Introduction to MANET, Its Threats and Counter Measures

SUMAN SINHA

1] ABSTRACT:

Mobile ad hoc networks (MANETs) are self-organizing and self-configuring mobile networks that do not depend on fixed infrastructure. MANETS are often used in situations where it is costly or unfeasible to put up a wired infrastructure, such as in disaster relief operations. There are several challenges inherent in Mobile Ad-Hoc Networks (MANETs). Even though these networks have several advantages over traditional wired networks, MANETs present unique challenges. For example, MANETs face difficulties in secure communication. Mobile nodes without adequate protection are vulnerable to compromise. The static configuration may not be adequate for the dynamically changing topology in terms of security solutions, and lack of cooperation and constrained capability are common. Due to the lack of protection mechanisms for MANETs, hostile attackers may quickly access the Ad Hoc Network. Although security challenges in Mobile Ad-hoc Networks (MANETs) have been a critical emphasis in recent years, the creation of the most secure algorithms for these networks has not been completed yet. Due to the autonomous nature of MANETs, they are especially vulnerable to security threats. This paper will explore the most common threats to a MANET and provide suggestions for how best to alleviate or avoid them.

2] Introduction:

MANET is a type of network that does not require fixed infrastructure, like base stations, to communicate and operate. In MANETs, the wireless devices or nodes communicate with each other without being dependent on any centralized management system.

Within the MANET, the nodes themselves are in charge of proactively finding new nodes with whom to connect. Because of the range limitations of wireless networking interfaces, it may be necessary for one wireless mobile node to use other hosts to send a packet to its intended destination.

Each wireless mobile node can function as a host and as a router, routing packets to and from other wireless mobile nodes in the network that are not necessarily within direct transmission range of one another.

The highlights of MANET networks are that they are peer-to-peer, self-forming, and self-healing in nature. MANET network primarily uses radio frequencies between 30MHz to 5GHz. MANET network applications can be helpful in road safety, home sensors and rescue operations.

3. FEATURES OF MANET:

1. Uses rapidly changing topologies
2. Restricted bandwidth links with fluctuating capacities
3. Self-monitored behavior independent of the environment
4. Operation with a Limited Energy Budget
5. Prone to security threats
6. Minimum human intervention

4. MANET COMMUNICATION PROCESS:

Mobile ad hoc networks, or MANETs, are groups of mobile nodes that can communicate with each other without being dependent on any infrastructure. In other words, they have no access point, base station, or gateway to organize their communications. Instead, they must organize themselves through a distributed approach using multi-hop communication.

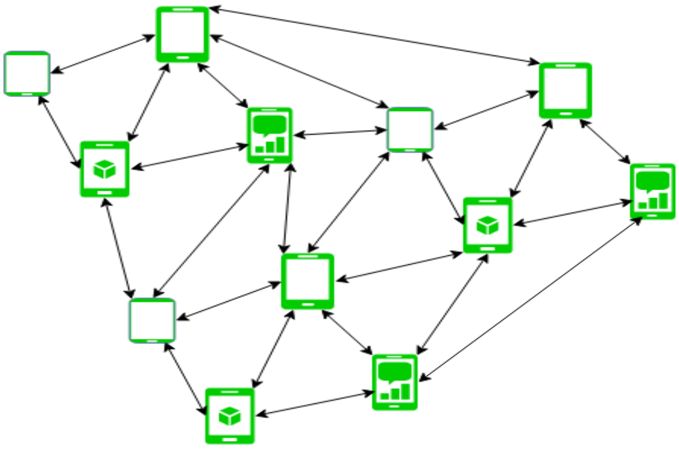

Figure - Mobile Ad Hoc Network

In typical networks, specialized nodes carry out fundamental activities such as packet forwarding, routing, and network administration to operate correctly. In mobile ad hoc networks, this is done collectively by all of the nodes that are currently accessible.

Nodes in MANETs connect through multi-hop communication: nodes within each other's radio range may communicate directly over wireless links, but nodes that are far away must depend on intermediary nodes to function as routers to transmit messages.

5. ADVANTAGES OF AD HOC NETWORKS:

Ad hoc networks are unique compared to traditional wired LANs and WLANs. Due to their unique characteristics, ad hoc networks are used in various circumstances.

The primary benefit of an ad hoc network is that it allows users to share resources without the need for costly infrastructures such as cables and routers. This allows users to more easily share information, which allows for greater collaboration between individuals. The cost savings make this type of network very appealing to many organizations, especially those that have limited financial resources or need to be able to deploy new technology quickly.

Ad hoc networks are quick to set up and can be easily modified to fit any situation, making them an excellent choice for various situations. Their flexibility and low cost make them an appealing option, and the fact that they don't require costly physical infrastructure to operate.

Another advantage to using this type of network is its ability to operate under adverse conditions such as low bandwidth or high latency due to interference from other networks nearby. This makes these networks ideal for situations where there may not be enough resources available on-site or where many people are trying to access the same resource at once.

6. DISADVANTAGES OF AD HOC NETWORKS:

There are several disadvantages associated with ad hoc networks that should be considered before implementing them in your organization. One of the most significant disadvantages is that they often do not provide enough security for sensitive data and applications, so it may be necessary for your organization to purchase additional security measures. There are no authorization facilities available. Because of the lack of physical protection, you are more vulnerable to assaults.

7. THREATS INVOLVED IN MANET:

The following are some of the more general challenges that are involved with mobile ad hoc network deployment:

- Wireless Links: Wireless networks often have smaller bandwidths than their wired counterparts. Attackers may exploit this limitation by wasting network capacity with relative ease, interfering with regular communication between nodes.

- Network Distribution: Similar to peer-to-peer (P2P) networks, distributed computing implies the absence of a centralized server to manage the clients' state.

- Rapid Topology: Consequently, the network's topology might alter regularly. Because the nodes are movable, the network can self-organize. It is difficult to distinguish between normal network behavior and abnormal or malicious behavior in this dynamic context.

- Power constraints: Power awareness is essential in a mobile ad hoc network because the devices are often powered by batteries, and the user may be in a hazardous environment, necessitating strict power requirements.

-Addressing scheme: Because of the decentralized nature of mobile ad hoc networks, the present addressing technique used by cellular networks is inapplicable to them. Through mobile IP, all of the network's nodes are addressed by a base station; however, this kind of system does not work within a mobile ad hoc network.

-Network size: A significant advantage of mobile ad hoc networks is their small network size. However, because of the latency introduced by the underlying protocols, the scale of the network is strictly limited.

- Lack of a Clear Line of Defense: In the absence of a clear line of defense, MANETs are vulnerable to assaults from all angles. The complex and dynamic topology often makes it impossible to establish a secure perimeter that can be easily defended. The devices themselves may be targeted through vulnerabilities in their operating systems or applications. Alternatively, an adversary can target the infrastructure between them, allowing for various attacks, including denial-of-service (DoS) and man-in-the-middle (MITM). Finally, even if there is no direct access to either device or infrastructure, attacks on one device can be propagated across all others via wireless transmissions such as Bluetooth or infrared communication

- Limited Resources: Devices on MANETs may include everything from computers to portable devices such as PDAs and mobile phones, among other things. These will often have varying computational and storage capacities, and they may be the target of new assaults as they emerge. This has resulted in the introduction of novel assaults that specifically target this system component.

- Routing Protocol Vulnerabilities: The ad-hoc nature of MANETs introduces several routing protocol vulnerabilities that need to be addressed for effective risk management.

- Lack of Cooperation among Nodes: Routing algorithms for MANETs are often designed to assume that nodes are cooperative and do not have evil intent. Consequently, a hostile attacker may simply establish himself as a significant routing agent and cause network activities to be disrupted by defying the protocol standards."

- Responsiveness: Responsiveness of routing algorithms for MANETs is often designed to assume that nodes are cooperative and do not have evil intent. Consequently, a hostile attacker may establish himself as a significant routing agent and cause network activities to be disrupted by defying the protocol standards.

8. ADHOC MOBILE NETWORK SECURITY ASPECTS:

The sender and receiver are not connected directly but instead through an open and shared network in wireless communication. Because of this, it is inherently less secure than conventional communication.

Furthermore, there are often limitations on mobile wireless devices – such as bandwidth, storage space, computing capabilities, and energy. This can make it difficult to guarantee the availability of wireless services when they are requested. Since this type of communication is open and shared, there is also a greater risk of leaking classified information to unapproved parties.

Security requirements for mobile wireless networks are divided into five categories: availability, information confidentiality, integrity, non-repudiation, and authentication.

Availability: Availability indicates that services are available at the time of the request, regardless of whether or not there is a probable failure in the system.

Information Confidentiality: Information confidentiality guarantees that classified information in the network is never leaked to unapproved parties.

Integrity: The integrity of a message being transported between nodes is also vulnerable: it is much easier for someone to corrupt or change the message when travelling over an open network that spans a large area. It's nearly impossible for the sender to prove that they did not send information – or even to claim that they didn't – when using this type of communication.

Non-repudiation: Non-repudiation assures that the sender of information cannot claim that they did not send the information.

Authentication: Authentication is a network service that allows a user's identity to be determined.

9. NEED OF UNDERSTANDING THE MANET NETWORK:

The development of mobile ad hoc networks (MANETs) was a big step forward in creating a network that could provide its users with more freedom. MANET's mobility of nodes, power restrictions, restricted wireless signal range from each mobile host, and security concerns have made it a complex subject to study over the past few years.

If we just consider a stand-alone MANET, it will only have minimal uses since it will only be able to connect to devices within the MANET itself. MANET users can only benefit from more significant network resource usage if their network is always connected to the Internet. However, global connectivity introduces additional security risks over existing active and passive threats to MANET.

A connection may be disrupted by attacks on any layer of an active network. As a result, practically all possible attacks in traditional active networks are also possible in mobile ad hoc networks.

There is a very high risk that attackers will be able to demonstrate their activities in the form of a reluctance to engage completely and accurately in communication between mobile nodes by the principles of integrity, authentication, secrecy, and collaboration no matter what the nature of the assaults is.

10. STATEMENT OF THE PROBLEM:

Mobile ad hoc networks (MANETs) are not immune to security concerns, and the general security issues and risks they offer have been investigated. Studies on MANET have tended to be more concentrated on single-target attacks in the past.

In contrast, several attacks that involve multiple nodes have received less attention because they are unpredictable combined attacks, which is understandable.

Mobile ad hoc networks have many vulnerabilities compared to traditional wired networks. As a result, maintaining security in MANET is significantly more challenging than maintaining security in a wired network.

There has been no consistent description or classification of these types of attacks (multiple node attacks). Taken to minimize methods have been offered to fight some forms of multiple node attacks; as a result, it is necessary to determine the effects of the category of collaborative assaults and the potential mitigation measures for these types of attacks.

This paper analyses a survey of multiple node attacks in mobile ad hoc networks (MANET). The main aim of this survey is to give a consistent definition and classification of these attacks and discuss some current defence methods against multiple node attacks.

11. LACK OF RESEARCH ON MANET IN INDIA:

MANET is an emerging field in India, with only a few researchers working on it. However, MANET has received much attention in other countries, including the US, the UK, and Canada. Many research topics are included in MANET research, including routing algorithms and security. Previous MANET research in India focused on routing protocols, internet connectivity in MANET, routing algorithms, MANET challenges, and security aspects.

12. AIM OF THE RESEARCH:

As the popularity of mobile ad hoc networks (MANET) continues to grow, so does the need for a thorough understanding of the security threats that exist within these systems. The following study will examine the security challenges inherent in MANET and potential solutions.

The study will examine various security risks, including application, transport, network, data link, and physical layers. Following this examination of existing threats, the study will provide an overview of optimal solutions for MANET systems.

The broad goals of this research are as follows:

1) Research and analyze security risks and vulnerabilities in MANET

2) Find effective solutions and remedies for these security risks

3) Identify and address the unique set of challenges present in MANET

13. METHODOLOGY FOR RESEARCH:

In this research, we will examine the problems of MANET and identify the most effective solutions and defenses for cybersecurity threats. We will investigate each layer of the MANET to identify security risks and weaknesses at each tier of the security architecture. The information gathered during this phase will serve as critical inputs for the study, and additional following studies and analyses will be carried out to determine the research objectives:

- Detailed investigation and analysis of each layer of the MANET.
- Identifying security risks and weaknesses at each tier of the security architecture.
- Identify the most effective solutions and defences for cybersecurity threats.
- An examination of the difficulties of MANET.
- The results of the research and the thesis

This paper describes a taxonomy of coordinated attacks. It also suggests mitigation plans for this type of attack.

Collaborative security attacks, unlike previous attacks, are performed by multiple malicious nodes that operate together against the network to achieve a common goal. Attackers have adopted this new paradigm due to the increasing difficulty of conducting attacks without being discovered and the lack of consequences for failure. Therefore, this form of attack is more difficult to detect and prevent than other attacks carried out by a single malicious node.

Therefore, it is essential to investigate and identify the various types of coordinated security attacks that can be carried out to mitigate them successfully. The collaborative attack taxonomy presented here is based on the attackers' goal and their relationship during the attack. The impact of these types of coordinated attacks on MANET performance is analyzed since it was an essential factor in determining their severity.

14. TYPES OF ATTACKS ON AD HOC NETWORK:

Security in MANETs is not unlike that of other networks: most often, it includes authentication, confidentiality, integrity, availability, and non-repudiation. Authentication is the process by which the identification of a source of information is confirmed.

Only authorized people or systems are permitted to read or execute protected data or programs—this is known as confidentiality. It should be emphasized that the sensitivity of the information in MANETs may deteriorate faster than that of other types of information.

The security objectives may vary depending on the mode of operation in MANETs. Because of properties unique to MANETs, they are vulnerable to a wide range of novel attacks. Attacks may be classed at the highest level based on the network protocol stacks used.

The attacks may be divided into passive attacks and active attacks.

A] Passive Attacks:

Passive attacks are one of the most common types of attacks. They are commonly called "passive" because they don't require a direct connection to the network. A passive attack may not even interfere with network communications. Instead, they aim to gather information about the network that can be used in future destructive attacks.

A passive attack does not require an attacker to connect to the network and involves no direct interaction with the target. Eavesdropping and traffic monitoring are examples of this type of attack.

Passive attacks include:

Eavesdropping:

In an eavesdropping attack, a node watches the data being sent back and forth on the network without interfering with or altering it. The attacker may simply be watching for some specific sensitive information or might want to know about all network traffic in general. The latter could allow them to plan a future attack more effectively.

Traffic Analysis:

A traffic analysis attack is similar to an eavesdropping attack, but rather than getting access to the content of messages sent back and forth. Attackers gather information about how messages are transmitted. This might include packet sizes and transmission times, among other pieces of data that could help attackers determine how best to launch future assaults on the network.

B] Active Attacks:

Active attacks are carried out by users or nodes who have been granted permission to function inside the network. They make changes in the network's state without the user's knowledge. Active assaults can be broken into four categories: dropping attacks, modification attacks, fabrication attacks, and timing attacks. However, an assault might be placed into more than one category, depending on its nature.

As the name implies, active attacks represent an attempt to modify, inject, or otherwise alter the data being sent across a network.

The following are some common active attacks that you will encounter:

Dropping Attacks: In this attack, information is simply destroyed or not delivered. Because this type of attack can be complicated to detect, it is often referred to as a "silent" attack. The most common example of this is when an attacker intercepts or removes data from a transmission.

Modification Attacks: In a modification attack, the attacker uses various methods to modify the contents of your information as it is being transmitted from one point to another. This could be something as simple as a man-in-the-middle (MITM) attack or more complex than packet sniffing and re-injection. Attackers may also use more advanced techniques such as spoofing and traffic injection to compromise sensitive information.

Fabrication Attacks: A fabrication attack is when an attacker creates false data and then transmits it across the network. The most common example of this is sending fake data to a server to access its resources.

Timing Attacks: Timing attacks are when a malicious user tries to discover information about the network's infrastructure by measuring the execution time for a particular task.

Security is a significant concern in mobile ad hoc networks, which are inherently open and vulnerable to security threats such as intrusion, information exposure, and denial of service. These networks require a higher level of security than wired networks as they are more vulnerable to security threats, which contrasts with the latter. This study explores various types of security risks and provides a solution for these types of security threats in the context of MANET problems.

15. ATTACKS ON THE LINK LAYER:

The data link layer may be categorized based on its network impact, depending on the overall status of the network.

It can be broadly categorized into three attack types: 1) Nodes acting selfishly, 2) Distributed denial of service (DDoS) attack, 3) Resource Exhaustion, 4) Nodes Engaging in Malicious Behavior and 5) Attacking neighbor sensing protocols.

1) Nodes acting selfishly: These nodes do not want to participate in the forwarding process, so they will not.

2) Distributed denial of service (DDoS) attack: A denial-of-service attack is a malicious attempt to disrupt the regular traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

3) Resource Exhaustion: where malicious nodes collide with each other repeatedly to drain the battery's power or malicious nodes that engage in malicious behavior. In this case, the primary goal is to interfere with the regular functioning of the routing protocol. When communication takes place between nodes that are close to one other, the effect of this assault is magnified even more.

4) Nodes Engage in Malicious Behavior: The primary goal of a rogue node is to interfere with the regular functioning of the routing protocol. When communication takes place between nodes that are close to one other, the effect of the assault is magnified even more.

5) Attacking neighbor sensing protocols: malicious nodes use bogus error signals to cause crucial connections' interfaces to be tagged as broken, a technique known as "neighbor sensing protocol attack.

16. ATTACKS ON THE NETWORK LAYER:

In this paper, we use the term attack to refer to any act by a node that deviates from the expected behavior of a typical node, which may jeopardize the network's routing functionality. We'll discuss four types of attacks in this section: black hole attacks and wormhole attacks.

A black hole attack can be executed by a malicious node that advertises to other nodes that it has the fastest path to the target node. A forged route, which includes the malicious node, will be constructed if this reply is received before the accurate reply is sent. The malicious node may now discard packets, launch a denial-of-service attack, or engage in a Man in the Middle assault.

A wormhole attack requires the collaboration of two attacking nodes, referred to as a coordinated attack. One attacker captures the packet and then tunnels it to the other attacker. There is a high-speed communication connection between the attackers and the victim.

These two attackers are responsible for bringing the topology under their control.

17. ATTACK ON THE ROUTING TABLE POSITIONING:

Routing attacks are a type of attack that targets routing protocols, which are used to determine the path data packets will follow across a network. These attacks work by sabotaging the routing tables, known as poisoning attacks, or overburdening a node's resources with fake requests for nonexistent destinations. An attacker can redirect traffic away from its intended destination and possibly intercept sensitive data with these attacks.

There are several kinds of routing attacks. For example, during a routing table poisoning attack, the attacker contaminates the routing table by altering the routes included inside the routing table. Alternatively, an RREQ packet with a high sequence number may be injected. The packet with a low sequence number will be removed from the network. This results in the selection of incorrect routes.

Sleep Deprivation: An attacker node can overburden resources by producing requests for nonexistent destinations. This results in battery depletion as well as network bandwidth depletion.

Attack with an impersonator: During an impersonation attack, the attacker node pretends to be sending messages from a trusted node. The attacker provides fake information about its routing status.

Node Isolation Attack: The attacker will block the network from receiving information about a specific node or group of nodes that it is targeting. As a result, other nodes will be utterly unaware of the presence of this node.

Attack on the location disclosure: This is when an attacker node, via probing or traffic analysis, determines the location of a node and the network topology.

Rush Attacking: An attacking node submits route requests to target nodes. Because of this, the genuine node route request is rejected by the target node, and the attacker node is allowed to inject itself into any conversation.

Blackmail: Blackmail is a way to attack the authenticity of the transmitted information.

For example, suppose Node B receives a message from Node A that claims that Node C is a malicious node. If this claim is valid, Node B will add Node C to its blacklist. However, it may be the case that Node A sent this message to Node B to isolate Node C from the network, even though there was no evidence that it was malicious.

This kind of attack is effective if the nodes use routing protocols designed to detect malicious nodes and transmit blacklisting messages.

Furthermore, if the messages could be fabricated by a node and then sent to other nodes on the network, it would cause them to include that particular node in their blacklists, resulting in the separation of legitimate nodes from others in the network.

18. THE INVISIBLE NODE ATTACK:

To better understand the INA, it is essential to understand the WSNs that are vulnerable to this attack. WSNs comprise several sensor nodes distributed in a field, interconnected through wireless links. Each node uses a battery for its operations and may also use energy harvesting techniques. The nodes communicate using a general protocol stack that comprises MAC protocol, routing protocol, transport protocol and application layer protocols. Also, each node has some local processing capabilities and may be equipped with a limited amount of memory [5].

The network is formed by having one node act as a base station (BS) while all other nodes work as sensor nodes. The BS may be connected to the Internet or external network and acts as a gateway for the sensor nodes. The sensor nodes sense information related to their surroundings and forward it to the BS using a routing protocol.

Andel and colleagues from the University of Arizona, USA, investigated various attacks on wireless ad hoc networks and proposed a new attack called the Invisible Node Attack (INA). INA is a non-solvable attack. They have shown that INA is a non-solvable assault by examining the consequences of the attack on various routing protocols to date.

The Byzantine attack:

It is one of the most challenging types of attacks to detect. One reason is that some nodes may be operating alone, or two or more compromised intermediate nodes may be acting in concert. The purpose of these exploits is to create a routing loop and cause packets to be sent on an inefficient pathway. This kind of assault is callous to detect.

Transport-layer attack:

An attack such as session hijacking can also be brutal to spot. In session hijacking, the attacker takes over a session after it has been established. In this case, the attacker spoofs the IP address and starts multiple assaults by selecting the appropriate sequence number from a list of options.

19. ATTACKS ON THE APPLICATION LAYER:

Malicious code is the most common type of application-layer attack. Viruses and worms are just two examples of malicious code that can target both the operating system and user applications.

20. ATTACKS ON THE MULTI-LAYERS:

Denial-of-service (DoS) attacks, impersonation attacks, man-in-the-middle attacks, and many other attacks can target multiple layers of the OSI model.

21. SECURITY SOLUTIONS FOR MANET:

Security is a significant issue in ad-hoc wireless networks. A mobile ad-hoc network (MANET) is a collection of mobile nodes connected by wireless links forming a temporary network without using centralized access points, moving randomly and organizing themselves arbitrarily. MANETs are vulnerable to attacks from malicious nodes. This paper presents MANET security solutions on the Physical, Link, and Network layers that provide secure communication between nodes.

Physical Layer:

At the Physical Layer, spread spectrum techniques such as Frequency Hopping (FHSS) and Direct Sequence (DSSS) can be used to protect against eavesdropping attacks. These techniques randomly change the frequency of transmission, thus making it difficult for the attacker to capture the signal. The use of spread spectrum technologies also minimizes the potential for interference with other radio and electromagnetic devices.

Link Layer:

The link-layer provides security through traffic analysis. WEP was previously used for this purpose but has been widely criticized. An alternative is the dynamic mix method, which uses cryptography to hide source and destination information during message delivery and "mix" nodes in the network. WEP and WPA provide authentication mechanisms for any node wishing to join the network. LLSP is used to provide security at the data link layer by using encryption algorithms, whereas SLSP is used to prevent DOS attacks and a man in the middle attack.

22. THE NETWORK LAYER SOLUTION:

To protect against black hole attacks, the SAODV routing protocol is used; however, it necessitates the use of a complex encryption algorithm. However, it is possible to protect against black hole assaults using the Secure Ad Hoc On-Demand Distance Vector (SAR). SAR uses an authentication mechanism that allows each node to authenticate its neighbor. It is necessary to do excessive encryption and decryption at each hop in SAR.

Authentication Routing for Ad hoc Networks (ARAN) may be used to guard against attacks using impersonation and repudiation. ARAN uses a centralized certificate server that authenticates the nodes they communicate and participates in authentication protocols. It may fail to guard against authorized selfish nodes.

Secure Ad hoc Distance Vector (SEAD), a security protocol, protects against data alteration attacks. SEAD provides digital signatures on every routing update sent out by a node, thus ensuring that no node can alter another's pocket without being detected.

TCP/IP (Transport Layer) Solution:
Several different types of attacks can be launched against transport layer protocols such as SSL. Denial-of-service (DoS) attacks aim to prevent the system from providing services to legitimate users by making the system unavailable. Impersonation attacks attempt to gain access to or disrupt the service by masquerading as a legitimate user. Man-in-the-middle attacks seek to intercept and alter messages between two nodes by impersonating each node.

A variety of countermeasures can help mitigate these attacks, but they must be deployed at several levels and across multiple layers of the network to be effective. Encryption and authentication at the session-level provide end-to-end security and protect confidentiality. Network administrators should also use firewalls, intrusion detection systems, honeypots, and other tools to foil traffic entering unauthorized channels. Finally, organizations should implement policies that encourage employees to adhere to online security practices.

The ability to protect against multi-layer attacks is vital for wireless sensor networks. Attacks can be launched from various layers to create service disruptions. For example, signal jamming attacks are used by an attacker at the physical layer to disrupt communication channels. Malicious nodes can occupy channels at the link layer by taking advantage of the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from gaining access to the channels in question. The routing table overflow attack occurs at the network layer and overflows the routing database with unneeded or fictitious routes, resulting in a denial of service attack. SYN flooding causes overloading of the other node at the transport and application levels, which results in denial of service attacks.

Protection against multi-layer attacks is crucial for ensuring that wireless sensor networks function correctly.

Application Layer:
The application layer is a layer of data processing responsible for managing communication between applications. Firewalls at this layer can prevent a wide range of attacks, including application-specific modules, and efficiently use an intrusion detection system (IDS) as a second line of defense.

Multi-layer Attack:
Some attacks use multiple layers of encryption to hide malicious code or content that can cause damage or harm. These attacks can be used at any layer: data link, network, and transport. Because they use multiple layers of encryption, they're difficult to detect.

Numerous intrusion detection systems (IDS) are currently available in MANET to detect intrusions. Any deviation from expected behavior will be flagged as an intrusion in anomaly detection and thus will be reported to the appropriate authorities. However, if it deviates from usual activity, it may not be detected using anomaly-based detection. There is a possibility of a high rate of false positives.

A possible solution to this problem is manually reviewing these false positives and adding them to the known-good category. A lower false-positive rate can be achieved by adding more known-good activities.

However, this solution has its problems: first, the human effort required to find and classify these activities is extremely high; second, it's hard to determine what other activities are similar enough to those already classified as good that they should also be added to the excellent list; third, if we add too many activities to the "good" list, then we increase our risk of a false negative—which means that an actual attack could go undetected.

23. CONCLUSION:

In this paper, we have examined the threats to mobile ad hoc networks and the distinct levels at which they occur. Because of their vulnerability to a range of attacks, securing mobile ad hoc networks is essential for academics. A variety of approaches for securing mobile ad hoc networks have been proposed by academics to prevent different varieties of attacks from occurring. These approaches have been discussed in detail in this paper. We have discussed several security issues that affect mobile ad hoc networks. For each group of threats, we have examined the methods for preventing them from occurring. We have discussed the significance of security issues at different network layers and presented the potential solutions to these problems.