IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Comparative Analysis of Black Hole attack on different nodes in Mobile Ad-hoc Network

Aruna Kumar[1], Mahendra Sharma[2]
IIMT College of Engineering, Greater Noida

1. Abstract

This paper discusses the effects of mobile ad hoc black hole attacks in the networks. To achieve this, it simulated the mobile ad hoc network scenarios which include black hole node using NS Network Simulator program. To simulate the black hole node in a mobile ad-hoc network.

Network security is one of the riskiest jobs carried out by network administrators. Network administrator carried out different security settings and configurations. This is a tedious task as the risks of network arise dynamically from time to time. The drawback of this is that network administrator needs to spend much time and needs expertise in safeguarding the network. Software Defined Networking (SDN) is the technology that helps in managing network security dynamically with programmatic approach. With SDN network administrator can programmatically and dynamically configure network security settings and control the network with ease. This invention is pertaining to network security architecture enables network administrators to control the security of the network from a central SDN controller in order to efficiently manage network security.

2. Introduction

The ad hoc network is a collection of wireless mobile nodes that can form a temporary network without any centralized management. In such an environment, due to the limited transmission range of the wireless network interface, the mobile node may need to teach other hosts to Send destination packets. Each mobile node works not only as a host but also as a packet redirector in the network that does not directly transmit to other mobile nodes within range. Each node participates in an ad hoc routing protocol that allows it to discover multi-hop paths to any other node through the network. This idea of ad-hoc mobile networks is also referred to as less network infrastructure because network nodes dynamically route between them to form their own networks in flight.

The Ad-hoc mobile network is an autonomous and decentralized wireless system. MANET consists of mobile nodes that are free in incoming and outgoing

network traffic. A node is a system or device that is a networked and mobile phone, laptop, personal digital assistant, and personal computer. These nodes can act as both a host/router and both. They can form any topology based on their mutual network connections. These nodes have self-configuring capabilities and self-configuring capabilities that can be deployed urgently without any infrastructure. The Internet Engineering Task Force (IETF) has a MANET (WG) working group dedicated to the development of IP routing protocols. Routing protocols are one of the challenging and exciting areas of research. Many routing protocols for MANETS have been developed, namely AODV, OLSR, DSR, etc.

The security of mobile Ad-Hoc networks is the most important consideration for the core functions of the network. By ensuring that security issues are met, the availability of network services, the confidentiality and integrity of data can be achieved. MANET is often subject to security attacks due to its open environment, dynamic topology changes, lack of monitoring and centralized management, cooperative algorithms, and lack of explicit defense mechanisms. These factors have changed the battlefield situation of MANET against security threats. MANET runs without centralized management, where nodes communicate with each other based on mutual trust. This feature makes MANET more vulnerable to attackers on the network. Wireless connectivity also makes MANET more responsive to attacks, making it easier for attackers to enter the network and have access to ongoing communications. Mobile nodes that exist within the wireless connection range can hear or even participate in the network.

MANET must have secure transport and communication paths, which is a very challenging and important issue because of the growing threat of attacking mobile networks. Safety is the cry of the day. To ensure secure communication and transmission, engineers need to understand the different types of attacks and their impact on MANET. Worm attacks, Black hole attacks, Sybil attacks, flood attacks, routing table coverage, denial of service (DoS), selfish episodes, confession attacks are all types of attacks on MANET may be subject to influences. MANET is more open to this kind of attack because communication is based on mutual trust between nodes, no central point of network management, no authorized facilities, topology changes and limited resources.

Keywords: MANET, AODV, adhoc, Black hole attack, Malicious Node

3. Probabilistic Modeling of Node Connectivity with the Network

A node is said to be in connected state to the network if it has k-cooperative neighbors where $1 \leq k \leq d$. Given node u with degree D(u) = d, u is said to be k-connected to the network if D(c,u) =k which holds only if u has no black hole neighbors and has k cooperative neighbors where D(c,u) denotes.

The number of cooperative degree of node u. so the probability of node u being k connected conditional on D(u) = d is given by

$Pr(D_{(c,u)}=k|D_{(u)} =d)$ $Pr(N_C=k,N_B=0|D=d)$

(4.6)

Then by binomial distribution

$Pr(D_{(c,u)}=k|D_{(u)}=d)=\binom{d}{k}P_C^k$ (4.7)

Where $P_C=1-P_B$ is the probability of cooperative neighbors. It can also be

Written $P_r(U_{(cs)}|D_{(u)}=d)=\binom{d}{k}P_C^k$

Suppose that there are N mobile nodes in a network M, a necessary condition for a network to be k-connected is that every node has at least k cooperative neighbors. The probability that a node has at least k cooperative neighbors is

$$\Pr(D_{(c,u)} \geq k) = \{1 - \Pr(D_{(c,u)} < k)\}^N \quad (4.8)$$

Then using (4.7) we immediately obtain

$$\Pr(D_{(c,u)}<k|D_{(u)}=d)=\sum_{m-0}^{k-1} Pc^m \quad (4.9)$$

4. Expermental set-up for Indivisual Attack Analysis

This set is executed under the NS2 plateform run on the linux operating system. The indivisual analysis form as below with some set of nodes.the whole excution divide in three phase under the primary where no attack come into the setup. Secondly when attack has been excuted on same setup and lasty when is has been detected using the predictive algorithms.

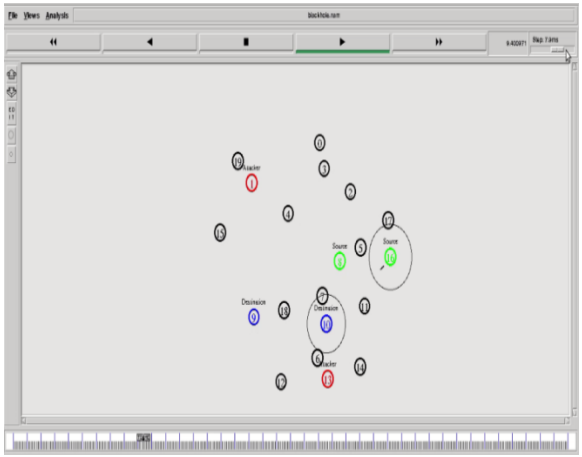
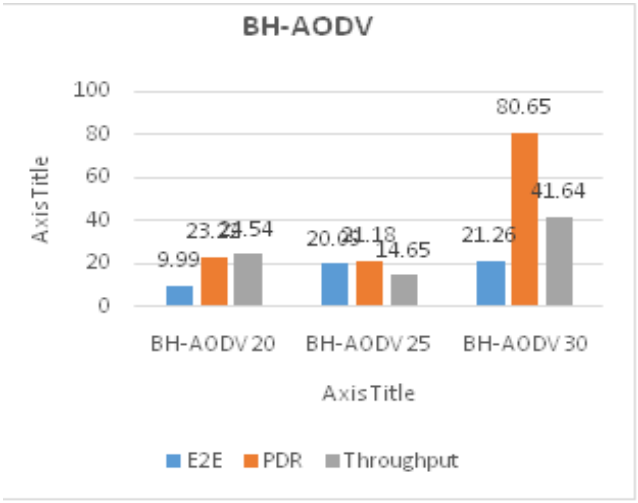


Fig.1: Simulation of Nodes on NS2.

Parameters	BH-AODV 20	BH-AODV 25	BH-AODV 30
E2E	9.99	20.09	21.26
PDR	23.22	21.18	80.65
Throughput	24.54	14.65	41.64

Fig.2: Comparative Analysis of Black Hole attack on different nodes.



5. Conclusion

In this study, we analyzed effect of the black hole in an AODV network. Black hole attack increases number of drop packets and decrease packet delivery ratio on MANET performance. After applying multiple numbers of black hole nodes on the network, drop packets will be more increased and packet delivery ratio drops off.

6. References:

[1] R. Manoharan and P.Thambidurai “Hypercube Based Team Multicast Routing Protocol for Mobile Ad hoc Networks” Proceedings of 9th International Conference on Information Technology (ICIT’06).

[2] Y Yi, M. Gerla, and K. Obraczka “Scalable Team Multicast Team in wireless networks exploiting

coordinated motion", Ad hoc Networks Journal, pp. 171-184, Aug 2003.

[3] Y. C. Hu, A. Perrig and D. B. Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Networks Routing Protocol" Proceedings of ACM WiSe2003, Sep, 2003.

[4] C. E. Perkins and E. M. Royer, "Multicast ad hoc on-demand Distance Vector (MAODV) routing," IETF draft, July 2001.Available: http://www.ietf.org/proceedings/00dec/ID/draft-ietf-manet-maodv-00.txt

[5] H. Yang, H Y. Luo, F Ye, S W. Lu and L Zhang "Security in mobile ad hoc networks: Challenges and solutions" Proceedings of IEEE Wireless Communications, Pages 38-47, 2004.

[6] Hoang Lan Nguyen and Uyen Trang Nguyen "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", Proceedings of the International Conference of Networking, International Conference on Systems and International Conference on Mobile Communication and Learning Technologies.

[7] Tamilselvan, L. Sankaranarayanan, V. "Prevention of Blackhole Attack in MANET", Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007. (AusWireless 2007).

[8] "The network simulator - ns2," http://www.isi.edu/nsnam/ns/.

[9] David B. Johnson, David A. Maltz and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad hoc Network", IETF draft, July 2004. Available: http://tools.ietf.org/html/draft-ietf-manet-dsr-10

[10] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black hole Attack in MANET", Proceedings of 42nd Annual Southeast Regional Conference

[11] C. E. Perkins and E. M. Royer, "Ad hoc on-demand Distance Vector (AODV) routing," IETF draft, July 2003. Available: http://www.ietf.org/rfc/rfc3561.txt

[12] The Network Simulator NS-2 Documentation http://www.isi.edu/nsnam/ns/ns-documentation.html

[13] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in Proc. of ICNP'06. IEEE, 2006.

[14] M. Dasgupta, S. Choudhury and N. Chaki, "SecureHypercube based team multicast routing protocol (S-HTMRP)", Proceedings of First IEEE International Advanced Computing Conference (IACC'09), March 2009.

[15] C. Perkings, E. Royer, "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys and Apps, 1999.

[16] D. B. Johnson, D. A. Maltz and Yih-Chun Hu available at: http://tools.ietf.org/html/draft-ietf-manet-dsr-10.

[17] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," Proceedings of the 3rd ACM Workshop on Wireless Security, 2002.

[18] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc

Networks," Proceedings of the 8th ACM International Conference onMobile Computing and Networking, 2002.

[19] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and Secure Source Authentication for Multicast," In Network and Distributed System Security Symposium, pp. 35–46, February 2001.

[20] J. T. A. Perrig, R. Canetti and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," In IEEE Sy