Sleep Deprivation Attack in MANETS: A Review

Srinivasan J.

Assistant professor, Department of Computer Science and Application,

SCSVMV University, TamilNadu, India

ABSTRACT- Ad hoc networks are the special networks formed for Mobile applications. Operating in ad-hoc mode allows all Mobile devices within range of each other to discover and communicate in a peer-to-peerfashion without involving central access points. Many routing protocols likeAODV, DSR, SAODV, SBR, ARSA etc have beenproposed for these networks to find an end to end path between the nodes. These routing protocols areprone to attacks like Sleep deprivation attack in common by the malicious nodes. There is a need to detect and prevent these Sleep deprivation attack in a timelymanner before destruction of network services.

KEYWORDS- *Network Protocols, Wireless Network, Mobile Network, Ad-hoc Networks, Routing Protocols, Security, andAttackers.*

1. INTRODUCTION

Ad hoc Networks are the networks formed for a particular purpose. These networks assume thatan end to end path between the nodes exists. They are often created on-the-fly and for one-time ortemporary use. They find their use in special applications like military, disaster relief etc.

Characteristics of Ad-hoc Networks are:

1) Lack of fixed infrastructure: An ad-hoc network is a collection of nodes that do not rely onpre-existing infrastructure for their connectivity. So these types of networks are flexible andeasily reconfigurable.

2) Dynamic Topology: Nodes in the ad hoc networks are often mobile wireless devices likelaptops, PDAs, smart-phones etc resulting in frequent change of their location, resulting in adynamic topology.

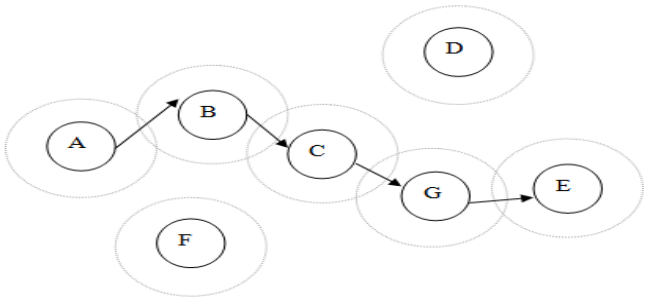

Figure 1 : An Example of Ad Hoc Networks

3) Autonomous Networks i.e. stand-alone self-organized system: Due to their decentralizednature, these networks eliminate the complexities of infrastructure setup, enabling devices tocreate and join networks "on the fly" anywhere, anytime, for any application. A node in thead hoc networks can communicate with all other nodes which are in its transmission range.Nodes in the network are self-sufficient for the purposes like routing application messages,assuring security of the network and so on.

An example of ad hoc networks is shown in Figure.1. Here ad hoc network is being establishedby communication between wireless mobile nodes A, B, C, D, E, F and G. Node A wants to senda message to another node E in the network. Routing in the network for such a scenario takesplace through multiple intermediate relay hops present in between A and E, assuming that allnodes in the network are trustworthy. Since A and B are in the wireless range of each other, Asends the message to B, B and C are in range of each other so message will get passed to C and soon till the message finally reaches E via the path A, B, C, G and E.The organization of this paper is as follows. Section II explores the various routing protocols inad-hoc networks. Network attacks are categorized in Section III. Section IV concludesthe paper.

2. ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS (MANETS) The main goal of routing protocols in ad hoc networks is to find out the optimal path withminimum overhead, minimum bandwidth consumption and minimum delay between the sourceand the destination node. As most of the nodes in ad hoc networks are wireless mobile nodes, thetopology of such type of a network does not remain fixed. As a result, it becomes the node'sresponsibility to regularly discover the network topology in order to route the messages properly.On the basis of the network topology, the routing protocols in MANETS are broadly categorizedas Proactive Routing Protocols, Reactive Routing Protocols and Hybrid Routing Protocols whichare discussed as follows:

1. Proactive Routing Protocols - In the proactive routing protocols, routing is done using theinformation present in routing tables maintained at each node i.e. table driven routing. Thesetables are exchanged on a periodic basis between the nodes. Each entry in the table contains theinformation of the next hop for reaching to a node or subnet and the cost of this route. Sinceinformation of the neighboring

nodes is maintained at each node, the time for route selectionbecomes minimal.

2. Reactive Routing Protocols - In case of Reactive Routing protocols, the routing is doneby the nodes only on demand i.e. only when the node needs to send a message. The sender floodsits neighbors with Route Request (RREQ) packets to find route in the network. Anydestination/intermediate node in the network having path to the destination will reply back withRoute Reply (RREP) to the sender and the routing is accomplished.

3. Hybrid Routing Protocols - Hybrid Routing Protocols takes the advantage of bothreactive and pro-active routing algorithms. In the initial stages, the nodes identify the routes usingsome pro-active algorithms and later on uses reactive algorithms for on demand routing. Bothpro-active and reactive nature of the protocol can be used interchangeably depending on thedifferent network scenarios. Since neither pure proactive nor the reactive approach can alonehandle all the network requirements, so the hybrid approach may be in general the optimal choice.

3. ROUTING ATTACK3.1. Sleep Deprivation Attack Sleep deprivation attack is a type of flooding attack where either a specific node or a group ofnodes is targeted whose resources need to be exhausted. This attack can be implemented byforcing the targeted node to use its vital resources e.g. battery, network bandwidth and computingpower by sending false requests for existent or non-existent destination nodes. In the mean time itcannot process the requests coming from genuine nodes. The main aim of the malicious node is tominimize the genuine nodes lifetime by wasting its valuable resources. As a result the victimnode is not able to participate in routing mechanisms and become unreachable by other nodes inthe network.

As an example, consider the network scenario in Figure 3 where a malicious node C is exhaustingthe resources of node D by sending bogus data packets or bogus RREQ packets for processing.

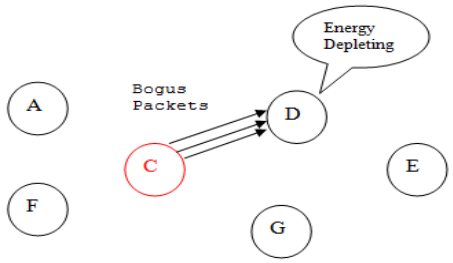

Figure 3: Example of Sleep Deprivation Attack

One of the proposed solutions to the sleep deprivation attack is:

1)A clustering based prevention method is proposed by Sarkar et al. in [18] which suggest theformation of clusters in the networks as in least cluster change algorithm. It proposes that thenode with the lowest node identifier number is assigned the cluster head. The cluster head isupdated whenever two cluster heads come in direct contact. A cluster head should forwardpackets for a particular source-destination pair in its cluster until a threshold value (say 10packets) is reached. After that the cluster head breaks its connection with that node. In this way, itresults in preventing a node from sending excessive traffic.

4. CONCLUSION AND FUTURE WORK

This paper presented a popular attack called sleep deprivation attack in MANETs. Various issues that need to be addressed keeping in view the security of MANETShave also been highlighted. The need of the hour is to detect and prevent these Sleep deprivation attack in a timelyfashion. In the future work, the author would like to propose an integrated security systemwhich will analyze the network for detecting the presence of these Sleep deprivation attack. After detection of theseparticular attack we will try to pinpoint the attacker nodes and then mitigate their affect byexcluding those nodes from the system.

REFERENCES

[1] S. Agrawal, S. Jain, and S. Sharma, "A survey of Routing Attacks and Security Measures in MobileAd-Hoc Networks," Journal of Computing, Volume 3, Issue 1, January 2011, ISSN 2151-9617.

[2] V. Balakrishnan, V. Varadharajan, U.K. Tupakula, "Fellowship: Defense Against Flooding andPacket Drop Attacks In MANET," Network Operations and Management Symposium, NOMS 2006,pp. 1- 4, 2006.

[3] Y. Guo, S. Gordon, S. Perreau, "A Flow Based Detection Mechanism against Flooding Attacks inMobile Ad Hoc Networks," Wireless Communications and Networking Conference, IEEE (WCNC2007), pp.3105-3110, March 2007.

[4] S. Desilva, and R.V. Boppana, "Mitigating Malicious Control Packet Floods In Ad Hoc Networks,"Proceedings of IEEE Wireless Communications and Networking Conference 2005, vol. -4, pp. 2112-2117, March 2005.

[5] Y. Sasson, D. Cavin, A. Schiper, "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hocNetworks," 2003 IEEE Wireless Communications and Networking, (WCNC 2003), New Orleans,LA, USA, vol.2, March 202003, pp.1124-1130.

[6] RevathiVenkataraman, M. Pushpalatha, and T. Rama Rao, "Performance Analysis of FloodingAttack Prevention Algorithm in MANETs," World Academy of Science, Engineering andTechnology 2009.

[7] M.A. Shurman, S.M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACMSoutheast Regional Conference, pp. 96-97, 2004.

[8] J. CAI, P. YI, J. CHEN, Z. WANG, N. LIU, "An Adaptive Approach to Detecting Black and GrayHole Attacks in Ad Hoc Network," 2010 24th IEEE International Conference on AdvancedInformation Networking and Applications (AINA),Perth, Australia, April 20-23, 2010, pp.775- 780,.

[9] Y.C. Hu, A. Perrig and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc NetworkRouting Protocols," Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego,California, pp. 30-40, September 2003.

[10] T.H. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The Optimized Link State RoutingProtocol, Evaluation Through Experiments and Simulation," Proceedings of IEEE Symposium onWireless Personal Mobile Communications 2001, September 2001.