Indian Journal of Science and Technology, Vol 10(30), DOI: 10.17485/ijst/2017/v10i30/115535, August 2017
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

The Impact of Resource Consumption Attack on Signal-Stability based Adaptive Routing Protocol in Manet

Shaveta Jain[1] and Kushagra Agrawal[2]

[1]Department of Computer Science, GGS Sachdeva Engineering College Kharar, Kharar - 140301, Chandigarh, India; shavetajn120@gmail.com

[2]Department of Computer Science, GD Goenka University Gurgaon, Gurgaon - 122103, Haryana, India; agrawal_kushagra@rediffmail.com

Abstract

Objectives: It analyzed the simulation based study for impact of resource consumption attack on Signal-Stability Based Adapting (SSA) routing protocol in MANET. The performance of routing protocol is calculated by using these different parameters like throughput, Packet Delivery Ratio (PDR), end to end delay (E2E), routing overhead and energy consumption. **Methods/ Statistical Analysis:** The whole simulation is carried out through NS-2. NS-2 (Network Simulator version 2) is used for this simulation which is developed by UC Berkely. NS-2 is basically a combination of two languages OTcl and C++. Components of NS-2 are NAM (Network Animator), Proposing, Post prosing. NS-2 is a discrete event simulator in this C++ is easy to code but slower to run whereas OTcl is fast to run and difficult to code. **Findings:** We see the impact of this attack with three different performance metrics such as End to End, routing overhead, energy consumption throughput and packet delivery ratio (PDR).

Keywords: Denial of Service (DoS) Attack, MANET, Performance Parameters, Resource Consumption Attack (RCA), Signal-Stability Based Adapting (SSA)

1. Introduction

MANET is a wireless infra-structured-less network, means there is no base station whereas cellular network is wired infrastructure network. In wireless ad-hoc network peer level multi-hopping technique is used for interconnection remote mobile node[1]. Every node acts as both router and host. There are various routing protocols introduced in MANET is shown in Figure 1. The basic classification of these is based on routing information update and temporal information for routing. In MANET there are two types of routing- unicast routing and multicast routing[2]. Unicast is for one-one communication and multicast is for one-much communication. Proactive routing protocol also known as table-driven routing protocol in which each and every node maintains its routing table. In reactive routing protocol which is also known as on-demand in this each node established the route on the basis of demand. Whereas in Hybrid routing protocol it combines the features of both proactive and reactive routing protocol. In attacks DDoS is an attack to make an online service inaccessible by flooding it with malicious traffic from multiple sources and directions. So, a multitude of compromised computers attack a single system and cause the Denial of Service (DoS)[3].

Now here is the classification of routing attacks in MANET. In passive attack data exchanged in the network is done without interrupt the operation of the communications, whereas an active attack contain the information of interruption, modification, or fabrication, which disrupting the normal functionality of a MANET[5] is shown in Figure 2. The severity of the attack depends on midway

*Author for correspondence

distance of the malicious nodes between the nodes, dropping of packets, misrouting of packets, providing false information etc.[6].The topology dynamic networks keep on changing so changes the attacks on these networks and in order to deal with these malicious attacks these routing protocols must be robustic[7].

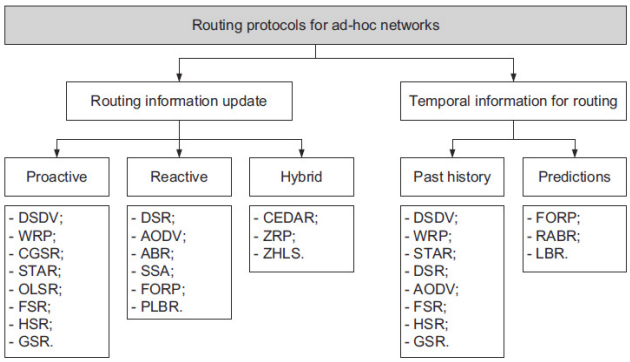

Figure 1. Classification of Routing Protocols[4].

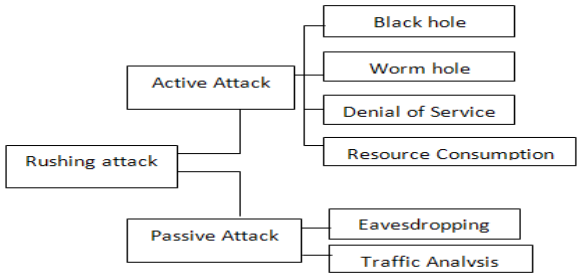

Figure 2. Types of Routing Attacks.[5]

This paper is structured in following sections: section 1 explains the introduction part. Section 2 presents SSA (Signal-Stability Based Adapting) routing protocol. Then section 3 explains Resource Consumption Attack (RCA). After that in section 4, the simulation environment and result analysis is discussed. Section 5 explains the conclusion of result and future work.

1.1 Signal-Stability Based Adapting (SSA) Routing Protocol

The SSA protocol is reactive routing protocol in which route is established on the basis of demand means when required, and are selected on temporal stability of wireless links[4]. In this longer-lived routes are selected on the basis of strength signal and location stability[8]. SSA routing protocol is similar to DSR protocol, the ROUTE_REQ packets are broadcast the discover routes[8]. Signal stability evaluated as a average of moving of the signal strength of packets received on the link in recent past[9]. In SSA (Signal stability based Adaptive routing) the routes are choose on the basis of that have stronger connectivity.

The SSA (Signal stability based Adaptive routing) protocol contains two protocols that are Forwarding Protocol (FP) and Dynamic Routing Protocol (DRP). Both of these protocols located at network layer and data link layer. The SSA packet format shown in Figure 3.

Where SA and DA refers to as source address and destination address, SEQ stands for sequence number, which is generated by source at the time of request sending. TTL is for time to live field. Type field indicates the type of message, whether it may be Route Reply, Route Request and Route error message. PREF is defined the quality of route desired[10]. LEN field define the length of the packet and CRC stands for Cyclic Redundancy Check is the checksum for error correction and detection[10]. SSA has two component co-operative protocols: that are Dynamic Routing Protocol and Static Routing Protocol[11] is shown in Figure 4.

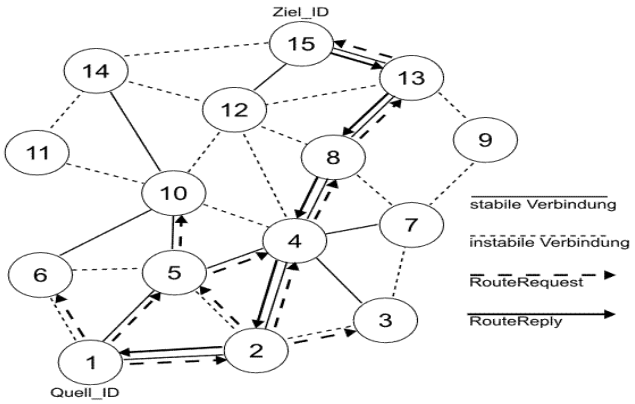

Figure 4. Routing in SSA[12].

Route Maintenance

In this when any route failure is occur, then intermediate node sends the route error message to the source node. Then source node sends the route search packet for finding the new route and send an erase message to remove the failure route is shown in Figure 5.

DA	SA	SEQ	TTL	TYPE	PREF	LEN	CRC	DATA

Figure 3. Packet Format.

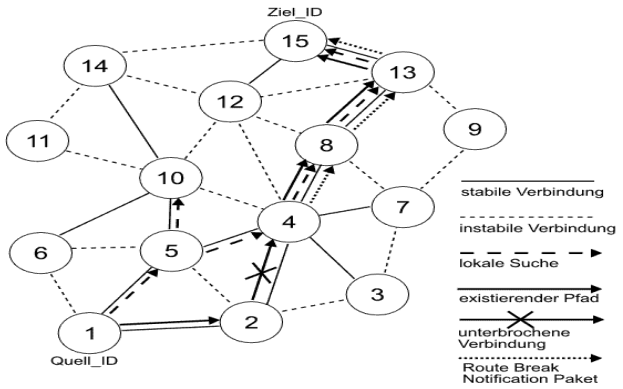

Figure 5. Route repair in SSA.[12]

2. Resource Consumption Attack (RCA)

Resource Consumption attack (RCA) is against on on-demand routing protocol. It is the one of DOS attack, in which attacker exploits the route discovery process[13-16]. During the route discovery process when the source node send the RREQ packet, then attacker node kept this packet with a different ID, in order to modify the processing ID of each node continuously and consume its limited energy of resource, memory and bandwidth[17] is shown in Figure 6. The main purpose of RCA is to consume the energy of legitimate nodes and to find the available link throughout.

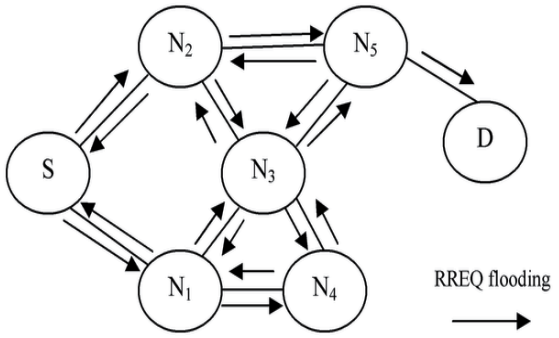

Figure 6. RREQ Continuously Broadcasted by RCA.

3. Simulation and Result Analysis

Table 1 contains the parameter value set according to particular scenario in ns2 simulation.

End to End Delay (E2E) - It is defined as the difference of time between the transmitted packets to the receiving packet from source to destination is shown in Figure 7. It is calculated as:-

Table 1. Simulation Environment

Parameters	Values
Traffic Type	TCP
Number of Nodes	40,80,120,200
Area Covered	500 X 500
Speed of the Node's	1,2 m/s
Routing Approaches	SSA
Observation Parameters	Throughput, Energy consumption, routing overhead PDR and E2E delay
Mobility Type	Critical Mobility

End to end delay = receiving time of packet – transmitting time of packet

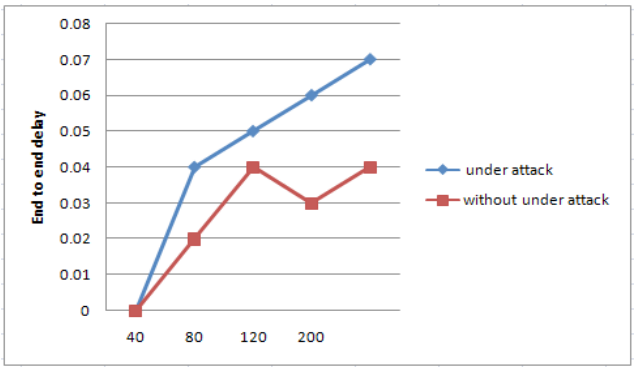

Figure 7. End to End Delay (E2E).

The above graph shows the effect of Resource Consumption Attack (RCA) on End to end delay metric in SSA protocol. In this graph the x-axis defines number of nodes and Y-axis defines the performance of network in terms of the milliseconds. The result after simulation under attack is that traditional routing produced more delay as compared to proposed technique.

Packet Delivery Ratio (PDR) – It is the ratio of successfully number of delivered packets to the destination generated by the source is shown in Figure 8.

PDR = Total number of received packet/total number of send packet

In this graph the X-axis defines the number of nodes whereas Y-axis is for packet delivery ratio which is measured in %. The amount of received packets became less under attack, whereas there are more packets received not in under attack condition.

Throughput–It is the number of packets sent per unit time. In this graph the X-axis defines the number of nodes whereas Y-axis is for throughput in terms of kbps.

The transmitting rate of packets became less during attack is shown in Figure 9.

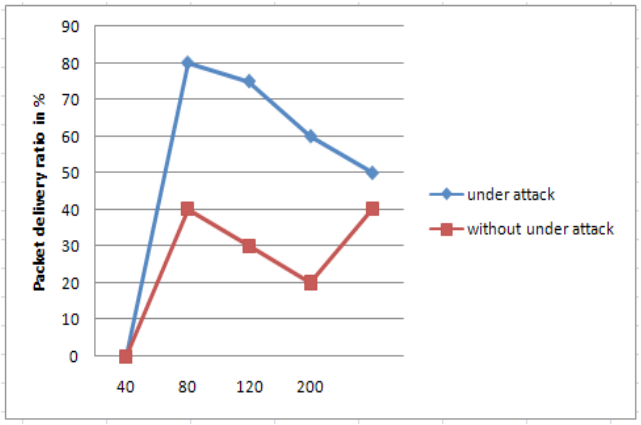

Figure 8. Packet Delivery Ratio(PDR).

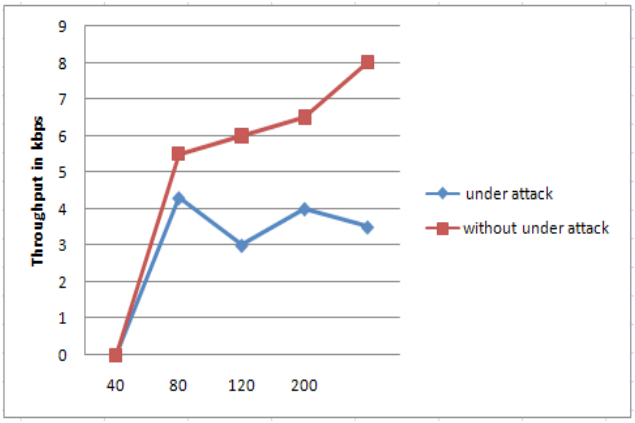

Figure 9. Throughput.

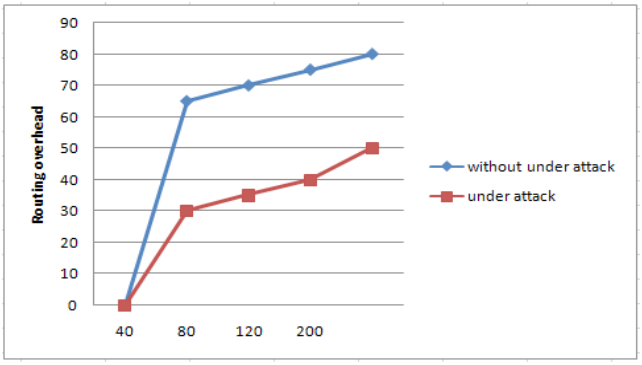

Figure 10. Routing Overhead.

Routing Overhead – In this scenario packets are exchange for different tracking and then monitoring, so that the additional injected packet is known as routing overhead. In this graph X-axis defines the number of nodes whereas Y-defines the routing overhead for network. Routing overhead under attack is less as compared to not in under attack position is shown in Figure 10.

Energy consumption – It is determined as the rate of change of energy level of Node from its initial level. In other words it is the rate of consumption of energy. In this graph X-axis defines the number of nodes whereas Y-axis defines the amount of energy consumed in termed of Joules. Consumption of energy under attack is more due to the effect of resource consumption attack is shown in Figure 11.

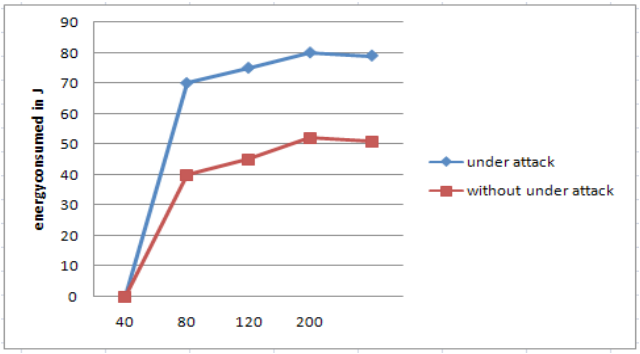

Figure 11. Energy Consumption.

4. Conclusion and Future Work

In this paper we have studied and see the impact of RCA on SSA routing protocol in MANET by varying the number of nodes. We see the impact of this attack with three different performance metrics such as End to End, routing overhead, energy consumption throughput and Packet Delivery Ratio (PDR).

In future our goal is to study the effect of RCA on other different routing protocol with different metrics like packet drop ratio and delay jitter and also discuss its prevention techniques.

5. References

1. Lee SJ, Gerla M, Toh CK. A Simulation Study of Table Driven and On Demand Routing Protocols for Mobile Ad Hoc Networks. IEEE Networks. 1999; 13(4):48-54. Crossref
2. Jain S, Agrawal K. Prevention against Rushing Attack on MZRP in Mobile Adhoc Network. International Journal of Computer Science and Technology. 2014 September; 5(3):124-27.
3. Ahamad T, Aljumah A. Detection and Defense Mechanism against DDoS in MANET. Indian Journal of Science and Technology. 2015 December; 8(33):1-4. Crossref

4. ELT-43506 (earlier TLT-5506) Laboratory Course in communication systems, 5-9 cr. Date Accessed: 12/09/2016: Available from: http://www.cs.tut.fi/kurssit/TLT-2616/lect05.pdf
5. Siddiqui T, Farooqui T. A Survey on Malicious Node Detection in MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2014
6. Vijayakumar K, Sundaram KS. Study on Reliable and Secure Routing Protocols on Manet. Indian Journal of Science and Technology. 2016; 9(14):1-10. Crossref
7. Abdelhaq M, Hassan R, Ismail M. A study on the vulnerability of AODV routing protocol to resource consumption attack. Indian Journal of Science and Technology. 2012; 5(11):1-5.
8. Tseng YC, Liao WH, Wu SL. Mobile Ad Hoc Networks and Routing Protocols. Handbook of Wireless Networks and Mobile Computing. 2002; p. 1-22.
9. Manet. IIT Bombay. Date Accessed: 23/12/2000: Available from: www.it.iitb.ac.in/sri/talks/manet.ppt.
10. Dube R, Rais CD, Wang KY, Tripathi SK. University of Maryland. Signal-Stability Based Adapting Routing (SSA) for Ad-Hoc Mobile Network. IEEE Personal Communications 1997. Crossref
11. Example of TORA operations. www.cs.ucr.edu/krish/lec8.ppt.
12. Signal stability – based adaptive routing protocol. Date Accessed: 26/11/2016: Available from: https://de.wikipedia.org/wiki/Signal_Stability-based_Adaptive_Routing_Protocol#/media/File:SSA1.GIF.
13. Abdelhaq M, Hassan R, Alsaqour R. Using dendritic cell algorithm to detect the resource consumption attack over MANET. Software Engineering and Computer Systems. 2011. Crossref
14. Agrawal S, Jain S, Sharma S. A survey of routing attacks and security measures in mobile ad-hoc networks. 2011.
15. Nadeem, Howarth M. Adaptive intrusion detection & prevention of denial of service attacks in MANETs. International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly 2009. Crossref
16. Wang D, Hu M, Zhi H. A survey of secure routing in ad hoc networks. The Ninth International Conference on Web-Age Information Management. 2008. Crossref
17. Abdelhaq M, Alsaqour R, Al-Hubaishi M, Alahdal T, Uddin M. The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing. International Journal of Network Security. 2014; 16(5):376-81.