YOUNG INTELLECTUAL
ESTABLISHED AUGUST - 2024
BILINGUAL (TELUGU AND ENGLISH)- QUARTERLY - MULTIDISCIPLINARY -
OPEN ACCESS - E - JOURNAL FOR DEGREE COLLEGE STUDENTS AND FACULTY
Published by : D. Yeswanth Reddy, c/o. Tirupathi Reddy, 16-183/1, Ramakrishna Colony,
Mylavaram, NTR District, Andhra Pradesh. Pin : 521230, mail ID : yeswanth.devarapalli@gmail.com
3

Simulation of wormhole and grey hole attacks using Python

N.Venkatadri
Lecturer, Department of Computer Science, Dr.Lakireddy Hanimireddy, Govt. Degree College, Mylavaram, NTR District.

Abstract:

Mobile Ad Hoc Network (MANET) is a type of wireless computer network where each device acts as a host and a router. This kind of network is easily prone to many kinds of threats. Due to this, network performance will be degraded. In emergency situations where deployment of physical infrastructure is no possible there deployment of MANET is easy.

In this paper, we used on-demand routing protocol TORA to analyze the network performance under wormhole and grey hole attacks. These attacks are kind of Denial of Serve (DoS) attack. Many other researchers and academicians generally use other on-demand protocols like DSR, AODV to carry out their inventions. Bu in this work we use Temporally Ordered Routing Algorithm (TORA) for analyzing performance metrics like Delay, Energy, Throughput and PDR. Python is more suitable for simulation and performance measurement because python has plenty of built in features than other Network Simulators.

Keywords:

Wireless Network, Routing , TORA, Performance Metrics, Python.

YOUNG INTELLECTUAL
BILINGUAL (TELUGU AND ENGLISH)- QUARTERLY - MULTIDISCIPLINARY -
OPEN ACCESS - E - JOURNAL FOR DEGREE COLLEGE STUDENTS AND FACULTY

1. INTRODUCTION

In wireless & mobile networks, MANET (Mobile Ad-hoc Network) provides promising solutions to actual problems. It is a collaborative collection of different wireless nodes that make a short-term network without the assistance of any self-contained infrastructure or central administration. The nodes in the network can join and leave at any time and change positions within the network. In this network nodes can directly communicate with any other node laying in their radio ranges [1]. Each and every node in the network is able to act as both host and router [1].

MANET consists of different characteristics like dynamic topology, bandwidth-limited connections, energy constraints, and limited protection at the physical level. Because of its great adaptability, it is widely used in various sets of applications like military operations, emergency or disaster relief operations, business meetings, and mine site operations. By Nature, these types of networks are fit for the case where either no stable infrastructure exists or arranging a network is not possible. The figure (1) shows the basic architecture of MANET [2].

For diffusion of information packets, some kind of protocol is required to form the routing decisions. Routing protocols can be categorized into three types as shown in figure [2][3].

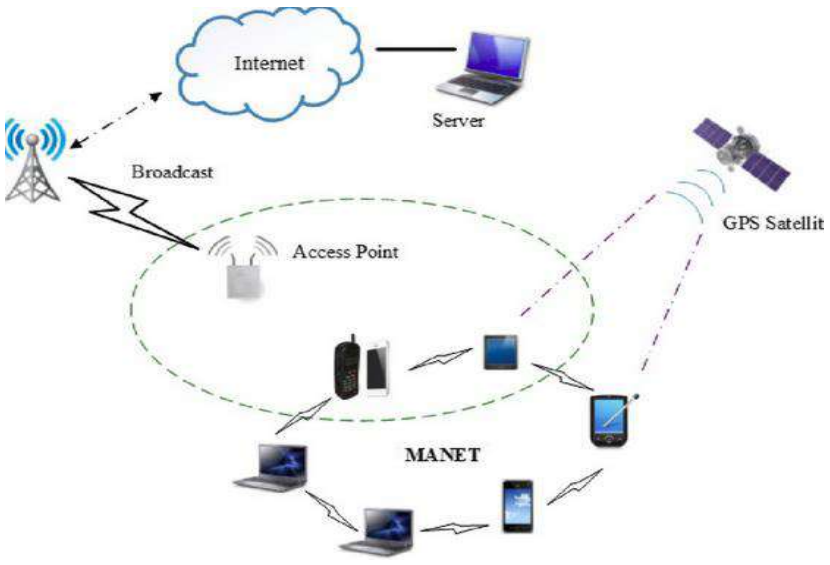


Figure 1: Basic Architecture of MANET

Proactive Protocols: These are also named as table-driven routing protocols. To transmit data from one node to a different node these protocols use pre-calculated routes. Every node in the network required to maintain a routing table containing the routing data of every other node. Routing tables will be reorganized periodically as the network topology is changed this leads to routing overhead and wastage of memory.

Reactive Protocols: These are also named as on-demand routing protocols. A path finding method is formed only when one node needs to transmits some data to another node. In this, every node not required to record information regarding each further node in the network. These protocols take more latency for the route set-up process.

Hybrid Protocols: These protocols combine the characteristics of proactive protocols and reactive protocols.

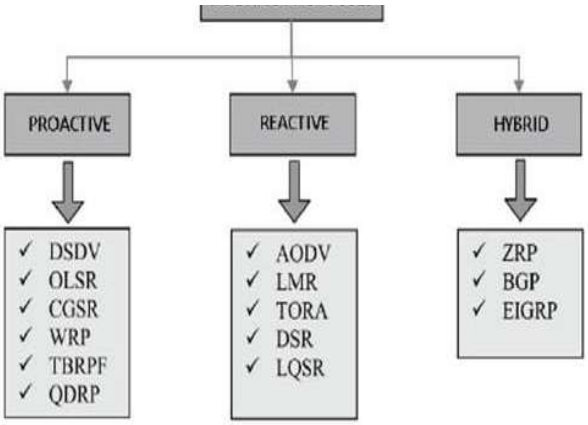


Figure 1. Types of Routing Protocols [2]

GRAY-HOLE ATTACK

A gray-hole attack is wing of black-hole attack used to bluff the source and monitoring the system by unfair forwarding. Here, attackers uses selective data packet dropping method to behave as genuine node and try to participate into full communication. Gray-hole nasty node participate into route discovery process and update the source route cache/ routing table as shortest path. Afterwards, source node always consider nasty node as next hop node and forward packet to same node. Malicious node accepts all the incoming packets but drop on arbitrary basis. The complete phenomena create hardiness against detection and prevention method because harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature [4].

Wormhole attacks: In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called „wormhole link". They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network [5].

2. Related Work

Rutvij H. Jhaveri[8] present the survey of a DoS (Denial-ofService) attacks on the network layer namely Grayhole attack, Wormhole attack, Blackhole attack and which are the serious threats for MANETs. also discuss few suggested solutions to detect and prevent these attacks. MANETs have unique characteristics like, limited resources, dynamic topology, lack of centralized administration and wireless radio medium; as a result, they are not protected to the several kinds of the attacks in several layers of the protocol stack. All node in a MANET is proficient of acting as arouter. Routing is one of the features having various security concerns[6].

Mukesh Kumar [7] a technique is proposed that can prevent a specific kind of DDoS attack named flood attack which Disable IP Broadcast. MANET has not clear line of the protection so it is accessible to the both malicious attackers and legitimate network users. In the presence of hostile nodes, one of the highest Tasks in MANET is to design the robust secure solution that can prevent MANET from various DDoS attacks. Separate mechanisms have been proposed applying several cryptographic methods to countermeasures these attacks against MANET.

3. Methodology

Most of the researchers are working with well known on-demand routing protocols DSR and AODV but in this work I used TORA to perform simulations under worm hole and grey hole attacks . Python is very useful to implement any on-demand protocol to find the performance of the protocol under normal conditions and under the presence of DoS attacks. In my previous papers I implemented black hole attack using TORA with NS2 in this also I use the same trust route mechanism to analyze TORA for various performance metrics.

Trust-Evaluation

Trust-evaluation performed at a node depends on the following factors-the position of the evaluating node, type of event and the context in which the evaluation is invoked. Note that the evaluating node may be source or destination or an intermediate node. Event types include route request, route reply, route error and data flow event. The context is a combination of decision policies [8].

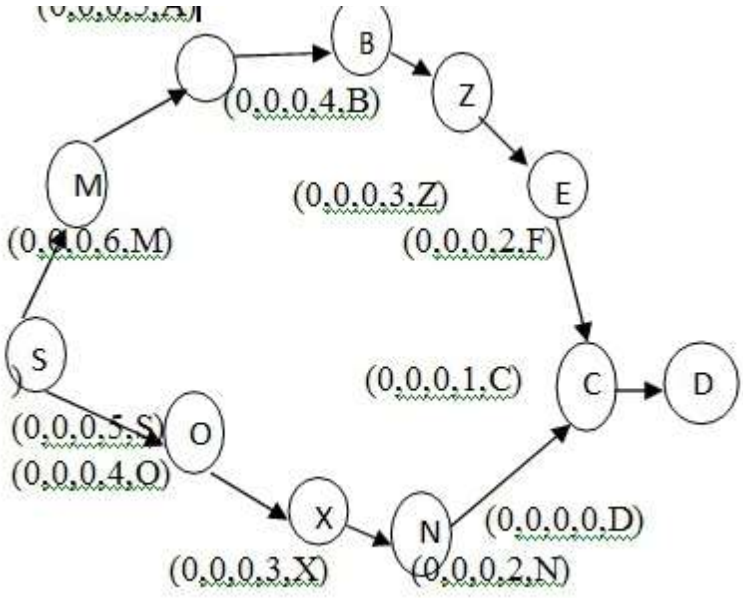


Figure1: RouteCreation inTORA

Let us consider the above scenario, in which intermediate node N has to decide whether to forward or ignore a received packet. Initially, the trust evaluation module extracts the nodes from the route, the position of extracted nodes are follows source, destination, prev-hop and next-hop. Now the trust-valuation module

calls the trust-over-reputation module to compute the trust for nodes.The trust-evaluation module then computes trust for packet by combining the trust values received for nodes S, D, X, and C from the trust-over-reputation module.

$$T_N\ Packet(t_a+1) = \sum I_{N\text{-}list} * T_N\ Node_{list}(t_a)$$

$$\sum I_{N\text{-}list} = 1$$

equation (1)

Where

List={source, destination, prev-hop and next-hop}

The trust computation $T_N\ Packet_k(t_a+1)$ for a packet k, by node N at time t_a+1 $I_{N\text{-}list}$ defines the importance given to the trust of an extracted node depending on the nodes' position in the route. Finally, the trust-evaluation module forwards the packet only if the trust for the packet is at least the threshold-limit (Δ) [8].

Trust-over-reputation

As mentioned in the trust-evaluation, the trust-over-reputation module computes trust for a node. Recall that trust is derived from the reputation ratings which represent the quantified evidence.

$$T_N\ Node_i(t_a+1) = \sum U_{N\text{-}i}^{type} * {}_{N\text{-}I}\ type(t_a)$$

$$\sum U_{N\text{-}i}^{type} = 1$$

Equation (2).

Where,

$T_N Node_i(t_a+1)$ represents N's trust for I at time t_a+1

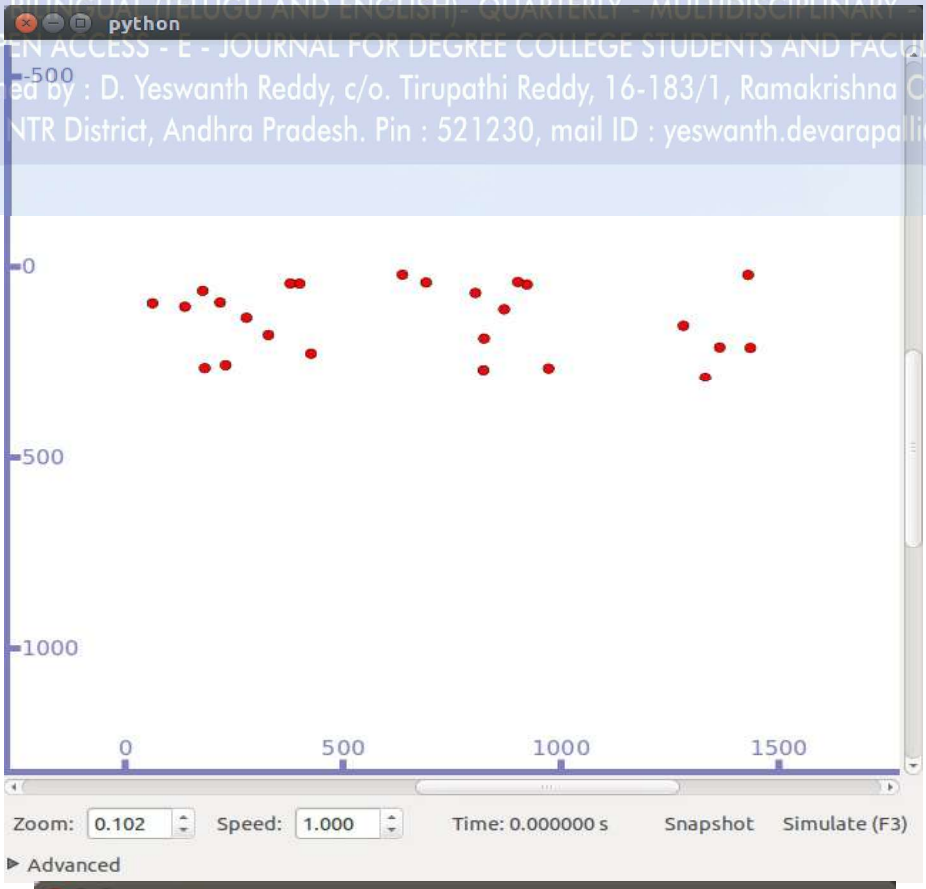
${}_{N\text{-}I}\ type(t_a)$ refers to the N'sreputation of type 'r' for 'I' at time t_a

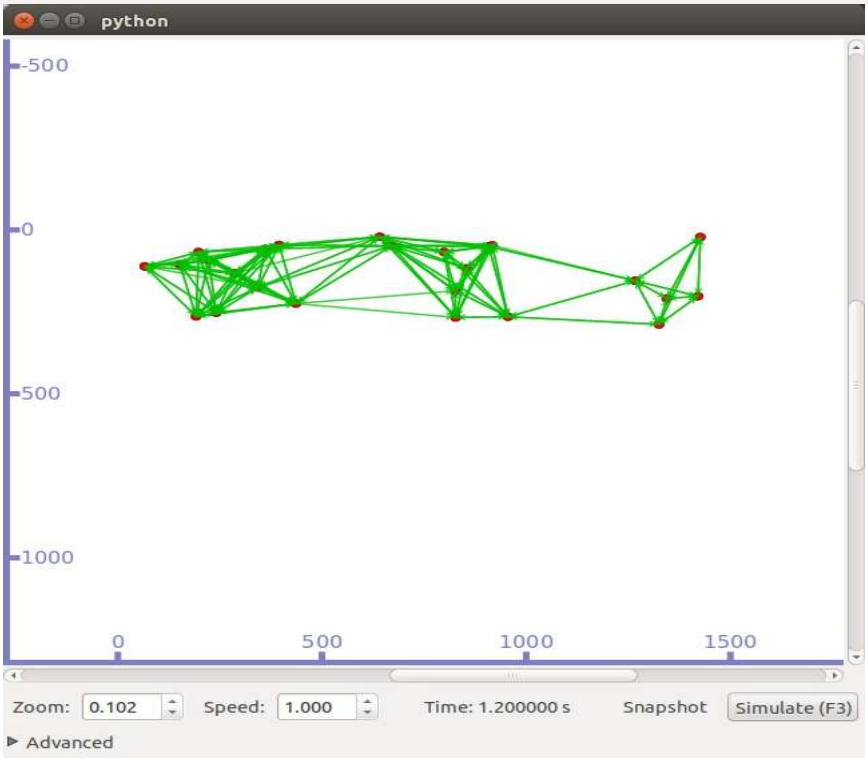
$U_{N\text{-}i}^{type}$ signifies the utility ofeach reputation type during the trust computation for a node.

Type={direct, observed orrecommended reputation}.

Now we detail the steps involved in capturing, quantifications and representing the evidence as reputation ratings by using the capture-reputation and reputation-evaluation modules [4].

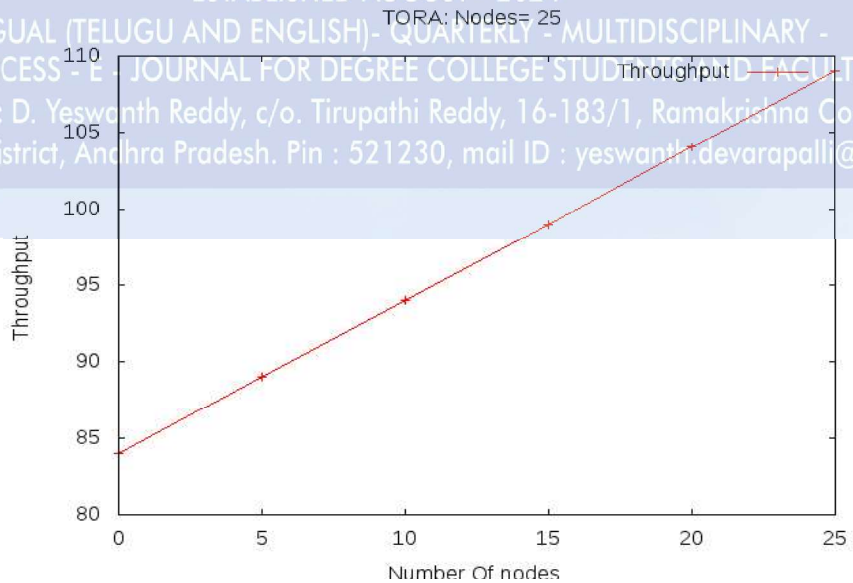
YOUNG INTELLECTUAL
ESTABLISHED AUGUST - 2024
BILINGUAL (TELUGU AND ENGLISH)- QUARTERLY - MULTIDISCIPLINARY
OPEN ACCESS - E - JOURNAL FOR DEGREE COLLEGE STUDENTS AND FACULTY
Published by : D. Yeswanth Reddy, c/o. Tirupathi Reddy, 16-183/1, Ramakrishna Colony,
Mylavaram, NTR District, Andhra Pradesh. Pin : 521230, mail ID : yeswanth.devarapalli@gmail.com



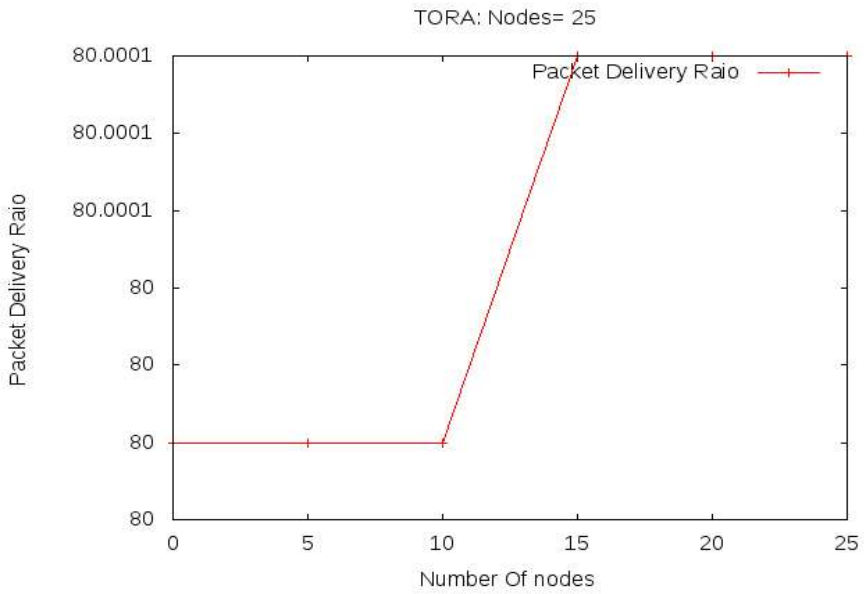


YOUNG INTELLECTUAL
ESTABLISHED AUGUST - 2024
BILINGUAL (TELUGU AND ENGLISH)- QUARTERLY - MULTIDISCIPLINARY -
OPEN ACCESS - E - JOURNAL FOR DEGREE COLLEGE STUDENTS AND FACULTY
Published by : D. Yeswanth Reddy, c/o. Tirupathi Reddy, 16-183/1, Ramakrishna Colony,
Mylavaram, NTR District, Andhra Pradesh. Pin : 521230, mail ID : yeswanth.devarapalli@gmail.com

4. Simulation Results



As shown in the above figure the performance of the TORA increases as increase in simulation time.



As shown in the above figure, up to simulation time 10 secons, there is no change in the packet delivery ratio. After 10 seconds there we can observe abnormal change in PDR.

Conclusions

In this paper, we analyzed on-demand routing protocol TORA under worm hole and grey hole attacks suing Python programming language. The performance metrics we considered for out investigations are PDR, and Throughput.

REFERENCES

1. Mohammed M. Alani , "MANET security: A survey" 10.1109/ICCSCE.2014.7072781, 2014 IEEE.

2. SubramaniyanSenthilkumar, Johnson William, SubramaniyanKarthikeyan"A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique" in EURASIP Journal on Wireless Communications and Networking,205, Springer, DOI 10.1186/1687-1499-2014-205, 2014.

3.SanamNagendram, K. Ramchand H Rao," Parametric Estimation of Various Protocols for Routing In Manets",International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7, May, 2019.

[4] Rupali Sharma, "Gray-hole Attack in Mobile Ad-hoc Networks : A Survey", Rupali Sharma / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1457-1460.

[5]. Rutvij H. Jhaveri1 and Ashish D. Patel etal, "MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[6] Mamta Jha, Rajesh Singh S.,S. Dhakad," A Review: Denial of Service Attack MANET", IJSRD - International Journal for Scientific Research & Development| Vol. 3, Issue 01, 2015 | ISSN (online): 2321-0613.

[7]. Rutvij H. Jhaveri, in Second International Conference on "Advanced Computing & Communication Technologies", 2012.

[8]. N.Venkatadri and K Ramesh Reddy, "Detection and Prevention of Black Hole Attack using Trust- TORA", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.5, No.2, April 2015.