Asian Journal of Information Technology 5(6): 657-665, 2006

An Efficient Method for Faulty Update Detection in Distance Vector Protocols

[1]R. Sabitha and [2]S.K. Srivatsa
[1]Sathyabama Institute of Science and Technology,
Jeppiaar Nagar, Chennai, 60019, Tamilnadu, India
[2]Madras Institute of Technology, Madras, India

Abstract: The importance of securing the Internet has grown rapidly due to series of attacks that shut down some of the world's most high profile Web sites, including Amazon and Yahoo. Most of the research concerning on securing the Internet focuses on protecting the data using techniques such as authentication and encryption rather than securing the Internet Infrastructure. This leads to many instances where the network infrastructure has been compromised by malicious adversaries. Thus, network infrastructure security is clearly a pressing need, since the attacks have the potential for affecting the entire Internet infrastructure, which may have serious consequences on the security and economic vitality of society. Among different network threats, the routing table poisoning attack is the most devasting and least researched topic which needs immediate research attention. In this paper, we develop an efficient method for faulty update detection of routing table in distance vector protocols. The method is able to detect faulty updates in the routing table, by calculating the predecessor information from the routing table at sending node and comparing it with that of the receiving node.

Key words: Link state protocols, distance vector protocols, routing information, secure routing protocols, routing security

INTRODUCTION

The Internet has been witnessing enormous growth over the last several years. Until now, the main research focus has been on improving the performance and scalability of the Internet. Although performance and scalability have their place in Internet research, the enormity of the Internet has forced the research community to look at its dependability aspects. The Internet, like any other product, is prone to failures and researchers have started to realize the importance of dependable communication in order to tolerate device failures (e.g., link and node failures) and to overcome the presence of malicious users or "hackers". The importance of securing the Internet has grown rapidly due to series of attacks that shut down some of the world's most high profile Web sites, including Amazon and Yahoo. Several such attacks have also been reported in CERT advisories[1]. These attacks, coupled with the growing fear of cyber terrorism, have made researchers think of possible means and methods to protect users from adversaries.

The majority of work on routing protocols for the Internet has proceeded in two main directions: distance vector protocols (e.g. RIP[2] and link state protocols (e.g. OSPF[3]). In distance vector protocols, each node sends the distance (in hops) to its neighbor nodes. In case of link state protocols, each node periodically floods the state of its links to all the nodes in the network. Distance vector protocols are less robust than the link vector protocols. This is because each router computes the routes based on the computation done in the other routes in the network. Distance vector protocols can be subjected to: (i) Link Attacks, where an adversary gets access to a link in the network and changes the distance vector update passing through the link and (ii) Router Attacks, where a malicious router (source or intermediate) changes the distance vector information. It is to be noted that such attacks are also possible in case of link state protocols. However, the attacks are much more lethal in case of distance vector because of the implicit trust relationship among the routers. In this study, we concentrate on router attacks in distance vector protocols.

RELATED WORK

The solution proposed for detecting distance vector attacks can be broadly classified into three categories.

Routing information techniques: In this type of techniques[4,5] digital signatures are used to detect malicious distance vector updates in case of link attacks. However, these schemes are unable to detect router attacks.

Corresponding Author: R. Sabitha, Sathyabama Institute of Science and Technology, Jeppiaar Nagar, Channai, 60019, Tamilnadu, India

Intrusion detection techniques: These techniques[6] are used to detect the anomalous behavior in the routers, assuming that intrusion detection devices are available in the network.

Routing protocol techniques: In this type of techniques, detection capability is built into the routing protocol itself. In Cisco White Papers[7], several techniques have been mentioned to detect bad /malicious routers. However, though the techniques are able to prevent looping, malicious distance vector updates cannot be detected using these techniques. One method of validating the integrity of the distance vector update, in presence of router attacks, is by using a technique called the "Consistency Check" (CC)[8]. In this technique, each router, in addition to the hop length information, also sends the predecessor information to its neighbors. In this paper, we adopt the principle of routing protocol techniques.

NETWORK MODEL

A network is modeled as an undirected connected graph where nodes in the graph are routers and links are sub-networks (subnets). Each link has two lengths or costs associated with it one in each direction. A network is defined by an IP address range and can either be a single link-level network (often called a local/metropolitan/wide area network or LAN/MAN/WAN), or, recursively, another set of networks sharing an IP address space. Such a set of interconnected networks is often referred to as an internet. Each node (router) and link (subnet) in the graph has a unique id. Each link has a cost, which can vary in time but is always positive. The distance between two nodes is the sum of the link costs in the path of least cost, or shortest path, between them. Fig. 1 shows a map of an example internet and Fig. 2 shows a schematic of

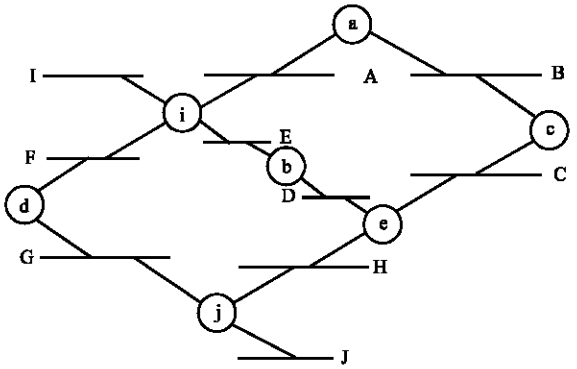

Fig. 1: Map of example internet

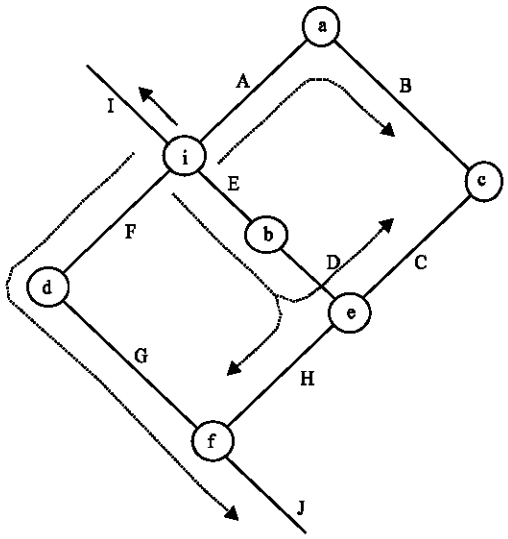

Fig. 2: Schematics of example Internet

the same network with arrowed lines drawn to show selected routes for use later in the paper. In these drawings lower case letters identify routers and upper case letters identify subnets.

ROUTING

Routing is the main process used by Internet hosts to deliver packets. Internet uses a hop-by-hop routing model, which means that each host or router that handles a packet examines the Destination Address in the IP header, computes the next hop that will bring the packet one step closer to its destination and delivers the packet to the next hop, where the process is repeated. To make this work, two things are needed. First, routing tables must match destination addresses with next hops. Second, routing protocols must determine the contents of these Tables.

Routing is a means of discovering paths in computer networks along which information can be sent. Routing directs forwarding, the passing of logically addressed packets from their source toward their ultimate destination through intermediary nodes, called routers. Forwarding is usually directed by routing tables within the routers, which maintain a record of the best routes to various network destination locations; thus, the construction of routing tables is the primary goal of routing.

Small networks may involve hand configuration of routing tables. Large networks involve complex topologies and may change constantly, making the

constructing of routing tables very problematic. Dynamic routing attempts to solve this problem by constructing routing tables automatically, based on information carried by routing protocols and allow the network to be nearly autonomous in avoiding network failures and blockages. Dynamic routing dominates the Internet. However, the configuration of the routing protocols often requires a skilled touch; it should not be supposed that networking technology has developed to the point where routing is a completely automatic operation.

In packet switched networks, such as the Internet, the data is split up into packets, each labeled with the complete destination address and routed individually. Circuit switched networks, such as the voice telephone network, also perform routing, to find paths for circuits, such as telephone calls, over which large amounts of data can be sent without continually repeating the complete destination address.

If a designated path is no longer available, the existing nodes must determine an alternate route to use to get their data to its destination. This is usually accomplished through the use of two routing protocols namely distance vector protocols and link state protocols.

Routing tables can take many forms, but here is a simple model that can explain most Internet routing. Each entry in a routing table has at least two fields - IP Address Prefix and Next Hop. The Next Hop is the IP address of another host or router that is directly reachable via an Ethernet, serial link, or some other physical connection. The IP Address Prefix specifies a set of destinations for which the routing entry is valid for. In order to be in this set, the beginning of the destination IP address must match the IP Address Prefix, which can have from 0 to 32 significant bits. For example, a IP Address Prefix of 128.8.0.0/16 would match any IP Destination Address of the form 128.8.X.X.

TYPES OF PROTOCOLS

Routing protocols support the delivery of packets, in spite of changes in network topology and usage patterns, by dynamically configuring the routing tables maintained at Routers in internets. The compromise of this routing function in an internet can lead to the denial of network service, the disclosure or modification of sensitive routing information, the disclosure of network traffic, or the inaccurate accounting of network resource usage.

The primary focus of security services in routing protocols is the protection of routing information from threats to the integrity, authenticity and in some cases the confidentiality of routing updates. The specific strategies and mechanisms most effective at securing this information depend on a number of attributes of routing protocols that determine specially what information is exchanged and which set of principles interact in the progression of a routing computation.

Routing protocols are method that routers can use to communicate information to each other. In other words, one router can share with other router information about the routes it knows.

The majority of work on routing protocols for the Internet has proceeded in two main directions: distance vector protocols (e.g., RIP[2]) and link state protocols (e.g., OSPF[3]).Since both link state and distance vector protocols exhibit different characteristics in state information and their exchange and route computation, they are exposed to different types of vulnerabilities, which provide unique sets of challenges for securing them. In a link state protocol, each node periodically floods the state of its links to all the nodes in the network. After receiving the link state updates (called a link state advertisement, LSA in OSPF), each router computes the shortest path tree (SPT) with itself as the root of the tree. In distance vector protocol, each node sends its routing distances (in the form of distance vector packet) to its neighbors. The description below describes a very simple distance-vector routing protocol:

In the first stage, the router makes a list of which networks it can reach and how many hops it will cost. In the outset this will be the two or more networks to which this router is connected. The number of hops for these networks will be 1. This Table is called a routing table.

Periodically (typically every 30 sec) the routing table is shared with other routers on each of the connected networks via some specified inter-router protocol. These routers will add 1 to every hop-count in the table, as it associates a hop cost of 1 for reaching the router that sent the table. This information is just shared in-between physically connected routers ("neighbors"), so routers on other networks are not reached by the new routing tables yet.

A new routing table is constructed based on the directly configured network interfaces, as before, with the addition of the new information received from other routers. The hop-count is used as a cost measure for each path. The table also contains a column stating which router offered this hop count, so that the router knows who is next in line for reaching a certain network.

Bad routing paths are then purged from the new routing table. If two identical paths to the same network exist, only the one with the smallest hop-count is kept. When the new table has been cleaned up, it may be used to replace the existing routing table used for packet forwarding.

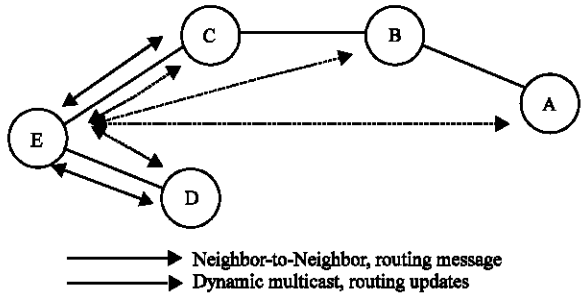

Fig. 3: Classes of routing information

Destination	Cost	Next Hop
1	0	-
2	1	1

Fig. 4: Routing table in distance vector protocol

The new routing table is then communicated to all neighbors of this router. This way the routing information will spread and eventually all routers know the routing path to each network, which router it shall use to reach this network and to which router it shall route next. Figure 3 shows the classes of Routing Information. Figure 4 shows the routing table in Distance Vector Protocol.

The countermeasures presented here assume that intruders can position themselves at any point in the network through which all traffic of interest flows and that an intruder has the capability to fabricate, replay, monitor, modify, or delete any of this traffic. Interpreting this description for a routing environment, the following general classes of intruders are identified:

Masquerading routers: A masquerading router is a node that successfully forges an authorized router's identity. This can be accomplished using the IP spoofing or Source routing attacks.

Subverted routers: A subverted router is one that is caused to violate the routing protocols or to inappropriately claim authority for network resources. This typically occurs due to bugs in the routing code, mistakes in the configuration information, or by causing a router to load unauthorized software or configuration information. The specifics of how this can occur depend on the design and configuration of the router.

Unauthorized routers: An unauthorized router is a node that is not authorized as a router that manages to circumvent any access control mechanisms in place and participates in the routing dialog and computation. How this is achieved depends on the design and configuration of existing authentication and access control mechanisms.

Subverted links: A subverted link is a channel controlled via access to the physical medium (e.g. network cable-plant, the \air-waves", or the electronics used to access them), or via compromise of the protocols underlying the routing protocol in a manner that allows control of the channel (e.g., the TCP session hijacking attack).

SECURING DISTANCE VECTOR PROTOCOLS

In distance vector protocols, if a malicious router creates a wrong distance Vector and sends it to all its neighbors, the neighbors accept the update since there is no way to validate it. Since the router itself is malicious, standard techniques like digital signatures do not work. The methods that are already existing are unable to detect router attacks when the malicious router changes the update intelligently, keeping the network topology in mind.

In this paper we propose an efficient method that deals with threats to the flow of routing traffic and does not address threats to the flow of data traffic Attacks are described in terms of different classes of internet nodes, including authorized routers and intruders. Authorized routers are those nodes intended by the authoritative network administrator to participate in the routing dialog and computation.

MATERIALS AND METHODS

The proposed work uses RIPv2 for transferring the routing tables. This will provide authentication to the packet that is sent. The structure of the packet that is sent for updating to the neighboring router includes two parts namely Header and Data. Header of packet contains time of packet sending, sequence number of the packet to the corresponding router and some control information. Data part of the packet contains routing table of the router and calculated predecessor information.

While receiving the packet, the receiving router should authenticate the packet that is provided by RIPv2 protocol. After this process, time interval and sequence number of the packet is checked. Then the predecessor information is calculated and it is checked with that of the received one. If the value matches, then the router allows the packet to update the routing information. Figure 5 shows the message format:

Message format consists of two parts, one is header and another is update part. The header part of the packet contains sequence number, time of the packet sent, etc.The update part contains some security data and routing table's data such as sequence number of the packet, sending time of the packet and predecessor information. This message is sent by RIPv2 protocol. It

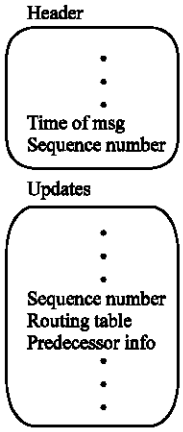

Fig. 5: Message formate

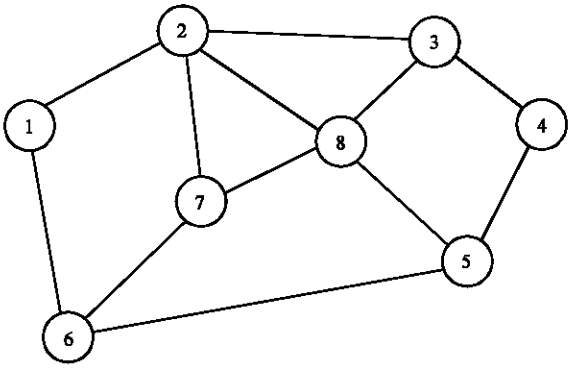

Fig. 6: Example network

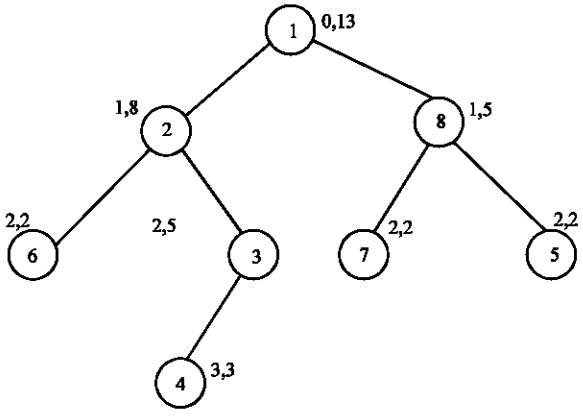

Fig. 7: Predecessor information calculation

provides authentication to the packet. Once the packet is authenticated by the router, the packet is allowed to the router for further updation. If authentication fails, the packet is not allowed to the router.

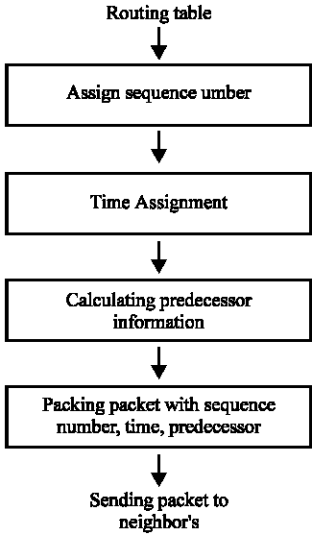

Fig. 8: Design to send the packet

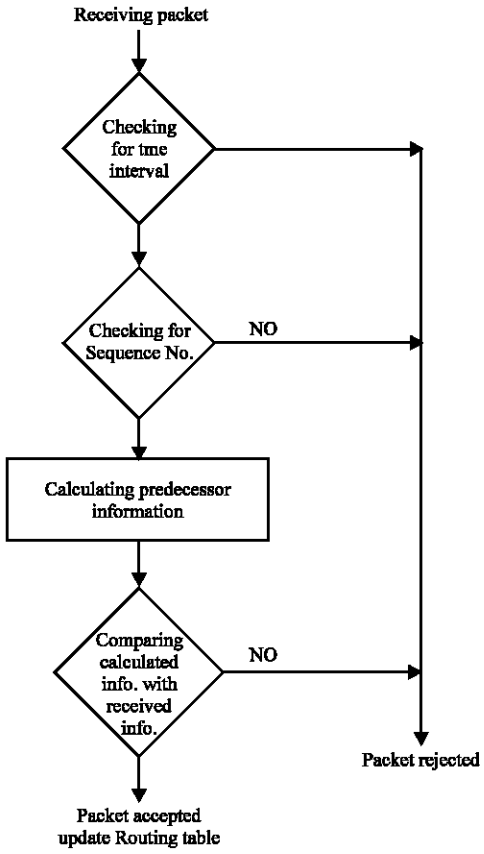

Fig. 9: Design for updating routing table from received packet

The different steps included in the proposed method are:

Sending node

Assigning Sequence number to the packet
Assigning Time Message
Calculating Predecessor Information
Sending the packet

Receving node

Sequence Number Checking
Time Interval Checking
Comparing Predecessor Information

Sending node

Assigning Sequence number: A sequence number is included in each routing message. This sequence number is initialized to zero on the initialization of a newly booted router and is incremented with each message. On detection of a skipped or repeated sequence number, a reset of the session is forced by the re-initialization of the routing process. The size of this sequence number is made large enough to minimize the chance of it is cycling back to zero. However, in the event that it does, the session is reset by the re-initialization of the routing process. This protects against the deletion and replay of routing messages.

Assigning timing information: To send packet to neighboring router, the router must add or assign the messaging time. This Time message is for checking at the receiver and for checking the Time interval between previous packet received from the corresponding router time and current packet time.

Calculating predecessor information: The predecessor information of the router that is needed to share routing information to neighboring router is calculated. This calculated predecessor information is added to packet with some security information. This information is useful at the receiver side for comparison. The predecessor is calculated as follows.Consider the following example network Fig. 6.

To calculate the predecessor information for a routing table, construct a tree from the routing table; identify the node which has cost zero (0) as root node of the tree. The routing table is invalid if there is more than one entry which has cost zero (0). Find the next level of cost in which destination entry is child to previous node and also check whether the next node is previous node or not. If not attach the node to corresponding previous node as child.

Table 1 shows the routing table for the router 1 and the corresponding predecessor information table and Fig. 7 shows the Tree construction using the Predecessor information

Table 1: Routing table and the predecessor information table for router 1

Routing table	Predecessor information table
Dest	ID
Cost	PRED
Next	1
Hop	0
1	2
0	1
1	3
2	2
1	4
1	3
3	5
2	8
2	6
4	2
3	7
3	8
5	8
2	1
8	
6	
2	
2	
7	
2	
8	
8	
1	
1	

The Sequence number, Time value and the calculated predecessor information are added to the packet along with some security information. This information is useful at the receiver side to compare the received information. The design for sending the packet for updating at the receiver is depicted in the Fig. 8.

Receiving node

Time interval checking: When the packet is received from router for updating,. The time interval of the packet is checked. The time interval between previous packet received from the corresponding router and time interval of the current packet from the same router is checked. The time interval should between 30 sec to 130 sec, if not the received packet is rejected.

Sequence number checking: After the time interval checking is over, router should check the sequence number of the packet. The sequence number of the previous packet from the corresponding router is compared with the received one. Once the sequence number is exactly greater than the previous packet's sequence number by one, the next step is performed.

Calculating predecessor information: Once the sequence number checking is successfully completed, the predecessor information is calculated for comparison. Calculation of the predecessor information is same as that of the sender side.

Comparing predecessors information: After calculating the predecessor information, the calculated information is compared with the received predecessor information. Comparing each field of the predecessor information table must be same. If any field differs from the received one, that packet will be rejected. Once the comparison is successful, the router allows the packet to update the router table. Updating the Routing Table

Before updating the routing table, router must change or save the time of packet to the previous packet time arrival and then router must change the sequence number of previous packet sequence number.

After the time and sequence number is updated, packet will allow updating the routing table of router. The design for updating the routing table is depicted in the Fig. 9.

SIMULATION STUDIES

In order to evaluate the performance of the work, simulation studies have been performed. The following figures show the result of the studies.

Figure 10 shows the example network and the routing table. This is sent from router 1 to router 2.

Figure 11 depicts that the packet sent form router 1 to router 3 is invalid. This checking is done at the receiving node by performing the different steps of the proposed method.

Figure 12 depicts that the packet sent form router 1 to router 2 is accepted at the receiving node by performing the different checking steps as explained by the proposed method.

Figure 13 shows that the packet is rejected after performing the steps and comparing the control information of the packet with that of the received packet.

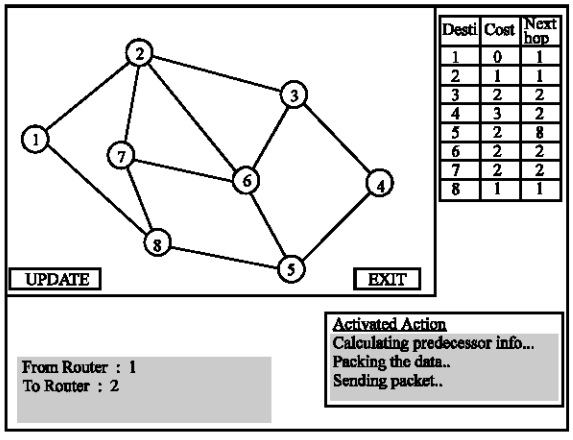

Fig. 10: Packet sent from Router 1 to Router 2

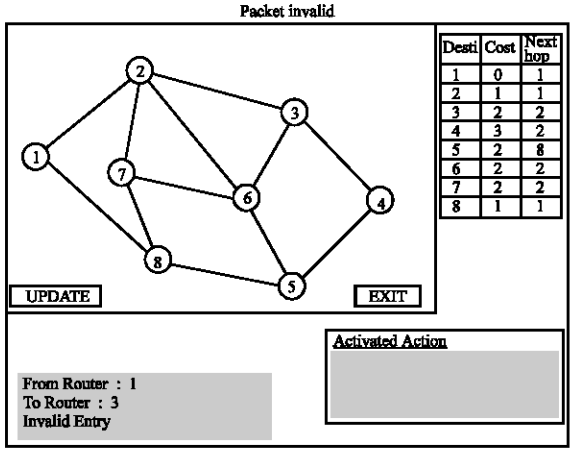

Fig. 11: Checking for packet invalid

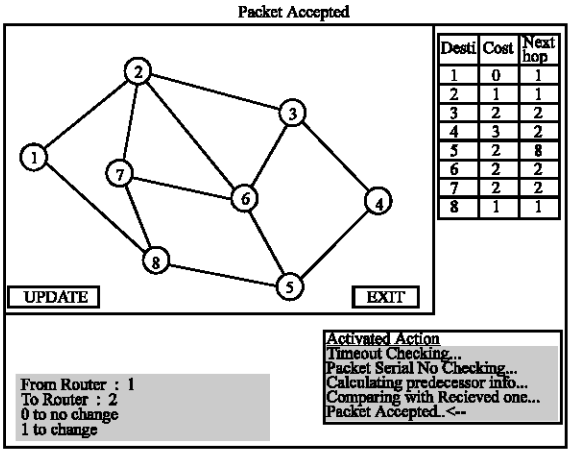

Fig. 12: Packet Acceptance at the receiving node

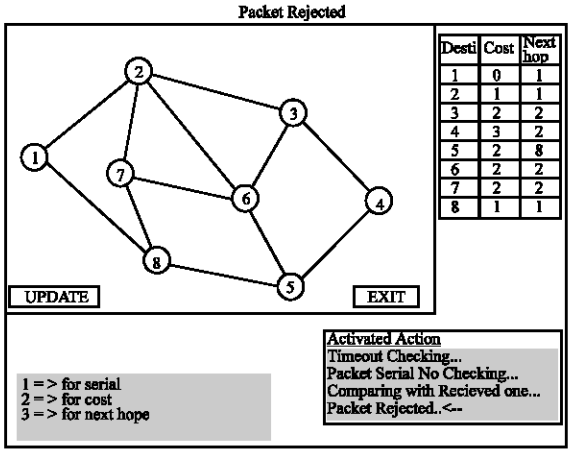

Fig. 13: Rejection of the packet

PERFORMANCE MEASURES

We choose the following metrics for measuring the proposed method: 1) Packet Delivery Rate, the ratio of total number of data packets received and the total number of data packets sent in application level. 2) Network Overhead, the ratio of total number of routing related transmissions and the total number of packet transmissions. Each packet hop is counted as one transmission.3) Detection Probability. The simulation results are shown in the form of graphs and all the graphs are plotted from the data averaged from the 5 runs.

Packet delivery rate: The graph (Fig. 14) of packet delivery rate has two curves and they represent the throughput of standard method and proposed method with the extension of calculating predecessor information. The graph demonstrates that the proposed method always performs better than the standard method. We can infer from the graph that packet delivery rate sometimes is higher when there are a higher percentage of malicious nodes than when there is a lower percentage of malicious nodes. As explained in[9], the randomness of NS-2 results in this effect due to the fact that route replies may arrive at nodes in different orders in different runs. Therefore, a node may choose a path with malicious nodes in one run but choose a good path in another run.

Overhead: As shown in Fig. 15 the routing overhead is increased significantly when the network topology changes faster or there is a high percentage of malicious nodes in the network. In both the scenarios, large number of messages has to be sent out to finalize the node states. The overhead can be reduced dramatically if messages piggyback normal data packets.

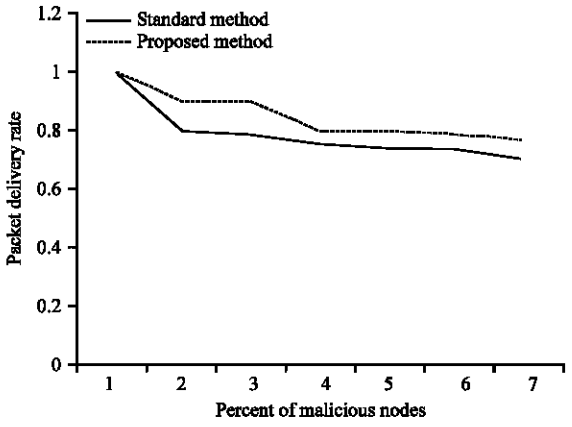

Fig. 14: Network throughput

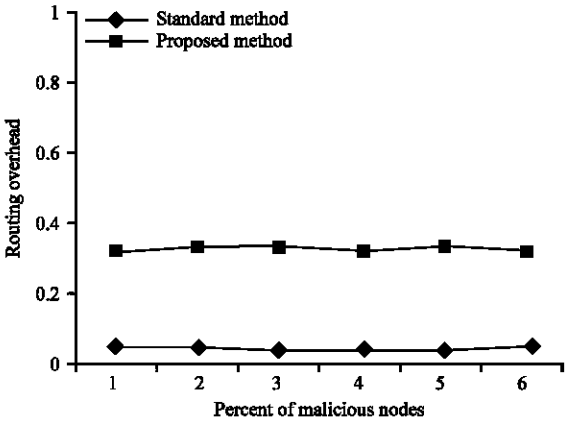

Fig. 15: Routing overhead

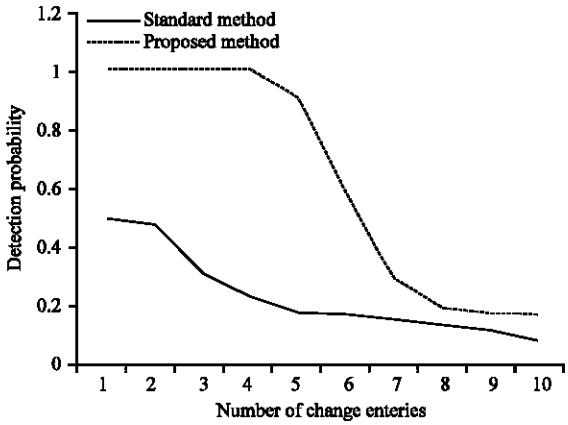

Fig. 16: Detection probability

Detection probability: In Fig. 16, the detection probability is varied with the number of pairs of changed entries in the distance vector update. The entries are selected to minimize the detection probability. Detection probability in the case of the proposed method is above 90%, when the number of entries changed is 4, or less than 4. After 4, the detection probability in case of the proposed method drops significantly and finally becomes more or less equal to the detection probability in the case of standard method, for number of changed entries equal to 8 or more.

CONCLUSION

In this study, we presented an efficient method to detect the faulty updates in distance vector protocols.. The method involves computing the predecessor information and sending along with the distance vector updates, instead of the traditional hop length information. We also carried out simulation studies to evaluate the method for three metrics viz. Packet Delivery Rate,

Network Overhead and Detection Probability. The studies shows that the packet delivery rate can also be increased if the node state information is shared with the routing cache The method is always able to detect faulty updates under certain well-defined conditions. Moreover Detection probability of the method is significantly higher than that of the existing methods.

REFERENCES

1. Houle K.J. and G.M. Weaver, 2001. Trends in Denial of Service Attack Technology, CERT Advisory.
2. Malkin, G., 1998. RIP Version 2, RFC 2453, Nov. RFC 1058.
3. May, J., 1994. OCPF Version 2, RFC 1583.
4. Murphy, S. M. Badger and B. Wellington, OSPF with Digital signatures, RFC 2154.
5. Zang, K., 1998. Efcient Protocols for Signing Routing Messages, in Proc. NDSS.
6. Kirk, A., S. Bradely, B. Cheung Mukherjee and A. Ronald Olsson, 1998. Detecting Disruptive Routers : A Distributed Network Monitoring Approach, In Proc. IEEE Symp. On Security and Privacy.
7. Cisco White Papers, 2000. Strtegies to Protect against Distributed Denial of Service Attacks (DDos).
8. Bradely, R., Smith, Shree Murthy and J.J. Garcia-Luna-Aceves, 1997. Securing Distance-Vector Protocols, in Proc. SNDSS.
9. Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating Routing Misbehavior in Mobile AdHoc Networks. In Proceedings of the Sixth Annual ACM/IEEE International Confeerence on Mobile Computing and Networking (MOBICOM 2000).