naeem, M.A. Khan, "Denial of service attacks and challenges in broadband wireless network," International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp.1-6, July 2008.

[2] R. Venkatesha Prasad, P. Pawtczak, J. A. Hoffmeyer, and H. S. Berger, "Cognitive functionality in next generation wireless networks: Standardization efforts," IEEE Communication Magazine, Vol. 46, Issue 4, pp. 72-78, April 2008.

[3] G. Glenn, "WLAN security challenges," Security White Papers and Articles, March 2005. Available at http://www.securitydocs.com/pdf/3534.PDF (accessed July 2008).

[4] D. Kalina ECE 478, March 2005: islab.oregonstate.edu/koc/ece478/05Report/ Kalina.doc (accessed August 2008).

[5] Y. Zhang, J. Luo, H. Hu, "Wireless mesh networking, architectures, protocols and standards," Auerbach Publications, Taylor & Francis Group, First Edition, NY, ISBN: 0849373999, 2006.

[6] N.B. Salem, J.-P. Hubaux, "Securing Wireless Mesh Networks," IEEE Wireless Communication Vol.13, Issues 2, pp. 50-55, April 2006.

[7] L. Santhanam, D. Nandiraju, N. Nandiraju, D.P. Agrawal, "Active cache based defence against DoS attacks in Wireless Mesh Network," 2nd IEEE International Symposium on Wireless Pervasive Computing, 2007.

[8] D. Kalina, "WAP, WPA, and EAP". Available at http://islab.oregonstate.edu/koc/ece478/05Report/Kalina.doc (accessed July 2008).

[9] Y. Xiao, C. Bandela, Y. Pan, "Vulnerabilities and security enhancement for the IEEE 802.11 WLANs," IEEE Global Telecommunications Conference (Globecom), 2005.

[10] Belair Networks, White Paper, Available at http://www.belairnetworks.com/resources/pdfs/Mesh%5FCapacity%5FBDMC00040%2DC02%2 Epdf (accessed August 2008).

[11] J. Bellardo, S. Savage, "802.11 Denial-of-service attacks: real vulnerabilities and practical solutions," Proc. of the 12th USENIX security symposium, pp.15-28, August 2003.

[12] F. Ferreri, M. Bernaschi, L. Valcamonici, "Access point vulnerabilities to DoS attacks in 802.11 networks," IEEE Wireless Communications and Networking Conference, March 2004.

[13] V. Chavoutier, D. Maniezzo, C. E. Palazzi, M. Gerla, "Multimedia over wireless mesh networks: Results from a real testbed evaluation," Proc. of the 6th annual Mediterranean Ad Hoc networking workshop, Greece, June 2007.

BIOGRAPHY

Shafiullah Khan (shafiullah.khan@brunel.ac.uk) is currently a PhD candidate in the School of Engineering and Design, Brunel University, West London, UK. He is also affiliated with the IIT, Kohat University of Science and Technology (KUST), N.W.F.P, Pakistan as a lecturer. His research mainly focuses on wireless broadband network security and privacy, security threats and mitigating techniques.

Noor Mast (noor.mast@brunel.ac.uk) is currently a PhD candidate in the School of Engineering and Design, Brunel University, West London, UK. He is also affiliated with the IIT, Kohat University of Science and Technology (KUST), N.W.F.P, Pakistan as a lecturer. His research mainly focuses on TCP issues and challenges in multi-hop wireless networks.

Kok-Keong Loo (Jonathan Loo) [M'01] (Jonathan.Loo@brunel.ac.uk) received his MSc (Distinction) and PhD at University of Hertfordshire, UK in 1998 and 2003, respectively. Thereafter, he joined the School of Engineering and Design, Brunel University, West London, UK, as a lecturer in multimedia communications. Currently, he serves as a course director for MSc Digital Signal Processing and heads a team of 9 active PhD candidates in the area of multimedia communications. His current research interests include visual media processing and transmission, digital/wireless signal processing, and wireless/broadband network architecture, protocols and securities.

Ayesha Salahuddin is currently an MS Computer Science student in the Department of Computer Science, Allama Iqbal University, Islamabad, Pakistan. Her research interest mainly focuses on security related issues.

Received September 23, 2008