International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 10 (2019) pp. 2383-2387
© Research India Publications. http://www.ripublication.com

Simulation-based comparative analysis on the effect of Black-hole attack and Rushing attack on the mobile ad-hoc network

Ratnadip Kuri, Syful Islam, Md. Javed Hossain, Md Humayun Kabir

Department of Computer Science and Telecommunication Engineering, NSTU, Noakhali, Bangladesh.

Abstract

Ad-hoc network is an infrastructure less network. It makes network structure dynamically on demand and creates a major security problem of data transferring between the sender and the receiver over the network. This security issue can be analyzed using the different type of attacks on MANET. In this paper, we shown a simulation-based study on the impacts of different kinds of attacks of mobile ad hoc network. Here we consider rushing attack and black hole attack to analyze its performance over the various network scenario; especially, consider performance parameter such as packet delivery ratio, throughput, end-to-end delay, etc. We investigated the impact of these three important parameters under three states of network such as normal state, black-hole attack state and rushing attacked state. This analysis clearly showed which attacking state affected which parameter of network most.

Keywords: MANET, Security, Black-hole attack, Rushing attack, Performance, Network.

INTRODUCTION

Mobile Ad-hoc network is autonomous and decentralizes wireless networks. MANET consists of nodes that can move within the network and out of the networks. These nodes can be a mobile phone, smartphone, tablet, laptop, MP3 player, etc. [3].

Security and reliability of the MANET network is an important factor because it configures its structure dynamically. Beside network congestion in the wireless link also makes the MANET more vulnerable to attacks, which make it easy for the attacker to go inside the network and get access to the ongoing communication [1][23]. MANET must have a secure way of transmission and interaction with each other under some security attack, such as Blackhole attack, Rushing attack, Denial of service (DoS), selfish node misbehaving, Sybil attack, and routing table overflow attack, etc[2]. In this paper, we expolre the effect of different type of attacks using network simulator (NS2) since it is one of the most popular simulators for simulating different network according to [22].

RELATED WORKS

Attacks against unicast communications in MANETs have been studied to some extent. The underlying property of MANET has been studied in some of the papers [2-5]. The weaknesses of the 802.11 MAC protocol by measuring the performance of affected nodes under flooding attacks, a type of resource consumption attack has been studied [21]. The study showed that the performances of all the affected nodes that were one hop away from the attackers degraded to almost zero. The damage was less severe if the attackers were two or more hops away. Other scenarios such as collisions between attackers with different attack rates were also considered. Most important type of attack has been studied in a few research papers [15-18].

DIFFERENT KIND OF ATTACKS ON MANET

A. Black Hole attack

In this attack, an affected node acts like a Blackhole, destroy all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network into two disconnected components. Once the node is set up, at the moment, it is up to the node whether to drop all the packet or familiar it to the nameless address [15].

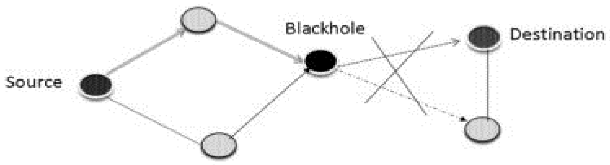

Fig1: Black Hole Attack

B. Cooperative Black-Hole Attack

In this type of attack, more than one malicious node with the properties of black hole node tries to shatter the network simultaneously. This kind is avoided only by finding an alternative route on the network [17].

C. Rushing attack

When source nodes flood the network with route discovery packets to find routes to the destinations, each intermediate node processes only the first no duplicate packet and discards any duplicate packets that arrive at a later time. A rushing attacker exploits this duplicate suppression mechanism by quickly forwarding route discovery packets to gain access to the forwarding group after own filtering of information attacker node does send the packet to the target node. So, from outside it looks nothing happens to the network. Although, it introduces some delay in delivering the packet to the destination node.

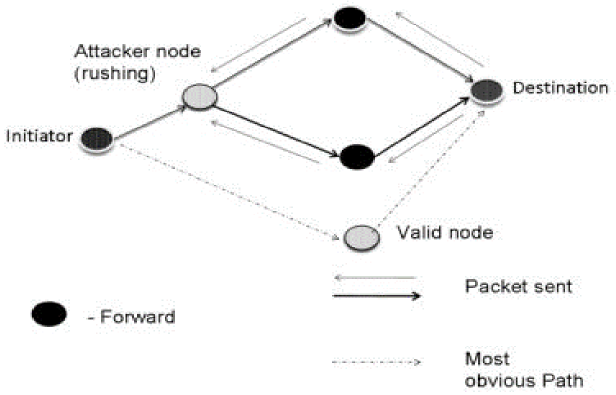

Fig2: Rushing attack

D. Gray Hole attack

Gray hole attack also drops data packet like black hole at-tack but, it has its characteristic for doing that. It has two common type of behavior as follows.

- **Node dependent attack** – drops DATA packets des-tined towards a particular victim node or coming from a specific node while for other nodes it behaves normally by routing DATA packets to the destination nodes correctly.

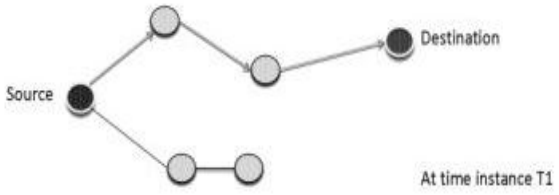

Fig3: Gray-Hole – Node dependent attack

- **Time-dependent attack** – drops DATA packets based on some predetermined/trigger time while behaving normally during the other instances.

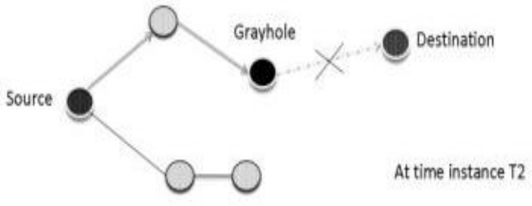

Fig4: Gray-Hole – Time-dependent attack

E. Flooding attack

Flooding is kind of Denial of Service (DoS) attack, designed to bring a network or a specific service down by flooding system with large amount of traffic. Flooding type attacks occur when a network service becomes heavily weighed down with packets and initiate unstable and unreliable connection requests that it can no longer able to process orig-inal connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the hosts' computers memory buffer. Once memory buffer is full, no further connections can be made, and the result is a Denial of Service.

F. Selfish attack

Selfish type attacks can be different depending on what and how they attack to pre-occupy CR spectrum resources. There are three different selfish attack types. A Type 1 attack is designed to prohibit a legitimate SU (LSU) from sensing available spectrum bands by sending faked PU signals. In type 2 attacks, a selfish SU emulates the characteristics of signals of a PU node and are carried out in dynamic multiple channel. In normal dynamic signal access process, the SUs will periodically sense the current operating band to know if the PU is active or not, and if it is, the SUs will immediately switch to use other available channels. In type 3 attack, also known as channel pre-occupation selfish attack where attacks can be occurred in the communication environment that is used to broadcast the currently available channel information to neighboring nodes for transmission.

G. Wormhole attack

In wormhole attack, an attacker periodically records packets of data from the specific location in the network, tunnels them selectively to another locations and retransmits them into the network. So, wormhole attack can be a form a seri-ous threat in wireless networks, especially for many ad-hoc routing protocols and also location-based wireless security systems. For example, most existing ad hoc routing network protocols, without using some mechanism to defend against the wormhole attack, would be not be able to find routes longer than one or two hops, severely disrupting communi-cation.

H. Jellyfish attack

Jellyfish attack is somewhat different from the Black-Hole & Gray-Hole attack. Instead of disappearing the data packets, it delays them before finally delivering them. A jellyfish attacker first needs to intrude into the multicast forwarding group. It then delays data packets unnecessarily for some amount of time before forwarding them. This results in significantly high end-to-end delay and thus degrades the performance of real-time applications [18].

I. Sybil attack

In MANET the medium of transmission of the packet is air, and they don’t have a central node to control the network. So, the routing is mainly based on a unique node address. The attacker can exploit this property of MANET by using fake identities. That is the attacker can either use random identity or the identity of a legitimate node

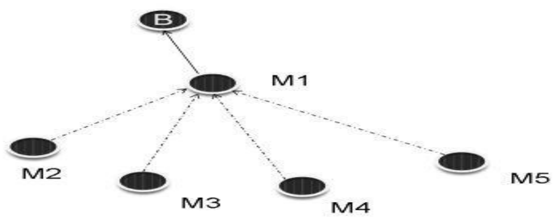

Fig5: Sybil attack

COMPARATIVE ANALYSIS OF BLACKHOLE AND RUSHING ATTACK

We analyze the effect of blackhole attack and rushing attack compared with the normal state of the network for different sizes such as 50 nodes, 100 nodes, 200 nodes, and 400 nodes network. These attacks are applied for AODV protocol on Ad-hoc network.

A. Throughput comparison for different state

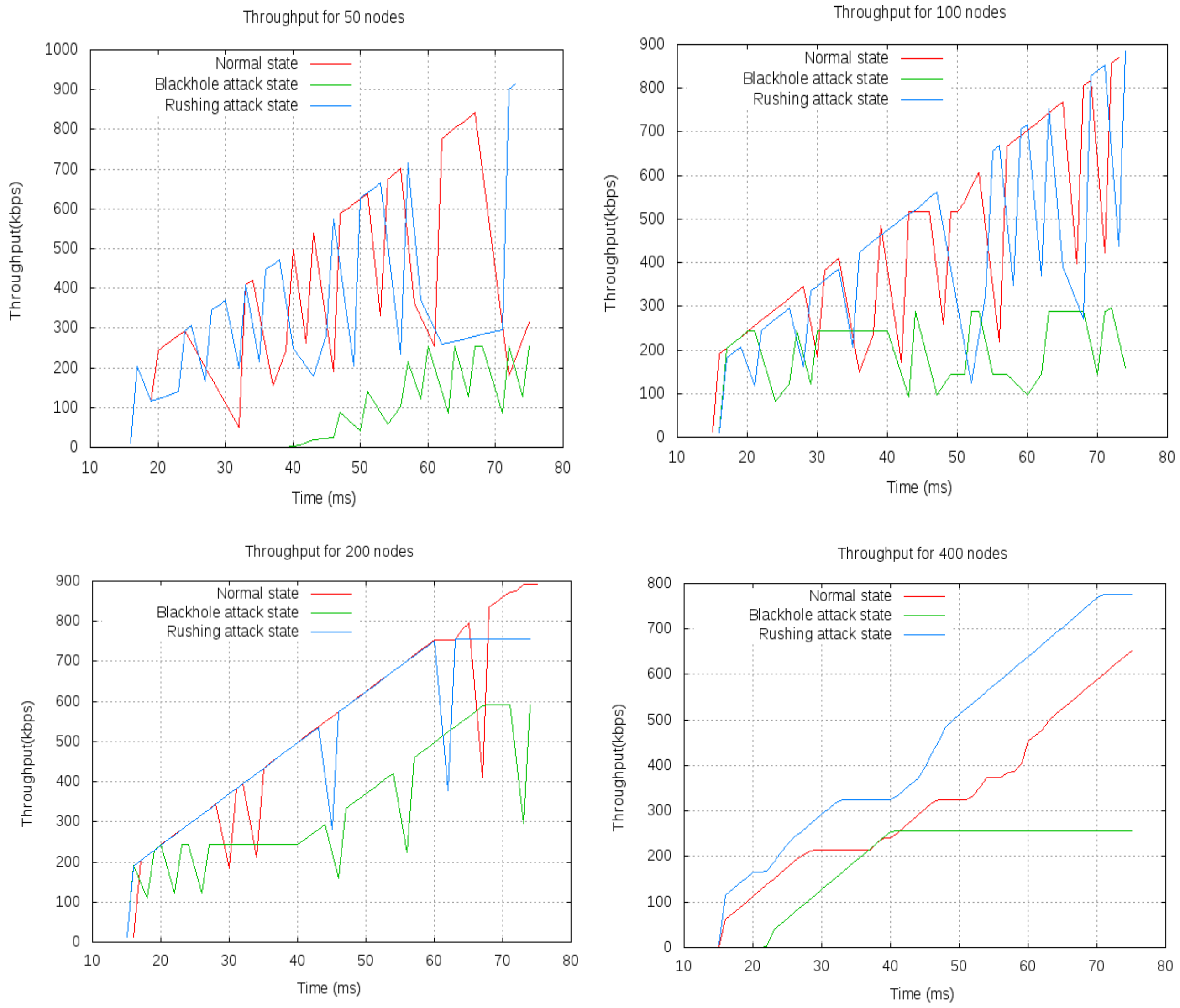

Fig6: Time vs. Throughput graph for a) 50 node networks, b) 100 node networks, c) 200 node networks, d) 400 node networks

Figure 6 shows the throughput graph in different states for different size of networks. Throughput in blackhole attack state is significantly low wherein rushing attack state its relatively high almost similar to normal state. In the blackhole attack, the black hole nodes vanish the data packet and don't allow it to next node. So, those packets are routed through blackhole node does not go to the final destination but, packet through rushing node reach to the final destination. That is why throughput in blackhole attack in low but in rushing attack its similar to the normal state of the network. Figure 7 replicate the similar result for average throughput also.

B. Packet delivery-based comparison

Packet delivery ratio shows the ratio of the number of the delivered data packet to the destination. In figure 2 we see the difference of packet delivery ratio for different states. The blackhole discards the packets before reaching to the destination. So, the packet delivery ratio is significantly low compared to the others states.

C. Average end to end delay comparison

End to end delay refers to the time taken by a packet to reach to the destination; it includes packet process time by a different node in the networks. Although, in blackhole attack, the packet discarded in the path but other packets reach to the destination node within the desired time whose are not affected by blackhole nodes. That is why the figure 9 shows the end to end delay for blackhole attack is normal. However, in the rushing attack, the rushing nodes examine the data packet without any prior permission which makes information security vulnerabilities. This step makes delay to the packets whose makes a route through the affected nodes. That is why the average end to end delay is significantly low in rushing attack compared to the others state of the net-works.

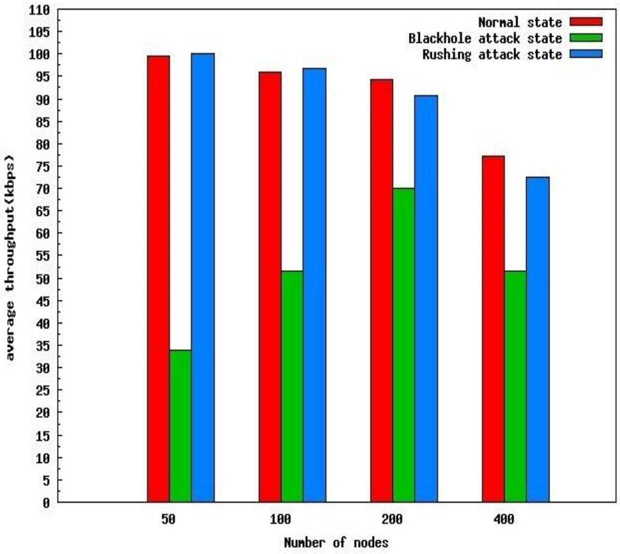

Fig7: Average throughput for a different number of nodes at different state

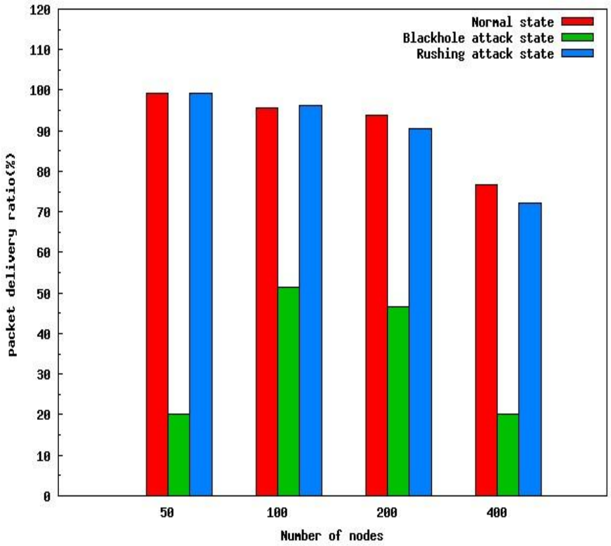

Fig8: packet delivery ratio comparison for different state

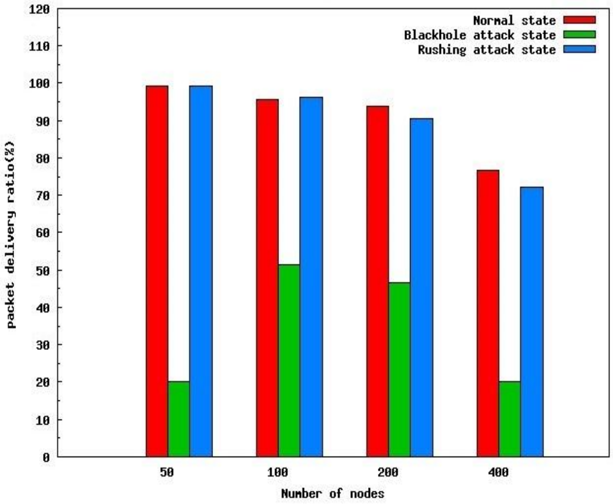

Fig9: End to end delay comparison for different state

CONCLUSION

MANET has a security problem due to its infrastructure less property. It connects with other nodes on demand. The receiving node must need to lie in the range of sender for communication if they are out of range then the intermediate node route the data packet. As a result, MANET has security problem against various type of attack. In this research, we show the simulation-based effect under black hole attack and rushing attack. In the time of blackhole attack, the system shows fewer throughputs than normal state and rushing attack. Packet delivery comparison shows that it is very low for blackhole attack while rushing attack gives almost the same packet delivery ratio as a normal state. However, an end to end delay is very high for rushing attack because it extracts information from the receiving packet before routing it to the original receiver. However, surprisingly blackhole attack shows much low average end to end delay than the normal state. However, an end to end delay for every single packet remains the same as the normal state.

ACKNOWLEDGMENT

The authors would like to thanks the department of computer science and Telecommunication Engineering for supporting the research.

REFERENCES

[1] Nishu Garg, R.P. Mahapatra, "MANET Security Issues," *International Journal of Computer Science and Network Security*, vol. 9, No 8, 2009.

[2] Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks," *I International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, Issue 5, May 2013.

[3] Aditya Bakshi, A.K Sharma, Atul Mishra, "Significance of Mobile AD-HOC Networks (MANETs)," *International Journal of Innovative Technology and Exploring Engineering*, vol. 2, Issue 4, March 2013.

[4] Ankur O. Bang, Prabhakar L. Ramteke, "MANET : History, Challenges And Applications," *International Journal of Application or Innovation in Engineering & Management*, vol. 2, No 8, September 2013.

[5] Satyam Shrivastava, Sonali Jain, "A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network," *International Journal of Computer Science & Engineering Technology*, vol. 4, No 3, March 2013.

[6] Charles E. Perkins, Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing," *In Proceedings of The 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp:90-100, 1997.

[7] Sheng Liu, Yang Yang, Weixing Wang, "Research of AODV Routing Protocol for Ad Hoc Networks" *AASRI Conference on Parallel and Distributed Computing and Systems*, vol. 5, pp:21-31, 2013.

[8] AODV, *Access Link: http://moment.cs.ucsb.edu/AODV, Access Date: 11 April 2018.*

[9] Elizabeth M. Royer, Charles E. Perkins, "An Implementation Study of the AODV Routing Protocol," *2000 IEEE Wireless Communications and Networking Conference*, September 2000.

[10] Mohammad Wazid, Rajesh Kumar Singh, R. H. Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques," *I International Conference on Computer Communication and Networks CSI- COMNET-2011 coment(1):52-57*, 2011.

[11] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, Daud Israf, "Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm," *International Journal on New Computer Architectures and Their Applications*, 2011.

[12] Hoang Lan Nguyen, Uyen Trang Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks," *IEEE International Conference on Networking*, 2006.

[13] Pradeep M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S. Ali, Prof. J.S. Deshpanday, "A survey of mobile Ad-Hoc Network attacks," *International Journal of Engineering Science & Technology*, vol. 2, pp: 4063-4071, 2010.

[14] Yingnua Guo, "Defending MANET against flooding attacks by detective measures," *Institute of Telecommunication Research, The University of South Australia*, April 2008.

[15] Harjeet Kaur, Manju Bala, Varsha Sahni, "Study of Blackhole Attack Using Different Routing Protocols in MANET," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, Issue 7, July 2013.

[16] Al-Shurman, Mohammad and Yoo, Seong-Moo and Park, Seungjin "Black Hole Attack in Mobile Ad Hoc Networks," *Proceedings of the 42Nd Annual Southeast Regional Conference*, pp: 96-97, 2004.

[17] Rashid Hafeez Khokhar, Md. Asri Ngadi, Satria Mandala, "A review of current routing attacks in Mobile Ad-Hoc Networks," *International Journal of Computer Science & Security*, vol. 2, Issue 3.

[18] I. Aad, J.P. Hubaux, E.W. Knightly, "Denial of service resilience in ad hoc networks," *Proceedings of ACM MobiCom* , September 2004.

[19] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," *International Journal of Computer Science and Security*, vol. 4, Issue 3.

[20] J. W. Creswell, Research Design: Qualitative, Quantitative and Mixed Methods Approach, *Sage Publications Inc.* 2rd ed., California, July 2002.

[21] V. Gupta, S. Krishnamurthy, M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc networks" , *In Proceedings of IEEE MILCOM'02*, 2002.

[22] Mohammed Humayun Kabir, Syful Islam, Md Javed Hoss-ain, Sazzad Hossain, "Detail comparison of network simulators," *International Journal of Scientific & Engineering Research*, Vol. 5, Issue 10, October 2014

[23] Mobile ad hoc network, *Access Link: https://en.wikipedia.org/wiki/Mobile_ad_hoc_network, Access date: May 2018.*

[24] Syful Islam, Ratnadip Kuri, Md. Humayun Kabir, Md. Javed Hossain, "Exploring Congestion Control Mechanism of TCP Vari-ants over Wired & Wireless Networks," *International Journal of Scientific & Engineering Research*, Vol. 9, Issue 9, September 2018.