JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452

Analysis on Essential Challenges and Attacks on MANET Security Appraisal

1. **Dr.N.Sivapriya,** Assistant Professor, Department of Computer Applications, Cauvery College for Women, Trichy, nmsivapriya@gmail.com
2. **Dr.R.Mohandas,** Associate Professor, Balaji Institute of Technology & Science, Warangal, Telangana, mohandasbe@gmail.com

Received 2022 April 02**; Revised** 2022 May 20**; Accepted** 2022 June 18

Abstract: One of the most important next-generation wireless network technologies is Mobile Ad Hoc Networks (MANETs). All of the mobile nodes in the MANET are self-configurable routers that allow data to transit around the network using multi-hop network routes. An important networking class, MANETs differ from traditional systems in a fundamental way. Although MANETs are being popularly employed in commercial as well as academic fields, these were primarily designed for deployment in areas like military battlefields, emergency rescue and search operations, and other challenging or hostile environments. Intruders can take advantage of the MANET's scattered and wireless design to decrease its capabilities. Because most MANET routing protocols are built under the assumption that there isn't a hostile intruder in the network, they are vulnerable to a variety of attacks at various tiers. As a result, it is critical to identify these dangers and devise strategies for countering them. Various security attributes, problems, attacks, and solutions for resisting attacks on numerous tiers are examined in this study.
Keywords: Intrusion detection system, MANET security, secure MANET routing, MANET security attacks.

I. INTRODUCTION

Mobile Adhoc Networks (MANETs) are a hot topic in the field of mobile communication technology. Groups of mobile nodes that lack a network infrastructure make up a MANET [1]. Radio waves are used to communicate between MANET nodes. Nodes in MANETs serve as both hosts and routers, making them unique in the networking world. (c) absence of infrastructure and decentralised control. Dynamic network topology changes followed by frequent upgrades to the routing protocol, easiness of implementation, fascinity of network expansion As a result, (g) the ability to administer oneself, configure oneself and create oneself Cooperative and dispersed working environments (ii) A limit on the size of the device It is straightforward to deploy, and bandwidth usage is restricted. (l) Device heterogeneity (n), autonomous reconfiguration (m), and multi-hop radio transmission (o) all require the least amount of human involvement in network configuration. [2] and [3].

Mobile Ad-hoc Networks (MANETs) are widely used in a variety of applications such as military operations and sensor networks as well as humanitarian relief and rescue efforts. [4]-[6]. Contrary to popular belief, there has been significant progress in the field of mobile ad hoc networks in recent years. This is due

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452
mostly to new hardware developments (smart vehicles, intelligent drone, unmanned aerial vehicle, etc.) and software innovation (embedded platforms) [7]. Sensor networks, a key component of MANETs, are also seeing more application/service-oriented research challenges integrated with the industrial and business-related services of the Internet of Things (IoT), such as smart house, smart vehicles, smart grid, etc. It is undeniable that this is a new trend that is characterised by a number of unique obstacles.

MANET research in the area of delay-tolerant networking, often known as DTN, has been particularly active in recent years. Insufficient transmission range, node moves, or environmental impediments might cause a DTN to briefly collapse into sub-networks. There are several different types of DTNs that can be found in the real world. MANETs are primarily concerned with making mobile resources available to its users. Mobile nodes in MANETs keep moving around and presuming that they won't be able to get to another location. Because of this structure, MANET nodes must have highly stable routing, as moving nodes increase the likelihood of an intermittent link. Additionally, mobile nodes must keep their routing tables up-to-date and be in a listening mode with the rest of the network at all times. As a result, huge amounts of energy are depleted, resulting in a decrease in node performance, which in turn affects the network's performance over time. There are a number of concerns with MANET, including bandwidth usage, inter-arrival time and energy drain, routing and latency as well as intermittent or unstable links. [1] and [8], respectively. Routing protocols have recently been the subject of extensive research with the purpose of improving and redesigning them.

More than ninety percent of the research on MANET routing protocols has focused on protocols such as DSDV (Destination Sequence Distance Vector), OLSR (Optimized Link State Routing), AODV (Adhoc On-DemanD Distance vector), and DSR (Dynamic Source Routing). For this reason, researchers are constantly looking for new ways to improve existing techniques or develop new ones. Another problem with MANETs, aside from their slow performance, is their lack of security [10]. In certain publications, such as, a variety of security dangers and mitigation methods have been described. In addition to Sybil attacks, black hole attacks, flooding or Denial of Service assaults, sinkhole attacks and rushing attacks that have been analysed so far are some of the other dangers and attacks that have been studied. In order to ensure safe MANET communication, it is necessary to have a thorough awareness of the numerous attacks that might be launched against the MANET. It is the goal of this study to provide a complete and systematic review of the most well-known MANET attacks, threats, and security methods. There are several sections to the report, including Section II focusing on MANET security flaws. In Section III, we looked at various MANET security attributes, and in Section IV, we considered trust as a critical MANET security component. Numerous MANET attacks and their ramifications are discussed in Section V, which goes into detail about the various attacks that can be found in MANETs. Section VII provides more in-depth information on MANET security measures, including both preventive and reactive measures. It ends with an explanation of the future research

direction in MANETs and final notes in Section VIII and IX.

II. SECURITY CHALLENGES IN MANET

It is the most intriguing network kind. Since air and hazardous environments are used as a medium, MANETs are vulnerable to a wide range of active and passive attacks. Opponents equipped with high-tech weapons engage in active attacks. It is possible for them to alter the data transmitted via the network and corrupt system operation by altering link-related updates, topology, and routing.. Blackhole attack, impersonation, denial-of-service, Byzantine attack, distributed denial-of-service, and wormhole assault are all examples of active attacks. Passive attacks, on the other hand, are made by opponents who lack the necessary skills. Examples of passive assaults include eavesdropping, traffic analysis, etc. In this part, some unresolved questions and fundamental limits of MANET security have been addressed.

A. Distributed Management

Because of the ad hoc nature of their setup and the peer-to-peer nature of their nodes, centralised management is impossible with MANETs. In the absence of centralised control and the distributed nature of the network, node generation, topology changes, authenticating new nodes and secure data dissemination as well as keying information are all affected. Due to this, the identification of an assault on a large-scale, very dynamic, adhoc network is made much more difficult.

B. Limited Resource

Temporary and ad hoc deployment in difficult environments with limited resources results in bandwidth, power, and computing limits in ad hoc networks. Ad hoc networks' solution space has been drastically reduced as a result of the limited resources, making them a playground for both developers and attackers.

C. Cooperativeness

Due to the lack of a centralised administrator and the peer-to-peer architecture, MANETs have evolved from client-server networks to cooperative networks. This collaborative character aims to build confidence among network nodes during routing or data exchange. Changing this cooperative character involves forced collaboration among MANET nodes and specific MANET security solutions.

D. Dynamic Topology

As the MANET system is dynamic, adaptive security solutions are needed to deal with energy depletion, mobility, physical obstacles, and node revocations caused by actions against selfish and malicious nodes and compromised nodes.

III. SECURITY REQUIREMENTS IN MANET

A network can be called secure if the following qualities are met. Security models should be implemented in systems that handle the sharing of sensitive information. Security demands of adhoc networks can be described by taking into account their complementing properties.

Because nodes in MANETs can only be linked for a short period of time, it is necessary to maintain real-time constraints in order to meet the goal of limiting access to scarce resources. The following are a network's most important requirements:

It's important to note that with MANET, each node or application is only authorised to access a limited set of services from the apps currently in use. For the sake of data

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452

security and to prevent an adversary from snooping, confidentiality is essential.

Integrity – Network nodes that have been permitted to do so have the ability to modify, delete, or create packets. Assailants can't alter messages or data while they're travelling through the system because of this characteristic. If not, users may be harmed by the tampered with vital information.

Authentication – Communication between two nodes must be secure. Only messages sent by legitimate members of the network should be acknowledged by nodes. Therefore, the message sender must be authenticated, and another node must be authorized to update or receive information.

Non-Repudiation – This feature ensures that neither the sender nor the receiver can dispute that any data has been exchanged. As a result, the bad nodes are more easily isolated. A node's identification must not be denied at any moment throughout an examination into its transmission.

Availability – The network makes it such that authorized nodes can continue to supply services and data even in the face of attacks. Alternative methods of accessing the system should not be hindered by an attack on it.

The certainty of discovery – It ensures that the source node acquires the destination node address before sending the packets to the destined node by applying a route discovery procedure.

Lightweight computations – Route finding computations may be carried out with simplicity.

IV. TRUST IN MANET

To put it simply, trust is a subjective opinion that one party or person uses to assess the likelihood that another party or person will take a favourable action when the opportunity presents itself and to monitor if that action has occurred [22]. Activities that are predicted to be carried out with high probability will be carried out in an advantageous manner. The ability to collaborate on programme metrics is critical when establishing confidence among the participating nodes. For the designers, this concept is essential to the development of communication and network capabilities. The need for trust in forming relationships when there is uncertainty underscores the significance of the topic of MANET security. As with MANETs, unpredictable behaviour is a major source of concern. Associative trust is defined as the behaviour of a group of associations among items contributing to a process, with the associations based on the proof provided by the prior communications of the entities involved. They could build trust with one other if their interactions are consistent with the procedure. Furthermore, the degree of confidence in new things' behaviour might be viewed as a measure of trust (representatives). This level of belief in the behaviour of nodes, agents, and other entities in MANETs can be defined as trust. There are two possible values for trust's probability: 0 indicates distrust and 1 indicates trust [23].

A. Features of Trust in MANETs

The wireless medium, properties, and theory of MANETs need a cautious definition of trust. MANET trust has the following features:

- It is imperative that the trustworthiness of a third party (e.g., a trusted central certification authority) be verified in order for a decision procedure to be used to verify the trustworthiness of an entity.
- Belief associations must be understood

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452

while trust is established in an efficient manner that does not place an undue burden on communication or computation.

- MANET decision support cannot take the nodes' cooperative behaviour for granted. When there is a lot of selfishness and little resources, it's possible to rise above teamwork.
- It is impossible to maintain a level of trust indefinitely. It's ever-changing.
- Belief is a personal matter.
- Trust is not a one-to-many thing. Despite the fact that A has faith in B and B has faith in C, this does not mean that A has faith in C.
- There are two types of trust: asymmetrical and reciprocal.
- Confidence is a product of context. When it comes to one thing, A may have faith in B, but not when it comes to another.

Almost all of the nodes involved in routing in MANETs demand considerable processing power. This means that although genuine (and not malicious) nodes with high battery power can be trusted, nodes with low battery power cannot.

B. Centralized Versus Decentralized Trust

The term "centralised trust" refers to a situation in which a single trustworthy node calculates trust values for all other nodes in the system. In order for the method's user nodes to benefit from the advise of this trustworthy node, they all ask for it (s). As a result of this situation, there are two main consequences. Because there are several user nodes, it's logical to assume that they'll have differing views on the same target node.

Another problem is that there is a single point of failure due to the fact that all other user nodes are dependent on this one. Decentralized trust schemes hide this truth because each node communicates with all other nodes, making it the centre of its world. That is to say, each user node is responsible for determining their own trust values for whatever target node they choose. Through this, fake routing packets are sent out. There is a black hole (or dark gap) where information continues to enter without exiting when the data packets reach the spot (as depicted in Fig. 1)

A. Based on Nature/Behaviour

a) Active attack – Attempts to change or update data without permission are known as active attacks. Such attacks also include inserting bogus packets into the actual data stream in order to acquire access. Attacks of this nature might be carried out from the outside or from within.

b) Passive attack – After observing network traffic, passive attacks attempt to gather sensitive information without disrupting the routing system.

B. Based on Processing Capacity

a) Wired – Unauthorized access is gained through the use of a wired medium by the intruders.

b) Mobile – Unauthorized access is gained through the use of a wireless media by the intruders.

C. Based on the Number of Attackers

a) Single – The normal flow of the network is disrupted only by a single individual or rogue node.

b) Multiple – In order to wreak havoc on a typical network, more than one individual or malicious node must join forces.

D. Attacks Corresponding to Different MANET Layers

Table I outlines several MANET attacks based on different layers of the network.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452

Table- I: Attacks on various MANET layers

Layer	Attack
Physical	Jamming, interceptions, eavesdropping, active interference, malicious message injecting
Data Link	Traffic analysis, monitoring, SYN flooding, TCP ACK storm
Network	Spoofing, wormhole, grey hole, Byzantine, blackhole, resource consumption, flooding, location disclosure attacks, Sybil, routing attacks, sinkhole
Application	Repudiation, malicious code, data corruption
Transport	Session hijacking, TCP ACK storm, SYN flooding, jellyfish
Multi-Layer	DoS, replay, man-in-the-middle, impersonation

The following is a list of the most recent attacks:

1) Black-Hole Attack

To get to a specific location, the attacker creates a route.

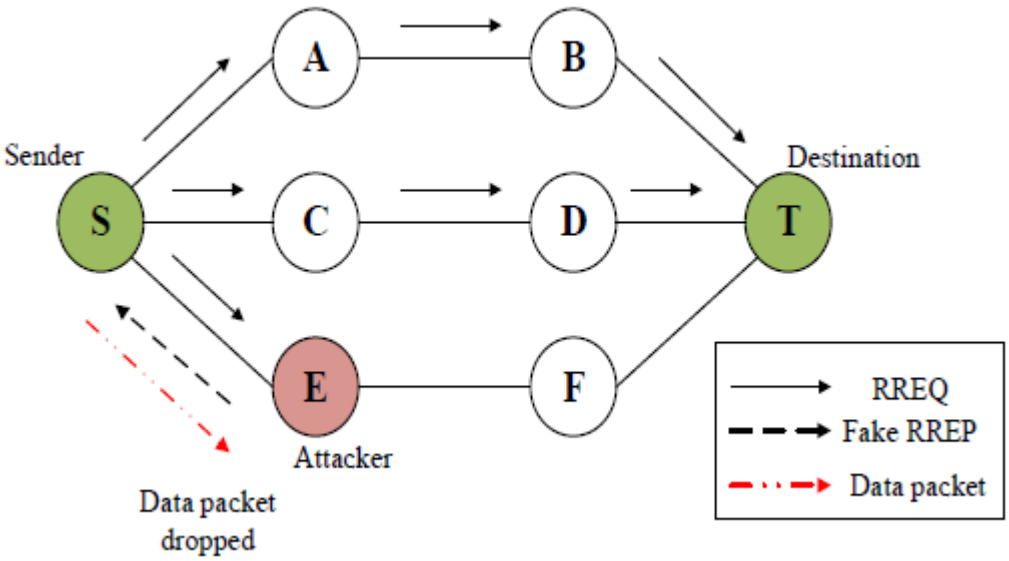

Fig. 1. Demonstration of blackhole attack.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452

2) Cooperative Black-Hole Attack

This is a complex assault that is carried out by a group of nodes working together. Nodes that are invisible to the source node engage in the attack and convince the source node that there is a reliable route.

3) Grey-Hole Attack

When a rogue node deliberately drops a packet, it is either completely or for a predetermined amount of time (Fig. 2). The rogue node's status is reversed, allowing it to function normally once more. Once a route has been discovered, the rogue node that received the message is removed.

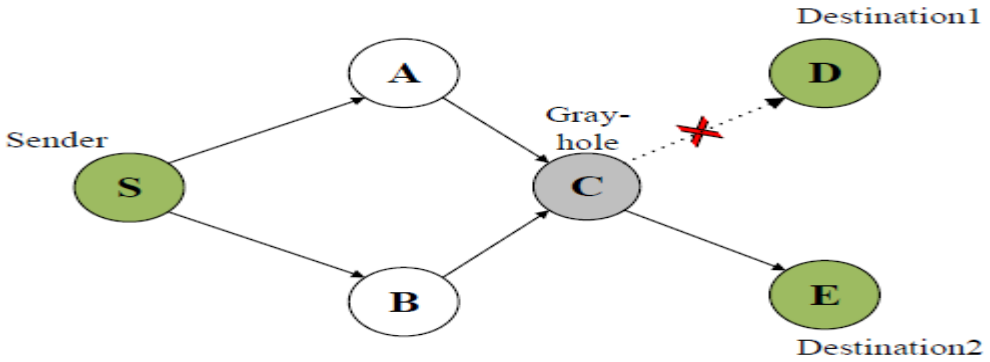

Fig. 2. Demonstration of grey-hole attack.

4) Jellyfish Attack

During a Jellyfish assault, an intruder gains access to the system, infiltrates the group, and merges with the system in order to send out data packets. Once it's integrated into the system, the packets are delayed and the End-to-End performance factor is raised to a very high number before being passed on. High delays have a negative influence on network communication as a whole.

5) Worm Hole Attack

A wormhole is a shortcut in cosmology that connects two distant points in space.

If one or more attacker nodes short-circuit the network (as depicted in Figure 3), it can disrupt the usual flow of packets

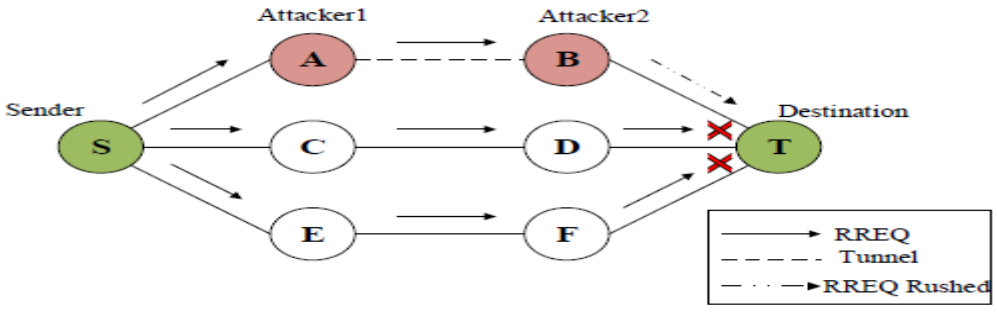

Fig. 3. Demonstration of wormhole attack.

HELLO Flood Attack

The networks are flooded with high-quality routes and powerful transmitters from attackers. To get to the destination,

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452

each node tries to pass on its own packets to that node, believing that it is the most direct route. It is possible that some nodes may send their packets to other nodes that are beyond of the reach of the attackers.

6) Bogus Registration Attack

Fake beacons are used to trick nodes into thinking they are communicating with a different node by sending out a signal that looks like it came from another node.

7) Man-in-the-Middle Attack

Sniffing packets as they pass over an authenticated path is the goal of this attack.

8) Rushing Attack

The attacker multiplies the sequence numbers of route request packets in this attack (Fig. 4). Sequence numbers for suppressing replica packets are maintained in the reactive protocols.

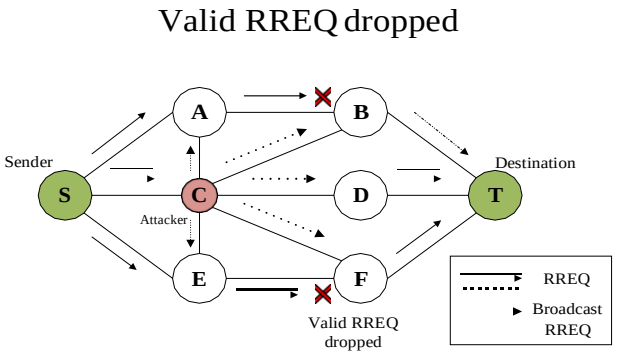

Fig. 4. Demonstration of the rushing attack.

9) Sybil Attack

As a result of pretending to be made up of several system nodes, the attacker creates multiple false identities. As a result, a single node can take on the role of multiple nodes (as shown in Fig. 5) and study or obstruct multiple nodes at the same time.

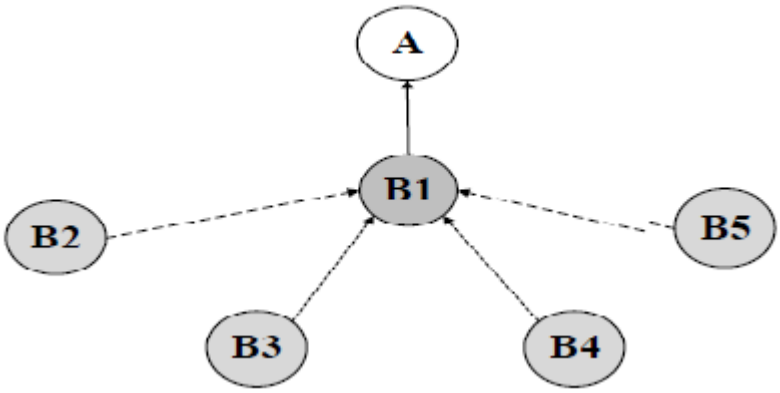

Fig. 5. Demonstration of Sybil attack

10) Byzantine Attack

As part of a Byzantine assault, a group of intermediate nodes collude to carry out operations that generate routing loops, pass on non-optimal routes, and disrupt network routing services.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452

11) Sinkhole

It is possible for attackers to eavesdrop on all data exchanged between neighbouring nodes in this attack. Using calculation to reduce hop counts and maximise the sequence network, a malicious node may appear to be the best way available for communication between nodes in a MANET like AODV protocol.

12) SYN Flooding

A Denial of Service attack is what this is. It is common for an opponent to submit connection requests until the amount of resources required for each connection is spent. SYN flooding reduces the amount of resources available to the nodes that are actually usable.

13) Eavesdropping

It's called eavesdropping if an attacker intercepts a message and reads it without altering its content. [29]. MANETs use a wireless channel where messages are broadcast and can be easily intercepted if the precise frequency of the message is tuned.

14) Routing Attack

Malicious nodes may attempt to alter or remove the routing tables of other network nodes in this type of attack [30, 31]. Processing time and packet overhead rise because the routing table's data is lost.

V. EFFECTS OF SECURITY ATTACKS IN MANET

When discussing various MANET security assaults, it is necessary to take into account the problems generated by the various attacks. Attacks on different tiers cause a variety of issues.

A. Time Delay

The receiver rejects a request because of a network latency caused by an attack.

B. Data Loss

Traffic is attracted to malicious nodes by displaying misleading routing information, and control packets and some/all data passing through the nodes are dropped. There is a high probability of data corruption or loss in these types of scenarios.

C. Full/Partial Network Paralysis

There is a risk of paralysing the network if the connection is disrupted or node routing tables are destroyed with wrong information in the event of a modification attack, fabrication attack, or similar.

D. Compromise QoS

Wormhole and tunnelling attacks weaken network security. The packets are rerouted to the network after being sent through a tunnel to nodes located a long way away [38]. As a result, the other node will have access to all of the network data that could have an impact on QoS.

E. Misuse of Services

When a node acts selfishly, it tends to take advantage of the mobile adhoc network's services, such as using bandwidth and flooding the network with traffic.

VI. SECURITY APPROACHES IN MANETS

Preventive and Reactive Mechanisms are the two types of security measures that have been developed for MANETs.

Preventive Mechanisms

The first line of defence in such processes is the use of encryption, digital signatures, authentication, access control, etc. to authenticate the data source and verify the integrity of the data. In order to ensure the integrity of a message while it is being transmitted, the message digest is

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2578-2589
https://publishoa.com
ISSN: 1309-3452

adequate. It is possible to hide data with threshold cryptography by dividing it up into many shares. Authentication and data integrity can be achieved through digital signatures. As long as an attacker has access to a decryption and encryption key, these measures fail to keep the network safe from internal attacks. The attackers may even try to launch new attacks that the safe system is unaware of.

Key Management Schemes and Routing Protocols are two forms of preventive methods that can be further characterised.

1)Secure Key Management Approaches: Prevention fromExternal Attacks

The use of key management, authentication, and encryption to prevent external assaults is widespread. Ad hoc networks, on the other hand, present a unique set of challenges for traditional key management techniques. Key revocation and key distribution are the two fundamental parts of a key management strategy. Nodes in the network can communicate with one other regarding the availability of key management services through the use of a Trusted Third Party (TTP). Offline, online, or in-line TTPs are all possible. In MANETs, a centralised certificate authority cannot be implemented because of the dynamic nature of the environment. For this reason, researchers have undertaken a number of attempts to divide CA jobs across nodes within the distributed and dynamic MANET environment It is possible to run the DCA in a distributed manner when mobile nodes work together.

Asymmetric Key Management, Symmetric Key Management, and Group Key Management are the three types of key management used in mobile ad hoc networks.

i) Asymmetric Key Management

Network communication is secured by using two keys (private and public). Private and public keys are transmitted to all network nodes by every receiving node.

ii)Symmetric Key Management

To communicate in both directions, a single key is used and such techniques are based on the already distributed key [2]. Secure network communication requires n(n 1)/2 key pairs for a network with n nodes.

iii) Group Key Management

In mobile ad hoc networks, group key management systems include SEGK (Simple and Efficient Group Key Management) and Hybrid or Composite Key Management Schemes. The advantages of one strategy can be balanced against the drawbacks of the other by combining these two approaches in a complementary manner.

Researchers have determined that most key management methodologies do not meet resource limits and other limitations of MANETs, notwithstanding their findings.

2)Secure Routing Protocols for Attack Prevention

Secure key management methods help authenticate mobile nodes and stop outsiders masquerading as interior nodes in an ad hoc network by using secure key management schemes. However, these methods fall short in the face of attacks on the adhoc routing process. These attacks necessitate the development of numerous safe routing protocols to enhance or replace the current ones. In this section, we've covered a few MANET-specific secure routing protocols:

By using the same key for both decryption and encryption, SAR incorporates the

trustworthiness of nodes into standard routing metrics.

3) Trust Management Based Schemes

Mobile ad hoc networks place a high value on trust when it comes to node coordination and security. In order to make conventional security solutions more reliable and resilient, Trust Management (TM) ensures that every communication node is trustworthy while the essential functions of MANETs are being carried out. The following is a list of trust-based routing protocols for MANETs:

When it comes to detecting selfish nodes in a MANET, CORE (COllaborative REputation) is identical to CONFIDANT (where reputation system and monitoring are considered). Only good reports are allowed through CORE, however negative reports are permitted through CONFIDANT.

CONCLUSION

In wireless networking, the MANET paradigm has rapidly grown as the basis for many future application scenarios.. Many underlying dangers and security vulnerabilities are emerging as a result of the ever-increasing proliferation of software applications. MANETs are vulnerable to a wide range of attacks that are not possible in other networking systems because of their unique properties. According to current research on MANET security, this study provided a well-organized and thorough overview of the numerous topics that have been discussed. As a result of this effort, we've identified the elements that contribute to threat scenarios, summarised network security needs, and categorised assaults based on the communication protocol stack. Additional research options for establishing promising future security systems for MANETs and other linked application paradigms are outlined in the article.

REFERENCES

1. S.B. Geetha, and V.C. Patel, “Evaluating the Research Trends and Techniques for Addressing Wormhole Attack in MANET”, International Journal of Computer Applications, vol. 110, no. 6, pp. 1-11, 2015.
2. S. Kumar, and K. Dutta, “Securing Mobile Ad Hoc Networks: Challenges and Solutions”, International Journal of Handheld Computing Research, vol. 7, no. 1, pp. 26-76, 2016.
3. B. U. I. Khan, R. F. Olanrewaju, F. Anwar and A. Shah, “Manifestation and Mitigation of Node Misbehavior in Adhoc Networks”, Wulfenia Journal, vol. 21, no. 3, pp. 462-470, 2014.
4. S. Sarika, A. Pravin, A. Vijayakumar, and K. Selvamani, “Security Issues In Mobile Ad Hoc Networks”, in 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), 2016, pp. 329-335.
5. B. U. I. Khan, R. F. Olanrewaju, R. N. Mir, S. H. Yusoff and M. L. Sanni, “Trust and Resource Oriented Communication Scheme in Mobile Ad Hoc Networks”, in Proceedings of SAI Intelligent Systems Conference, Springer, Cham, 2016, pp. 414-430.
6. R.F. Olanrewaju, B.U.I. Khan, F. Anwar, A.R. Khan, F.A. Shaikh, and

M.S. Mir, “MANET – A Cogitation of its Design and Security Issues”, Middle-East Journal of Scientific Research, vol. 24, no. 10, pp. 3094-3107, 2016.

7. L. Fratta, M. Gerla, and K.W. Lim, “Emerging Trends and Applications in Ad

Hoc Networks", Annals of Telecommunications, vol. 73, pp. 547–548, 2018.

8. B. U. I. Khan, R. F. Olanrewaju, R. N. Mir, A. Baba and B. W. Adebayo, "Strategic Profiling for Behaviour Visualization of Malicious Node in MANETs Using Game Theory", Journal of Theoretical & Applied Information Technology, vol. 77, no. 1, pp. 25-43, 2015.
9. Priyanshu and A.K. Maurya, "Survey: Comparison Estimation of Various Routing Protocols in Mobile Ad-Hoc Network", International Journal of Distributed and Parallel Systems, vol. 5, no. 1/2/3, pp. 87-96, 2014.
10. B. U. I. Khan, R. F. Olanrewaju, A. M. Baba, R. N. Mir, and S. A. Lone, "DTASR: Dual Threshold-Based Authentication for Secure Routing in Mobile Adhoc Network," World Engineering and Applied Sciences Journal, vol. 7, no. 2, pp. 68-73, 2016.
11. K. Udhayakumar, T.P. Venkatesan, and R. Ramkumar, "Security Attacks and Detection Techniques for MANET", Discovery, vol. 15. no. 42, pp. 89-93, 2014.
12. H.N. Saha, D. Bhattacharyya, B. Banerjee, S. Mukherjee, R. Singh, and D. Ghosh, "A Review on Attacks and Secure Routing Protocols in MANET", International Journal of Innovative Research and Review, vol. 1, pp. 12-36, 2013.
13. B. U. I. Khan, R. F. Olanrewaju, and M. H. Habaebi, "Malicious Behaviour of Node and its Significant Security Techniques in MANET-A REView", Australian Journal of Basic and Applied Sciences, vol. 7, no. 12, pp. 286-293, 2013.
14. R. F. Olanrewaju, B. U. I. Khan, R. N. Mir, and A. Shah, "Behaviour Visualization for Malicious-Attacker Node Collusion in MANET based on Probabilistic Approach," American Journal of Computer Science and Engineering, vol. 2, no. 3, pp. 10-19, 2015.
15. B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. Najeeb, and M. Yaacob, "A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions", Indonesian Journal of Electrical Engineering and Computer Science, vol. 12, no. 2, pp. 832-842, 2018.