International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 01, January 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

# SECURITY ISSUES IN WIRELESS AD-HOC NETWORK: A REVIEW

**Sumit Gupta[1], Dr. Shiva Prakash[2]**

[1,2]*Department of Computer Science and Engineering,*
*Madan Mohan Malaviya University of Technology, Gorakhpur, Uttar Pradesh, (India)*

**ABSTRACT**

*We have huge development in wireless technology in recent years. As we know we have different security issues in the wireless network communication. Intruders and attackers can make utilization of the loopholes in the wireless network communication. Daily use of wireless networks for business purpose and communication purpose created a need for strong safety mechanism. Attacks on wireless network can be classified as active and passive attacks or internal and external Attacks, security services are confidentiality, authenticity and data integrity also necessary for both wired and wireless network for protection of basic application. This paper deals with the different kind of wireless security issues and discuss about their current solution.*

***Index Terms— Wireless Ad-hoc Network, Confidentiality, Integrity, Authentication, Wi-Fi protocol, Temporal key Integrity Protocol, Advanced Encryption Standard, WLANimprovement, Security threat.***

## I. INTRODUCTION

Ad hoc wireless networks are pre-deployed infrastructurethat is available for routing packets end-to-end in a network, and instead of rely on intermediary peers. It refers to the networks connection established for a single and does not require a router or a wireless base station.Electromagnetic wireless telecommunication is well known wirelesstechnologies. It is part of multi- hop wireless network.E.g. radio communication, remote control etc.It includes different sorts of fixed, mobile and portable applications, including radios, cell phones, wireless networking .Wi-Fi is also local area wireless network that is used to connect portable computing devices to the internet .These are also uses in house, offices and public hotspot. Cellular services coverage in the range of 10-20 kmfrom nearest cell site or tower. Technology has evolved as speedincreaseslike GSM, CDMA, and, GPRS, and 3g Network such as CDMA2000 and EDGE. Wireless technology uses in long range communication .It can't be implemented by the use of wires. It is widely used in radio communication, transmitters, receiver, computer network and its terminal.

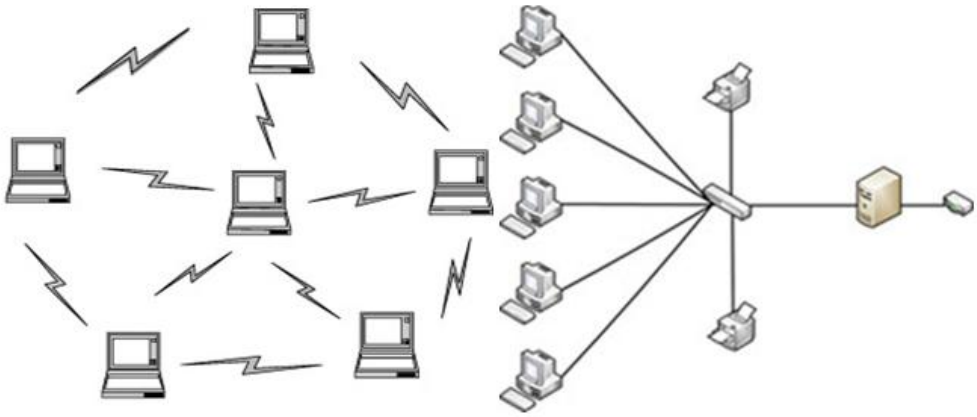

**Fig.1 Adhoc network**

Rest of the paper is organized as follows characteristicsofad-hoc network and need of wireless security. Section II presents modes of unauthorized access. Section IIIpresent Security threat to wireless network. Section IVpresent WI-FI protocol. Section Vpresent 802.1 xits advantage and authentication process and finally section VI Conclude the paper and introduce best way for security of wireless ad-hoc network.

### 1.1 Characteristics of ad-hoc network

1) No need of infrastructure.
2) It can be distributed quickly.
3) It can act as extension to existing network.
4) Cost effective.
5) Nodes act as routers and end to end communication in adhoc network.

.

### 1.2 Need of wireless security

Security is one of the challenges in wireless technology. Current Security standard is showing that security is missing in growing uses of wireless standard. This is prevention of unauthorized access or any damage to the wireless computer network. Wireless network are common for organization and individual. Wireless networks provide potential for exploitation for two reasons; they take the help of airwaves for communication, and wireless-enabled laptops. To make the most of their security planning, enterprises need to focus on menace that poses the greatest risk. Additional wireless access security challenges come by the use of wireless-enabled devices by employees, the amount of growing of confidential data that reside on those devices, by which users can engage in risky wireless behavior. Hackers and intruders have found wireless network and wired network are relatively easy to break. As a result, an effective action should be taken against unauthorized Access to important resources.

### 1.3 Modes of Unauthorized Access

1) Apply security patches: This is also called security holes or vulnerabilities. If we are using operating system having security hole then there might be unauthorized access due to which data may be deleted. To secure our operating system we have to apply a patch to fix the detective hole. Windows user should perform Windows update features.
2) Password should not be seen by any one. User ID and password supplied to the user should be checked by information system. To protect it from any unauthorized user password should be changed alternatively.
3) Disable the file sharing features so that no one can look into your system.
4) Uses of firewall software should be recommended because firewall is a tool to prevent from unauthorized access.
5) If any computer that has received and unauthorized access and data is lost then it is Important that data should be backup on regular basis. It will keep data safe from intruders.

### 1.4 Security Threat to Wireless Network

If an organization wants to protect its valuable data, to detect the altering of dataand access control over authorized individuals, then various industries must also follow the regulation and industry requirements and guidelines. This protocol should be followed by all the member of the industries. Protection of wireless networks means it should be protected from attacks on availability, confidentiality and integrity. Vulnerabilities in the security protocols ensure the possibilities of attacks. This section explains different types of security attack. This method can be applied to break both confidentiality and integrity [1-3].

1) *Traffic analysis:* It is very simple techniques that attacker can take information over a packet during its transmission .Attacker uses these techniques to access three type of information .The first one is activities and identification of user on the network, second one is the physical location of the user by the IP address and Mac address and third one information about communication protocol. Attacker has to collect information about the sizes and number of packet on certain period of time.

2) *Passive eavesdropping:* This technique is to watch over an unlimited wireless session. In decrypted session the attacker is able to read the data during its transmission and assemble them indirectly by surveying the packets. Thiskind of attack is not based on violation of privacy,but information assembled in this way canbe used for more dangerous kinds of attacks.

3) *Unauthorized access:* An unauthorized access is the act of gaining access to any network client or users. It is by the help of user ID and password.VPN (virtual private network) can protect from attacks that influence the confidentiality of data but it cannot prevent attack that destroy confidentiality e.g. man in middle attack, replay attack and high jacking attack.

4) *Man-in-middle-attack:* This attack is type of cyber attack that enables data reading from the session or modifications of the packet by hackers. They insert him-self into the conversation between two clients without their permission. There are several ways to implement this type of attack theyexploit real time processing of transaction and conversation or other data. The first one is when attacker interrupts the session and do not give permission to the station tore-establish communications with inAP(access point). The station tries to establish session with the wireless networkby the access point, but can be done by the help of workstation of the attacker that act to be an AP. At the same time, the attacker establishes connection and authentication with the AP.Now there are two encrypted tunnels in place of one: one is established between the attacker and access point, otheris established between the attacker and station. This enables the attacker to get access to the data exchanged between the workstation and the network.

5) *High jacking attack:* In this type of attack, attacker takes control over a communication between two entities (clients)and masquerades as one of them. In this type of connection the culprit takes control of an established connection that is in progress. The client knows that he has no access to the session any more but he does not know that attacker has control over his session. Once the attacker handlesthe session, he can use it for various purposes [4-6].

6) *Replay attack:*This is the network attack in which attacker used to access the network through authorization. In replay attack the attacker gives the proof of his identity. Attacker listens to the communication between sender and receiver to get the authorization and when the original session expires attacker get access to it.

7) *Denial of serviceattack:* This is an incident in which user lost his authority of serviceresources. When this attack occurs a network user is unable to access resourcessuch as email or network connection. This cause denial of services [7-8].

8) *Jamming:* This is signal from one device to other device that collision has occurred. It means that device was trying to send a frame and other device also trying to put the frame on the same line. By this collision will occur and signal will be jammed. In the security problem, this is performed by attacker to disable the communication between the users. Hackers or attacker send many frames in same network so that collision will occur [9-10].

## II. WI-FI PROTOCOL

Wireless Fidelity, well known by its short form of Wi-Fi. It is a digital communications protocol by which electronic gadgets can communicate with each other in a unicast or broadcasting manner without any wires but Security is one of the major deficiencies in Wi-Fi by which better encryption systems are now available. Encryption is not compulsory in WIFI it is optional. There are three different techniques. These techniques are:

### 2.1 Wired equivalent privacy (WEP)

Wired equivalent privacy (WEP) protocol: It is basic part of IEEE 802.11(Institutes of Electrical and electronics) standard for the protection of WLAN (wireless local area network).The function of WEP is to provide data security in wireless network and wired network. If protocol is working on 2nd layer of OSI model then this is the best way to protect the data during the transmission. To transmit the data from sender to receiver or any communicating parties, WEP uses shared key of 40 to 128bits. It has 3 steps [11].

a) *CRC (cyclic redundancy check): It*is error detecting code used in network to detect the fault in the raw data. In this message is calculated and added to the original message of receiver.
b) Encryption is second method in WEP protocol. In this firstly random data of three byte is generate. By the help of initialization vector.RC4 algorithm will help to generate key based on new key. RC4 algorithm is used for encryption and decryption. Such that data stream may XORED by generated key.

(c) The last step is to transmit the sequence of initialization vector message that is encrypted. In this way message will generate. Once the message to come its final process then again key is generated On the basis of initialization vector and shared key after that rc4 algorithm will generate key by the of XOR function this will calculated the accuracy of message will be checked by decrypted message of CRC. Then it compared to send CRC if that message is same as sent CRCthen received message matches with sent message.

### 2.2 WEP protocol uses three safety mechanisms.

a) Authentication: It is used to check the identity of communicating parties or user and take the assurance that user in communicating parties is genuine. There are open system authentication and shared key authentication in IEEE802.11.Open system authentication help mobile station to access the access point without confirmation of identity of station. Shared key authentication is used in encryption techniques and conversation between the access point and station. At last it is end by decryption of shared key and that key should be match with sent key.

b) Confidentiality: It means that information is accessible to those who is authorized to access it by the help of valid user ID and password. In 802.11the confidentiality is done by encryption techniques by the help of RC4 algorithm and symmetric key. In this if key length is increases protection increases and this ensured the identity of user.

c) Integrity: It involves maintaining the consistency, trustworthiness and accuracy of data must be same at any cost, it should not be altered. By the help of CRC techniques, WEP provide integrity of message that transmitted between station and access point.

## III. WIFI PROTOCOL ACCESS (WPA) IEEE 802.11I / WPA 2.

WPA2 established secure communication in four ways

a) The AP and the user will agree by the help of authentication and pre authentication method.
b) Generation of master key.
c) Create temporary key.
d) The key generated in third step will be used by CCMP protocol to provide data confidentiality and integrity.

## IV LACK OF WEP PROTOCOL

The risk of symmetric key in WEP protocol is due to repetition of initialization vector. We know that the key is changeable but it change rarely. If the key is not change then we might get a repeated key stream. By this attacker can easily access the IV so that is not encrypted during transmission of packet. Some of the card such as PCMCIreset to zero each time they initialized. Then it is prescribe by WEP standard protocol in such a way that length of initialization vector cannot be changed.

1) Key management of WEP protocol:WEP protocol use CRC 32 algorithm to check that message is changed during transmission .checksum cannot prevent attackers or hackers from altering message that made to detect error in message and its modification.
2) Message modification: Modification of message during the transmission. This is not notice by the receiver. It means that it is possible to do any modification in any encrypted message.
3) Message injection: In this an attacker can encrypt his own message by knowing the key and send this message to receiver. Then receiver will decrypt the message without knowing that message was injected.
4) Message decryption: It means that modification of encrypted message is possible and it can send to receiver without any interruption. Recipients can decrypt the message if they have secret key.
5) Temporal key integrity: It is collection of algorithm used for improving and solving the security problem of WEP.Shared key is used in WEP for encryption purpose while in TKIP it is used for generating other keys.

**TKIP [12] makes improvement on the old mechanism which is stated as below**.

1) Message falsification is prevented by Encrypted message integrity code: False message occur when attacker meets the message send it as original but by modification. This problem is solved by MIC key and linking IV. If MIC key is repeated more then one times then there is false in the message.
2) Initialization vector is used to prevent replay attacks.
3) Key generating code: A new key is generated by hash function based on temporal key and initialization vector. In this hash function is based on calculation of MAC address that 32 bits of IV.

4) In order to prevent repetition of key we have to refresh key always. We discuss three types of refresh key mechanism.
5) Temporal key has 128 bit and 64 bit key for encryption of data integrity. It uses separate key on both side. TKIP identifies 2 bit of identification. When the connection is established the first set of connection is established to the two sets of WEP key id. When connection established then transfer of message is possible.
6) Encryption key: It is for protecting temporal key.
7) Master key: This key is related to authentication purpose and to secure distribution of key stream. It is for one session only.

**V. 802.1x**:It is intended to provide strong authentication, port based access control, and key management and allow WLANs to scale by centralized authentication of wireless users or stations .It is based on EAP(extensible authentication protocol) which is itself an extension of PPP(point to point protocol) Thus, we considered as 802.1x maps EAP to the physical medium whether it is Ethernet, Token Ring or wireless LAN and It support multiple authentication methods like token cards, one-time passwords, and public key etc.

**801.1x authentication process:**

1) The request is send from client side for authentication to the access point.
2) AP verifies the client identities by the help of authentication server and blocks all traffic like HTTP, DHCPetc.
3) The client sends response to the authentication server that he is authorized user.
4) By receiving the request authentication server uses an appropriate algorithm to verify the user or client identity. If user is identified then message is sent to access point otherwise it is rejected.
5) At last AP will convert user port to authorized state.

TABLE 1 802.11 Security Solution

| **Mechanism** | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| Access control | 802.1x | Pre-shared key or 802.1x | Pre-shared key or 802.1x |
| Authentication | EAP method | EAP method | EAP method |
| Encryption | RC4 | TKIP(RC4) | TKIP(RC4) |

**Advantages of 801.1 x**

1) The user responsibility in the network is define by administrator and can easily find mistakes.
2) According to the manufacturer standard administrator allow access to the network.
3) If there is any non-client in801.1 x then he can access the network.
4) The client can re authenticate before the port is locked during a certain session.
5) As in hub it is allowed for access the network by shared mediator.
6) In the access point ,the protection is imposed to all user or client.

***RC4 algorithm****:* This algorithm belongs to cryptographic algorithm and uses in process of encryption and decryption techniques. It is termed as rivest cipher 4.It has different key stream cipher with byte oriented operation. This algorithm used as encryption and decryption in such a way that data stream should be Xored by the help of key sequence. It is used by standard such as IEEE802.11 using 40 and 128 bit keys.

Advantages of rc4

1) It is used to know the difficulties of any values in the table and its location.
2) This key can be used only once.
3) It is faster thanDES (Data encryption standard)

***AES algorithm****:* This algorithm is known as Advanced Encryption standard. It is symmetric block cipher that is used to replace DES. It is used as encryption and decryption method. It encrypt and decrypt data blocks of 128,192or256 bits depend on key size. It is fast and flexible. Both AES And RC4 algorithm contain symmetric encryption system of five element: plaintext, encryption and decryption algorithm, secret key and ciphertext.There are five cryptographic modes of cipher system: Electronic codebook(ECB),Cipher block chaining(CBC),Cipher feedback(CFB),output feedback(OFB),and counter mode(CTR)[13-14]

**Comparison analysisof WLANsafety mechanism**

| **Key Term** | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| Cipher | RC4 | 128bits | AES |
| Key size | 40 bits | 64bits authentication | AES |
| Initialization vector (IV) | 24 bits | 48bits | 48bits |
| Packet key | Concatenate | Mix function | No need |
| Data | CRC3 | Michael | CCMP |

| | | | |
|---|---|---|---|
| integrity | 2 | | |
| Header integrity | None | Michael | CCMP |
| Replay attack | None | IV sequence | IV sequence |
| Management key | None | EAP based | EAP based |

## VI. CONCLUSION

In this survey paper one can see different kind of security attacks in wireless network. We have briefly introduced basic characteristics of wireless ad-hoc network its security and solution. WEP which is known as wired equivalent protocol is the first data protection protocol in wireless network. We use three safety mechanisms to protect the data in wireless network. They are authentication, confidentiality and integrity. This is based on RC4 and AES algorithm. But still there is some demerit in WEP. Its demerit is unsafe authentication, repeated use and open transfer of initialization vector. Key management system, integrity of message should be maintained but it is not ensure properly. WPA increase communication of wireless protection through increased level of data protection by the help of WI-FI standard. IEEE 802.11i helps in software up gradation of current devices. There is also TKIP algorithm to improve the safety mechanism and it provides strong safety procedure. Robust security network defined by 802.11i and it provide mutually strong authentication.802.11i provide high level of protection but cannot help in problem caused by dos (denial of service) attacks like jamming signal.

## REFERENCES

1. Stamatios and V. Kartalopoulos, Editors, "Differentiating Data security and Network Security", *IEEE International Conference on Communications, (2008) May 19-23, Beijing.*
2. S. D. Kanawat and P. S. Parihar, Editors, "Attacks in Wireless Networks", *International Journal of Smart Sensors and Adhoc Networks, (2011) May 18-23.*
3. Y. X. Lim and T. Schmoyer, Editors, "Wireless Intrusion detection and response", *IEEE InformationAssurance Workshop, (2003) June 18-20, WestPoint, Newyork.*
4. Radomirprodanovic and Simic,"*A survey of wireless security "Journal of computing and Information Technology-CIT* 15, 2007, 3,237-255 date of issues (1998)10.24.98/cit1000877
5. F. De Rango, D. C. Lentini and S. Marano, Editors, *"Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i", EURASIP Journal on Wireless Communications and Networking, (2006) June.*

6. Umesh Kumar and Sapnagambhir, editors,"A literature review of Security threat to wireless networks, "International journal of future generation Communication and networking"Vol.7, No.4 (2014), pp. 25-34 http://dx.doi.org/10.14257/ijfgcn.2014.7.4.03.
7. AUSCERTAA-2004.02, Denial of Service Vulnerability in IEEE 802.11 wireless devices. (2004).
8. C.WULLEMS, K. THAM, J. SMITH, M. LOOI,ATrivial Denial of Service Attack on IEEE 802.11
9. Hamieh CNRS-PRISM lab,univ of Versailles ,versailiesfrance;BenothmenJ.''Detection of jamming attacks in wireless adhoc network using error distribution. Communication, 2009.ICC 09.IEEE International conference.DOI:10.1109/ICC 2009.5198912. pp 1-6(2009)
10. Chan, X. Liu, G. Noubir, and B. Thapa. *Control channel jamming: Resilience and identification of traitors. In Proceedings of the IEEEISIT*, 2007.
11. White paper: Testing for Wi-Fi Protected Access (WPA) inWLAN Access Points. Net-O2 Technologies,(2004).http://whitepapers.zdnet.co.uk/0, 39025942,60152756p,00.htm
12. W. HAN, D. ZHENG, K. CHEN, Some Remarks on the TKIP Key Mixing Function of IEEE 802.11i. *Cryptology ePrint Archive*, (2006).http://eprint.iacr.org/2006/129.pdf
13. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Request for Candidate Algorithm Nominations for the Advanced Encryption Standard. Federal Register, September 12, (1997).*
14. J. DAEMEN, V. RIJMEN, *AES Proposal: Rijndael, Version 2. Submission to NIST*, March (1999). http://csrc.nist.gov/ encryption/aes