Compromised Security of Wireless Ad-Hoc Networks & its Implications

Komal
Assistant Professor
Amity University Haryana

ABSTRACT
Networks have become an integral part of all communications, associations, businesses, services, government/public organizations and human interactions around the globe. Emergence of technologies and dynamism of user needs & access pattern of network resources have shifted paradigm to wireless ad-hoc network infrastructure supporting mobile devices. Ad-hoc networking means building spontaneous networks with self-governed devices having peer-to-peer, real-time communication. Wireless ad-hoc networks have applicability in numerous areas including critical ones like disaster relief, crisis management, alert systems and military purposes. However, the autonomous nature of wireless ad-hoc networks (WANETs) makes them vulnerable to security breaches and attacks. The paper presents a security model for wireless ad-hoc networks and discusses security loopholes in ad-hoc networking with their repercussions.

General Terms
Ad-hoc network, WANET.

Keywords
Ad-hoc Networks, WANETs, IEEE 802.11, Security, Attacks, Vulnerability.

1. INTRODUCTION
Wireless networks can be of two types- access-point based and ad-hoc. Ad-hoc networks don't require any access-point or base station to establish communication between two nodes. Ad-hoc network's components are only end devices having transceivers (able to transmit signals and receiver signals) and complying with IEEE 802.11 standard. End devices can be laptops, PDAs (Personal Digital Assistants), mobile phones, wireless cam, sensors etc.

Wireless ad-hoc networks can be defined as interconnection of nodes together on the fly using wireless links without any centralized or predetermined architecture. There is no fixed topology and availability of interconnection devices like switches, routers and access-points for transmitting and routing data packets from a source to destination. Nodes in an ad-hoc network are themselves responsible for discovering their peer neighbors and finding out route to send data to an intended device. In ad-hoc networks, any two devices can communicate with each other if they lie within their radio range of transmission. This puts a limitation on geographic distance within which two devices can communicate by building ad-hoc network. However, different small transmission areas can be overlapped or combined to form a larger transmission area, which enables two far off devices to communicate using overlapped transmission area devices as relays.

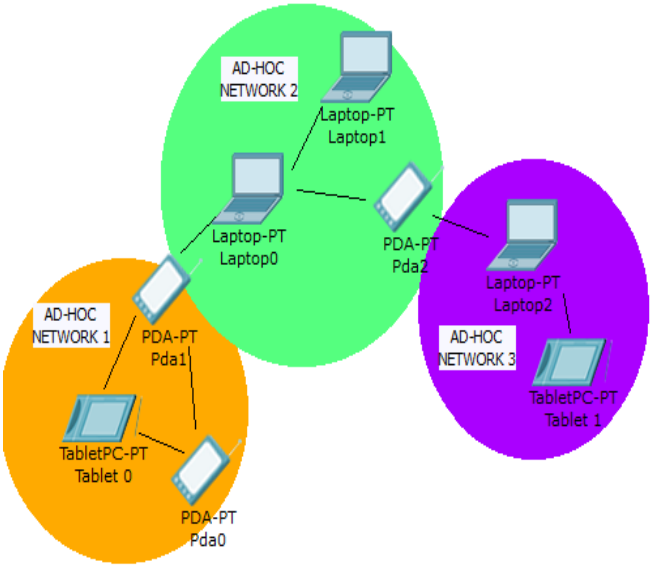

Fig 1: Transmission areas in wireless ad-hoc network

Wireless ad-hoc networking is a cheap and convenient approach to disseminate information between nodes which are in the same transmission area without any underlying architecture. Nodes of ad-hoc network rely on other nodes in the neighborhood for information transfer and trust the routes and information as transmitted by their peers. They have their applicability in broad range of areas –business meetings, classroom discussion, network games, telecare system[1], cab services and emergency situations like- warfare activities, disaster management, rescue activities, military intelligence and spy operations. In critical applications, information integrity, confidentiality and efficiency of communication are some vital factors to be looked at.

The paper is structured into 5 sections including the Introduction. Section 2 presents security model for ad-hoc networks that consists of various parameters, which collectively make the system secure. Section 3 discusses vulnerabilities of characteristics of ad-hoc networks. Section 4 provides a detailed classification of different security attacks that can be exercised in ad-hoc networking environment and their aftereffects. Section 5 concludes the paper with significant observations.

2. SECURITY MODEL FOR AD-HOC NETWORKS
Security is the most critical aspect of any communication system. Wireless networks are inherently insecure due to autonomous and unpredictable behavior of devices which are having close coordination together. To identify the level of security implemented in ad-hoc networks, there should be a security model that consists of various security parameters for

evaluating the security of critical information and communication. The suggested security model of ad-hoc network consists of following security parameters [3][7][8]:

a) Confidentiality- This parameter ascertains that the information travelling on the communication link is accessed only by authorized users (which are involved in communication). No other user or device can eavesdrop or receive the communication data of other devices. It means private information remains private and can't be misused.

b) Integrity- This parameter ensures that the data/information received by a device is same as it was sent by the sending device and there has been no manipulation of the data intentionally or unintentionally on the communication path.

c) Authentication- This parameter ensures the identity of the devices/entities that are part of network and participate in the communication. It makes sure that there is no impersonation of identity and the data has been received from and sent to intended users only.

d) Authorization- This parameter specifies the access rights and privileges of each authenticated user/device. Thus, it provides a limitation on the extent and type of resources that can be used or accessed b established entities/users in the network.

e) Availability- This parameter necessitates the 24x7 presence of resources and devices so as to provide their designated services in emergency situations (where unavailability for even fraction of seconds can cause serious issues). Denial of service is an attack that hampers availability of services/device. Thus, ensuring availability is a good criterion to achieve secure communication.

f) Dependability- This is a critical parameter as far as emergency situations are concerned. The network should be able to communicate somehow to the devices when there are no other options available and all services have been down. Users can rely upon WANET for accessing and sharing useful information even in worst case scenarios.

g) Accountability- Accountability means that all activities should be logged so as to find misbehavior and unexpected responses during communication. It helps to detect malicious intents and attempts exercised on the network resources so that proper measures can be taken to avoid such happenings in the future.

h) Anonymity- This parameter states that though the identities of the users participating in a communication are recognized to be true but they are never disclosed in public so as to protect critical devices (like servers) from targeted attacks.

i) Non-repudiation- This aspect of security model ensures that having sent a message and/or received a particular message, sender and/or receiver can't deny that it has sent/received that message.

j) Efficiency- Security model needs to consider CPU and memory efficiency of devices as most of the attacks target the processing power and memory space of resources to be exhausted.

3. VULNERABLE FEATURES OF WIRELESS AD HOC NETWORKS

Security has always been top-priority in sensitive communication scenarios. The inherent characteristics of wireless ad-hoc networks make them prone to security breaches and attacks. These features are discussed as follows [2][4][8]:

a) Dynamic Network Topology [2]- Since mobile nodes keep changing their locations, they leave and join network rapidly. Due to highly dynamic nature of network topology, traditional security tools can't observe network traffic and hence can't discriminate between genuine and malicious nodes.

b) Decentralized architecture- Wireless ad-hoc networks do not have centralized architecture. So there is no fixed network component where different security measures like Intrusion Detection System (IDS), traffic monitoring tools can be deployed.

c) Shared medium- There is no dedicated, point-to-point connection between any two nodes in WANETs. Wireless medium is susceptible to eavesdropping and also, spreading rumors is easier. Any malicious node lying in the same transmission area can mislead other nodes and can overhear other's transmission.

d) Variable link capacity [2]- Since the transmission medium is shared between all the nodes lying within a particular range; the bandwidth is also divided between all the users. As the no. of nodes within an ad-hoc network keeps changing, the link capacity used for communication also changes. This may lead to loss of information in some cases.

e) Critical power resources[2]- As the mobile nodes are fitted with battery that has a limited life, power failure can be fatal for critical communication scenarios.

f) Absence of well-defined network boundaries[8]- Network edge is considered the only point of entry and exit of traffic and hence, most vulnerable to attacks. That is why all boundary routers are configured with security features like firewalls, Access Control Lists (ACLs), IDS etc. Devices inside the boundary are considered safe from external attacks. In ad-hoc networks, there is no clear edge or boundary and all devices inside the network are vulnerable to external attacks.

g) Lacks of proper addressing [8]- Ad-hoc networks do not follow a proper addressing scheme. Devices configure themselves on their own, scan the medium for information signal, discover their neighbors and start communication. Due to the absence of proper addresses, it is quite difficult to identify and isolate a malicious node.

h) Interdependence of neighbors- Nodes in WANET depend on their neighbors for taking routing decisions and any malicious node can pose as a trustworthy neighbor and poison the routing table by participating in the decision making process.

i) Limited availability- Network resources are not available all the time due to various factors-limited batteries, mobility of nodes, hostile environment, less bandwidth of link, high interferences.

j) Increased error rate[4]- Unlike wired transmission medium, signal travelling on wireless medium faces reflection, refraction, diffraction from obstacles which leads to deterioration of signal and increased chances of error in the information signal.

k) Limited scalability- Ad-hoc networks are not much scalable due to limited transmission areas, lesser link bandwidth and high interference risks.

l) High latency- There is significant amount of time needed for processing data for transmission as each node has to

compute the route in ad-hoc network. Thus, any transmission between two nodes in ad-hoc network has higher latency including the processing of signal at each intermediate node.

m) Autonomous behavior of nodes- The convenience of being self-sufficient is problematic too. All nodes take their routing decisions independently using the information acquired from their neighbors. Any malicious node can spoil routing table of a particular host intentionally and create chaos in the network.

n) Compromised nodes- Ad-hoc networks are created on the fly without any network administrator's intervention. Nodes within such networks may not have required resources, proper security measures and well-defined access policies. Such nodes (having no security configuration enforced) are called compromised nodes and provide easy access to malware and untrustworthy sources.

o) Limited memory & processing power- Nodes in an ad-hoc network range from laptops to PDAs to mobile phones. Different devices have different computing power and memory support. Denial-of-Service (DoS) attacks target memory and computing power of a compromised node. Since most of the devices in ad-hoc networks have both limited resources, they are easy targets of such attacks.

p) No physical protection- In wired networks, Critical components of a network like servers, data centers, routers, switches, printers etc. can be physically protected and isolated from every user's reach by locking them in separate rooms and cabinets. However, physical security can't be ensured for roaming devices of ad-hoc networks.

q) Route discovery overhead- Infrastructure based networks use specific devices (routers, access-points) which are responsible for discovering routes and transferring packets on the selected path. Ad-hoc networks don't have such infrastructure and all the nodes are themselves responsible for route discovery. This overhead wastes significant memory and processing power of devices.

4. CLASSIFICATION OF ATTACKS

Owing to the vulnerabilities of features of wireless ad-hoc networks, malevolent nodes can take advantage and perform a number of attacks on the participating nodes. Different researchers [2][3][5][6][7][8] have discussed different security threats posed to wireless ad-hoc networks. Security threats and attacks can be classified based on various parameters- nature of attack, domain of attack, severity of attack, protocol based attacks, layer specific attacks, no. of attackers involved, no. of nodes affected etc. Broadly we can classify attacks into two categories[2]: External attacks and internal attacks.

4.1 External attacks

Security attacks which are performed on the nodes of a wireless ad-hoc network by an external agent are often referred as "External Attacks" or "Outdoor Attacks". Due to absence of clear boundary of an ad-hoc network, all nodes within the network are equally susceptible to security menace. External attacks can further be classified into two categories[3]- Active and Passive attacks. Active attacks are meant for malfunctioning the network devices such as node failure, resource consumption and misuse, alter information and create chaos in the network. Passive attacks are exercised by competitors or rivalries to obtain private information of the network and misuse it for their personal gain.

4.1.1 Snooping

This is type of passive attack which aims to collect information about an ad-hoc network. Overhearing on a particular wireless link enables an outsider to figure out if there is a network existing nearby. Eavesdropping intercepts messages communicated by nodes for their local purposes.

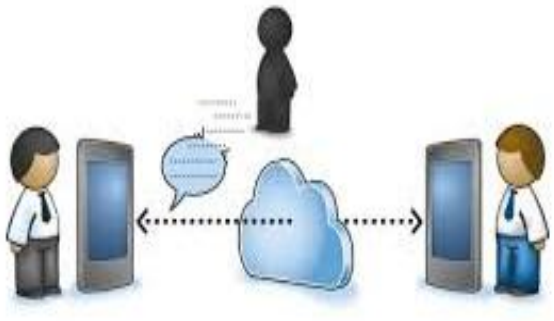

Fig 2: Snooping Attack

Acquiring private information of a network by an unauthorized node is the breach of confidentiality principle of security model and can have serious consequences-

- Disclosure of network existence in hostile environment
- Disclosure of location of busiest device/resource in the network which can be targeted to breakdown critical service in the network.
- Theft and misuse of confidential information.

4.1.2 Spoofing attack

Impersonation of any kind is a security threat since anyone who poses to be a reliable/known host can spread rumors and deliver fake routing information which in turn disrupts the co-ordination of other devices. Spoofed packets are used to realize a node that it is receiving information from an authorized node.

Consequences of spoofing can be-

- Confusion between genuine and spoofed routing information.
- Flooding of responses on a host whose address/location was spoofed in a query.
- Directing the communication towards a fake node isolating the genuine node from network.

4.1.3 Man-in-the-middle attack

This attack is similar to active eavesdropping where attacker establishes links with two victim nodes independently and provides a communication channel so as every message is transferred to attacker first, which can then modify, drop or inject new message while it is sent to the other host. Victim nodes are unaware of the presence of the attacker on their communication link and presume their communication as confidential.

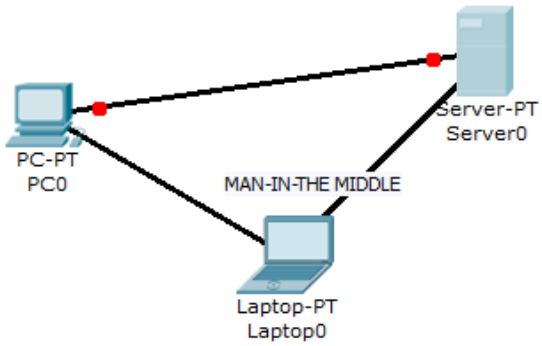

Fig 3: Man-in-the-middle scenario

Implications of such an attack can be-

- Miscommunication and no synchronization between nodes.
- Nodes behavior influenced by attacker's will.
- End devices are held liable for information leakage.

4.1.4 Denial-of-Service attack [2][3]

Denial-of-Service attack aims to consume battery, processing power and memory resources of a host so as to make it unavailable to respond to genuine requests of hosts. The most common DoS attack is flooding a targeted host with fake requests/ routing updates that consume significant amount of battery and CPU cycles making it too busy to address other requests.

There are several consequences of this attack-

- Unavailability of critical resource due to battery discharge.
- Long queues of pending requests at different resources.
- Dropped packets at the service end due to memory overflow.

4.1.5 Protocol specific attack

Various protocols are used by nodes for communication, each having its own pre-defined types of messages. There are different stages in a protocol communication right from node discovery to negotiation to connection establishment and communication. Messages like HELLO packets (used for discovering neighbors) can be misused to discover active nodes and to initiate communication with them by intruders. Implications of protocol specific attacks-

- Routing table poisoning.
- SYN flood attack.
- Hijacking session using ARP spoofed packets.

4.1.6 Distributed Denial-of-Service attack [2]

Distributed Denial-of-Service attack makes use of compromised hosts (having no anti-virus or security enforced) in a network and uses them to reflect the attack towards a targeted host. Such compromised nodes are called as "Zombies" which work on behalf of attacker. Thus an outsider can exploit the inside nodes and misuse them for fulfilling their malicious intents.

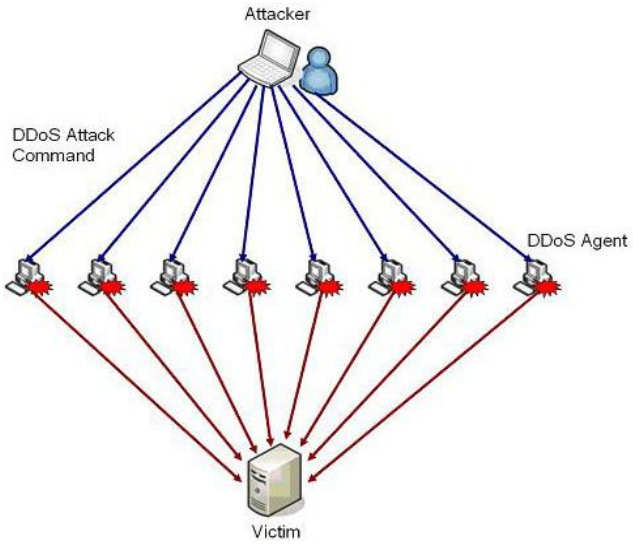

Fig 5: Distributed Denial-of-Service attack

Consequences of this attack are similar to DoS but the mode of implementing it is different.

- Unavailability of critical resource due to battery discharge.
- Long queues of pending requests at different resources.
- Dropped packets at the service end due to memory overflow.

4.1.7 Cryptanalytic attack

Cryptanalysis is used to find associated information with cipher-texts created by cryptographic algorithms. Such an attack can also attack digitally signed encrypted documents. Cryptanalyst is able to break through the code without even acquiring secret key used for encryption. Implications of cryptanalytic attack are-

- Safest information transmission technique failure.
- Requirement of more complex encryption techniques requiring significant computation time.
- Replay attacks after passwords being cracked.

4.1.8 Jamming attack [3]

Jamming attack is instigated on physical layer to interrupt network communication by deploying radio jammers or by transmitting noise on a particular radio frequency so as to corrupt underlying communication on that frequency. Noise transmission can be continuous or periodic depending upon the frequency of communication. Repercussions of jamming are-

- Disrupts the co-operation of nodes for taking routing decisions.
- Failure of communication link.
- Decreased throughput.

4.1.9 Byzantine attack [2]

Byzantine attack is where a system behaves in completely unexpected way which may be failure to process a request or processing a request incorrectly. Even coded communication can be modified to influence a node's behavior. Some of the consequences of Byzantine attack are-

- Congestion in the network due to non-processing of requests.
- Hardware or software failure of a node.
- Disconnection of communication link.

4.2 Internal attacks

Though security is always enforced for external entities, internal nodes harm the network much greater than externals as they exploit the trustworthiness of nodes of same network and fulfill their malicious intents. An insider is more dangerous than many outsiders when it comes to security of network. Thus proper measures must be taken to look into the intents of internal nodes during communications and any malicious move should be dealt seriously. If security of a network is violated due to the activities of internal nodes only, then such security threats are called "Internal Attacks" or "Indoor Attacks". Like external attacks, internal attacks can also be categorized as- Active and Passive attacks. Specification of indoor attacks is given as follows.

4.2.1 Sniffing

It is a kind of passive attack where some malicious nodes join a network with the purpose of monitoring activities within network, intercepting the communication of other nodes, so as to acquire internal statistics of the network, which may be circulated to adversaries outside the network. Implications of inside sniffers are as follows-

- Confidential data of authorized nodes being leaked.
- Compromised nodes of network are identified by sniffers.

4.2.2 Forgery

Forgery can be done in a number of ways like forging the identity of some other device, introducing fake data packets into the network, forging routing update messages to spoil routing decisions. Forgery attracts many serious consequences-

- Network congestion due to extra introduced packets.
- Transmission of critical information to adversaries.
- Poisoning routing table of nodes.

4.2.3 Black hole attack [2]

In black hole attack, a malicious node attracts all the traffic of network towards itself by promoting that it has shortest routes to various destinations. Thus, all the nodes start directing their traffic towards that malicious node for delivering it to the intended recipient. But the node discards all the packets instead of its transmission further. Thus all the communication inside the network is pictured as reaching a big hole, from where it is discarded. Black hole attack results in following consequences-

- Reduced throughput in the network.
- Node unreachable condition for maximum hosts besides their existence.
- Complete network failure or down state.

4.2.4 Wormhole attack [5]

Wormhole is a topological arrangement that connects two end-points in the form of a tunnel. Adversary node is the one end of the tunnel and other point may be lying at any arbitrary location inside the network. Wormhole is misused by adversaries to tunnel all the packets received on the network to the other end with less latency and then replay them into network from that point, without affecting the integrity of the information.

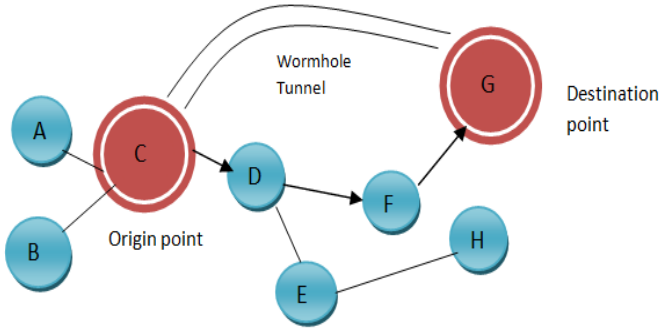

Fig 6: Representation of Wormhole attack

Implications of wormhole attack are-

- Network bandwidth exhaustion due to replicated messages being float.
- Leakage of network-specific information to remote hosts on tunnel end.
- Sometimes original messages are dumped by considering them as duplicates.

4.2.5 Gray hole attack [2]

Gray hole attack is similar to black hole attack in the manner that adversary node catches the attention of other nodes and pull all the traffic towards itself by offering lucrative route options. However, unlike a black hole attack, the nasty node doesn't drop all the data packets received by it. The node drops some selective packets or drops packet with certain probability to give an impression of normal working condition of network. Consequences of gray hole attack are discussed as follows-

- Fault identification is very difficult due to dropping of packets randomly.
- Reduced throughput of network communication.
- Communication link failure for some targeted nodes.

4.2.6 Rushing attack [2]

In this attack, attacker tries to send the route request messages as received from a node hurriedly to other nodes in the network, so that the nodes assume attacker as the actual source of enquiry and discard genuine requests as duplicate. The intent of the attacker is to receive routing information from various nodes and let the original enquiry node suffer. Aftereffects of such an attack will be-

- Responses of various enquiries within the network being submitted to adversary node in place of the intended seekers.
- Subserviced requests amongst various hosts.

4.2.7 Replay attack

Replay attack is to broadcast or execute single request or routing update message multiple times from various locations in the network. Replay attacks can also intercept authorization related information like passwords and apply them no. of times to forge identity of authorized node. Implications of replay attacks would be-

- Cracking security checks with replay attacks.
- Causing bad congestion in the network.
- Collision of data packets and dropping of original ones.

4.2.8 Selfish node attack [3][7]

Selfish nodes in an ad-hoc network can overuse the resources such as bandwidth, battery power, processing speed for their own personal profit and make other nodes in the network to starve for the same resources. Thus genuine nodes are deprived of resources (due to selfish intents and activities of others). Implications of selfish nodes' behavior can be-

- Degraded throughput of affected nodes.
- Complete failure of communication link.
- Resource starvation and long waiting queues of processes.

4.2.9 Sybil attack [2]

In Sybil attack, a spiteful remote node can pose multiple identities which are physically non-existent. This attack relates to the notion of multiple personality disorder, where single entity exhibits multiple behaviors at different times. Sybil attack is a conspiracy to establish multiple links to a network by showing multiple existences. Security implications of Sybil attack can be-

- Numerous nodes targeted for the security attack at the same time.
- Damage caused by Sybil attack is manifold as done by single attacking node.
- Uncertain behavior exhibited by nodes.

4.2.10 Jellyfish attack [6]

Jellyfish attack is a kind of passive attack which is quite difficult to detect. Node exercising jellyfish attack introduces variable delays before packet transmissions to affect the performance of various protocols within the network. For real-time communication traffic, this attack is fatal. Various repercussions of jellyfish attack are-

- Missed order of data packets.
- Dropped packets due to expired time-to-live field.
- Decreased throughput and increased latency.
- Partitioning of network.

4.2.11 Infrastructure disclosure attack

An insider node, who receives routing updates and control packets of various protocols, is able to discover the topology of network, identity of nodes and location of nodes. Such information is more crucial than application based data. Any compromised inside node can accidentally leak the information related to infrastructure to adversaries outside the network. Such a security threat results in following consequences-

- Identification of weak spots within the network.
- Geographic locations of critical resources known to adversaries.
- Type and multiplicity of resources known to adversaries.

5. CONCLUSION

Wireless ad-hoc networking has provided a new dimension to the world of communication. Mobile nodes can establish communication links with each other in a hostile environment or a scenario where all infrastructures have been demolished. Since cooperation between nodes is the key to achieve a common goal in critical situations like rescue operation, spy work in enemy domain, military communication in wartime; any break or halt in the communication results in complete failure of operations. Adversaries exploit the spontaneous nature and other vulnerabilities of ad-hoc networks to divide & isolate their nodes in order to disable their co-operation. The paper has discussed the features which need to be ascertained for a secure ad-hoc communications. It has addressed the security loopholes of ad-hoc networks and the extent of damage various security attacks make in the network.

6. REFERENCES

[1] "Security Issues in Wireless Adhoc Networks and The Application to the telecare project", Proceedings of 2007 15th International Conference on Digital Signal Processing,pp 491-494, 2007.

[2] Sarvesh Tanwar, Prema K.V, "Threats & Security Issues in Ad hoc network : A Survey Report", International Journal of Soft Computing and Engineering, volume-2, Issue-6, January 2013.

[3] Safdar Ali Soomro, Sajjad Ahmed Soomro, Abdul Ghafoor Memom,Abdul Baqi, "Denial of Service Attacks in Wireless Ad hoc Networks" , Journal of Information & Communication Technology, Vol. 4, No. 2, (Fall 2010),pp 01-10.

[4] Martinus Dipobagio, "An overview on Ad hoc Networks", Institute of Computer Science (ICS),Freie Universitat Berlin.

[5] Yurong Xu, Guanling Chen, James Ford, Filia Makedon, "Detecting wormhole attacks in wireless sensor networks", Critical Infrastrcuture Protection, International Federation of Information Processing, volume 253, pp 267-279, 2008.

[6] Fahad Samad, Qassem Abu Ahmed,Asadullah Shaikh,Abdul Aziz, "JAM: Mitigating Jellyfish Attacks in Wireless Ad Hoc Networks", Emerging Trends and Applications in Information Communication Technologies, Communication in Computer and Information Science, volume 281,pp 432-444, 2012.

[7] Po-Wah Yau, Chris J. Mitchell, "Security vulnerabilities in Ad hoc Networks", The Seventh International Symposium on Communication Theory and Applications, July 13–18, 2003, Ambleside, Lake District, UK, pages99–104. HW Communications Ltd, July 2003.

[8] Rakesh Kumar Singh, Rajesh Joshi, Mayank Singhal," Analysis of security threats & vulnerabilities in Mobile Ad Hoc Network (MANET), International Journal of Computer Applications,Volume-68, No.4, April 2013.