INTERNATIONAL JOURNAL OF RESEARCH
AVAILABLE AT HTTPS://JOURNALS.PEN2PRINT.ORG/INDEX.PHP/IJR/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

A Noval Approach to Minimize Effect of Black Hole Attack

Ritika Gupta & Alok Srivastava

ritika200690@gmail.com , aloksr11@gmail.com

[1]M.Tech Student, Department of ECE, Chadrawati Group of Institution

Abstract— *Everyday use of internet is increasing. Now most of services are available either in the form of mobile app or in the form of website. This has brought services to door step of common people and this is the main reason for increasing popularity of internet. With the advent of Internet of Things use of internet is achieving a new height. But as use of internet is increasing security issues in internet are also increasing specially cyber attacks. These attacks can be avoided easily in case of wired network or in wireless networks based on infrastructure. But as new arrangements for wireless communication like co-operative communication and Ad-hoc networking, are proposed the security threats are increasing. There are various types of attacks but denial of service attacks is most powerful. In this paper black hole attack has been studied.*

Keywords: — Back hole attacks, Security issues, Adhoc Network, Cooperative communication.

1.0 Introduction — Cyber attacks are the major issues of security in data packet transmission. These attacks can be divided in two parts on the basis of working

i) Installing malicious software at nodes

ii) Attack during transmission of data

Both type of attacks are lethal and can harm the entire system or particular node. The new systems of wireless communications like Adhoc networking or Cooperative communication are more vulnerable to these attacks. Since in Cooperative communication or Adhoc networking is based on mobile nodes which are obviously low powered devices so increasing complexity of algorithms which eventually leads to more power consumption should be avoided. But attacks on nodes can be avoided by using some software and precautions. Main problem is to secure network during data transmission. There are many types of cyber attacks out of which denial of service attacks is most common type of attack.

2.0 Denial of Service Attacks

In this type of attack a system is flooded with so many service requests that it eats up all the resources and server becomes so busy to these artificial requests that it could not respond to original service requests. The whole system can work in two ways

(i) Make many copies of message and route it to destination

(ii) Make proxy sources and send message by different routes towards destination.

In first case sender just flooded the server with huge amount of data. These data packets are the packets for pinging and are bigger than normally used. These senders can easily be identified and blocks. In second case sender sends data through different routes thus packets are bombarded through different routes. It looks like traffic at a

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

particular server increases and server cannot easily identify actual culprit.

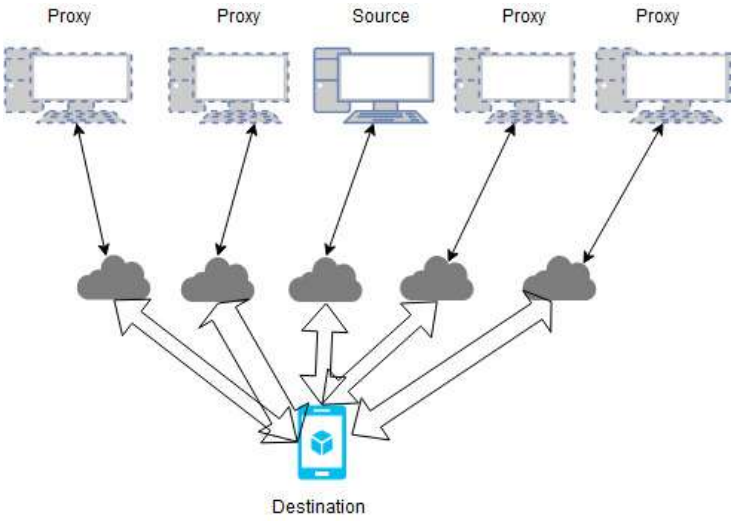


Fig :1 Block diagram of denial of service attack

3.0 Black Hole Attack

Black hole attack is also a type of denial of service attack. Black hole attack is also known as packet drop attack.

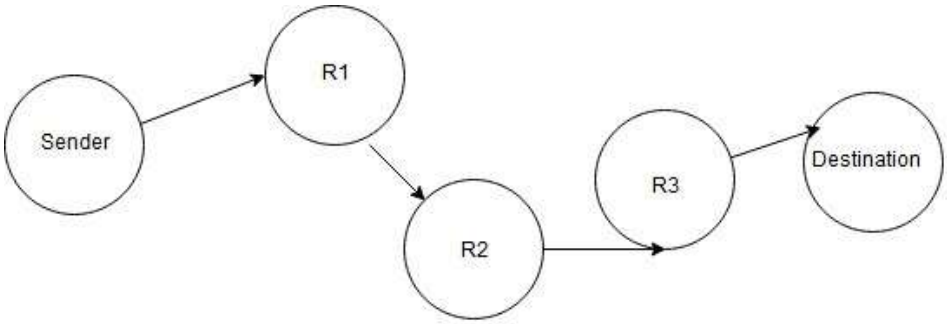
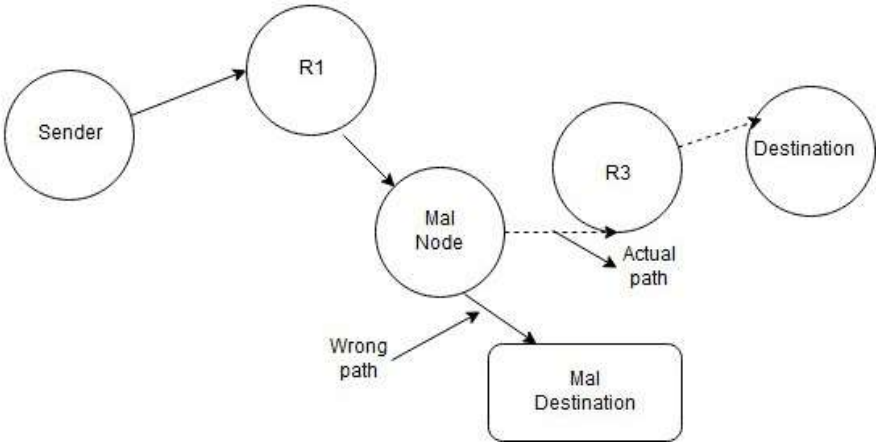


Fig: 2 Path find by path finder algorithm



e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Fig: 3 Path modified by black hole attack

In this method the attacker inserts its own node in the path and pretends like this is right path to send data. When sender starts sending data through new suggested path the malicious node may transmit it to new malicious destination. This new malicious destination may drop these packets through lossy networks or may use it. This attack is very dangerous as black hole attacks can improvise it. Black hole attacks can be designed to attack only on selected packets/ portion of complete communication.

In this paper we have created a wireless network and find a path between source and destination then black hole attack has been created.

4.0 Results

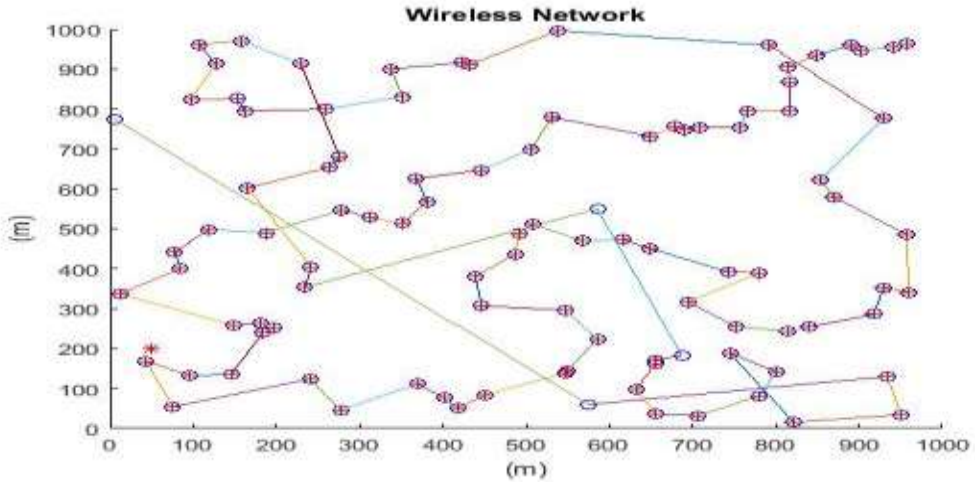


Fig 4 Wireless network

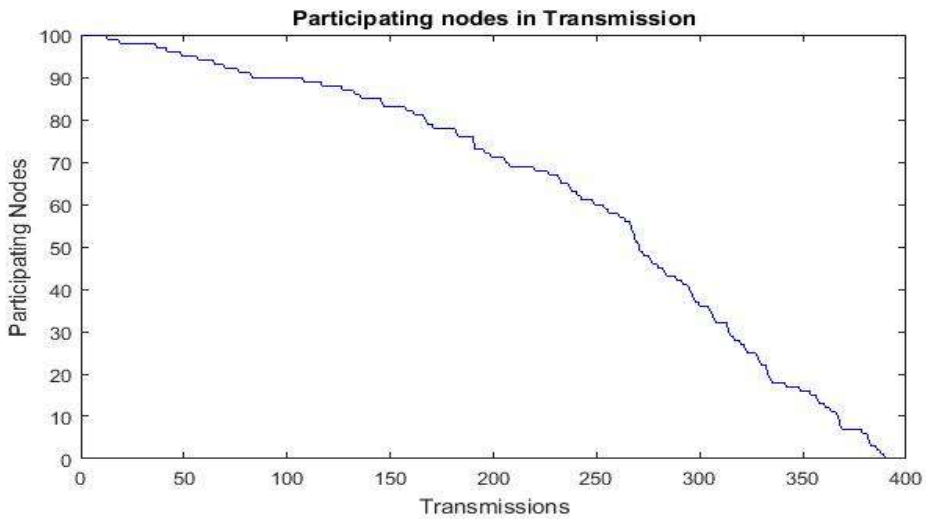


Fig 5 Reduction of nodes in transmission of data

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

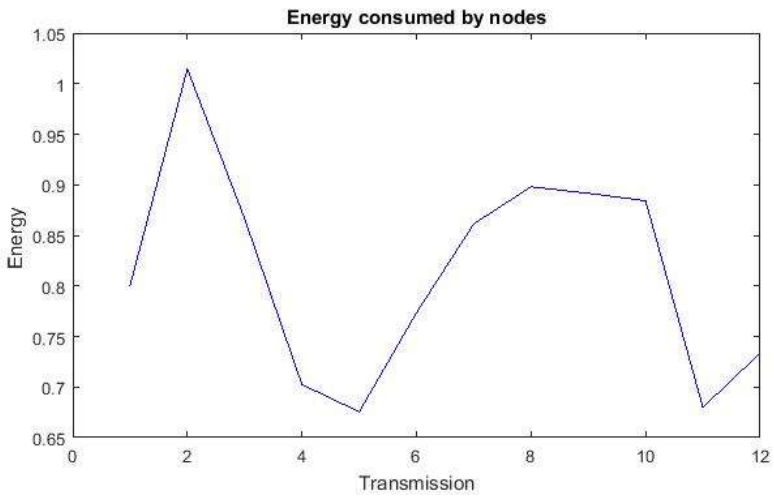


Fig 6 Energy consumption by nodes in transmission

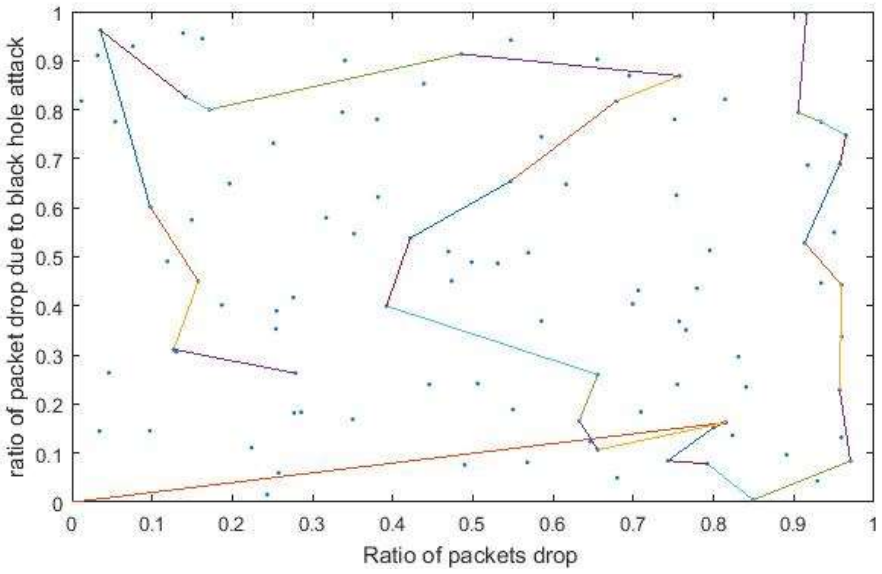


Fig 7 Packet drop ratio

5.0 Conclusion

It is very clear from packet drop ratio graph that initially when participating nodes were high. But as the route involves lesser no of nodes in data transmission the energy loss starts decreasing. We are suggesting here that nodes should not only continue updation of routing options and these routing options should be verified by other nodes as well. This updation can be done by comparing energy level of packets instead of voting or routing options provided by other nodes. By opting energy comparison shortest path can be made as well influence of other nodes can be minimized.

6.0 REFERENCES:

[1] Sneha Vinod Kumar, Yashashwini V, Anusha Pai G, and Dr.Yuvaraju B.N, "Security of the Network Based on Duration of Attack," *Int'l research Journal* of *Engineering and*

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Technology (IRJET), vol. 04, no. 4, pp. 2315-2318, April 2017.

[2] A. Sharma, G. Tripathi, Mohd. S. Kahan, and K. Anil Kumar, "A Survey on Security Protocols of Wireless Sensor Networks," *Int'l research Journal of Engineering and Technology (IRJET)*, vol. 02, no. 08, pp. 1548-1552, Nov 2015.

[3] S.K. Singh, M.P. Singh, and D.K. Singh, "A Survey on Network Security and Attack Defense Mechanisms for wireless sensor network," *Int'l Journal of computer trends and Technology*, pp. 2231-2803, May-June 2011.

[4] Agustinus Jacobus and Alicia A.E. Sinusw, "Network Packet Data online Processing for Intrusion Detection System," *in Proc. IEEE Int'l Conf. on Information and Automation (ICIA)*, 2015.

[5] G.S. Mamatha and S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- a Survey," *Int'l Journal of Computer Applications (0975 – 8887)* vol. 09, pp.09, November 2010.

[6] Shailja pandey, "Modern Network security: issues and challenges," *Int'l research Journal of Engineering and Technology (IRJET)*, vol. 03, no. 5, pp. 4351-4352, May 2011

[7] Raju Ramaswamy, "Design of a secure packet voice communication system in wide area networks," *in IEEE on Network 1(2):6-10*, pp. 43-50 April 1987.

[8] M. Sifalakis, S. Schmid, and D. Hutchison, "Network Address Hopping: A mechanism to Enhance Data Protection for Packet Communication, "Design of a secure packet voice communication system in wide area networks," in *IEEE Int'l Conf. on communication*, pp. 1518-1523, 2005.

[9] Surjit Paul and Sanjay Kumar, "A survey on wireless security," *Int'l research Journal of Engineering and Technology (IRJET)*, vol. 03, no. 11, pp. 396-410, December 2016

[10] G. Ambika and P. Srivaramangai, "A Study on Data Security in Internet of Things," *Int'l Journal of computer trends and Technology*, vol. 05, no. 02, pp. 464-469, March-April 2017

[11] Abdel-Karim R. Al Tamimi, "Security in Wireless Data Networks: A Survey Paper," *Int'l Journal of computer trends and Technology*, Apr 23, 2006.

[12] Sandra Kay Miller, "Facing the Challenge of Wireless Security," *July 2001*.

[13] T. Kiravuo, M. Sarela, and J. Manner, "A Survey of Ethernet LAN Security," *in IEEE Communications surveys & tutorials*, 2013.

[14] Jose Perez, "A survey of wireless network security protocols," *Int'l Journal of Computer Applications*, 2005.

[15] Gurkas G.Z., Zaim A.H., and Aydin M.A., "Security Mechanisms and their Performance Impacts on Wireless Local Area Networks, *2006 International Symposium*, vol. 01, no.05, pp.16-18 June 2006.

[16]Nisarg Gandhewar, Rahila Patel, 2012 "Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", Fourth International Conference on

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Computational Intelligence and Communication Networks, IEEE 2012.

[17]N.Jaisankar, R.Saravanan, K.Durai swamy, 2009 "An agent based security framework for protecting routing layer operations in MANET" First International Conference on Networks & Communications, IEEE 2009.

[18]Anoosha Prathapani, Lakshmi Santhanam, Dharma P. Agrawal, 2009 "Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks", IEEE 2009.

[19]S. Xu, 2009 “Integrated Prevention and Detection of Byzantine Attacks in Mobile Ad Hoc Networks”, PhD thesis, PhD in computer science , The University of texas at san Antonio,2009.

[20] Alex Ali Hamidian, 2003 "A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS 2" january 2003.

[21]Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Department of Information Technology Ghent University – IMEC vzw,Belgium.

[22]Nishu Garg,R.P.Mahapatra, 2009 "IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009".

[23]Sevil Sen, John A. Clark, Juan E. Tapiador,"Security Threats in Mobile Ad Hoc Networks", Department of Computer Science, University of York, YO10 5DD, UK.

[24]Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105.

[25]Emmanouil A. Panaousis, Christos Politis, 2009 "A Game Theoretic Approach for Securing AODV in Emergency Mobile Ad Hoc Networks", International Workshop on Wireless Local Networks (WLN 2009) Zürich, Switzerland, IEEE 2009.