Dynamic Routing With Security Considerations

K.V.S.Mounika, Nanduri Jyothirmai, A.Rama Krishna

Abstract – One of the major issues for data communication over wired and wireless networks is the security. Different from the past works which includes the Cryptography algorithms and System Infrastructures, we are proposing a dynamic routing algorithm that could randomize the delivery of packets for data transmission as it is compatible and also easy to implement. It is compatible with some of the popular routing protocols such as the Routing Information Protocol which uses hop-count as its metric in the wired networks and Destination-Sequenced Distance Vector protocol in the wireless networks. In the RIP where the hop-count is considered only a limited number of hops are chosen and data transmission are done by selecting the hops randomly in a network. This improves security as well as controls traffic in a network. The routing table in this algorithm is based on the one of the Dynamic routing algorithms known as "Bellman-Ford algorithm" or "Ford Fulkerson Routing algorithm". An analytical study on the proposed algorithm is presented and the results are verified to show the capability of the proposed algorithm.

Keywords - Bellman Ford algorithm, Dynamic Routing, IP Security, Routing Information Protocol (RIP), Secure Socket Layer.

I. INTRODUCTION

In the past decades, various security-enhanced measures have been proposed to improve the security of data transmission over public networks. Existing work on the security enhanced techniques of data transmission includes the designs of cryptographic algorithms, system infrastructures; security enhanced routing methods and its techniques.

Among many well known designs for the systems based on cryptography, the IP security and the Secure Socket layer (SSL) are popularly supported and implemented in many systems and platforms. Although IP Security and SSL greatly improve the security level for data transmission, they introduce substantial overheads especially on host performance and effective network bandwidth which are unavoidable. For example, the data transmission overhead is 5 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 58 cycles/byte when Advanced Encryption Standard (AES) is used for encryption or decryption for IP Security.

Another alternative for security enhanced data transmissions is to dynamically route packets between each source and its destination so that the chance for routing system break-in, due to successful interception of consecutive packets for a session is low. The intention of security enhanced routing is different from the adopting of multiple paths between a source and a destination.

A secure routing protocol is proposed to improve the security of end-to-end data transmission based on multiple path deliveries. The set of multiple paths between each source and its destination is determined in an online fashion and extra control message exchanging is needed and a secure routing mechanism is proposed to improve routing security. Similar to the work proposed by an engineer a set of paths is discovered for each source and its destination in an online fashion based on message flooding. Thus, there is a need of mass of control messages. Yang and Papavassiliou explored the trading of the security level and problems with the traffic dispersion. They proposed a traffic dispersion scheme which will help in reducing the probability of eavesdropped information along the used paths provided that the set of the data delivery paths is discovered in advance. Although excellent research results have been proposed for security-enhanced dynamic routing, many of them rely on the discovery of multiple paths either in an online or offline fashion. For those online path searching approaches the discovery of multiple paths involves a number of control signals over the internet. On the other hand, in an offline fashion finding of paths may not be suitable to the dynamic changing configuration networks. So, we propose a dynamic routing algorithm which provides effective security enhanced data delivery without any extra control messages.

II. SECURE SOCKET LAYER

In SSL we concern with implementation of client and server entities and the SSL transaction between client and the server respectively. This transaction contains authentication, large data transfer and key exchange. Our implementation gives reliable and secure communication i.e, message exchange and data transfer between the two entities.

Now-a-days information is one of the most valuable resources in the world. Whether it is a personal letter or an industrial secret, all information or data has a worth to someone. This considers issues of security and privacy for such information or data that is stored. It discusses the reasons for wishing to provide security for the data and the methods available for doing so. For secure transferring of the information between the sockets at distant places which mainly requires security so that the massage or data may not be tampered while it has been transferred.

When a client and server communicate with each other, SSL ensures that the connection is private and secure by providing authentication and encryption. Authentication confirms that the server and the client are trustworthy. Encryption then creates a secure "tunnel" between the two, which prevents any unauthorized system from reading the data. SSL enabled Clients and Servers confirm each other's identities using digital certificates. Digital certificates are issued by the third parties called Certificate Authorities and

Manuscript Received on November, 2012

K.V. S. Mounika, Electronics and Computer Engineering, KL University, Guntur, Krishna District, Andhra Pradesh, India.

Nanduri Jyothirmai, Electronics and Computer Engineering, KL University, Guntur, Krishna District, Andhra Pradesh, India.

Asst. Prof. A. Rama Krishna, Electronics and Computer Engineering, KL University, Guntur, Krishna District, Andhra Pradesh, India.

provide information about an individual's claimed identity, as well as their public key. By validating digital certificates both parties can ensure that an imposter has not intercepted a transmission.

III. PRESENT SYSTEM

Present network on security-enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats over the internet, including eavesdropping, spoofing, session hijacking, etc. Among many well-known designs for cryptography based systems, the IP Security and the Secure Socket Layer are popularly supported and implemented in many systems and platforms. Although IP Security and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads, especially on gateway or host performance and effective network bandwidth.

IV. PROPOSED SYSYTEM

We will propose a dynamic routing algorithm that could randomize delivery paths for data transmission. The algorithm is easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector Protocol in wireless networks, without introducing extra control messages.

V. METHODS APPLIED

A.Bellman Ford Algorithm

Bellman Ford algorithm computes single source shortest paths in a weighted digraph. For graphs with only non-negative edge weights, the faster Dijkstra's algorithm also gives solution to the problem. Thus, Bellman Ford is used for graphs with negative edge weights.

Bellman Ford's basic structure is very similar to Dijkstra's algorithm, but instead of greedily selecting the minimum-weight node not yet processed to relax, it simply relaxes all the edges, and does this |V|-1 time, where |V| is the number of vertices in the graph. The repetitions allow minimum distances to accurately propagate throughout the graph, since, in the absence of negative cycles; the shortest path can only visit each node at most once. Unlike the greedy approach, which depends on some specific structural assumptions derive from positive weights; this straight forward approach extends to the general case.

B.Routing Information Protocol

The Routing Information Protocol (RIP) is a distance vector routing protocol, which employs the hop count as a routing metric. The hold down time is 180 seconds. This protocol prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15. The hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 can be considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP implements the split horizon, route positioning and hold-down mechanisms to prevent in-correct routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the Routing Information Protocol with Metric-based Topology Investigation (RMTI) algorithm to cope with the count-to-infinity problem. With its help, it is possible to detect every possible loop with a very small computation effort.

C.Destination-Sequenced Distance-Vector Routing

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad-hoc mobile networks based on the Bellman Ford algorithm. The main aim of the algorithm was to solve the routing loop problem where each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present or else an odd number is used. The number is generated by the destination, and the emitter has to send out the next update with this number. The routing information is distributed among the nodes by sending full dumps infrequently and smaller updates more frequently which are incremental.

The procedure in section of the router is as follows. If a router receives a new information, them it uses the latest sequence number. If the sequence number is same as the one which is already present in the table, then the route with the better metric is used. And the left over entries which have not been updated for a while are called stale entries. Such entries and the routes using those nodes as next hops are deleted.

D. Adaptive Multipath Routing for Dynamic Traffic Engineering

Concurrent Multipath Routing (CMR) is often taken to mean simultaneous management and utilization of the multiple paths available for the transmission of streams of data emanating from an application or multiple applications. In this form, each stream is assigned a separate path, uniquely to the extent supported by the number of paths available. If there are more streams than available paths, some streams will share paths. This provides better utilization of available bandwidth by creating multiple active transmission queues. This also provides a measure of fault tolerance in order to prevent the path failure, and also the problem occurred due to the traffic assignment to that path. His method provides better transmission performance and fault tolerance by providing:

- Simultaneous, parallel transport over multiple carriers.
- Load balancing over available assets.
- Avoidance of path discovery when reassigning an interrupted stream.

One of the most powerful forms of CMR goes beyond merely presenting paths to the applications to which they can bind. Powerful form of CMR otherwise known as True CMR aggregates all available paths into a single, virtual path. All application offer their packets to its virtual path which is de-multiplexed at the network layer, the packets are then distributed to the actual paths via some method such as Round Robin or Weighted Fair queuing. If a link or relay node fails, thus invalidating one or more paths, the succeeding packets are not directed to hose paths. The stream continues uninterrupted and transparently to the application.

This method provides significant performance benefits over the former:

- By continually offering packets to all paths, the paths are more fully utilized.
- No matter how many nodes and paths fail, as long as at least one path constituting the virtual path is still available, all sessions remain connected. Therefore it means that no streams need to be restarted from the beginning and no reconnection penalty is incurred.

It is noted that the powerful CMR is by its nature cause Out-Of-Order-Delivery (OOOD) of packets, which is severely debilitating for standard TCP. However has been exhaustively proven to be inappropriate for use in challenge wireless environments and must, many case, be augmented by a facility, such as TCP gateway, that is designed to meet the challenge. One such gateway tool is SCPS-TP. Through which its Selective Negative acknowledgment capability deals successful with the OOOD problem.

Another important benefit of true CMR, desperately needed in wireless network communications is its support for enhance security. In other words, for an exchange to be compromised many of the routes it traverses must be compromised.

E. Analysis of an Equal-Cost Multi-Path Algorithm.

Equal cost multi path-routing (ECMP) is a routing strategy where next hope packet is forwarded to a single destination, where it can occur over multiple best paths which tie for top place in routing metric calculations. Multi path routing can be used in conjunction with most routing protocols, since it is a path-hop decision that is limited to a single router. It potentially offers substantial increases in the bandwidth by load balancing traffic over multiple paths. However, there can be significant problems in its deployment in practice.

Load balancing per packet multipath routing is generally deprecated due to the impact of rapidly changing latency, packet re-ordering and maximum transmission units(MTU) differences within a network flow, which can disrupt the operation of many internet protocols, most notably TCP and path MTU discovery.

In many situations, ECMP may not offer the real advantage over best-path routing. For example if the multiple best next-hop paths to a destination recon verge downstream into a single low-bandwidth path, it will merely add complexity to the traffic paths to that destination without improving available bandwidth.

ECMP may also interact negatively with other routing algorithms where the physical topology of the system differs from the logical topology, for example in systems that employ VLAN's at layer 2 or virtual circuit-based architectures such as ATM or MPLS.

Multipath routing is one of the most important routing techniques of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth and improved security. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other. Extensive research has been done on multi-path routing techniques, but multi-path routing is not yet widely deployed in practice.

1) Equal Cost Load Balancing:

It may be a surprising aspect that what happens if a routing table has two or more paths with the same metric to the same destination network. When a router has multiple paths to a destination network and the value of that metric is the same, this is known as an equal cost metric, and the router will perform equal cost load balancing. The routing table will contain the single destination network but will have multiple exit interfaces, one for each equal cost path. The router will forward packets using the multiple exit interfaces listed in the routing table.

F. RIP Version2 Carrying Additional Information

The Routing Information Protocol (RIP) is a distance –vector protocol that uses hop count as it's metric. RIP is widely used for routing traffic in the global Internet and is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system. Exterior gateway protocols, such as the Border Gateway Protocol (BGP), perform routing between different autonomous systems.

1) Routing Updates:

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by one, and the sender is indicated as the next hop. RIP routers maintain only the best route i.e. the route with the lowest metric value to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

VI. SYSTEM DESIGN

Identification of classes, their relationships as well as their collaboration in objector, classes were divided into Entity classes, design involves interface classes and the control classes. The Computer Aided Software engineering tools that are available commercially do not provide any assistance in this transition. Even research CASE tools take advantage of meta-modeling are helpful only after the construction of class diagram is completed. In the Fusion method, it used some object-oriented approaches like Object Modeling Technique, Class Responsibility Collaborator and Objector used the term Agents to represent some of the hardware and software systems. In the Fusion method, there was no requirement phase, where in a user will supply the initial requirement document. Any software project is worked out by both analyst and designer. The analyst creates the Use case diagram. The designer creates the Class diagram. But the designer can do this only after the analyst has created the Use case diagram. Once the design is over it needs to decide which software is suitable for the application.

VII. CONCLUSION AND ENHANCEMENTS

This paper has proposed a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. The proposed algorithm is easy to implement and compatible with popular routing protocols, such as RIP and DSDV, over existing infrastructures. An analytic study was developed for the proposed algorithm and was verified against the experimental results. A series of simulation experiments were conducted to show the capability of the proposed algorithm, for which we have very encouraging results. We must point out that the proposed algorithm is completely orthogonal to the work based on the designs of cryptography algorithms and system infrastructures. Our security enhanced dynamic routing could be used with cryptography-based system designs to further improve the security of data transmission over networks. Satellite network capacity, adaptability and responsiveness are enhanced with onboard capabilities for packet switching, bandwidth allocation and spot-beams which facilitate uplink and downlink spectral reuse. A recent over-the-air (OTA) test of the SPACEWAY system, a Ka-band regenerative satellite mesh network supporting IP packet services, provides definitive demonstration of key capabilities in the areas of quality-of-service, routing for unicast and multicast traffic, dynamic bandwidth resource allocation, security and configurable satellite uplink and downlink components. Leveraging SPACEWAY system technologies and operational capabilities serves as a pragmatic step towards the development of future multi-satellite networks with more advanced features including on-board packet routing, multi-mode radio transmission and inter-satellite links, which are now being considered for transformational satellite networks.

REFERENCES

1. T.H. Cormen, C.E. Leiserson and R.L. Rivest, Introduction to Algorithms.
2. D. Collins, Carrier Grade Voice over IP. McGraw-Hill, 2003.
3. G. Malvin, Routing Information Protocol (RIP) Version 2 Carrying additional Information, Request for comments (RFC 1723), Nov. 1994.
4. Secure Socket Layer (SSL), http://www.openssl.org/, 2008.
5. P. Erdo's and A. Renyi, "On Random Graphs", Publications.
6. W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery".

AUTHOR PROFILE

K.V.S.Mounika was born in 1992 at Kadapah District, Andhra Pradesh. She is pursuing her B.Tech in Koneru Lakshmaih University. Her interested areas are Networking and Data Communications.

Nanduri Jyothirmai was born in 1992 at Krishna district, Andhra Pradesh. She is pursuing B.Tech in Koneru Lakshmaih University, Guntur. Her interested areas are Data Communications and Transmission.

A. Rama Krishna was born in 1987 at West Godavari District, Andhra Pradesh. He is working as a Assistant Professor, Dept.of ECM, K.L.University, Vaddeswaram, A.P, India.