EasyChair Preprint

№ 96

Security Mechanisms for attacks on MAC Layer of Wireless Mesh Networks

Sadaf Ilyas, Sohail Ahmed, M. Saad Bin Ilyas and Shamsa Umar

April 25, 2018

Security Mechanisms for attacks on MAC Layer of Wireless Mesh Networks

Sadaf Ilyas[1], Sohail Ahmed[2] and M. Saad Bin Ilyas[3]
[1]Department of Information Technology, University of Lahore, Pakistan.
[2,3]Department of Computer Science, University of Lahore, Gujrat Campus, Pakistan.
sohail.ahmed@cs.uol.edu.pk

Abstract. In modern era wireless mesh networking has evolved as high throughput technology to handle the services of broadband in coming era. WMN has provided the opportunity for the economical services in the field of defense, natural disaster and the internet availability in the developed areas. However, one of the key encounters in the scheme of these networks is their susceptibility to security attacks. In this paper, we examine the security goals of these networks, categorize some likely attacks on Media Access Control layer, and review numerous prevention methods about intrusion, detection protocols, reported in the scientific writings. The paper also pro-vides the basic information about the architecture of WMNs.

Keywords: Wireless Mesh Networks (WMNs), Security, Intrusion Detection System, Advanced Encryption Standard.

.

1. Introduction

A WMN basically can be defined as the unified radio nodes by means of mesh topology. The WMN formation is done by a net access point, a net user, and gateway for the activity. A best illustration to know the clients of mesh are smart phones, individual digital subordinate while the access point conveys the traffic in the direction of gateway. In wireless mesh network, it's not essential for the node of gateway to be linked to WWW (World Wide Web). WMN is too starting to be employed with existing IEEE standards e.g. 802.11, 802.15, 802.16, etc. [1]. Application of WMN can be easily found as military communications, satellite phones and smart energy systems etc. The WMN is an imminent invention that can transport broadband access, distant access, and system obtainability for net-work system connectivity amongst the administrators and the clients at fewer expenses. It is communication systems that have increasingly dragged in the Internet Service Providers (ISPs) owing to its wild emergent and development of remote progressions. WMN is a gifted novelty in giving in height data transmission capacity system choice. WMNs will extremely benefit the clients to be continually online any place at all time by connecting with distant cross-sectional switches. Due to the dependency on the middle nodes for routing and broadcast nature of transmission the user communication leads to security susceptibilities making WMN disposed to numerous attacks. It is obvious that without addressing the internal and external security matters true potential of WMN cannot be misused. In this paper, we recognize the security issues in WMN with the detail of attacks on WMN. The main concern will be the attacks that affect the MAC layer of WMN [2].

2. Wireless Mesh Networks Architectural

WMNs (Wireless Mesh Networks) are considered by active self-organization, self-configuration, and self-healing to allow flexible incorporation, swift placement, easy conservation, and low price to advance the presentation of multi-hop ad hoc networks, WLANs (Wireless Local Areas Networks) and WMNs (Wireless Metropolitan Area Networks). WMNs can also offer wireless connectivity of Internet low cost than the classic Wireless Fidelity networks. Numerous architectures of wireless mesh networks have been projected based on their attributes and applications, the broadly recognized one is the three-tier framework. At the inferior level of the mentioned architecture, mesh clients (MCs) are obtainable which or well known as the mobile users with insufficient mobility and reserve. At the middle tier, a set of mesh routers (MRs) for the linkage of wireless base is used and existing MCs are connected with these MRs. At the upper tier of the following architecture there is a group of Internet gateways (IGWs) existed. A mesh network offers the multi-hop system of communication between the MRs and MCs. Though such multi-hop generates the absence of safety, the active topology and the connectivity with users at the end this will generate the vulnerability and increase the routing overheads [3]. The below figure 1 shows the architecture explained above.

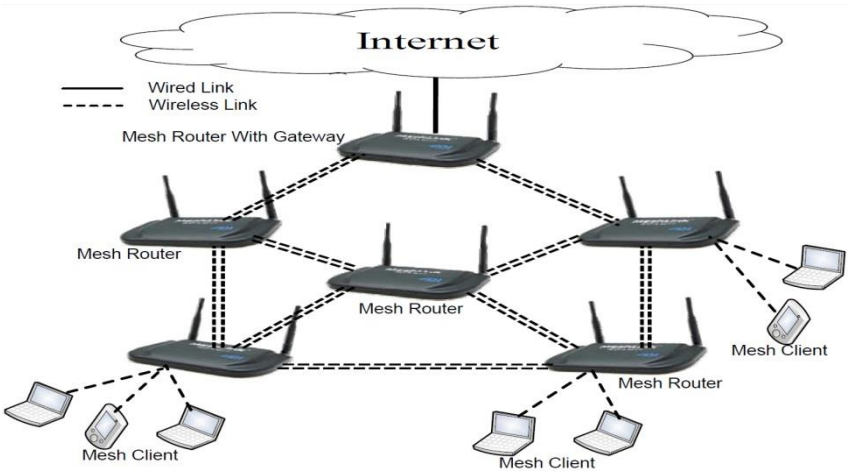


Fig. 1. Wireless Mesh Network

3. Security Goals of Wireless Mesh Networks

The security goals for mesh networks are essentially alike to safety necessities for any type of statement system. These goals comprise the following.

Availability: It guarantees the survivability of mesh network services notwithstanding the attacks.
Integrity: It provides surety about the data that the data cannot be altered without the detection.
Confidentiality: It confirms that the info is only available to only authorized individuals.
Non-Repudiation: It confirms that the users on both ends deny the acceptance and request of the message in a network.
Authorization: In this method an entity is supplied identifications by the reliable authority. It is normally used to allocate diverse right of entry rights to diverse level of users.
Anonymity: This system identifies the user and owner and keep secret both user and owner and prohibit the sharing of info among other parties.
Access Control: It confirms that solitary legal activities can be done. This control comprised of all authentic entities [4].

4. Security Attacks in Wireless Mesh Networks

The classification of security attacks based on the scope, nature, protocol layer and behavior of the attacker's target. The attacks may be categorized either it is passive attack or active attack. Active attack is made with full intention to disrupt the operation of the network, to steal the info and collapse the network operation. Passive attack should be compromised attack while on other hand active attack may result in violation of availability and integrity. External attacks are led by intruders who are not part of a WMN and try to gain illegitimate access to the network. Internal attacks are led by the members of the WMNs and these cause serious threats to the system. It is very difficult to handle these attacks [5]. Furthermore, the attacks can also be categorized, on the base of method of attack used by the attackers to complete their Objective, on impression, alteration, assembly, rerun, and Rejection of Service (Daniel of Service) attacks.

5. Security Attacks at the MAC Layer of WMNs

Attacks of various types are possible on mesh network layer of MAC.

5.1 Passive Eavesdropping

It may be intervening by the interior as well as exterior nodes. As the fate of transmission of the wireless mesh networks, it is suitable for the attackers of exterior type in the boundaries of broadcasting of the cooperating nodes to

launch spying activities of passive type. By targeting the hops in the middle this type of networks is liable for the spying activities internally [6]. Activities of passive nature points the deficiencies in the privacy of data and its integrity. All the data examines by the passive attackers during the transmission of it. It is very hard to pin point these attacks on any layer of data because of not changing the information as transmitted by service provider. Both the transmitter and receiver of data are not conscious about the intruder. To avoid this encryption procedures are adopted by using the inert keys of encryption to secure the integrity and level of confidence of the data.

5.2 Jamming Attacks

Jamming attacks are more complex as compared to blind physical layer radio jamming attacks. Rather than transmitting random bits constantly, the attacker may transmit regular MAC frame headers on the transmission channel which conform to the MAC protocol being used in the victim network. Consequently, the legitimate nodes always find the channel busy and back off for random period of time before sensing the channel again. This leads to the denial of service for the legitimate nodes and also enables the jamming node to conserve its energy resources. In addition to the MAC layer, jamming can also be used to exploit the network and transport layer protocols. Attacks for the jamming of network on MAC layer are also possible easily [7]. These possible types are shown in the following table 1.

Table 1. Types of Attack

Types of Attack	Description of Attack
Unpromoted clear to send(CTS) Attack	An attacker transmits a CTS message with a long message duration causing all recipients to halt transmission for this duration.
Reactive Request to Send (RTS) Jamming Attack	In this type of attack, whenever an attacker detects an RTS message, it disrupts these messages by immediately initiating a transmission.
CTS corrupt Jamming	Upon receipt of an RTS message, an attacker transmits noise during the CTS response.

5.3 MAC Spoofing Attack

In transmitted frame MAC address can be changed by the attackers in an attempt. In wireless and wired LANs usage of MAC address as unique identifier of layer 2 is very common. As globally unique MAC addresses normally used as factor for the authentication for the network levels freedoms to the user. This is specifically common in Wi-Fi 801.11 networks. However, protocols of MACs of these days and interface of network card do not offer any protection that would stop a probable invader from adjusting MAC address foundation in the transmitted frames. On the conflicting, normally full sport is provided by the manufactures in the form of device drivers that make it very simple to do. MAC spoofing is referred to as altering the addresses of MAC in transmitted layers and attackers used it many different ways. MAC spoofing permits the invaders to escape Intrusion Detection Systems (IDS) which are present there. MAC addresses in the access control lists normally used by the administrators of networks of this era. Access point are offered only to registered addresses of MACs. To determine the genuine MAC address of a device the attacker easily perform spy activities. This make the attacker to cover-up as an authentic user and acquire network access. An invader can introduce large number of fake address of frames in the network to diminish the possessions which may result in refusal of services for the valid node [8].

6. Security mechanisms for wireless mesh networks

In instruction to diminish the difficulties in the security issues of WMNs, plentiful safety measures have been done to these mentioned three categories: intrusion detection, prevention and response of intrusion. In situation of the intrusion prevention, actions are reserved to halt the assailant from obtrusive hooked on the network and initiation the occurrence on the mesh network. There is a great need of security from external as well as internal attackers. Intrusion prevention can be led by the access control, data integrity, security service confirmation and data privacy. Though, prevention from the intrusion is not sufficient to secure the network from all types of attacks due to the lacking of techniques for the complete assurance of security [9]. Consequently, the mechanism for the intrusion prevention is approved by the detection of intrusion and mechanism of response. For the identification of dishonest activities,

detection of intrusion plays an important role which is due to the attacks. In time identification of attack and response can stop the dangerous effects of it. The aim of the intrusion detection mechanism, liability and service obtainability of the network. We deliberate the mechanism of intrusion prevention as well as mechanism of intrusion identification at the WMNs' MAC layer.

7. MAC Layer Security Mechanisms

7.1 Intrusion Prevention Mechanisms for Eavesdropping Attack

Many security frameworks have been developed with slight modifications in the frameworks of multiple hope networks for the usage of WMNs. Authenticated services of security are provided by theses frameworks, integrity and confidentiality of data at network's MAC layer. Many frameworks of security hire the primitives of cryptography. Mechanisms that are based on conventional cryptography are non-appropriate to WMNs. For the solution of this problem protocols of neighbor collaboration authentication have been suggested by the groups of researchers. For the prevention of eavesdropping attacks authentication based on identity and management of hop wireless networks will be used. Cryptographic solutions are proposed for the master key distribution (i.e. private key, public key) and private key based node authentication. In these suggestions nodes own key publicly on other hand each node has taken a part of private key. For nodes the generation of private key is hired by undisclosed sharing that 'n' out of 'k' contributions of private key are needed to build whole private key. Residing on this scheme, whenever node of private key needs to refresh, it needs 'n' neighbors to deliver the share secretly to rebuild the key privately and none of the node build the private key by using its personal information [9]. The method of the generation of private key is revealed in the following Fig. 2.

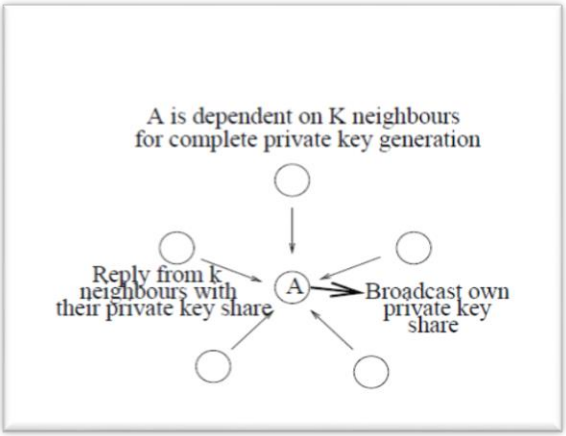


Fig. 2. Private Key Generation in WMNs

Broadcasting of request in form of message with its verification share. The other adjacent node generates a reply against the request in a secret way by sending a request to the responding node. Private Key is than generated by getting the message request from 'k' with its own share.in this manner the intruding node unable to broadcast the request until or unless a response is generated and verified by 'k' adjacent node. In the same way the violent nodes' private key is not reinvigorated by adjacent node. Consequently, authentication is served by the top secret sharing and solution for the key management. Afore mentioned mechanism of security for the MAC layer attacks proved as a preventing measure. The security package data concealment leads to the preventive mechanism in response of eavesdropping attack. Confidentiality service of data provides the secured mechanism of protection with the help of encryption between the communication nodes as the nodes can yet overhear the communication. Then this information is impractical after receiving, if brute force method is used for the decryption of useless message keeping the attacks' cost in comparison with the worth of acquired information.

7.2 Jamming Attacks Mechanism for Defense

7.2.1 Cryptographic Puzzles Based on Hiding

In this section of paper, we introduce the method of hiding the packet involved in cryptographic puzzles. Execution of set of computational instructions which are predefined, the idea in the background is to compel the acceptor before enabling to retrieve top secret information of interest. Both the time required and ability of the problem solver based on the toughness of the puzzle. The advantage of scheme that is based on puzzle rely on the parameters of PHY layer. Though it has greater communication and computational over-heads. Cryptographic puzzles in our context are used to mask the transmitted packets temporarily. A key k of interested length s randomly picked for encoding a packet. The acceptor got the blind key transmitted by the cryptographic puzzle. Before the completion of "m" the puzzle holding "k" cannot be explained. Hereafter the challenger cannot categorize m for the sake of blocking selectively [10].

7.2.2 Cryptographic Puzzle Hiding Scheme (CPHS)

Suppose a transmitter S have target packet m for the purpose of transmission. The transmitter pics a key k arbitrarily of the length of interest. S produces a puzzle P where the function for generating the puzzle is used as puzzle () holding the parameters puzzle (k, tp), and the time assigns as tp the time duration for solving the puzzle. This tp is measured in sense of time parameter and it is supposed as the capability of challenger computationally, represented by N and calculated at the rate of per seconds computationally. After initialization the P transmitter transmits (C, P), at this place C= Ek (π1 (m)). At the accepter side, a receptor R resolves the accepted P puzzle for the regeneration of k´ Key and after it calculates m´π-1(Dk´ (C´)). If the packet is meaningful that encrypted, the accepter takes that m´= m. otherwise accepter rejects m´. The detailed info of CPHS is shown in the following figure 3.

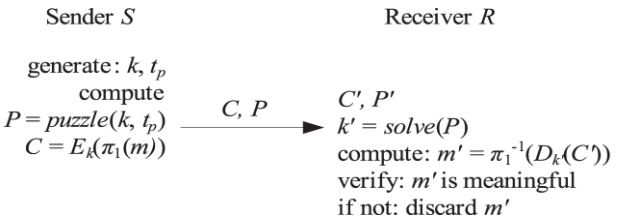


Fig. 3. The cryptographic puzzle-based hiding scheme.

7.3 Prevention Mechanism for MAC Spoofing

In this portion we target on the issues related to security of MAC 802.11 that is utilized in mesh networks. Encryption on the freight of MAC data has been familiarized but now till MAC layer is non-encrypted. Code for the message integrity is used for the MAC header authentication. Header of MAC comprised on three different fields: one is auxiliary security, frame control and addresses. Security against attacks MAC header includes destination and source address sequence number, frame control and header for the auxiliary security (ASH) are necessary to encrypt like snooping attack, replay protection attack, RTS replay CTS replay and denial of service attack. MAC spoofing attacks are hindered by header and data veracity services. Check for the integrity will fail by the spoofing attack at accepting node and discarded at meanwhile. To prevent the attack on MAC header different algorithms and text codes are available to cope u with this problem. We suggest to utilize the Efficient Standard MAC header algorithm that comprises of 40 bytes. We are recommending the use of two AES algorithm. One of 16 bytes and the second one is of 24 bytes [11].

7.3.1 Encryption by AES Algorithm

As elaborated in the above section, few values are calculated in the AES algorithm. The following figure 4 demonstrates the detailed steps for the frames in AES. Every step of algorithm comprised of few mathematical calculations; mix column, sub byte, shift rows and odd round keys. AES equips with best solution to our problem. We suggested for MAC header 192 bits and 128 bits algorithm working in parallel fashion.

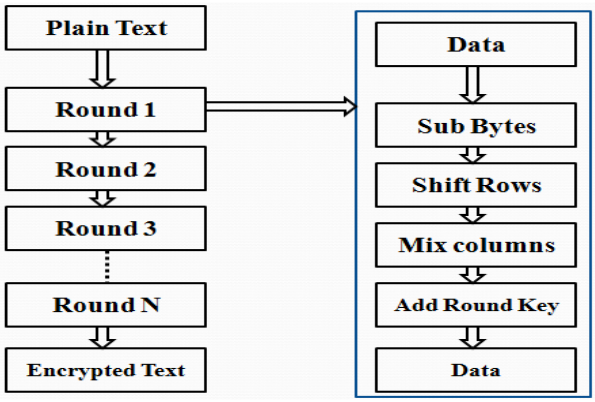


Fig. 4. AES algorithm for all frames and steps in one round

7.3.2 Implementation

We are suggesting to device AES algorithms, the pattern of working of these algorithms is in parallel. For the security of headers' 40 bytes, we are utilizing an algorithm of 128 bits and of 192 bits. The frame of this AES algorithm comprises of ten rounds that contain the different mathematical calculations except 10th round. the algorithm used different number of bytes 16, 15, 2, 1 and 2 for MAC header, auxiliary security, sequence number and destination address respectively. Encryption in 192-bit algorithm is same as in 128-bit algorithm of AES but key length and repetitions of round are different from afore mentioned algorithm. Twelve rounds and 24 bytes lengthy key. In addition to its final round has not operation of mix column as in 128-bit algorithm [12].
Sub-bytes keeping in view first MAC header of 128 bits: frame counter has 16 bits; destination address of 88 bits sequence number of 8 bits length and source address bits are 16 in number. The following fig 5 A and B exhibits the 128 bits sub bytes' first round.

00	2C	1B	08
CA	F1	2B	4A
8D	14	9E	17
6F	10	1F	C3

Fig 5 A. Bits 128 before sub byte operation

63	71	AF	C5
74	A1	F1	D6
5D	FA	0B	F0
A8	CA	C0	2E

Fig 5 B. Bits 128 after sub bytes operation

7.3.2.1 Shift row

Next to the sub byte operation is shift row operation. It is an operation of mathematical calculations. In this operation bytes are shifted in a 4 bytes row. No shifting occurs in the beginning. After this in consecutive three rows shifting accurse one time greater than the previous row respectively (i.e. 2, 3 and times). The main function of the current operation is to offer diffusion among the all 128 bits. This may result due to change in single bit. The following figure 6 elaborate the shift row operation.

63	71	AF	C5
A1	F1	D6	74
0B	F0	5D	FA
2E	A8	CA	C0

Fig 6. Operation of shift Row

7.3.2.2 Mix column

In this operation a multiplication calculation is done in a group of 4 bytes with a constant number after the shift row operation. Polynomial functions are generated by the conversion of hexadecimal numbers. The key function of this operation is to facilitate with the diffusions in operational results after multiplication of constant matrix. This all creates the problem for the attacker in the identification of real data. The operation is given in the form of following equations.

Matrix multiplication is done like,

A= (02*63) + (03*71) + (01*AF) + (01*C5)
B= (01*63) + (01*71) + (02*AF) + (03*C5)
C= (01*63) + (01*71) + (02*AF) + (03*C5)
D= (03*63) + (01*71) + (01*AF) + (02*C5)

7.3.2.3 Add Round key

At the end the after the mix columns' results the round key operation is performed. At the end of each round of 128-bit data a round key is introduced. The following figure 7 shows results are obtained after the addition of round key in each step.

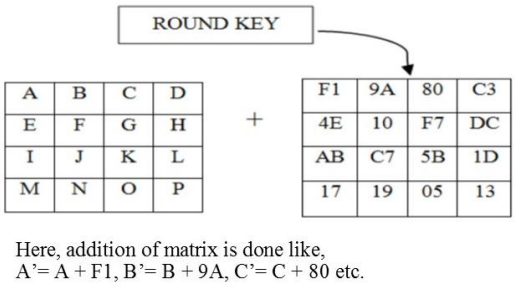


Fig. 7. Addition of Round Key Results

Every round of this operation has its specific key that is added in each round. The process of adding up the round key prolonged to the round 10. While final round doesn't contain operation of mix column. Encryption of both 128 bit and 192-bit algorithm is same regard-less of size of the key and round numbers. The round key is added on either two positions, first at the start and then at the last of each round. Significance of this operation is furnishing the program with high level of security and known as key widening.

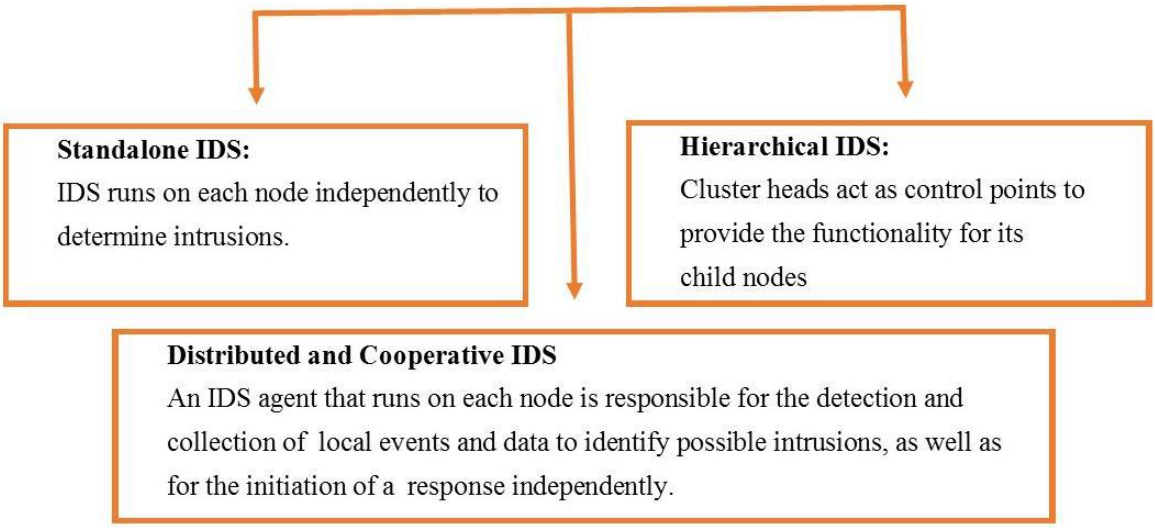
8. Intrusion Detection Mechanism

Very few intrusion detection systems have been proposed at the MAC layer of wireless networks. It is not sufficient and effective to protect mesh networks by encryption and protection software. Systems for Intrusion detection are also organized to offer a line of defense at second level. These systems alert the wireless and wired networks about the attacks, so that in time action is taken to stop the attack or alleviate the damage by the attack. The functions are given in table 2.

Table 2: Function for Attacks

Function	Description
Event Monitoring	The intrusion Detection System(IDS) must monitor some type of events and maintain the history of data related to these events.
Analysis engine	The IDS must be equipped with an analysis engine that processes the collected data to detect unusual or malicious behavior.
Response	The IDS must generate a response, which is typically an alert to system administrator.

Classification of IDEs based on monitoring events is represented as:



More specifically, the authors propose a simple modification at the MAC layer in order to detect inauthentic acknowledgments in encrypted data frames and to suppress the initial acknowledge when required. Experimental results showed that the proposed mechanism presents a high detection rate, no false positives, and a small computational and communication overhead. Khan et al. propose cooperative and hierarchical IDS for WMNs. In this system, each mesh node has an IDS agent, which monitors independently its neighbor nodes and, in case of misbehavior detection, broadcasts the in-formation to its neighbors, as well as sends report to the serving mesh router for action. Also, the IDS agent of the mesh router has capabilities for cross-layer monitoring and detection (link, network, and transport). By this cooperation, the proposed IDS achieve to identify several attacks, such as MAC spoofing, jamming, eavesdropping attacks [13].

9. Conclusion

In current era WMN has very famous technology due to its easy handling, fast speed and cheaper network deployment. Though due to flexible characteristics, open medium, nature of multi hop, dynamic topology of network and low number of monitoring points for the data traffic. Wireless Mesh Networks carriage advance challenges in acquiring the security. In this article, we established a thorough counter analysis of issues related to security and attacks related to networks. Also, classification is given of the attacks that are possible in variable circumstances. Brief account has also provided about mechanisms of defense related to mesh networks, adding prevention of intrusions and mechanisms of detection noticed in previous studies by different research groups. This topic triggers the mind of researchers to find out the best possible solution against the attacks on WMNs.

Acknowledgement

The author would like to thank Sir Sohail Ahmed from University of Lahore for their useful suggestions and comments on this paper. This work is supported by him and this work will have not been possible without the help of Sir Sohail Ahmed. We acknowledge that this work is possible due to his collaboration.

References

1. Naveen, T., and Vasanth, G.: Qualitative Study of Existing Research Techniques on Wireless Mesh Network, International journal of advanced computer science and applications, 2017, 8, (3), pp. 49-57.

2. S.gora, A. Vergados, D. D. and Chatzimisios, P.: A survey on security and privacy issues in wireless mesh networks, Security and Communication Networks, 2016, 9, (13), pp. 1877-1889.

3. Radunović, B. Gkantsidis, C. Gunawardena, D. and Key. P.: Horizon: Balancing TCP over multiple paths in wireless mesh network', in Editor (Ed.) (Eds.): 'Book 9 Horizon: Balancing TCP over multiple paths in wireless mesh network' (ACM, 2008, edn.), pp. 247-258.

4. Regan, R., and Manickam, J.M.L.: 'A Survey on Wireless Mesh Networks and its Security Issues', International Journal of Security and Its Applications, 2016, 10, (3), pp. 405-418.

5. Akyildiz, I., and Wang, X.: 'Wireless Mesh Networks (Advanced Texts in Com-munications and Networking)', 2007
6. F. Samad.: 'Securing wireless mesh networks: a three-dimensional perspective', RWTH Aachen University, 2011

7. Seth, and Gankotiya.: 'Denial of service attacks and detection methods in wireless mesh networks', in Editor (Ed.): 'Book Denial of service attacks and detection methods in wireless mesh networks' (IEEE, 2010, edn.), pp. 238-240.
8. C. Lee: 'Security in wireless mesh networks': 'Wireless Network Security' (Springer, 2013), pp. 229-246.

9. Falk, R. Huang, C.T. Kohlmayer, and Sui.: 'Security in wireless mesh networks', in Editor (Ed.): 'Book Security in wireless mesh networks' (Auer-bach Publications, Taylor & Francis Group, 2006, (ed.), pp.

10. Proano and Lazos L.: 'Packet-hiding methods for preventing selective jamming attacks', IEEE Transactions on dependable and secure computing, 2012, 9, (1), pp. 101-114.

11. Dalal, H.N. Soni and A. Razaque.: 'Header encryption of IEEE802. 15.4', in Editor (Ed.): 'Book Header encryption of IEEE802. 15.4' (IEEE, 2016, edn.), pp. 1-6.

12. Yang, J., Chen, Y., and Trappe, W.: 'Detecting spoofing attacks in mobile wire-less environments', in Editor (Ed.): 'Book Detecting spoofing attacks in mobile wireless environments' (IEEE, 2009, ed.), pp. 1-9.
13. M. Siddiqui.: 'Security issues in wireless mesh networks', in Editor (Ed.): 'Book Security issues in wireless mesh networks' (IEEE, 2007, ed.), pp. 717-722