Dynamic Recognition of Malicious Routers

Hemanth S
Assistant Professor, Vel Tech University, Chennai, India
G Sudhakar
Software Engineer,TCS, Hyderabad, India
Chaitanya K
Software Engineer, Infosys, Hyderabad, India

Abstract

In this paper, we considered the problem of detecting whether a compromised router is maliciously dropping packets in the network. Packet dropping from a network of two reasons those is congestion route and malicious attacks. In particular, we are concerned with a simple yet effective attack in which a router selectively drops packets destined for some victim. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion canproduce the same effect. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities.Previous detection protocols have tried to address this problem with a user-defined threshold value but in this method we added the buffer size dynamically, because of this congestion get removed as possible. Goal is to differentiate the packet dropping of congestion route from the malicious attacks with protocol X. The proposed method includes broadcasting and also used for large networks.

Keywords: *Malicious attacks, compromise routers, DoS attacks, Broadcasting.*

1. Introduction

The Internet is on the mode of turning the worldwide communication network, and then desires to offer various services with assured quality for all kinds of applications [1]. From last 20 years have been seen an enormous [2] increase of the Internet. Several services of socio-economic interest in societytoday, many of them involving critical considerations, are offered over the Internet. Their exposure to the comprehensive networking environment leaves them susceptible to dissimilar types of computer attacks, amongst which DoS (Denial of Service) attacks, due to their high alike catastrophic index, are decorated [3].

Among these incidents, Denial-of-Service (DoS) attacks cause one of the mostserious threats to internet service applications [2]. Such attacks are not simple theoretical curiosities, but they are vigorously employed in practice. Attackers have continually confirmed their ability to compromise routers, through combinations of social engineering and exploitation of weak passwords or latent software vulnerabilities [4], [5], [6]. This paper addresses the increasing security problem regarding malicious attacks of a particular router in a network.

Ambiguity around packet losses can be resolved [7] using traffic validation protocol, absence of packet be seen as malicious or benign. Three approaches to detect the packet loss are:

1) Static threshold
2) Traffic modeling
3) Traffic measurement.

In the every approach mentioned above packet loss is due to malicious intent and as our proposed model focuses on malicious packet loss, it satisfies the all approaches.

In this paper, we developed a protocol x that dynamically infers the precise number of congestive packet losses that will occur as previous work carried out statically. In the previous work the congestion ambiguity is removed by retransmitting the packets but in our proposed we removed the congestion ambiguity by setting the queue size unlimited. In the previous work link state routing protocol is used to find the shortest path between source and destination for packet transmission in the proposed work we considered distance vector routing protocol. By using the link state routing protocol flooding occurs by using distance vector routing protocol this flooding can be eliminated. As there are number of algorithms in distance vector routing [9] protocol but for efficient purpose we considered DIJKSTRA's algorithm. In this method we broadcast the packet, and neighbor to the router may receive the packet where in previous work unicast is considered. In previous work the proposed protocol was evaluated on small experimental network but in our work we extended for large networks also.

2. Background

Previous works related to the malicious attacks worked [10] on the uni-casting of packets to the redirectors. Broadcasting is not supported, it is not taking [6] into consideration about network parameters like network size, network delay, dynamic routing. Instead, we have focused on the less well-appreciated threat of an attacker subverting the packet forwarding process on a compromised router. Such an attack presents a wide set of opportunities including DoS, surveillance, man-in-the-middle attacks, replay and insertion attacks, and so on. Moreover, most of these attacks can be trivially implemented via the existing command shell languages in commodity routers.

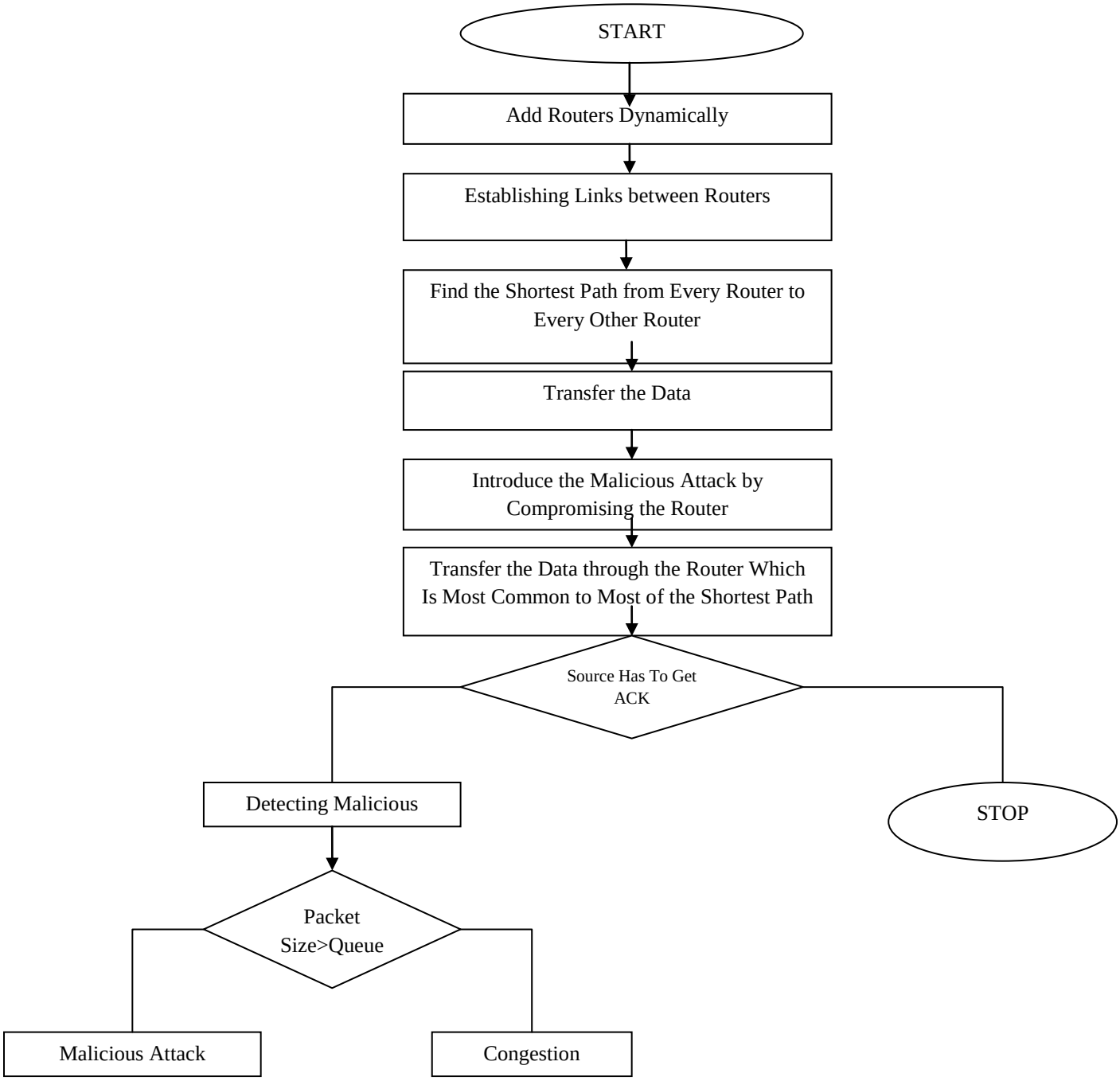
The term routing encapsulates two tasks. These tasks are deciding the paths for data transferred and sending the packets on these paths. The routing is a process that is a function carried out at layer 3 of the OSI reference model. The routing algorithm decides the output line to transfer the incoming packets. The routing algorithms are based [8] on the routing protocol that uses metrics to assess whether a particular path is the optimal path available for transfer of the data packets. The metrics used for evaluating the paths are bandwidth, delay and reliability. The routing algorithms use these protocols to determine an optimal path from the source to the destination. The routing tables maintain all the information related to routing. There are various routing algorithms and depending on these routing algorithms, the information stored in the routing table varies. Every router has its own routing table and it fills this table with the required information to calculate the optimal path between the source router and the destination router.

3. Proposed Model

Packets are forwarded from every router to every other router based on the shortest path via distance vector routing protocol such as DIJKSTRA's algorithm. There is a less possibility to drop the packets due to congestion because in this model every router maintains a queue with some size without limitation. In this model packets are forwarded in broadcast manner to its neighbors. This model can be used to biggest networks also.

3.1 Methodology

The following flow chart shows detecting the malicious intent or congestion route:



The steps in the flow chart are described as:

1. Build a network using direct point to point links between routers.
2. Add routers dynamically in a network and links also.
3. Finding the shortest paths from every router to every other router.
4. Maintains a Queue with some size at every router for stores the incoming packets.
5. Transfers the data through packets from some sources to particular router.
6. Introduce the malicious attacks by compromising node.
7. Transfer the data through the router which is common to most of the shortest paths.
8. If source router will get the Acknowledgement from the destination router then stop.
9. Otherwise detect the malicious intent.
10. At that particular router, consider the sizes of incoming packets and Queue.
11. If PS is less than Q, then the loss can be considered as malicious attack.
12. Otherwise loss can be considered due to Congestion.

PS = Incoming packets size.
Q = Queue size.

The following are different modules in the algorithm:

3.2 Network Model

Consider a network that having individual homogeneous routers connected via point to point links using digraph.

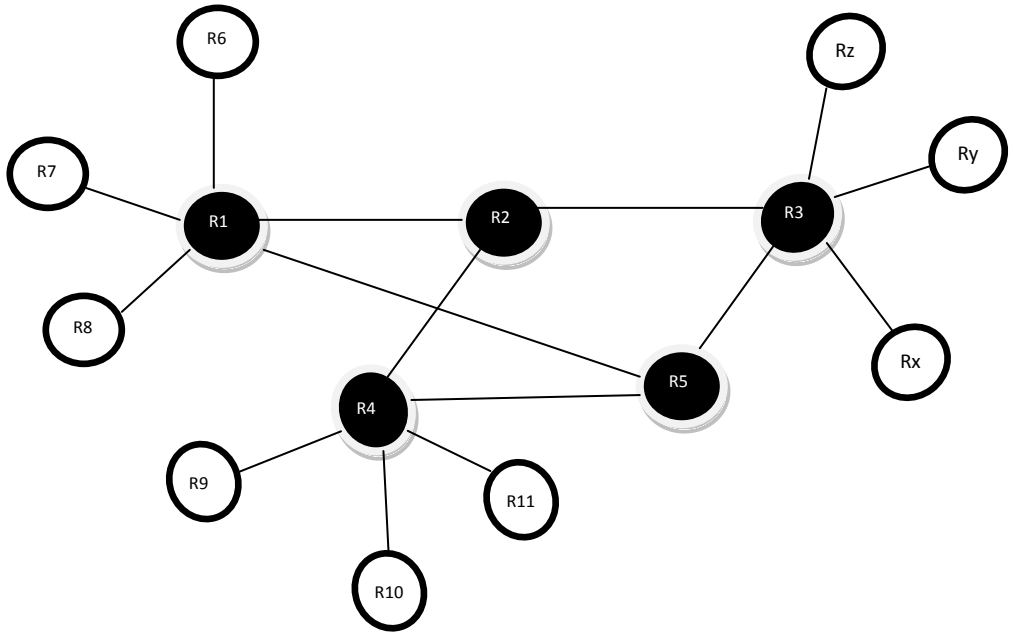


Figure 1: Representation of Network Model

The figure 1 shows the graph of network model using direct point to point links between the routers. That is represented as G= (V, E), where V is the set of homogeneous routers and E is the set of directed links among routers. We can add the routers and links among routers on demand.

In network model routers are connected using direct point to point links in a star topology manner. These star topologies of different networks are connected using different LANs.
We define a path to be a sequence **<R_1,R_2,…….,R_n>** of adjacent routers. A path defines a sequence of routers a packet can follow. In this path first router is source and the last router is sink both routers are called terminal routers. If a network consists of a single path **<R_1,R_2,R_3,R_4>** , then **<R_1,R_2>** and **<R_2,R_3>** are two path segments. But **<R_2,R_4>** is not a path segment because **R_2** and **R_4** are not adjacent.

3.3 Protocol X

Packet dropping can be detected using Protocol X. Initially every router will maintain a Queue with some size. If the packet can be transferred from a source to some destination, then many redirectors can be participated. If more than one router will feed the data into the routers Queue, then packets may be forwarded or dropped. If that router is compromised then it will be blocked and drop the packets or it will misguide the route. In that case calculate the incoming packet size with the Queue size. If Queue size is less than the incoming packet size at a particular time't', then find out that whether the packet is dropped due to congestion, or due to malicious attack. Protocol x detects the traffic faulty routers by validating the Queue of each output interface for each router. Given the buffer size and the rate at which traffic enters and exits a Queue, the behavior of the Queue is determined. If the actual behavior is deviates then the failures occurred.

In traffic validation (TV): what information is collected about traffic and how it is used to determine that a router has been compromised.

Consider the Queue Q in a router r associated with the output interface of link <R, r_d>. the neighbor routers r_{s1} ,r_{s2} ,r_{s3} ,……, r_{sn} feed the data into Q.

$T_{info}(r, Q_{dir}, \pi, t)$ is the traffic information collected by router r that traversed path segment π over the time interval t. Q_{dir} is either Q_{in} or Q_{out} .

Q_{in} is traffic into Q.

Q_{out} is traffic out of Q.

At an abstract level we represent the traffic, a validation mechanism associated with Q, as a predicate TV (Q, q_{pred}(t), S,D), where

q_{pred}(t) is the predicated state of Q at time t.

S= {$\forall i \in \{1,2,\ldots,n\}$: $T_{info}(r_s, Q_{in}, <r_s, r, r_d>, t)$} is a set of information coming into Q as collected by neighbor routers.

D = $T_{info}(r_d, Q_{out}, <r, r_d>, t)$ is the traffic information outgoing traffic from Q collected at router r_d.

TV(Q, $q_{pred}(t)$,S,D) evaluates to false if and only if r was traffic faulty and dropped packets maliciously during time t. T_{info} is represented in different ways. We use three-tuple for each packet traversing Q includes: fp – fingerprint of packet, ps – packet size and the time that

The packet entered or exited based on Q_{dir} , i.e. Q_{in} or Q_{out}.

Practically, the behavior of queue cannot be predicted with complete accuracy. Let $q_{act}(t)$ is the actual length at time t . Based on central limit theorem [11], our assumption tells us that the error, $\mathbf{q_{error} = q_{act} - q_{pred}}$, can be approximated with normal distribution. This suggests the packet loss tests by using this formula.

i.e. $\mathbf{C_{single}}$= Prob (fp is maliciously dropped).

=prob(there is enough space in the queue to buffer fp).

=prob($q_{act} + ps \leq q_{limit}$).

=prob($X + q_{pred}(ts) + ps \leq q_{limit}$). Where X is a random variable $X= q_{act}(ts) - q_{pred}(ts)$.

=prob ($X \leq q_{limit} - q_{pred} - ps$).

=prob($Y \leq (q_{limit} - q_{pred}(ts) - ps - \mu)/\sigma$). Where $Y=(X - \mu)/\sigma$.

=prob($Y \leq y_1$). Where $Y_1= (q_{limit} - q_{pred}(ts) - ps - \mu)/\sigma$.

$\mathbf{C_{single}}= (1+erf(y_{1/\sqrt{2}}))/ 2$. erf is the error function.

3.4 Router Configuration

Every router is having IP address and port number and these are maintained by routing table. Router always must be in listening mode for network sniffing. It will maintain a packet Queue to store incoming packets. Here assume that size of the Queue is fixed. The role of the router is any one of the source, redirector or destination. In general redirectors will be compromised.

3.4.1 ROUTING TABLE

A routing table is a document stored in the router or a network computer. The routing table is stored in the form of a database or is simply a file stored in the router. The data entered in the routing table is referred to when the best possible path to transfer information across two computers in a network is to be determined. The two classifications, viz., static and dynamic routing, are based on the way in which the routing tables are updated every time they are used. The routers in which the data is stored and updated manually are called static routers. On the other hand, the routers, in which the information is changed dynamically, by the router itself, are referred to as dynamic routers.

Cost matrix of routing table:

Distance between two routers is calculated using IP-Address of routers in real networks .In this case we have to use co-ordinates of the routers which are located at different places using Maps.

999.0	999.0	999.0	321.22	999.0
999.0	999.0	999.0	259.16	999.0
999.0	999.0	999.0	307.38	999.0
321.22	259.16	307.38	999.0	218.66
999.0	999.0	999.0	999.0	999.0

Above matrix shows the distances between every router to every other router. This matrix is used for maintains a routing table internally at every router. It is used for selecting a convenient route for transmitting the packet. Based on the adjacent matrix a cost matrix was constructed using the (x,y) coordinates of any two router, then distance would be obtained if both coordinates are known.

THREAT MODEL

Initially find out the shortest path from every router to every other router, later consider the router having maximum incoming sources, then we try to compromise that router, so that there is chance to evaluate the performance of protocol x with effective manner. Our model is easily extended to address other attacks discussed in [12,13,14], such as packet modification or reordering. In a topology any router can harm the incoming packets due to virus attacks, in this case that router changes the data format or encrypt the actual data format and sends that data to the destination router without compromising the router. A threat model is to introduce malicious attacks at a particular router; the following figure shows a sample threat model.

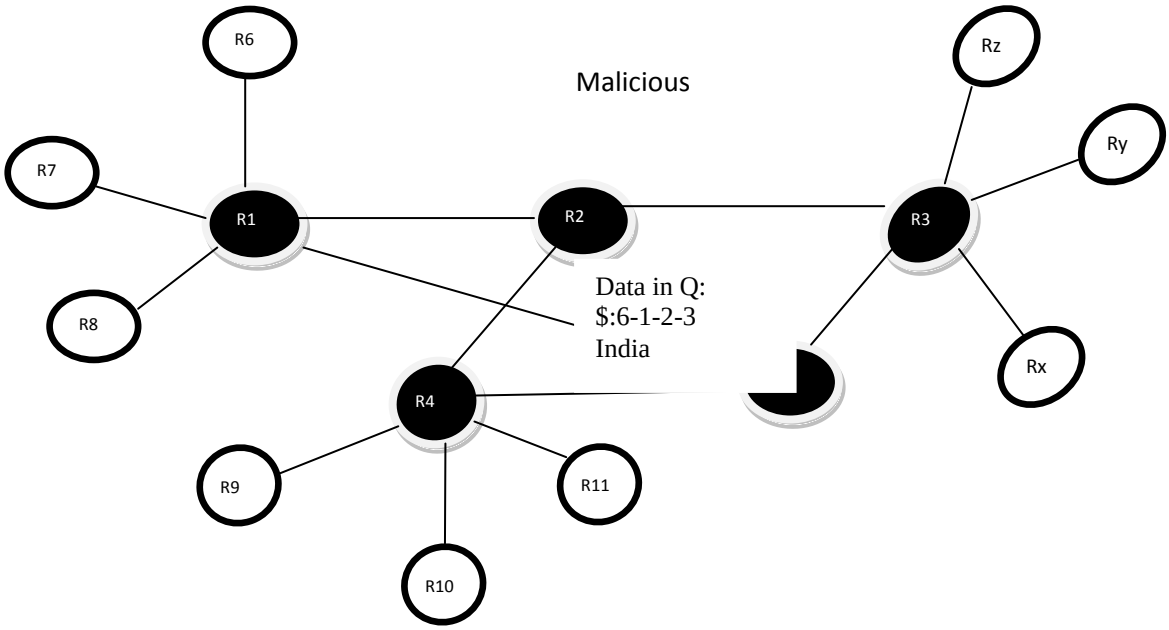


Figure 2: Threat model showing data at malicious router

In figure 2 R2 router represent malicious, if the data comes to that malicious router the further continuation of data is not possible.

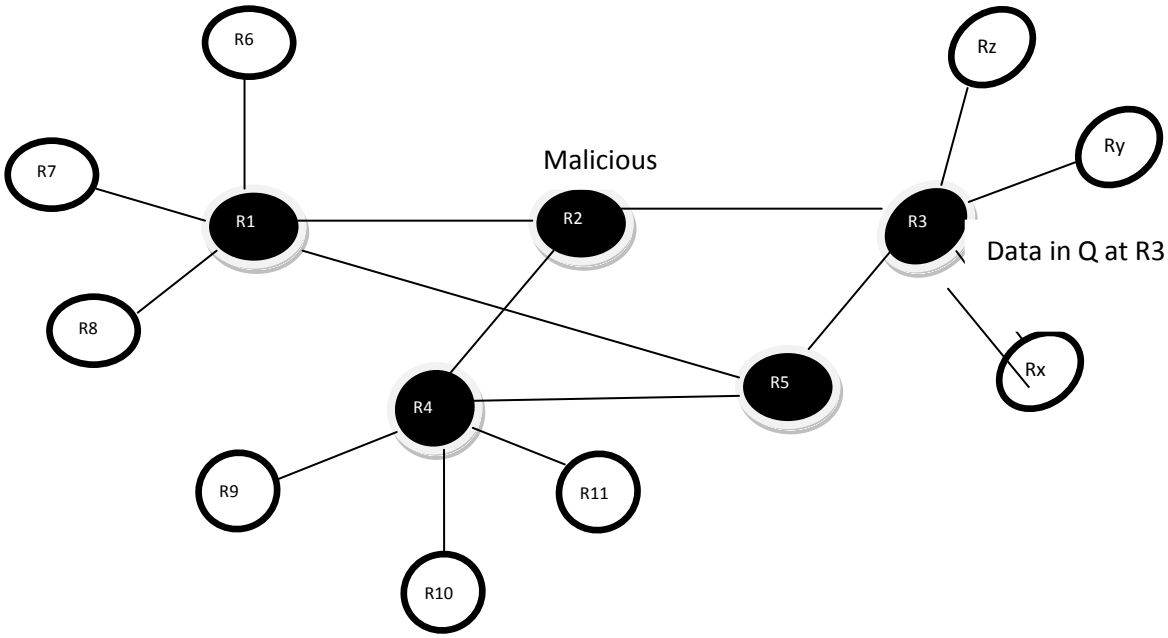


Figure 3: Threat model showing that no data is received from malicious router.

Figure 3 represents that the queue of the router that has receive data from malicious router is empty. If the malicious router appears in the shortest path, then another shortest path needed to be identified to send the packet to destination.

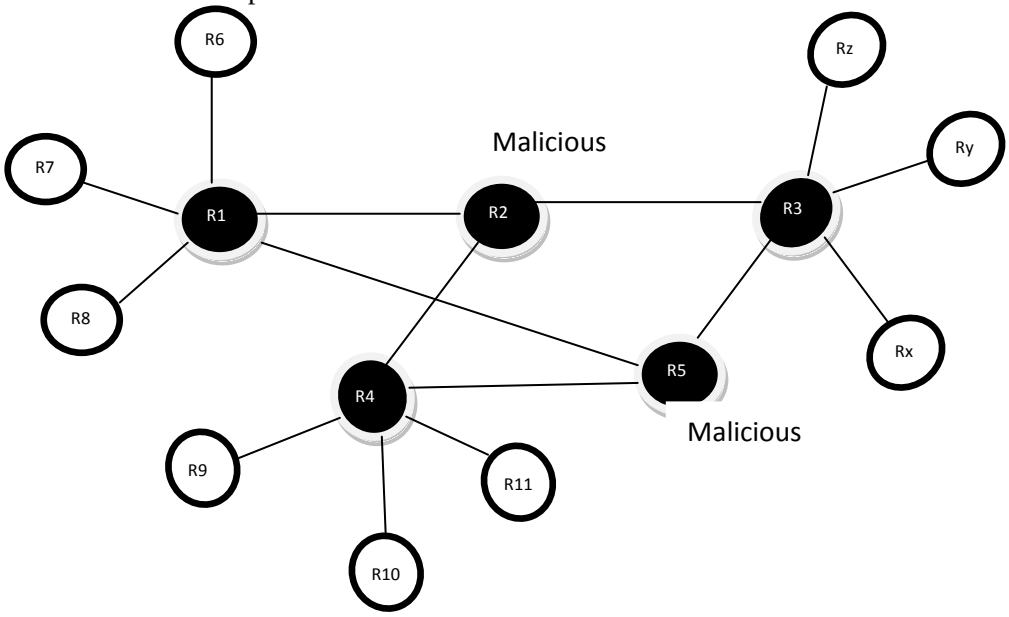


Figure 4: Shows the number of malicious routers in largest networks.

Figure 4 explains in smallest network we have to find the shortest paths from every router to every other router, from those shortest paths select the router which is most common router in those paths. In this network only one router is able to do the compromise for malicious intent. But

in large networks there are many smallest networks which are interconnected with LAN or WAN , for this network we are able to do more than one router as a compromise for malicious intent, why because if only one router is compromised in one LAN then the routers which are in other LANs will be transmitting the packets between the routers. That's why we have to do more than one router as compromise for malicious intent.

BROADCASTING

The previous work does not support broadcasting, it only supports [8] unicasting. Unicasting means communication provides from one source to one destination. But our work supports Broadcasting. Broadcasting provides communication from one host or router to it all neighbor hosts or routers. For this, in our work we have to find the neighbors using adjacency matrix. Using this broadcasting we have to send the data or packet at a time to its all neighbors.

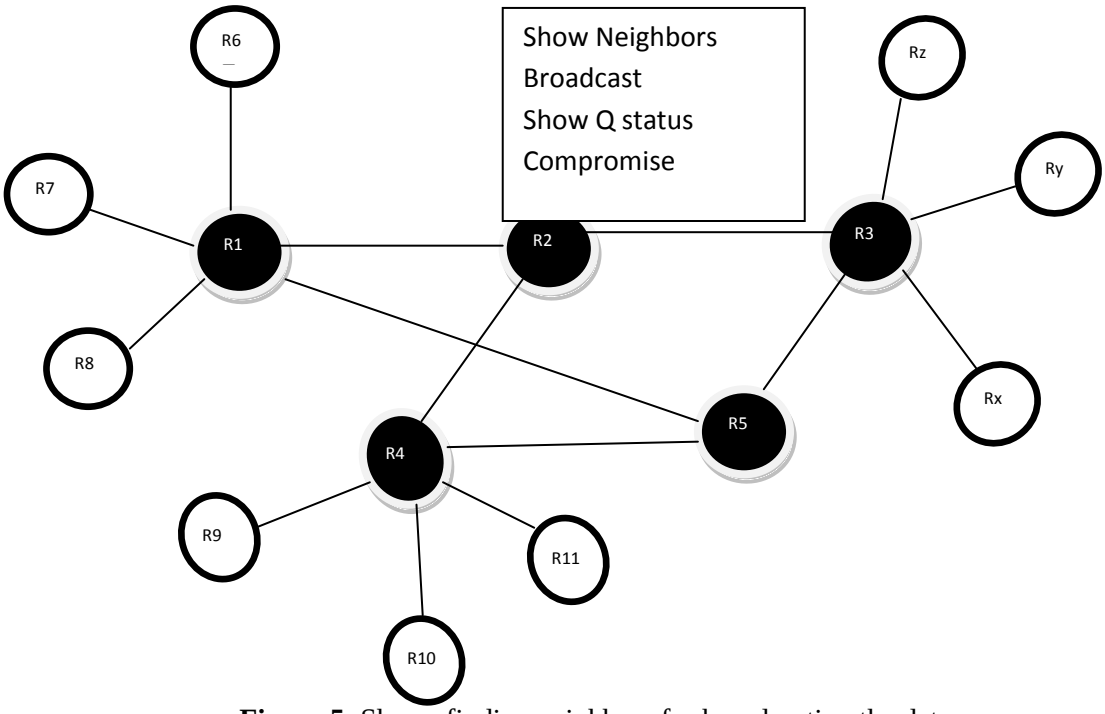


Figure 5: Shows finding neighbors for broadcasting the data.

From figure 5 says:

Show neighbors: find the neighbors for a particular router.

Broadcast: to send the data to its neighbors.

Show Q status: for storing the packets at a router.

Compromise: for malicious attack.

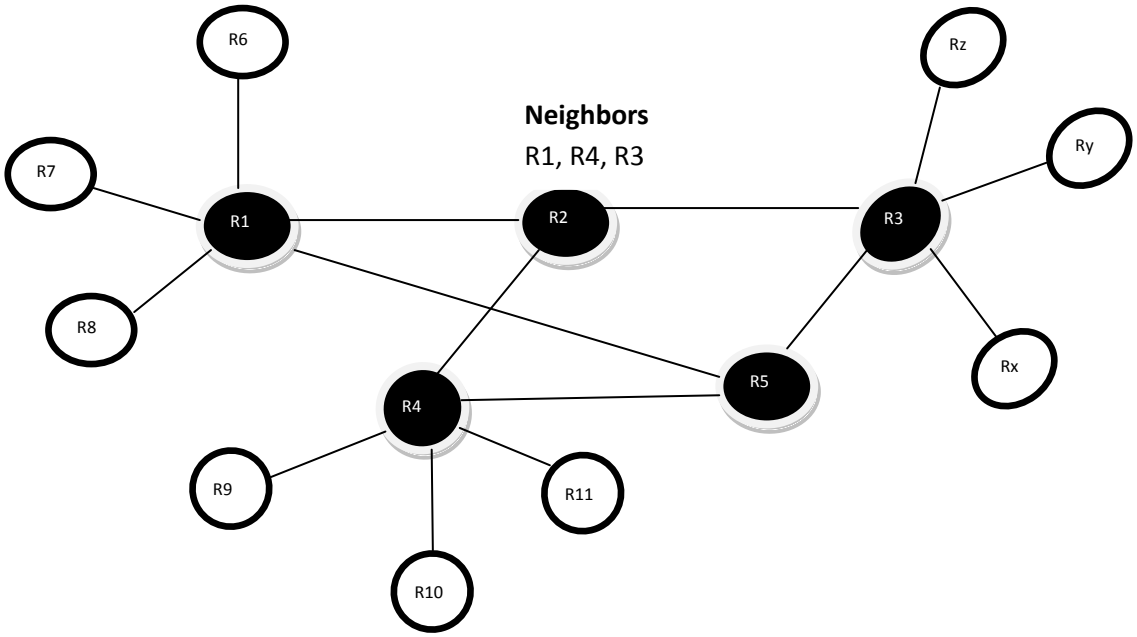


Figure 6: Shows neighbors of any particular router.

The figure 6 shows that neighbors of the particular router, the neighboros are identified using the adjacent matrix.

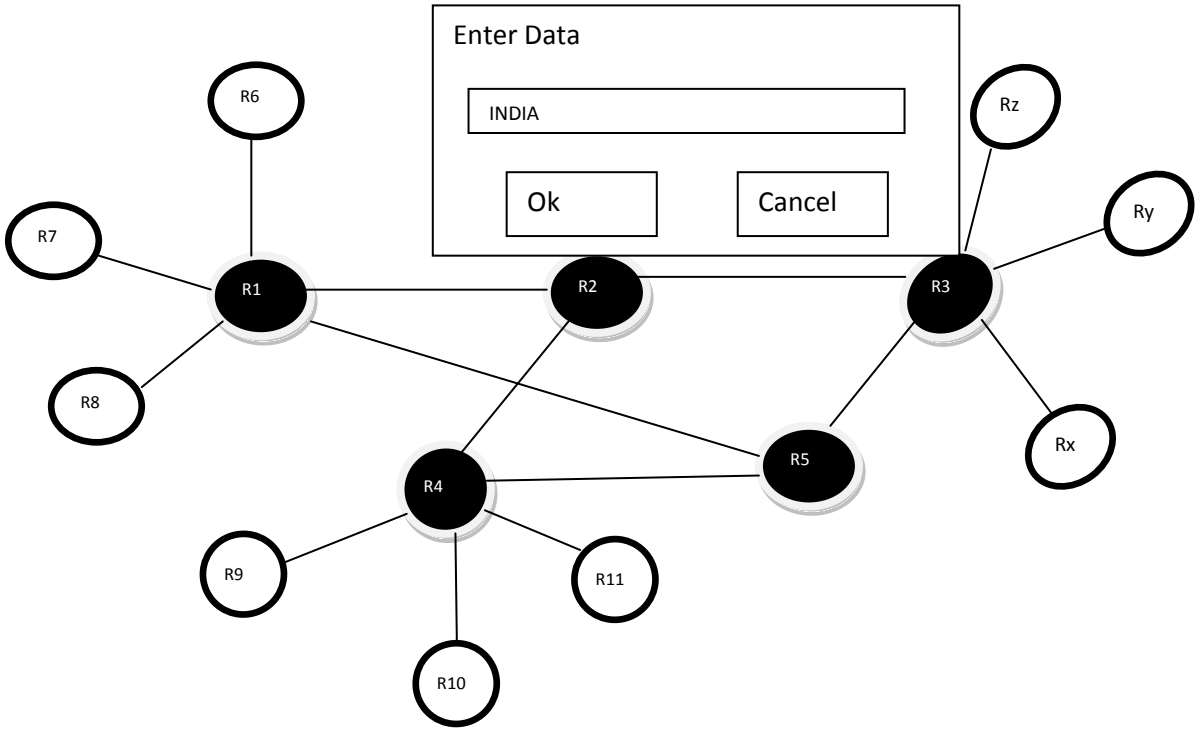


Figure 7: shows the broadcast message

Every router maintains the neighbor's information for broadcasting the message and figure 7 shows the message to be broadcasted.

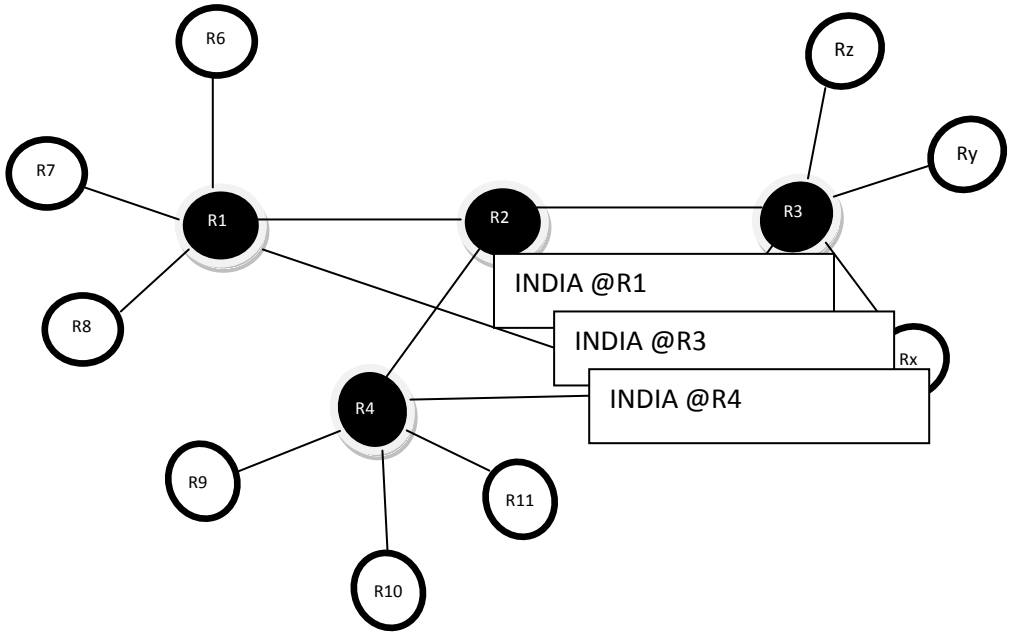


Figure 8: Receive the broadcast message from a router to its all neighbors**.**

Figure 8 show that router R2 broadcasts the data to R1, R3, R4.

The main advantage of proposed model was fast detection, this fast detection can be done by finding the shortest paths among all the routers and prior knowledge about the size of the queue will allow differentiating malicious attack from route congestion quickly. In general malicious attack will be detected if the data size exceeds the queue size of the router. Until that movement we can't imagine that it may be malicious attack. So, the proposed model will wait for an acknowledgement from the receiver. If the ultimate receiver can't acknowledge in mean time, this model will vary the routing path about malicious attacks. If it founds then immediately it will divert the traffic through safety path.

CONCLUSION

In this proposed scheme we consider the scalability of the network i.e. dynamically add the new routers and provide communication with existing network.

We also consider a possibility of attacks in two ways.

1. By making the router which is participating in highest transmission path as compromised router.

2. Based on the selection of any router to compromise.

In both of the situations, if the data is transmitted through that compromised router, further then it cannot forward the packets to the next node in the transmission path.

According to our assumptions there are some refinements are also possible for future work.

Future work:

1. Consideration of mobility of routers. In the sense routers were placed dynamically, but routers cannot move i.e. static.
2. By passing of data transfer from the malicious router after detection i.e., in the transmission path if the malicious router is occurred then find out the alternate path to send the packet to the destination.

3. Intimation about malicious router to the neighboring routers i.e., in our model malicious router can also broadcasting the packets to its neighbors.

REFERENCES

1. P.Owezarski, "On the Impact of DoS Attacks on Internet Traffic Characteristics and QoS" 14th International conference Computer communication and networks, ICCN proceedings,2005.
2. Aye, M.M, "A Queuing Analysis of Tolerating for Denial-of-Service (DoS) Attacks with a Proxy Network" International conference on computer engineering and technology, 2009.
3. D.Pino, M.A.Perez, P.Garcia, P.Fernandez, C.P.Suarez, "Towards self-organizing maps based Computational Intelligent System for denial of Service Attacks Detection", 14th international conference on Intelligent engineering systems, 2010.
4. X.Ao, "Report on DIMACS workshop on large scale Internet Attacks." 2003.
5. K.J.Houle, G.M.Weaver, "Trends in Denial of Service Attack Technology" 2001.
6. C.Labovitz, A.Ahuja, M.Bailey, "Shining Light on Dark Address space" 2001.
7. A.T.Mizrak, Y.C.Cheng, K.Marzullo, S.Savage, "Detecting and isolating Malicious Routers" IEEE transactions on Dependable and secure computing, Vol 3, Iss. 3, pg:230-244, 2006.
8. W.Khan, LB.Le, E.Modiano, "Autonomous routing algorithms for networks with wide-spread failures" Military communications conference 2009.
9. D.C.Lee, "Proof of a modified Dijkstra's algorithm for computing shortest bundle delay in networks with deterministically time-varying links" IEEE transactions of communications letters, Vol:10, iss:10, pg:734-736, 2006
10. A.T.Mizrak, S.Savage, K.Marzullo, "Detecting Malicious Packet Losses" IEEE Transactions on Parallel and distributed systems, Vol.20,No.2,2009.
11. R.J.Larsen, M.L.Marx, "Introduction to Mathematical Statistics and its Applications", 4th edition, Prentice Hall 2005.
12. S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure Border Gateway Protocol (Secure-BGP)," IEEE Journal on Selected Areas inCommunications, vol. 18, no. 4, pp. 582–592, Apr. 2000.
13. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in The 8th ACM Int.Conf. on MobiCom, Sep 2002.
14. S. Cheung, "An efficient message authentication scheme for link state routing," in *ACSAC*, 1997, pp. 90–98.