Enhancing the Distance Vector Routing Protocol with Fault Detection Capability

R.Sabitha[1], Dr.S.K.Srivatsa[2]

[1] Research Scholar, Sathyabama University, Old Mahabalipuram Road,Jeppiaar Nagar, Chennai – 119, Tamil Nadu, India. sabitha_ramadoss@yahoo.com
[2] Senior Professor, St.Joseph's College of Engineering, Old Mahabalipuram Road, Chennai – 119, Tamil Nadu, India.

Abstract

The demand for the Internet has grown tremendously. The Internet has become the foundation for world wide digital communication. The survivability of this critical network infrastructure is important to businesses, universities and government agencies. So, it is mandatory to secure the Internet. 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. 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 propose an efficient method to secure the distance vector routing protocols.

Keywords: *Internet Security, Routing table attacks, Distance vector routing, Link state routing.*

1. 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]. Internet security is based on three principles, namely, confidentiality, authenticity and integrity. Confidentiality indicates the ability to ensure that information is not disclosed to people who aren't explicitly intended to receive it. Authenticity indicates the ability to ensure that the given information was in fact produced by the entity whose name it carries and that it was not forged or modified. Integrity indicates the ability to ensure that information is not modified except by people who are explicitly intended to modify it. In spite of the presence of the above mentioned principles, the existence of malicious routers, covert channels and eavesdroppers in the Internet make this problem quite a challenging one.

To have a secure foundation for the critical Internet applications of the future, several weaknesses must be addressed: lack of encryption to preserve privacy, lack of cryptographic authentication to identify the source of information, and lack of cryptographic checksums to preserve the integrity of data (and the integrity of the packet routing information itself). Therefore, it is mandatory to secure the existing internetworking protocols, particularly the routing protocols.

Cryptographic techniques can be used to authenticate the originator of a packet and to protect the integrity and confidentiality of routing data.

Routing protocols are methods 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]). In a distance vector routing protocol, each router shares its knowledge (in the form of distance vector packet) about the entire network with its neighbors. A neighbor after receiving the distance vector packet updates its routing table if necessary. The lack of knowledge about the topology of the network leads to variety of attacks in the distance vector protocol. In a link state routing protocol, each router shares its knowledge of its neighborhood with every other router in the network. After receiving the link state update, each router computes the shortest path tree (SPT) with itself as the root of the tree.

Distance vector protocols are less robust than the link state protocols. They are subjected to various kinds of attacks like link and router attacks [4]. Several schemes and techniques have been developed to detect these attacks in distance vector protocols. The techniques that are developed are unable to detect the wrong updates in the distance vector updates. Any method, which is used to validate the router data in distance vector routing protocol should maximize the detection of faulty updates.

We propose an efficient method for inconsistency detection in the distance vector routing protocols. This method performs better than the traditional distance vector method

2. RELATED WORK

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

(i) Routing Information Techniques: In this type of techniques [5],[6] digital signatures are used to detect malicious distance vector updates in case of link attacks. However, these schemes are unable to detect router attacks.

(ii) Intrusion Detection Techniques: These techniques [7] are used to detect the anomalous behavior in the routers, assuming that intrusion detection devices are available in the network.

(iii) Routing Protocol Techniques: In this type of techniques, detection n capability is built into the routing protocol itself. In Cisco White Papers [8], 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) [9]. 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.

3. METHODOLOGY IN SECURING ROUTING PROTOCOLS

The proposed work is used to find the faulty updates in the distance vector updates. The method also protects the routing updates against the replay of old routing information.

In our method, every node 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 Update. Header of packet contains digital signature and some control information. Each routing message is digitally signed by the sender. This provides authenticity to the routing message. Update part of the packet contains routing

table of the router, sequence number and some control information. The sequence number in the update part is used to protect against the replay of old routing information. This sequence information can be in the form of sequence number or a timestamp. Routing table part contains five fields, namely Destination id, Next hop, Cost, Predecessor information and the path sum.

Figure 1 show the message format used in the proposed method. Figure 2 shows the fields in the routing table.

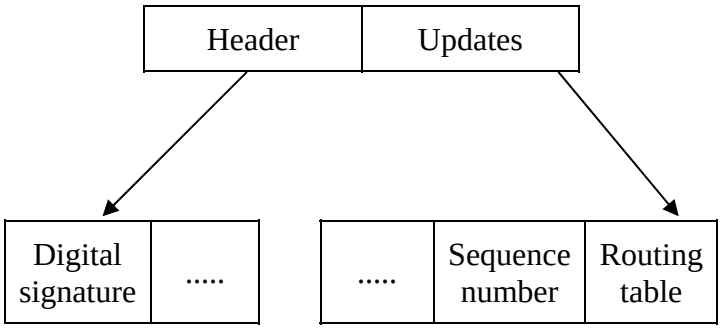

Figure 1. Routing message format

Destination id	Next hop	Hop count	Predecessor	Path sum

Figure 2. Fields in the routing table

In our method, sending node is the node sending the routing message and receiving node is the node receiving the routing message. The routing message contains both the header and the routing updates.

The different steps included in the proposed method are:

SENDING NODE

1. Distance vector tree based on shortest path is computed.
2. Predecessor information and the path sum for each destination based on the distance vector tree are calculated.

Predecessor (p) of a node x in the distance vector tree is y, if x is a descendant of y. Therefore,

$$p_x = y$$

Descendants (D) of node x in distance vector tree is defined as the children of x.

Hop length (hl) of a node x is defined as the number of hops in the shortest path from the root node to x in the distance vector tree.

Path sum (ps) of node x in the distance vector tree is defined as the sum of all path lengths passing through and terminating in x. Therefore,

$$ps_{x=}\ hl_x + \sum_{\forall j \varepsilon D_x} ps_y$$

Predecessor and the path sum for each destination are sent to all its neighbors.

RECEIVING NODE

On receiving the routing update, the router accepts the update based on the updating algorithm.

The updating algorithm requires that the router first add one hop field for each advertised route.

1. If the advertised destination is not in the routing table, the router should add the advertised information to the table.

2. If the advertised destination is in the routing table, then

(a) If the next-hop field is the same, the router should replace the entry in the table with the advertised one.

(b)If the next-hop field is not the same, then

(i) If the advertised hop count is smaller than the one in the table, the router should replace the entry in the table with the new one.

(ii) If the advertised hop count is not smaller, the router should do nothing.

3. After the complete routing table is formed, tree is constructed using the predecessor information present in the update.

3.1. In tree construction step, for each node in the distance vector update, the node is added to the list of descendant nodes of the predecessor node.

4. Hop length and path sum are calculated based on the constructed tree.

5. The calculated result and the received information are compared for checking the validity of the packet.

5.1. The net path sum (nps) of a node x is calculated by the formula

$nps_x = ps_x - ps^r_x$, where

ps_x is the calculated path sum and

ps^r_x is the received path sum

5.2. If the difference is non-zero, then the routing update is detected as malicious and it is dropped.

The proposed algorithm is able to provide higher detection probability. It does not introduce any extra overhead when it is compared with the Consistency check algorithm. The method also has a lower running time.

4. RESULTS AND DISCUSSION

This proposal implements asymmetric key cryptography and secure hash function to secure the Domain Name System. It also implements faulty update detection in the routing table to secure routing protocols.

Figures 3, 4 and 5 show the performance measures.

Packet Delivery Ratio: Figure 3 shows the packet delivery ratio. Packet delivery ratio is the ratio of number of packets that are received by the destination to the number of packets submitted to the network. Figure 6 has three curves and they represent the throughput of proposed method, consistency check method and standard method. The proposed method incorporates extension of calculating predecessor information and path sum.

$$\text{Packet delivery ratio} = \frac{\text{Number of packets received}}{\text{Total number of packets submitted}}$$

Figure 3 shows the simulation result. It demonstrates that the proposed method always performs better than the other two. We can infer that packet delivery rate sometimes is higher when

there are a higher number of malicious nodes than when there are a lower number of malicious nodes.

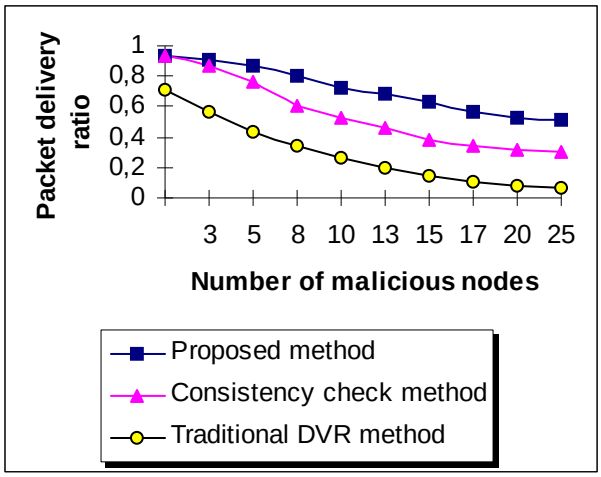

Figure 3. Packet delivery ratio

Detection rate: It is the probability that a malicious update can be detected. In Figure 4, the detection rate is varied with the number of pair of changed entries in the distance vector update. Inspecting the results, the proposed method performs better in terms of detection when the number of entries changed is low. Detection rate in the case of the proposed method is above 90%, when the number of entries changed is 6 or less than 6.After 6, the detection rate in case of the proposed method drops significantly and becomes more or less equal to the Consistency check method and the standard method. However, this is fair when compared with existing methods.

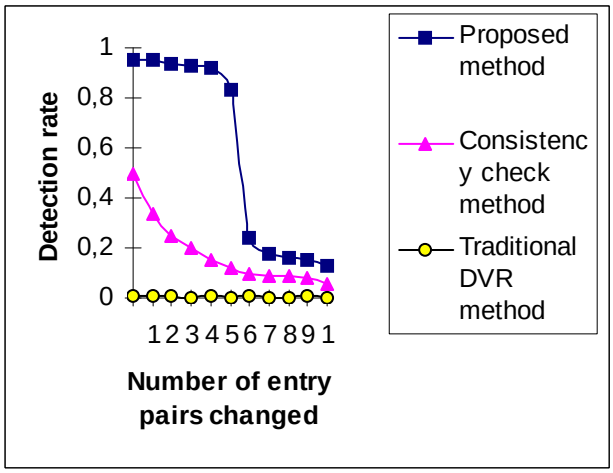

Figure 4. Detection rate

Network Overhead: It is the ratio of total number of routing related transmissions and the total number of packet transmissions. As shown in the Figure 5, the routing overhead is increased significantly when the network topology changes or there is a high number of malicious nodes in the network. However, the proposed method provides low routing overhead when it is compared with the CC method.

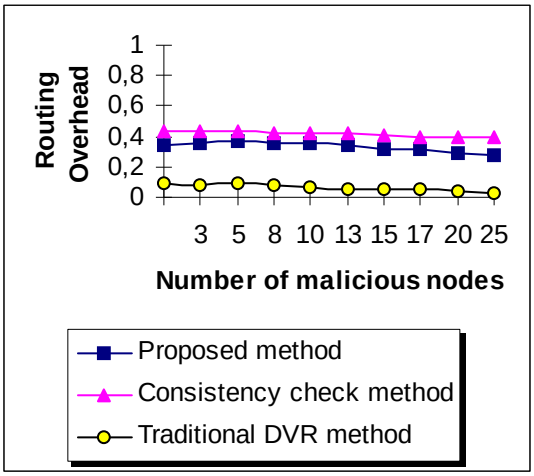

Figure 5. Routing overhead

5. CONCLUSION

We present effective and efficient methods for improving the Internet security.. Security is provided to the distance vector routing protocol by adding the predecessor information and path sum metrics. The method involves sending the predecessor information and the path sum along with the distance vector updates, in addition with traditional hop length information. This method which is based on predecessor information protects the routing updates as they traverse an Internet from subverted routers. We show that it is possible to effectively and efficiently secure distance-vector protocols. We accomplish this using the predecessor information specified in the path finding class of distance-vector protocols. We also carried out extensive simulation studies to evaluate the method for three different metrics viz. Detection Rate, Packet delivery Rate and Routing overhead. Our simulation studies show that the method achieves the following: (i) It requires fewer bytes of extra information per node in the distance vector packet. (ii) It is always able to detect malicious updates under certain well-defined conditions. (iii) Detection rate of the method is significantly higher than that of the existing methods.

REFERENCES

[1] K.J.Houle and G.M. Weaver, “Trends in Denial of Service Attack Technology,” CERT Advisory, v1.0, Oct 2001.
[2] G.Malkin, “RIP Version 2,”RFC 2453, Nov. 1998. RFC 1058, June 1988.
[3] J.May,”OCPF Version 2, “RFC 1583, Mar. 1994.
[4] Anirban Chakrabarti and G.Manimaran (2002), “Internet Infrastructure Security: A Taxoomy”, IEEE Network, vol. 16, no.6, pp 13-21.
[5] S.Murphy, M.Badger, and B. Wellington, “OSPF with Digital signatures,” RFC 2154.
[6] K. Zang, “Efficient Protocols for Signing Routing Messages,” in *Proc. NDSS*, 1998.
[7] Kirk. A. Bradely, S. Cheung, B. Mukherjee, and Ronald. A. Olsson, “Detecting Disruptive Routers: A Distributed Network Monitoring Approach,” in *Proc. IEEE Symp*. On Security and Privacy. 1998.
[8] Cisco White Papers, “Strategies to Protect against Distributed Denial of Service Attacks (DDos),” Feb. 2000.
[9] Bradely R. Smith, Shree Murthy, and J.J.Garcia-Luna-Aceves, “Securing Distance-Vector Protocols,” in *Proc. SNDSS*, 1997.

Paper received: 2008-08-05