TEST Engineering & Management

January – February 2020
ISSN: 0193-4120 Page No. 13832 – 13837

Review of Security Attacks in Mobile Ad-Hoc Network

Vikas Tulshyan[1], Dr.Kinjal Adhvaryu[2]

[1,2]CU Shah University , ShankersinhVaghelaBapu Institute of Technology
[1]vikasntulshyan@gmail.com,[2]kinjalvk@yahoo.com

Article Info
Volume 82
Page Number: 13832 – 13837
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 24 February 2020*

Abstract

A MANET is an infrastructure-less network consisting of a variety of wireless network interface mobile nodes. The nodes dynamically create paths between each other in order to make contact between the nodes. Such networks ' nature and structure make it attractive to different types of attackers. Safety is a major concern for the mobile nodes ' safe contact. Therefore, the MANET doesn't have an away from of barrier, it is accessible to both authentic system clients and pernicious assailants. Within the sight of pernicious hubs, one of the fundamental difficulties in the MANET is the formation of a strong wellbeing arrangement that can verify the MANET from various routes. We try to introduce all the attacks based on nature, location and protocol stack in detail.

Keywords; *MANET, Security*

INTRODUCTION

The Mobile Ad-hoc Network is an infrastructure-free and autonomous network of wireless communication. This makes it possible to transfer information between networks using independent mobile nodes without any centralized authority. [10][18].

In the MANET, all nodes in the contact range are connected to the nodes. Consequently, if a hub wishes to speak with the other hub, it sends the information through the neighboring hub to the goal hub. The neighboring hub will currently go about as a switch. Security conventions will be presented in a switch hub in a wired system. Implementing protection in a MANET, however, is a challenging task, as here node must operate as a router node itself.In MANET, distinguishing the neighboring hub as an authentic hub or pernicious hub is a hard thing. [6] [7].

There are some reality MANET systems such as Military Battlefield, Business Market, Local Network, Personal Area Network, Wireless Mesh Network, and Wireless Hybrid Network.

We have looked at the types of attacks that exist in this paper. The first section describes security encounters and goals needed to secure a MANET routing. The second section explains the various attacks on a MANET in detail. There will be several DOS attacks in the third section. Details on future directions for a secure MANET are given in the last section.

II. SECURITY ENCOUNTERS AND GOALS

A security issue in MANETs has become a primary concern for secure communication. Not a single system will provide all of the MANET's security services. Therefore, below are the major security targets that need to prevent attacks.

1. Availability

Availability expresses that nodes need to be provided regularly to the facilities and services. Data and properties are subject to availability. The availability ensures that even in the presence of the

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13832 – 13837

attacks the services should be available. Frameworks ought to have the option to deal with different assaults, for example, administration refusal, assaults on vitality exhaustion, and hub misuse.

2. Confidentiality

Confidentiality expresses that in advertising node thumping facts. Only certain information that the legitimate node can read and access. Confidentiality guarantees that only the intended party should have access to the data. No other node can read the information except for the sender and receiver node. This is implemented through the techniques of data encryption.

3. Reliabilty

Reliability refers to the transmission of messages to the intended party without any change or modification. This ensures that changes are made only by licensed users and in the appropriate manner as well. Transition includes writing, and manufacturing. [4] [13].

4. Authentication

It expresses that it comes from a genuine user to endorse information. It ensures that only the authorized nodes are used to communicate or transmit data[5]. Each malignant hub can profess to be a confided in hub in the system without verification and can antagonistically influence the exchange of information between the hubs.

5. Non Repudiation

Non-denial implies that a transmitted message should not be rejected by either a sender or a recipient. This is beneficial when we have to perceive whether or not a node with some unwanted power is trading off [4][11][13].

6. Authorization

Hubs engaged with a system need to have effective authentication on that network to share resources.There are different access privileges for various types of users. For example, network administration should be possible by arrange executive.

III. TAXONOMY OF SECURITY ATTACKS

A. On the Basis of Location

1. External Attacks

Outer Attacks are the assaults by unapproved hubs that don't shape some portion of the system. Outer assailants in the system may flood counterfeit parcels, pantomime, and so on. Their target might be to cause blockage or upset the ordinary working of the system.

2.Internal Attacks

The approved hubs in the system cause interior assaults. The clarification for their pernicious conduct may be:

a) Hijacking those (approved) hubs by some outer assailants and afterward utilizing them to dispatch inside system assaults.

b) Egoism in overseeing restricted assets, for example, battery power, handling abilities and correspondence transfer speed, and utilizing different hubs furthering their potential benefit.

External attacks are more serious because the attacker distinguishes useful and secret information and has exclusive access rights [20].

B. On the Basis of Protocol Attacks

(a) Physical Layer

1) Eavesdropping: Attacker attempts to obtain secret information during communication during this attack.

2) Jamming: knowing the recurrence of malevolent hubs sends a jam sign to upset the correspondence will be executed.

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13832 – 13837

3) Dynamic impedance: this is a sort of administration forswearing assault that twists correspondence.

(b) Data Link Layer

1) Selfish node misconduct: these are childish hubs that deliberately drop parcels to keep up battery control or stay away from undesirable transfer speed shares.

2) Node pernicious conduct: it meddles with the activity of the steering convention and its impact might be huge if there is more communication between neighboring nodes[1].

3) Traffic analysis: they analyze the traffic flow in this type of attack to obtain important information on the topology of the network, which thus uncovers data about the hubs.

(c) Transport Layer

1)Session commandeering: the unfortunate casualty's IP address is utilized in this sort of assault to locate the right number of arrangements and triggers DoS assault. The point is to gather safe hub information.

2) SYN Flooding Attack: This aggressor has various half opened TCP associations so the handshake isn't completely associated.. [4].

(d) Network Layer

Throughout network layer, the basic idea is to infuse or consume network traffic in the dynamic way from source to goal.

(e) Application Layer

1) Misleading code assault: it contains infection, worm and steed trojan.

2) Repudiation ambush: This sort of assault is activated by declining to take an interest in correspondence. In this assault, the assailant acts as a prideful hub and rejects the contact information or movement.

(f) Multilayer

Multi-layer assaults are instances of forswearing of administration assaults, pantomime assault, and man-in - the-center assault. Pantomime assaults are started utilizing the uniqueness of different hubs, for example, MAC or IP address.

C. On the Basis of Nature

1. Active Attacks

Carried out by attackers to replicate, modify and delete data exchanged. They are trying to change the protocol behavior[3]. Such assaults are proposed to upset or square the progression of messages between the hubs. These assaults can be named all things considered as DOS assaults that either debilitate or square contact between hubs totally. Another kind of assault includes embeddings outsider parcels into the system so as to cause clog. It is conceivable to replay obsolete steering data back to the system hubs. Dynamic assaults can now and then be identified, which is why an attacker uses active attack less. The characteristics of active attacks are:-

(A) Disruption of routing A malignant code either devastates a current course or forestalls the production of another course.

(B)Routing Incursion A malicious node is attached to the way between the source hubs and the objective hubs.

(C) Node segregation Differs from route disorder, which route disorder is directed to a route with two nodes, whereas node isolation is directed to or from any probable route to that node.

(D) Consumption of resources The network or storage space communication bandwidth of the individual node is expanded [2].

2. Passive Attacks

This sort of assault includes unapproved directing bundle tuning in. Aggressor can listen stealthily on all updates to the directing. For this situation, an

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13832 – 13837

Attacker doesn't meddle with the activity of a directing convention, yet tunes in to it just to find important steering data. It is hard to distinguish such assaults. From the steering bundles, an assailant will comprehend a hub that is significant in the system and all the time each other hub requests course to that hub. An aggressor along these lines attempts to debilitate this hub so as to cut down the system. This requires systems served and investigation of traffic.

IV. DENIAL OF SERVICE(DOS) ATTACKS

1. Black Hole Attack

The aggressor utilizes vulnerabilities in AODV's directing disclosure technique, DSR steering protocols[4], in dark opening assault. On the off chance that a source hub is required to send information to the goal hub, it will communicate RREQ solicitation to all so the hub with the most elevated goal grouping number than the present goal succession number will react and the goal arrangement number is higher than the present goal succession number. At that point they send it to the hub of the source. The source hub will pick the way through this noxious hub on the off chance that it gets this bogus RREP parcel, expecting it is the new and most limited way to goal. The source hub at that point dismisses the RREP parcel from different hubs and starts to send the bundle by means of malevolent hub. At that point, rather than sending it, this malevolent hub can drop the bundle. This assault is alluded to as an assault on the dark gap.

2. Gray Hole Attack

Dark gap assault is an exceptional dark opening assault variety. The aggressor positions itself in dark opening assault between the source. The aggressor attracts the information bundles to it by promoting itself with the most limited course to goal and afterward getting and dropping the information parcel. The information parcels are dropped in a dark gap assault specifically or measurably. For example, packets can be dropped from a specific node or in some other pattern [4].

3.Wormhole Attack

Two malevolent hubs in the wormhole assault make a passage between them. This passage is known as a wormhole between them. This draws the information parcels here by publicizing itself giving the most limited way to goal. At the point when a wormhole assault happens in a system, it forestalls courses other than the course through the wormhole from being found. Every one of the information will in this way just go through the wormhole.

It would then be able to drop the bundles just as tune in to classified data or change the information parcels that have been moved.

4. Rushing Attacks

One of the properties of an on-request directing convention is that hubs can just advance the first RREQ that Arrives for steering disclosure and disposes of all other RREQ that shows up after the expected time. Hurrying assault misuses this property. The attacker will forward the request for RREQ earlier, thereby suppressing the legitimate RREQ. They will use a wormhole to rush packets in the most efficient Rushing attack.

5. Byzantine Attacks

A compromised intermediate node operates alone or collusion works with a group of compromised intermediate node and they execute assaults. These assaults make circles for routing, forward parcels through ways that are not ideal. This attack is difficult to detect. [19]

6. Jellyfish Attack

Closed-loop flows are targeted at jellyfish attacks. While attacking jellyfish, the interloper hub or vindictive hub totally complies with the principles of the convention. It's a uninvolved assault, so it's hard to detect. Jellyfish node's goal is to decrease the positive put that can be accomplished by dropping some of the packets. Jellyfish assault is additionally ordered into three sub-classes: Jellyfish recorder

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13832 – 13837

assault, Jellyfish falling occasionally and Jellyfish postpone change assault [1].

(a) Jellyfish Reorder Attack

In view of the TCP powerlessness, Jelly Fish Reorder assault is conceivable. This weakness is utilized by Jelly fish aggressor to catch bundles. [2]

(b) Jellyfish Periodic Dropping Attack

Occasional decrease is conceivable because of the evil hub's snidely picked period. This type of occasional drop at transfer hubs is conceivable. Assume misfortunes of clog cause a hub to drop a level of parcels. At that point accept that the hub loses a level of bundles routinely then the throughput of TCPs can be measured to very nearly zero in any event, for little estimations of a. [5].

(c) Jellyfish Delay Variance Attack

The malevolent hub postpones parcel arbitrarily in this kind of assault without changing the bundle request. [1].

CONCLUSION

MANET's dynamic nature makes it more powerless against different layers of assaults. One of the most commonly targeted MANET layers is the network layer From one perspective, specially appointed system security-touchy applications need an elevated level of security on the other, impromptu system is innately powerless against security assaults. We want to suggest an integrated security system as a future work that will examine the network to detect the presence of these attacks. We will try to identify the attacker nodes after detecting a particular attack and afterward limit their impact by barring those hubs from the system.

REFERENCES

[1] A. Jain and A. Choorasiya, "Security Enhancement of AODV Routing Protocol in Mobile Ad Hoc Network," in Proc. of the 2nd Int. Conference on Communication andElectronicsSystems,Coimbatore,India,19-20Oct. 2017, pp. 958–964.

[2] S. Strogatz, "Nonlinear Dynamics and Chaos: With Applications to Physics, Biology Chemistry, and Engineering," Westview Press, 2nd edition, 2015, ISBN: 978-0-813-34910-7.

[3] K. S. Praveen, H. L. Gururaj, and B. Ramesh, "Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols," Procedia Computer Science, vol. 85, pp. 325–330, 2016.

[4] Khan,M.S., Jadoon, Q.K. and Khan,M.I. A comparative performance analysis of MANET routing protocols under security attacks, Lecture notes in electrical engineering 310, DOI:10.1007/978-3-662-476697_16, springer(2015)

[4] T. Issariyakuland E. Hossain,"Introduction to Network Simulator NS2," Springer, Boston, MA, 2009. Available: https://link.springer.com/chapter/10.1007/978-0387-71760-9_2.

[5] M. Faghihniya, S. Hosseini, and M. Tahmasebi, "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network," Wireless Networks, vol. 23, no. 6, pp. 1863–1874, 2017.

[6] H. Yang, X. Mengand] S. Lu: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks, ACM, 2002

[7] D. R. Choudhury, L. Ragha, and N. Marathe, "Implementing and improving the performance of AODV by receive reply method and securing it from black hole attack," Procedia Computer Science, vol. 45, pp. 564– 570, 2015.

[8] Ahmed W., Elhadef M.,"DoS Attacks and Countermeasures in VANETs". In: Park J., Loia V., Choo KK., Yi G. (eds) Advanced Multimedia and Ubiquitous Engineering. MUE 2018, FutureTech 2018. Lecture Notes in Electrical Engineering, vol 518. Springer, Singapore

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13832 – 13837

[9] Singh, M.M. and Mandal, J.K., Reliability of MANET under the influence of black hole attack in ad hoc on demand distance vector routing, Journal of Scientific & Industrial Research, Vol 76(07)2017,pp 423-426,ISSN: 0022-4456.

[10] Singh, M.M. and Mandal, J.K., Effect of black hole attack on MANET reliability in DSR routing protocol, In: R.K.Chaudhary et al. (eds.), Advanced Computing and Communication Technologies, Advances in Intelligent Systems and Computing 562, pp 275-283. Springer Nature Singapore Pte. Ltd, (2018)

[11] Khan,M.S., Jadoon, Q.K. and Khan,M.I. A comparative performance analysis of MANET routing protocols under security attacks, Lecture notes in electrical engineering 310, DOI:10.1007/978-3-662-476697_16, springer(2015)

[12] Sarkar, S.K., Basabaraju,T.G. and Puttamadappa,C. Adhoc Mobile Wireless Networks:principles,protocols and applications, 2nd edition ,CRC Press 2013.

[13] Basagni, S., Conti,M.,Giordano,S. and Stojmenovic, I. Mobile Ad hoc Networking: Cutting Edge Directions, second edition, John Wiley & Sons Inc. (2013)

[14] H. Yang, X. Meng and S. Lu: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks, ACM, 2002

[15] L. Mejaele and E. O. Ochola, "Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor," in the 2nd Int. Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa, 15–17 Nov. 2015, pp. 140– 144.

[16] T. Issariyakuland E. Hossain,"Introduction to Network Simulator NS2," Springer, Boston, MA, 2009. Available: https://link.springer.com/chapter/10.1007/978-0387-71760-9_2.

Published by: The Mattingley Publishing Co., Inc.