ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICACTRP 2017

International Conference on Advances in Computational Techniques and Research Practices

Noida Institute of Engineering & Technology, Greater Noida

Vol. 6, Special Issue 2, February 2017

Network and Transport Layer Attacks in Ad-hoc Network

Chitvan Gupta[1], Dr. Prashant Singh[2], Dr. Rajdev Tiwari[3]

Assistant Professor, Department of CSE, NIET, Greater Noida, India[1]

Professor, Department of IT, NIEC, Delhi, India[2]

Professor, Department of CSE, GNIT, Gr. Noida, India[3]

Abstract: Security issues in Mobile Ad-hoc Networks have been a major focus in recent years. The development of fully secure schemes for these networks has not been entirely achieved till now. While a wireless network is more versatile than a wired one, it is also more vulnerable to attacks. This is due to the nature of radio transmissions, which are made on the air. On a wired network, an intruder would need to break into a machine of the network or to physically wiretap a cable. On a wireless network, an adversary is able to eavesdrop on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer. The two most important security problems in MANET are Authentication and Cooperation. Due to absence of any centralized controller, the detection of problems and recovery from such issues is difficult. Different types of attacks are discussed in this paper.

Keywords: DoS, MANET, AODV, DSR.

I. INTRODUCTION

Ad hoc networks are wireless multi-hop packet networks without any fixed infrastructure. An Ad-hoc network is formed solely by its terminals so that each terminal connected to the network provides also relaying service for others, i.e. acts as a router. Advantages of such system are rapid deployment, robustness, flexibility and inherent support for mobility. Ad-hoc network can work as a stand-alone autonomous network providing internal connections for a group. Demand for such networks could arise in the contexts of shared desktop meeting, disaster recovery, or in various military applications. There are challenges or issues [1] in ad-hoc networks due to the peculiar features such as:

- Dynamic topology of network
- Some or all nodes may be mobile
- Limited bandwidth
- Constrained power
- Broadcast nature of transmission
- Scalability
- Quality of Service
- Client server model shift
- Security
- Interoperation with the Internet
- Node cooperation
- Support for different routing protocols
- Interoperation with other wireless networks
- Aggregation

In this paper the node cooperation is discussed. It is also observed that how cooperation of nodes affect the network performance. In the area of commercial applications of ad-hoc network the node cooperation is a security issue. The fundamental question is why a node in ad-hoc network should relay others' node data? The answer is straightforward: to receive the corresponding service from the others. But the situation is more complex when every node tries to save its energy by not forwarding received packets. Surely it would not waste its batteries for relaying gaming data. [2] Node misbehavior that affects network operations like routing, packet forwarding may range from simple selfishness or lack of collaboration due to the need for power saving to active attacks aiming at denial of service (DoS) and subversion of traffic. Selfish nodes are the nodes that do not intend to damage the network but it simply does not forward the packet to save its own battery life whereas malicious node aim is to damage the network by different means like snooping, spoofing etc. Selfish nodes are those nodes which act in the context of enhancing its performance while malicious nodes are those which mortifies the functions of network through its continual activity. On the basis of abnormal behaviour of node there are two types of attacks: active attack and passive attack. In this paper the type of attacks and affect of these attacks on network performance are explained.

II TYPE OF ATTACKS

A. Passive Attacks

A passive attack does not disrupt proper operation of the mobile nodes in the network. The attacker snoops the data exchanged in the network without altering it [19]. Fig. 1shows the example of passive attack, where node 3 monitors/reads the data flow between the source and destination. Detection of passive attacks is very difficult as the operation of network itself does not get affected.

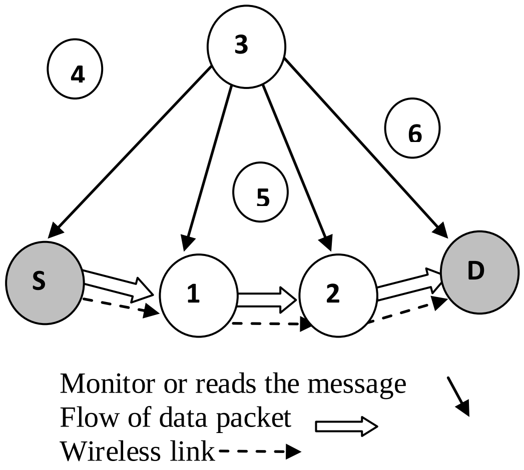

Fig. 1. Passive attack

Malicious nodes are cause of passive attack. One technique of avoiding such problems is to use powerful encryption mechanisms. So that selfish nodes would not be able to read the message of other nodes.

B. Active attack

Active attacks are very severe attacks on the network that prevent message flow between the nodes. In active attacks, intruders launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data of packets, resulting in various disruptions to the existing network [7], [5]. It can bring down the entire network or degrade performance significantly. Selfish nodes are cause of active attack. It is also need to state here that a selfish node becomes a malicious node in future.

III ACTIVE ATTACK CLASSIFICATION

A. Eavesdropping

Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers [4]. A message sent by a node can be heard by every device equipped with a transceiver within the radio range, and if no encryption is used then the attacker can get useful information [5]. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. Eavesdropping on a network conversation, involves copying packets as they are sent on the shared medium. These captured packets can be decoded with methods identical to the decoding done on the intended recipient. As such, the entire communication can be replayed for the eavesdropper.

B. Snooping

Snooping, the unauthorized interception of information is a form of disclosure. It is suggesting simply that some entity is listening to or reading communications or browsing through files or system information. Wiretapping is a form of snooping in which a network is monitored [6]. Snooping can involve very minor invasions of privacy like looking through someone's mail.

C. Spoofing

Masquerading or spoofing, is an impersonation of one entity by another, is a type of together deception and usurpation. It attracts a sufferer into believing that the entity with which it is communicating is a different entity [6]. If a user tries to log into a computer across the Internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. Similarly, if a user tries to read a file, but an attacker has arranged for the user to be given a different file, another spoof has taken place.

IV PASSIVE ATTACK CLASSIFICATION

A. Blackhole Attack

MANET uses a reactive routing protocol such as Ad hoc on demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Secure Aware routing (SAR) for the routing of the data packets. When the AODV routing protocol is used to discover the routes it works based on two types packets such as Route request (RREQ) packet and Route reply (RREP) packet. The source node sends the RREQ packets to all other nodes to find the shortest route between the source and the destination in the network. The malicious node receives the RREQ packet and claim that it is having the shortest route or optimum path to the node it wanted to actually transmit (destination). The malicious node sends the response by using the RREP packet that is having the shortest and fresh route for the destination from the source. It is the fake RREP with extremely short route. Upon sending the fake RREP packet to the source node, the malicious node can able to place itself in the communicating network. It means that the transmitting packets are should be passed only by this malicious node only [4]. After sending the RREP packet, the malicious node receives the data packets from the source and does not forwards to the neighbour nodes or simply drops the packets that they received without sending to the destination node as shown in the Fig. 2.

The Fig. 2 shows that the source node S sends the RREQ packet to all other nodes [1, 2, 3, 4, 5, 6, 7] in network to find the shortest route to the destination for the data packet transmission. Then the malicious node 1 sends the fake RREP with shortest route [S, 2, 1 D]. And the other actual routes for reaching the destination are [S, 3, 4, D], [S, 2, 5, D] and[S, 2, 5, 6].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICACTRP 2017

International Conference on Advances in Computational Techniques and Research Practices

Noida Institute of Engineering & Technology, Greater Noida

Vol. 6, Special Issue 2, February 2017

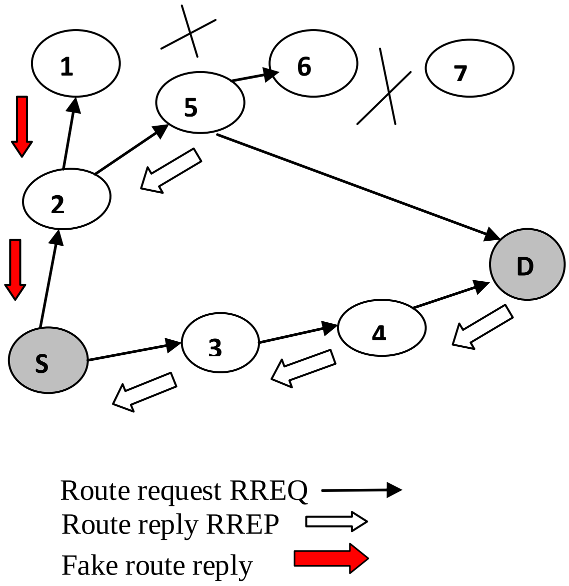

Fig2. Black hole attack

Whenever the source node receives the RREP by node 1 it concludes that this is the shortest valid route sends the packet to this route. Then the node 1 does not forward to the nodes or simply drops the packets that they receive.

B. Wormhole Attack

The colluding nodes creates an illusion [9] that two geographically separated (remote) nodes are directly connected and appears that the nodes as neighbors. But actually they are distinct from each other. The aim of the wormhole attack is to create the man in the middle attack and dropping the packets. The malicious node receives data packets at one node and tunnels them to another malicious node. The tunnel is created either using a wired link or by having a long range high bandwidth wireless link operating at a different frequency band.

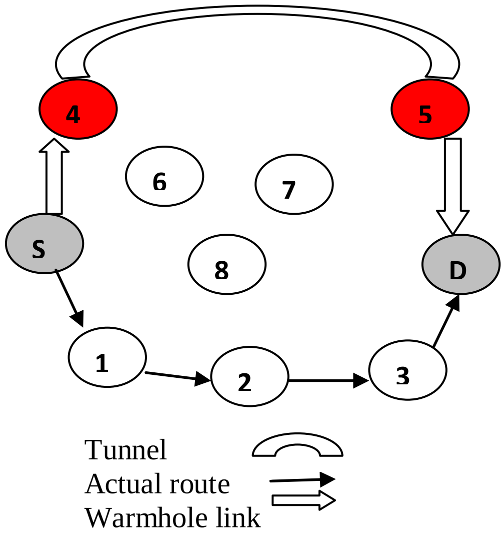

Fig3.Wormhole Attack

As shown in the Fig. 3, this tunnel is called as wormhole. It makes the node as attractive and so that more packets are routed through these nodes. This type of attack prevents the discovery of any actual routes. In the Fig. 3, the malicious node e.g. (4, 5) connects two distinct points in the space via the shortcut (A, B) route. It will disrupt the routing by short circuiting the network. This wormhole link becomes the lowest cost of path to the destination. Therefore these nodes are included for the transmission to the destination.

C. Rushing Attack

In AODV routing protocol, when source nodes flood the network with route discovery packets (RREQ, RREP) in order to find routes to the destinations, every in-between node process only the first non replica packet and throw-outs any replica packets that arrive at a later time. A rushing attacker utilize this replica repression mechanism by quickly forwarding route discovery packets with a malicious RREP on behalf of some other node skipping any proper processing in order to gain access to the forwarding group [10]. In rushing attack, an intruder will “rush” (transmit early) the RREQ packet to suppress any later legitimate RREQs as shown in the Fig. 5. The source node S broadcasts a RREQ for node 1 and node 2. Now, on hearing the RREQ, the malicious node 2 rushes the RREQ to suppress the later legitimate RREQ. The rushing may in the following ways [10]. Malicious node 2 ignores the request forwarding delay (this is a randomized delay used by the routing protocol to avoid collision of broadcast packets). Malicious node 2 rushes the RREQ with a higher source sequence number. This rushed RREQ from Malicious node 2 arrives first at node 4, and therefore node 4 will discard the legitimate RREQ from node 5 when it arrives later via 1, as shown in Fig. 4.

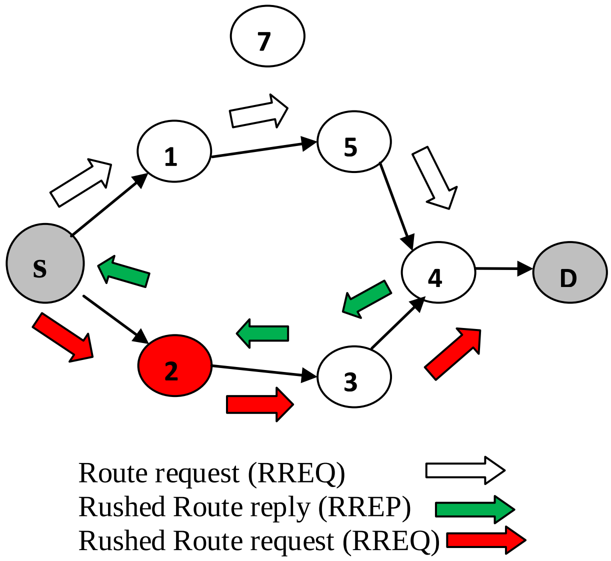

Fig 4.

Due to duplicate suppression, the actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker node, send packets to proper node after its own filtering is done, so from outside the network, the nodes behaves normally and nothing was happened. But it might increase the delay in packet delivering to destination node [11].In this section it is briefly detailed about the active attacks on the network layer with the examples. These researches on attack are concluded that the attacks degrade the performance of the network as fit as data packet transmission.

D. Grayhole Attack

A gray hole attack is a variation of black hole attack, where an adversary first behave as an honest node during the route discovery process, and then silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. A gray hole is a node that selectively drops and forwards data packets after it advertises itself as having the shortest path to the destination node in response to a route request message from a source node. Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature.[12] Black hole attack is type of routing attack and can bring harm to whole network. Grey hole attack is the kind of denial of service attack. In this attack, the router which is mesh behave just not well and a subset of packets are forward and handle by receiver but leave by others. The presences of these attackers are hard to detect in wireless networks because over the wireless link the packets are lost due to bad channel quality.

E. Jellyfish attack

The uncooperative node Delay the data packets transmission. It receives the packet but does not unexpectedly transmit the packets. Jellyfish attack is related to transport layer of MANET. The JF attacker disrupts the TCP connection which is established for communication. Jellyfish attacker intrudes into forwarding group and delays data packets unnecessarily for some amount of time before forwarding them. Due to JF attack, high end to end delay is introduced in the 295 network resulting in poor performance of the network. Many applications such as file transfer, messaging, and web require reliable, congestion controlled delivery as provided by protocols such as TCP. JF attacker disrupts the whole functionality of TCP. As a result of which performance of real time applications becomes worse. JF attack is further divided into three categories i.e. JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack [13]. Jellyfish attack is related to transport layer of MANET. The JF attacker disrupts the TCP connection which is established for communication. JellyFish attacker intrudes into forwarding group and delays data packets unnecessarily for some amount of time before forwarding them. Due to JF attack, high end to end delay is introduced in the network resulting in poor performance of the network. Many applications such as file transfer, messaging, and web require reliable, congestion controlled delivery as provided by protocols such as TCP. JF attacker disrupts the whole functionality of TCP. As a result of which performance of real time applications becomes worse. JF attack is further divided into three categories i.e. JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack [1]. JellyFish attack is related to transport layer of MANET. The JF attacker disrupts the TCP connection which is established for communication. JellyFish attacker intrudes into forwarding group and delays data packets unnecessarily for some amount of time before forwarding them. Due to JF attack, high end to end delay is introduced in the 295 network resulting in poor performance of the network. Many applications such as file transfer, messaging, and web require reliable, congestion controlled delivery as provided by protocols such as TCP. JF attacker disrupts the whole functionality of TCP. As a result of which performance of real time applications becomes worse. JF attack is further divided into three categories i.e. JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack. It is same as black hole attack but the difference is that the black hole attacker node drops all the data packets but jelly fish attacker node produces delay during forwarding packets. The performance of a connection in a MANET under Jellyfish attack depends heavily on many factors such as the number of flows, node mobility, traffic load, and the number of attackers as well as their positions.[14]

Table 1. A comparison of Active attacks

Type of active attack	**Routing protocol (Area)**	**Description of attack**	**Detection Mechanism**
Black hole attack	AODV, DSR, SAR	Malicious node receives RREQ and send fake RREP with high sequence Number there after received the message from sender and not forward the message	1. SAR[15] 2 .DPRAODV 3. CORE[16]
Wormhole attack	AODV	Known as man in the middle attack, Two geographically estranged adversaries create subway it can drop	SECTOR mechanism[17]
Greyhole	AODV	Selectively drops the packet by a selfish node due to	DCA-update key

attack		congestion it is DoS (denial of service) type of attack	management[18]
Jellyfish attack	Routing	Delaying the data packet transmission	SCAN-secure packet delivery[20]
Rushing attack	Routing discovery	An intruder will "rush" (transmit early) the RREQ packet to suppress any later legitimate RREQs	SMT-secure end to end data forwarding[19]

CONCLUSION

In this paper different network layer attacks in ad-hoc network are described. It is also explained that how different attacks take place and degrades the network performance. There are number of security mechanism already implemented to prevent from these attacks or to detect and remove the affect of these attacks. But still attackers often find new ways to harm the computer systems and networks. So protection mechanism is required to prevent the network from attackers. Knowledge of existing attacks is required to infer and to find new intrusive activities in MANET. An exclusive research need to be concentrated on development and deployment of network security policies, which will be established along with direction-finding protocols in the networks with a dynamic environment such as in MANETs. It is also noticed that the protection mechanisms need to be robust enough to protect themselves and not introduce new vulnerabilities into the system. Our aim is to prevent the network layer from these attack in which false node act as regular node. That node is difficult to detect, because the nodes here in this type of attack are very much unpredictable and volatile as they varies from normal to adversary and adversary to normal nodes.

REFERENCES

[1] Charles E. Perkins (Ed.), Ad Hoc Networking. Addison- Wesley, December 2000.

[2] Aleksi Penttinen, "Research On Ad Hoc Networking: Current Activity And Future Directions", Networking Laboratory, Helsinki University of Technology, P.O.Box 3000 FIN-02015 HUT, Finland

[3] A. Nadeem and M.P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, 2013.

[4] B. Wu, J. Chen and M. Cardei, "A survey on attacks,countermeasures in MANET", Springer, 2006.

[5] A. Nadeem and M.P. Howarth, "A Survey of MANET Intrusion Detection & Prevention approaches for Network Layer attacks",IEEE Communications Surveys & Tutorials, 2013.

[6] M. Bishop, "Computer Security: Art and Science", Addison Wesley, Nov. 2002.

[7] Gagandeep, Aashima and P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology, 2012.

[8] X. Y. Zhang, Y. Sekiya and Y. Wakahara, "Proposal of a Method to Detect Black Hole Attack in MANETs", Proc. IEEE International symposium on Autonomous Decentralized System ISADS, 2009.

[9] E. A. Panaousis, L. Nazaryan and C. Politis, "Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications", Sep. 7-9, 2009, London, UK.

[10] A. Nadeem and M.P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks",IEEE Communications Surveys & Tutorials, 2013.

[11] H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks on multicast in MANET", Elsevier, Ad Hoc Networks, 2008.

[12] C. Wei, L. Xiang, B. Yuebin and G.Xiopeng, "A New Solution for Resisting Grey Hole Attack in Mobile Ad Hoc Networks", Proc. IEEE Conf. on Communication and Networking, 2007.

[13] Syed Atiya Begum, L.Mohan, B.Ranjitha, " Techniques for Resilience of Denial of Service Attacks in Mobile Ad Hoc Networks", Proceedings published by International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X National Conference on Research Trends in Computer Science and Technology – 2012

[14] Imad Aad, Jean-Pierre Hubaux, "Impact of Denial of Service Attacks on Ad Hoc Networks", IEEE/ACM Transaction on Networking, Vol. 16, No. 4, Aug 2008.

[15] X. Y. Zhang, Y. Sekiya and Y. Wakahara, "Proposal of a Method to Detect Black Hole Attack in MANET", Proc. IEEE International Symposium on Autonomous Decentralized System ISADS, 2009.

[16] CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks Pietro Michiardi and Refik Molva(r5) B. Jerman-Blaži et al.(eds.), Advanced Communications and Multimedia Security © Springer Science Business Media New York 2002

[17] S. Capkun, L. Buttyan, and J. Hubaux, "Sector: secure Tracking of Node Encounters in Multi-hop WirelessNetworks", Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[18] C. Wei, L. Xiang, B. Yuebin and G.Xiopeng, "A New Solution for Resisting Grey Hole Attack in Mobile Ad Hoc Networks", Proc. IEEE Conf. on Communication and Networking, 2007.

[19] P. Papadimitratos and Z.J. Haas, "Secure Message Transmission in MANET", Elsevier Journal of Ad Hoc Networks, 2003.

[20] H.Yang, J. Shu, X.Meng, S.Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, vol. 24, issue 2, pp. 261-273