International Journal Of Core Engineering & Management
Volume-3, Issue-11, February-2017, ISSN No: 2348-9510

A SURVEY ON MANETS AND DIFFERENT TYPES OF ATTACK AND PROTECTION MECHANISM FOR BLACK HOLE ATTACK

Ritu Sharma
Dept. of Electronics & Communication Engineering
Chandigarh University, Gharuan
Mohali, India
Sarasharma04@gmail.com

Abstract

(MANETs) have emerged as a major next-generation wireless networking technology. However, MANETs are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network. In this paper, we present a survey of the main types of attack at the network layer, and we then review intrusion detection and protection mechanisms against black hole attack.

I. INTRODUCTION

In MANETs, each node acts as router/network manager for other nodes. MANETs are vulnerable due to their basic characteristics which include topological changes, no point of network management, restriction of resources, no certifiable or centralized authority, etc. Threats to personal and company privacy and assets by attacks upon networks and computers continue in spite of efforts of network administrators and IT vendors to safeguard such environments. Secured transmission and communication in MANET is a major challenge as this network is open to many types of attacks. Understanding probable security attacks to MANETs is a serious issue as they are targeted by attacks including Flooding attack, Wormhole attack, Blackhole attack, Denial of Service (DoS),), Selfish-node misbehaving, Routing table overflow attack, Impersonation attack, etc. Earlier studies reveal the different attack categories on MANETs like Passive/Active attacks, Internal/External attacks and Routing and Packet Forwarding attacks. Some of the attacks aim at single nodes and others aim at multiple nodes. Malicious and selfish nodes are other types of attack which severely degrade the security and performance of the network. MANETs use IEEE 802.11 architecture components as described in The Basic Service Set (BSS) defines an architecture in which all stations can communicate between themselves using IEEE 802.11 wireless LAN technology. A BSS consists of an access point (AP) and all the stations associated with it. Figure 1 shows the alternative ad hoc network architecture using the IEEE 802.11 independent basic service set (IBSS). In this mode, no access point is required, and nodes communicate in a distributed peer-to-peer manner. The minimum requirement for IBSS operation is that two nodes be within radio range of each other.

International Journal Of Core Engineering & Management
Volume-3, Issue-11, February-2017, ISSN No: 2348-9510

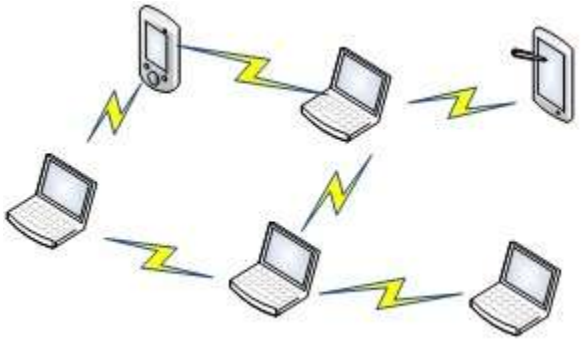

Fig.1. Ad hoc architecture using IEEE 802.11 IBSS

Points of interest and inconveniences:
MANETs have wide applications in various fields. For example, they have been used in a military context since the 1970s to ensure the timely flow of information and command in battle, contributing to the success of a mission. Another major application of MANETs is on-the-fly collaborative computing outside an office environment, for example during fieldwork, in a team project offsite, or during an offsite meeting. Even when machines are not mobile, wireless networks are not burdened with cables between them. In contrast, setting up a wireless network is simpler and faster. It may be impossible to lay cables because of the nature of the terrain such as search-and-rescue operations, battlefields, standard communication needs in public exhibitions and inter-building areas. Mutating wireless network topology such as to add, to remove or to displace a machine can also be easy.
Inconveniences:
Depending on the limited and possible interference, the data rate is often lower than wired Networks. Now some standards offer data rates comparable to Ethernet

II. ATTACKS IN MANETS

Various types of network layer attacks or intrusions are known for MANETs. In this Section, we first present a classification of major network layer attacks and introduce some individual attacks. MANETs can be divided into two main categories, namely passive attacks and active attacks

Passive Attacks: Passive attacks are those where the attacker does not disturb the operation of the routing protocol but attempts to seek some valuable information through traffic analysis. Some examples of passive attacks are as follows:

Eavesdropping: Because of the wireless links in MANETs, a message sent by a node can be heard by every device equipped with a transceiver and within radio range, and if no encryption is used then the attacker can get useful information

International Journal Of Core Engineering & Management
Volume-3, Issue-11, February-2017, ISSN No: 2348-9510

Traffic Analysis and Location Disclosure: Attackers can listen to the traffic on wireless links to discover the location of target nodes by analyzing the communication pattern, the amount of data transmitted by nodes and the characteristics of the transmission. Even if the data in a message is protected by encryption, traffic analysis can still be performed to extract some useful information.

Active Attacks: : In active attacks, intruders launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data or routing packets, resulting in various disruptions to the network. Some of these attacks are caused by a single activity of an intruder and others can be caused by a sequence of activities by colluding intruders. Active attacks (as compared to passive attacks) disturb the operations of the network and can be so severe that they can bring down the entire network or degrade the network performance significantly, as in the case of denial of service attacks. Active attacks can be further divided into malicious packet dropping attacks and routing attacks.

Malicious Packet Dropping: A path between a source node and a destination node in a MANET is established using a route discovery process. The source node starts sending the data packet to the next node along the path; this intermediate node identifies the next hop node towards the destination along the established path and forwards the data packet to it. To achieve the desired operation of a MANET, it is important that intermediate nodes forward data packets for any and all source nodes**.** Packet dropping attacks differ from the black hole and gray hole attacks.

Routing Attacks: Both the reactive and proactive routing protocols are vulnerable to routing attacks because they route based on the assumption that all nodes cooperate to find the best path. In particular, the on-demand (reactive) MANET routing protocols, such as AODV and DSR allow intruders to launch a wide variety of attacks.

Sleep Deprivation Attack: Sleep deprivation (SD) is a distributed denial of service attack in which an attacker interacts with the node in a manner that appears to be legitimate.

Malicious RREQ Flooding 1: An intruder broadcasts an RREQ with a destination IP address that is within the network address range but where the corresponding node does not exist.this forward the request message because no one has the destination path.

Malicious RREQ Flooding 2: After broadcasting an RREQ an intruder does not wait for the ring traversal time, but it continues resending the RREQ for the same destination with higher TTL values.

Black Hole Attack: Intruders can exploit the vulnerability in route discovery procedures of on-demand routing protocols, such as AODV and DSR when a node requires a route towards the destination. The node sends an RREQ and an intruder advertises itself as having the fresh route. By repeating this for route requests received from other nodes, the intruder may succeed in becoming part of many routes in the network. The way the intruder initiates the black hole attack and captures the routes may vary in different routing protocols. When a malicious node impersonates the

destination node or forges a route reply message forwarded to the source node which does not contain areal route to the destination, then it is called black hole attack. When a malicious node (Black hole node) affects one or more nodes, making them malicious as well, then this attack is labeled multiple node attack or collaborative attack.

Grey Hole Attack: A gray hole attack (GH) is a special case of the BH attack, in which an intruder first captures the routes, i.e. becomes part of the routes in the network (as with the BH attack), and then drops packets selectively. As we noted above, BH and GH attacks are different in nature from packet dropping attacks, where the attacker simply fails to forward packets for some reason. BH and GH attacks, on the other hand, comprise two tasks: the attacker first captures routes and then either drops all packets (BH attack) or some packets (GH attack).

Rushing Attack: In order to limit the control packet overhead, an on-demand protocol only requires nodes to forward the first RREQ that arrives for each route discovery. An attacker can exploit this property by spreading RREQ packets quickly throughout the network to suppress any later legitimate RREQ packets.

Sybil attack: A Sybil attack is where a malicious node acts like two or more nodes. The Sybil nodes are formed by imitation, false identities, or impersonation of nodes in a network. These additional node identities can be generated by a physical device. These attacks as can be launched in three ways as follows:

Direct or Indirect Communication: In direct communication, Sybil nodes get in touch with quiet nodes directly. A malicious tool in the Sybil node listens to messages sent from the quiet node to the Sybil node.

Stolen or Fabricated Identity: Two alternatives used by a Sybil node to get a node's identity for itself are either through identity theft of node or by devising a fresh identity. Stolen identity by a Sybil node is the general method as this can be achieved by using node impersonation.

Simultaneous or Non-Simultaneous: In the simultaneous type of Sybil attack, the attacker tries to launch all available node identities simultaneously or one after the other in the MANET. In such cases, a hardware or node entity may act as identity one time then switch through other identities to make them appear concurrently.

Protecting Against Black Hole Attacks: To guard MANETs against black hole attacks several mechanisms have been proposed using different strategies TOGBAD is an example of a black hole detection mechanism. It detects the attack using a topology graph, looking at the number of neighbors a node claims to have and the actual number of neighbors according to the graph. TOGBAD was developed for the OLSR proactive routing protocol, where topology information can be obtained; however it would not be effective for reactive routing protocols, where acquiring complete topology

information is not operationally feasible. In [41] the authors proposed a black hole detection method for AODV in which, on receiving a reply, the receiver node initiates a judgment process about the replier. Neighbors share their opinion about the replier. . A decision is made based on the number (a fixed threshold) such that if a node receives many packets but does not send a certain number of packets then it is considered to be malicious. In our opinion, considering the dynamic environment of MANETs, such mechanisms based on fixed thresholds to detect black hole attacks suffer from high false alarm rates since they have no means to adapt to changes caused by node mobility. The destination node responds by sending a packet containing its sequence number to the source node. The source node then checks the freshness of the route by comparing the sequence number of the RREP received from the intermediate node (suspect) with the sequence number reply packet from the destination node; it consequently detects an attack if the comparison fails. However, the introduction of two new packets with every reply not only increases the routing overhead but also the nodes have to ensure that the attacker does not drop or modify these sequence request and sequence reply messages.

III. CONCLUSION

It has been concluded that Manets are wireless routers that are susceptible to various types of attacks. In this paper, I present prevention methods of Black hole attack.

REFERENCES

[1] IETF Ad-Hoc Networks Autoconfigurations (autoconf) Working Group, IETF website http://datatracker.ietf.org/wg/autoconf/charter/

[2] IEEE Std 802.11-2007, IEEE standard for information technologyTelecommunication and information exchange between systems- Local and metropolitan area network-Specific requirement, Part 11 Wireless LAN medium access control and physical layer specifications, June 2007

[3] J. Anderson “Computer Security, Threat monitoring and surveillance”, Fort Washington PA, James P, Anderson & Co, 1980.

[4] H. Debar, M. Dacier and A.Wespi, “A Revised Taxonomy for Intrusion Detection Systems”, Annals of Telecommunications, Vol.55, No.7, pp 361-378, July 2000.

[5] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Communications Magazine, special issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Vol.14, No.5, pp. 56-63, Oct. 2007.

[6] T. He, H. Wang and K.W. Lee, “Traffic analysis in anonyms MANETs”, Proc. IEEE Military Communication Conference MILCOM, November 2008.

[7] E. Perkins and M. Royer, “Ad Hoc On-Demand Distance Vector Routing”, Sun Microsystem Laboratories Advance Development Group, Proceeding of the IEEE MOBICOM, pp 90-100, 1999.

[8] B. Johnson and A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Proc. Mobile Computing Journal, Vol.353, pp 153-181, 1996.

[9] M. Pirrete and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defence", International Journal of Distributed Sensor Networks, Vol.2, No.3, pp 267-287, 2006.

[10] A.Nadeem and M.Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs", Proc. ACM International Wireless Communication and Mobile Computing Conference (IWCMC 09), Leipzig Germany, June 2009.

[11] S. Kurosawa and A. Jamalipour, "Detecting Blackhole Attack on AODVbased Mobile Ad Hoc Networks by Dynamic Learning method", International Journal of Network Security, Vol.5, No.3, pp 338-345, November 2007.

[12] J.Sen, M.Chandra, S.G. Harihara, H.Reddy and P.Balamuralidhar, "A Mechanism for Detection of Gray Hole Attacks in Mobile Ad Hoc Networks", Proc. IEEE International Conference on Information Communication and Signal Processing ICICS, Singapore, Dec. 2007.

[13] Y.Hu, A. Perrig and B. Johnson, "Rushing Attack and Defence in Wireless Ad Hoc Networks Routing Protocol", Proc. ACM Workshop on Wireless Security, pp. 30-40, 2003.

[14] C.Piro, C.Shields, and B.Levine, "Detecting the Sybil Attack in Mobile Ad hoc Networks", Proc. IEEE International Conference on Security and Privacy in Communication Networks, Aug-Sep. 2006.

[15] P.Yi, Z.Dai, Y. Zhong and S.Zhang, "Resisting Flooding Attack in Ad Hoc Networks", Proc. IEEE International Conference on Information Technology Coding & Computing ITCC, April 2005.

[16] J. Sen, M. Chandra, P. Balamurlidhar, S.G. Harihara and H.Reddy, "A Distributed Protocol for Detection of Packet Dropping Attack in Mobile Ad hoc Networks", Proc. IEEE Conference on Telecommunication and Malaysian International Conference on Communication (ICT-MICC), 2007

[17] S. Marti, T.J. Giuli, K.Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", Proc. International Conference on Mobile Computing and Networking, pp 255- 265, 2000.

[18] S.B. Lee and Y.H. Choi, "A Resilient Packet Forwarding Scheme against Maliciously Packet Dropping Nodes in Sensor Networks", Proc. ACM workshop on Security of Ad Hoc and Sensor Networks (SANS 2006),pp 59-70, USA, Oct. 2006.

[19] Networks", IEEE Journal on Selected Areas in Communications, Vol.24, No.2, pp 343-356, Feb. 2006.

[20] O.F. Gonzalez-Duque, M. Howarth, and G. Pavlou, "Detection of Packet Forwarding Misbehaviour in Mobile Ad hoc Networks", Proc. International Conference on Wired/Wireless Internet Communications (WWIC 2007), pp 302-314, Portugal, June 2007.

[21] O.F. Gonzalez-Duque, G. Ansa, M. Howarth and G. Pavlou, "Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad hoc Networks", Journal of Internet Engineering, Vol.2, No.8, pp 181-192, June 2008.

[22] O.F. Gonzalez-Duque, A.M. Hadjiantonis, G. Pavlou and M. Howarth, "Adaptive Misbehaviour Detection and Isolation in Wireless Ad Hoc networks Using Policies", Proc. IFIP/IEEE International Symposium on Integrated Network Management (IM 2009), pp 242-250, NY, USA, June 2009.

[23] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-Organized NetworkLayer Security in Mobile Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 261-273, 2006.

[24] Y. Guo and S. Perreau, "Detect DDoS Flooding Attacks in Mobile Ad Hoc Networks," International Journal of Security and Networks, Vol. 5, No.4, pp. 259 - 269, 2010.

[25] T. Martin, M. Hsiao, H. Dong and J. Krishnaswamy, "Denial-ofService Attacks on Battery Powered Mobile Computers", Proc. IEEE International Conference on Pervasive Computing and Communications (PerCom), March 2004.

[26] H. Hsu, S. Zhu, and A. R. Hurson, "LIP: a Lightweight Interlayer Protocol for Preventing Packet Injection Attacks in Mobile Ad Hoc Networks," International Journal of Security and Networks, Vol. 2, Nos. 3/4, pp. 202 - 215, 2007.

[27] W.Yu and K.Ray, "Defense Against Injecting Traffic Attack in Cooperative Ad Hoc Networks", Proc. IEEE GLOBECOM, St. Louis, Missouri, USA, Dec. 2005.

[28] E.Padilla, N.Aschenbruck, P.Martini, M.Jahnke and J.Tolle, "Detecting Black Hole Attack in Tactical MANETs using Topology Graph", Proc. IEEE Conference on Local Computer Networks, 2007.

[29] M. Medadian, M.H. Yektaie and A.M. Rehmani, "Combat with Black Hole Attack in AODV Routing Protocol in MANETs", Proc. IEEE Asian Himalayas International Conference on Internet, Nov. 2009.

[30] 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.

[31] G.Xiaopeng and C.Wei, "A Novel Grey Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", Proc. IFIP International Conference on Network and Parallel Computing, 2007.

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

[33] N.Ye, X.Li, Q.Chen, M.Emran and M.Xu, "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data", IEEE Transactions on Systems, Man, and, Cybernetics, Vol. 31, No. 4, July 2001.

[34] N.Ye and Q.Chen, "An Anomaly Detection Technique based on a CHISQUARE Statistics for Detecting Intrusion into Information System", International Journal of Quality and Reliability Engineering International, Vol.17, No.6, pp 105-112, 2001.

[35] G.F.Cretu, J.Parekh, K.Wang and S.J.Stolfo, "Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks", Proc. IEEE Consumer Communication and Networking Conference, 2006.

[36] Y. Liu, C. Comaniciu and H. Man, "Modelling Misbehaviour in Ad

[37] Hoc Networks: a Game Theoretic Approach for Intrusion Detection", International Journal of Security and Networks, Vol. 1, Nos.3/4, pp. 243 - 254, 2006.

[38] H.Jiang and H.Wang, "Markov Chain Based Anomaly Detection for Wireless Ad-Hoc Distribution Power Communication Networks", Proc. IEEE Power Engineering Conference, 2005.

[39] B.Sun, K.Wu, Y.Xiao and R.Wang, "Integration of Mobility and Intrusion Detection Wireless Ad Hoc Networks", Journal of Communication Systems, Wiley International, Vol. 20, No. 6, pp. 695-721, 2007.

[40] Y.Zhang and W.Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", Proc. ACM International Conference on Mobile Computing and Networking(MobiCom), pp 275-283, Boston, US, 2000.

[41] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM Wireless Networks, Vol. 9, No. 5, pp. 545–56, Sep. 2003.

[42] P.Albers, O.Camp, and R.Puttini, "Security in Ad-Hoc Networks: A General ID Architecture Enhancing Trust Based Approaches", Proc. IEEE International Workshop on Wireless Information Systems, 2002.

[43] V.M.Potdar, S.Han, and E.Chang, "A Survey of Digital Image Watermarking Techniques", Proc. IEEE International Conference on Industrial Informatics, Aug. 2005.