A proposed algorithm for securing OSPF with using Symmetric key and Encryption techniques based on Image

Jignesh Shaparia[1] Prof. Shahida Chauhan[2]
[1] PG-Scholar [2]Assistant Professor
[1, 2]Computer Engineering Department
[1,2]Atmiya Institute of Technology and Science (GTU), Rajkot, Gujarat, India

Abstract—Network reliability is becoming increasingly important issue today. So to remain resistant to attacks is the fundamental thing for it. Securing routing protocol involves protecting the authenticity and integrity of routing protocol messages. The protocols which used as network routing deployed in internal networks is Open Shortest Path First Protocol (OSPF). OSPF is based on the relative costs of transferring information between routers and networks. In OSPF, a group of routers collaborate, exchange routing information, and forward packets for each other. Attacks on routing protocol OSPF can be launched either as insider attacks or as outsider attacks. Earlier works have addressed these two problems independently with many interesting solutions. Like Digital Signatures, MD5, MAC, RSA etc. Due to the nature of these solutions, network architects cannot deploy without increasing the overhead on the network. Also they all are having their own advantages as well as disadvantages. So in this research the proposed algorithm is working for this solution. Use of Symmetric Key techniques, Diffie Hellman and Image based encryption makes the mechanism more secure against attacks.

Key words: LSA, Autonomous System, Symmetric key, Authentication, Intruders, Falsification of LSA

I. INTRODUCTION

The purpose of any routing protocol is to efficiently distribute dynamic topological information among its participants to facilitate routing calculations upon which packet forwarding decisions are then based. In a link-state routing protocol such as OSPF, each router is independently responsible for describing the state of its local neighborhood (e.g. links to neighboring networks, routers, and hosts) to the rest of the network.

In OSPF, the first step in the exchange of routing information is the creation of adjacencies between neighboring routers. A router first uses a Hello Protocol to discover its neighbors. Once neighboring routers have 'met' via the Hello Protocol, they then go through a Database Exchange Process to synchronize their databases with one another. Only then can neighboring routers become adjacent and exchange routing protocol information.

Information about the state of a router's local neighborhood is then assembled into a link-state advertisement (LSA), which is then distributed to every other router by reliable intelligent flooding. The basic flooding process is straightforward: upon receiving an advertisement from a neighbor, a router acknowledges receipt of the advertisement and, if new, forwards the advertisement to all other neighbors. Thus, after a short period of convergence, each router in the network will have an identical topological database of LSAs to be used for routing calculations.

OSPF is an interior routing protocol, designed to be used within a single autonomous system (AS). OSPF allows the AS to be divided into groups of networks called areas. Each area runs a separate copy of the basic link-state algorithm, and the topological details of the area are hidden from the rest of the AS, reducing routing traffic. All areas are connected by a single backbone area, in a logical hub and spoke configuration.

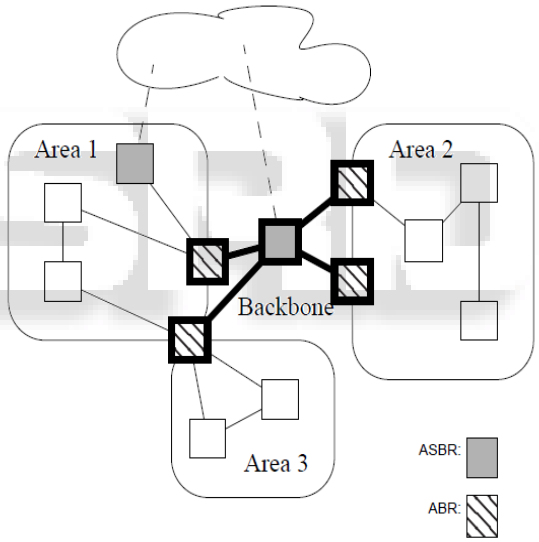

Fig. 1 OSPF Terminology

Routers belonging to a single area are called internal routers. Routers which belong to more than one area are called area border routers (ABRs). All ABRs belong to the backbone by definition. Any router which exchanges routing information with an external AS is called an Autonomous System Boundary Router (ASBR).

II. LINK STATE ADVERTISEMENT

OSPF defines five LSA types which correspond to router's respective roles. All routers generate router links (type 1) LSAs for each area they belong to, which describe the state and cost of routers links to that area. Designated routers generate network links (type 2) LSAs which describe all routers attached to the transit network (subnet). ABRs generate summary link (type 3 & 4) LSAs, which inject into an area a single destination (a network or ASBR

respectively) outside of that area. ASBRs generate AS External (Type 5) LSAs, which describe a single destination external to the AS. Of the five types, only AS external LSAs are flooded throughout the AS, all others are only flooded within a single area.

In link-state protocols, e.g., OSPF [3] a router learns of the entire topology of the network before computing the best routing paths. For a router, the link-state typically consists of the list of active neighbors and the estimated link costs to them. For example, in Figure3, the link-state of A is hB, 2i and hC, 3i. Typically, a router generates a link-state advertisement (LSA) of its link-state and floods it to the entire network using a reliable flooding mechanism [3]. Upon receiving all the LSAs from all routers, each router builds an identical view of the network topology. Note that, link costs can be asymmetric i.e., link cost of A to B is not necessarily the same as B to A. Using Dijkstra's [3] algorithm, each router builds a shortest-path tree with itself as the root node. In Figure 3, we show the propagation of the LSA by A and the shortest-path tree computed by router A (bold lines) using the LSAs received from other routers.

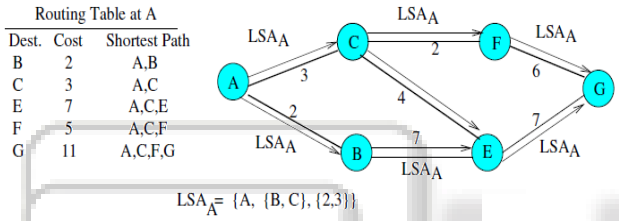

Fig. 2 Operation of the OSPF Protocol[2]

It is possible for more than one instance of an LSA to exist in the system at any one time. Thus each LSA has a sequence number. When encountering multiple instances, the LSA with the greatest sequence number is considered newer. If the sequence numbers are equal, the age field and finally checksum are used as tie-breakers.

III. ATTACKS IN OSPF

Providing security in a routing protocol involves protecting the authenticity and integrity of routing protocol messages. In our context, authenticity is a guarantee of the identity of the source of a particular piece of routing information, and integrity is an assurance that the information transmitted is consistent with the information received.

Cryptography is a powerful security tool, but comes at a performance cost. Primarily, we are concerned with threats to the integrity and authenticity of routing protocol information. These threats can generally be separated into two classes: external and internal.

A. *External Attacks*

We define external threats as those from non-protocol participants (outsiders or intruders), such as an attacker with access to a link between routers. Such an intruder might delete, modify, replay, or forge protocol packets. This poses a threat to the flow and content of routing updates (LSAs), to the neighbor relationships of existing routers, and of an outsider becoming a protocol participant. Threats from outsiders can be countered using authentication, i.e. requiring that routers participating in the protocol possess shared secrets which, by definition, an outsider does not have access to.

With cryptographic authentication, the integrity and authenticity of protocol exchanges between neighboring routers is secured from outside threats. While cryptographic authentication does prevent forging, replay, and modification of protocol messages by outsiders, an intruder can still block (delete) protocol messages transmitted on the link.

B. *Internal Attacks*

We define internal threats as those from protocol participants (insiders), such as subverted or faulty routers. As we have seen, the integrity and authenticity of routing information can be protected with cryptographic methods. However, in the case of insider threats, conventional cryptographic solutions are impractical. A router essentially plays two distinct roles in the routing protocol - generating local information (LSAs) and forwarding the LSAs of other routers. We first consider the possible threats to the protocol from an insider modifying or deleting the LSAs of other routers.

1) *Modifying Information*

Since multiple instances of an LSA are compared to determine which is newer, by examining their sequence number, age, and checksum fields, we know that any changes made by a bad of faulty intermediate router to an LSA in transit will result in one of two cases in the receiver(s) of the LSA. The modified LSA will be (1) rejected, i.e. considered to be an older instance or the same instance and is thus discarded, or (2) accepted, i.e. considered to be a new or newer instance and is thus installed in the receiver's database and propagated by flooding. Clearly, case (1) does not pose a threat to the protocol. In case (2), the possible results depend on the bad router's topological position in the network.

We now consider a bad internal router which does partition the area, i.e. the bad router is the only path between at least two good routers. In general, we can view the area as divided into several groups of good routers, or fragments, between which the bad router completely controls all communication. One obvious threat is that of the bad router failing to forward LSAs from one fragment into the other. This has the effect of isolating the bad router, i.e. causes it to not be used to forward user traffic, and we note that the resulting unreachability should detectable by higher level (e.g. network management) services.

Now consider an LSA originated at A for an existing destination in fragment F1, which is modified and introduced into fragment F2. Clearly, this cannot be detected by A. We also note that this cannot affect routing internal to F2.Finally, we can see that unless the change is to effectively delete the destination, routing from F2 to the destination in F1 will actually be correct, since the bad router is along the only path to the misadvertised destination, routing within the fragment. Thus any change in routing within the fragment can again only be to decrease reachability.

2) *Generating Bogus Information*

It is fundamentally difficult for the protocol itself to provide protection against a bad router's origination of bogus local information. Cryptography, for instance, cannot prevent a valid router from generating incorrect information. Luckily, the nature of OSPF does provide some inherent protections from internal threats.

First, since routing within each area is independent, bad information in one area cannot affect routing in within other areas. Second, the natural duplication of information in a link-state routing protocol lends itself to corroboration. Any time several routers have access to the same set of information (e.g. two ABRs common to a particular area), they have the potential of checking each other and detecting problems[3]. Finally, the SPF calculation will not consider a link unless the database contains a corresponding LSA from the other end of the link, preventing a router from claiming non-existent transit networks.

IV. RELATED WORK

Murphy and Badger from TIS proposed different digital signature schemes [4] to prevent tampered link-state advertisements (LSAs). Please note that PFA based protocols are in between link state and distance vector. In fact, we consider that PFA is still a link state protocol without fully replicating the routing tables. Furthermore, An Experimental Study of Insider Attacks for the OSPF Routing Protocol 4Another approach is to detect (instead of prevent) problems when the network infrastructure is under attacks[6].

Murphy and Badger from TIS proposed a public key signature scheme[4] to protect the integrity of LSAs flooded through the network. With a public key infrastructure, the source router uses its private key to sign the MD5 value for every LSA created. Since the intermediate routers do not know the private key of the source router, they can not tamper the LSAs without being detected. On the other hand, every receiver of LSAs must use the source router's public key to verify its integrity. Therefore, their scheme is very secure against compromised intermediate routers. There are two potential problems with this public key signature approach: First, public key systems (e.g., RSA) are usually very expensive to run at least in software. Comparing to symmetric authentication schemes, RSA is about 1,000 times slower even with low RSA exponents. Second and more importantly, in order to implement the public key signature scheme in OSPF, we need to modify the standard and upgrade the implementation for all the routers.

B. Bruhadeshwar proposed a technique the use of symmetric key protocols for addressing the security at both the control and data planes. They describe approaches that enable the reuse of the symmetric key protocols thereby eliminating the need for separate solutions at different planes. They used symmetric key Protocols as they are efficient and scalable [2].

Ming Yu presents some enhancements to the routing protocols that have been used in large-scale backbone networks. By using limited key distribution and double message hashing, the routing protocols have improved computational efficiency and the ability to verify the authenticity and integrity of a routing message. Also proposes a novel algorithm that can detect internal attacks, by using both message and route redundancy during route discovery also proposes an optimal routing algorithm with routing metrics combining both requirements on a node's trustworthiness and performance[5].

V. PROPOSED ALGORITHM TO PROVIDE SECURITY IN OSPF PROTOCOL

Step 1: In wired Network first to find shortest path using Dijkstra's Algorithm.
Step 2: Generating Random key.
Step 3: Diffie Hellman Key Exchange for Authentication.
Step 4: Taking message input.
Step 5: Convert it into ASCII and add 0 at MSB.
Step 6: Now using the 8 bits Key which is generated in previous step, Encryption of the message.
- *a)* Binary division of message by this key.
- *b)* XORing reminder and quotient.
- *c)* Reverse the number.

Step 7: XORing it with message.
- *a)* Convert it into 1's Complement.

Step 8: Convert this value in matrix and Transpose it.
Step 9: Convert that matrix into binary image.
Step 10: Image compression using JPEG.
Step 11: Decryption is same but in reverse order at Receiver's side.

VI. CONCLUSION

Issue of Authentication and Integrity in interior routing protocol OSPF is solved by previous techniques but all the solutions are having advantages and disadvantages. This proposed algorithm with Diffie Hellmen key exchange, Symmetric Key and Encryption technique based on Image remove the difficulties of security with less overhead and makes the mechanism more reliable.

REFERENCES

[1] Casey T. Deccio, Mark Clement & Kent Seamons, "Securing OSPF Using Digital Signatures and Neighbour Checking", Computer Science Journal, 2003.
[2] Bezawada Bruhadeshwar, Kishore Kothapalli, M.Poornima and M. Divya, "Routing Protocol Security Using Symmetric Key Based Techniques", IEEE International Conference on Availability, Reliability and Security, 2009 .
[3] John Moy, OSPF Version 2, RFC 2328, April 1998.
[4] S.L. Murphy, Badger, M.R., and Wellington B., "OSPF with Digital Signatures", RFC 2154, June 1997
[5] Ming Yu, "Security Enhancements to Routing Protocols for Backbone Networks", International Conference on Systems, Man, and Cybernetics IEEE,2006 (ISSN : 1-4244-0100-3)
[6] G. Qu, J. Rudraraju, R. Modukuri, S.Hariri, and C. Raghavendra, "A framework for network vulnerability analysis", IASTED International Conference on Communications, Internet and Information Technology (CIIT 2002), Nov 2002.
[7] Jeremy Goold & Dr. Mark Clement, "Improving Routing Security Using a Decentralized Public Key Distribution Algorithm", Second International

Conference on Internet Monitoring and Protection, 2007 IEEE(ISSN : 0-7695-2911-9)

[8] Monu Singh, Rajesh Tanwar, Rajkumar and P.Gope, "Image Based Encryption Decryption Algorithm", 3rd International Conference on recent trends in information, telecommunication and computing, 2012.

[9] Prosanta Gope, Ajit Singh, Ashwani Sharma and Nikhil Pahwa, "An Efficient Cryptographic Approach for Secure Policy Based Routing (TACIT Encryption Technique)", IEEE, 2011(978-1-4244-8679-3/11/)