JOURNAL OF
Emerging Paradigms
in Computing Systems
JEPCS

Journal of Emerging Paradigms in Computing Systems (JEPCS) | Volume 01, Issue No. 01, 2025

ARTICLE TYPE: Research Article

Article ID: JEPCS-2025-0101-0012

Securing OSPF Routing Against Link-State Threats: Vulnerability Analysis, Authentication, and GNS3-Based Validation

Atif Manzoor[1]

[1] Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore, Pakistan

* Corresponding author: f2018288005@umt.edu.pk

Received: September 02, 2024 **Accepted:** November 15, 2024

Abstract- Routing protocols are used to keep the network up and running. All distribution of different routes and best path selection is depending on routing protocols. A slight miscalculation or wrong path selection could lead to a total network collapse. Now a day's routing protocols security features have become the most important aspect of any network. OSPF (open shortest path first) is open source routing protocol that is link-state in routing algorithm. The primary security and threat mitigation issues of OSPF are addressed like security mechanism, authentication mechanism, Hierarchical Routing Mechanism and fight back mechanism in case of fake LSA (Link State Advertisement). This research article is focused on to avoid such security and threats mitigations of OSPF routing protocol. Some appropriate remedial measures and noninvasive methods like Digital signatures with link encryption and hashing algorithm MD5 (Message Digest) are used for avoiding security threats in the network running OSPF protocol. A simulated network model is established in GNS3 simulator. Two Cisco routers are used in this simulated topology which are directly connected via serial links. OSPF routing protocols with hashing algorithm is configured and results shows OSPF routing information is secure.

Keywords- OSPF; Routing Protocol; Link-State; Data Packet; Authentication Key

1. Introduction

Routing determines how packets are forwarded between interconnected IP networks. Routers make these forwarding decisions from the routing information maintained in their routing tables, which identify reachable networks and the paths available to them. In enterprise and service-provider environments, routing protocols are responsible for learning and exchanging this information. Their behavior therefore has a direct effect on path selection, convergence, and overall network availability. The exchange of routing information allows routers to identify suitable paths from a source network to a destination network. Each routing protocol follows its own rules for discovering routes, evaluating alternative paths, and updating the routing table. These processes enable routers to respond to changes in network connectivity and maintain communication across multiple IP networks [1].

Open Shortest Path First (OSPF) is a link-state Interior Gateway Protocol (IGP) used for routing within an autonomous system. It applies the Shortest Path First (SPF) calculation based on Dijkstra's algorithm to determine the lowest-cost paths to known destinations. OSPF organizes a network into areas, with the backbone identified as Area 0. Routers maintain detailed link-state information for their own area, while communication between areas is handled through the OSPF hierarchical structure [2]. This organization limits the amount of topology information that must be maintained by every router and can reduce routing-table and link-state database overhead. OSPF uses interface cost, commonly derived from bandwidth, as the metric for path calculation and exchanges link-state information among neighboring routers to maintain a consistent view of the network topology. When OSPF is configured on the routers, it shares the whole topology of the network among all the neighboring routers by exchanging link state information. OSPF is considered to be an

efficient routing protocol due to its capability of fast convergence and scalability. OSPF has good built in mechanisms for security but still there are some vulnerabilities in the protocol [6].

This research has focused on the security features of OSPF routing protocol. Initially a brief introduction of OSPF is presented and related work in this particular topic is discussed. In the second segment the primary emphasis is on security mechanism which is implemented in OSPF routing protocol. In this phase the authentication mechanism, Hierarchical Routing Mechanism and fight back mechanism in case of Fake LSA is mainly discussed. In third phase, OSPF internal and external security threats have been identified and appropriate remedial measures have been proposed.

Noninvasive methods have been used for threat detection in the network running OSPF protocol. A network topology has been designed in simulated software GNS3 with two cisco routers with complete configurations of hashing algorithm MD5 to secure the source and destination packets have been implanted. With the help of this algorithm unauthorized user is unable to tempered data. Digital signature with link encryption is also anther method which must be integrated to advance and secure the network end to end. After implementation of these two methods routing network of OSPF is safe and reliable.

2. Related Work

Some vulnerabilities are identified by Esmail Kaffashi in his research article [1]. According to his findings OSPF routing capabilities can be disturbed by of denial of service attack. According to their findings and analysis attacks like MAXAGE, Sequence Number Increment, Max Sequence Number and Bogus LSA mostly used for denial of service attack. They take the system resources down and in most cases routers fails to respond to the incoming requests and ultimately crash. The built in fight back mechanism in OSPF works in some cases but sometimes the attack can't be identified by it and the routers goes into a state of not responding. They have simulated an attack in a test environment and showed the security vulnerabilities in OSPF.

Murphy and Badger [2] research has focused on implementing OSPF security with the help of cryptographic techniques. They used digital signatures to protect the information exchange. The routing information packets of the OSPF are signed with an asymmetric cryptographic algorithm. After the implementation of this technique each router at the other end can confirm the source and reliability of data. Their research has deliberated the important security analysis of routing protocols, go through the fundamentals of OSPF procedure and has described the suggested design. The mechanism of digital signatures is not new it has been successfully used to implement security features in network protocol.

A thesis done by Perlman and Radia [3] has focused on implementing digital signatures in link state information exchange and distribution. They have used public keys. Certain mechanisms are used to implement security measures; Non-Wrapping finite length sequence numbers were implemented instead of the conventional sequence number scheme. In the presented design when a source whose sequence number does reach the limit can become a new node and it changes its public key. Restructuring of database is also proposed in this design which enables to receive more number of packet as compared to the conventional design. Another design aspect is proposed for flow of data packets in this packet verification is done on the basis of direction of recipient. Link encryption is proposed in the design, a hop by hop encryption mechanism was presented. This design helps in fault isolation as each source generates its own signature using a public key cryptography scheme. A Node, Key pair mechanism was implemented in the design, each such pair is considered a distinct node. It is observed that there is no disruption of service to a node when the key is changed by a node. By large the proposed model works well and shows positive improvements in implementing security to the basic design of the protocol.

A research by kumar and coauthors [4], implementation of secret and public key authentication has been discussed and authentication mechanism has implemented. The security requirements in Inter-domain routing protocols have been presented. It is crucial to incorporate security measures as only directly connected neighbors take part in the interchange of routing updates. Integration of source authenticity mechanism is a difficult task because of hop-by-hop routing of data packets. In this research a balanced design is presented for secure flow and good network performance. With the help of latest technology for conventional cryptosystems through which security mechanism is integrated with inter domain routing protocols. With the help of this approach the design is robust and well aware of malicious threats. This mechanism ensures the security of the protocol without effecting the efficiency of the network.

Finn [5] has discussed the usage of private and public key authentication of different routing protocols. The mechanism elaborated in his research using the identical elementary concepts as mentioned in above research [3]. Another security aspect that is covered here is that it also provided some mechanism to protect forwarding of data packets. The design proposed here outlines some facts to advance the attack confrontation of a network. It is suggested in the design that there link should not be multiplexed into the same physical medium, Link encryption should be implemented using unique private keys. For routing it is suggested in the design that one should engage on the procedure of routing to concurrently preserve set of separate tracks between source and destination. The pair of routers on such tracks must be as closely disjoint as likely. The authors [18] evaluates IPv4 and IPv6 performance under several network conditions, including packet size, routing protocol, and the distance between routers. The authors constructed a virtual network in GNS3 and

examined the combined effect of these parameters using RIP, EORGP, and OSPF. Based on the reported experiments, IPv6 achieved better overall performance than IPv4 under the configurations considered in the study.

Alabady et al. [19] compared the behavior of three dynamic routing protocols, namely EIGRP, OSPF, and RIP, with particular attention to network reliability and performance. Their evaluation considered the convergence characteristics of the protocols under the tested conditions. The reported results indicate that OSPF converged faster than both RIP and EIGRP in their experimental setting. Network security is very important now a days and very challenging task. For network security different deep learning approaches have been investigated of intrusion detection system (IDS) to secure the network [20,21].

More recent studies have continued to examine both the security and design limitations of OSPF. Sawalmeh et al. [22] investigated OSPF-related route spoofing in VPN environments and considered intrusion-detection-based countermeasures. Zhu et al. [23] provided a detailed analysis of OSPF vulnerabilities and evaluated several attack mechanisms together with possible defensive measures. More recently, Gomes et al. [24] addressed limitations of conventional multiarea OSPF routing and proposed an extension for arbitrary multiarea topologies, demonstrating that OSPF continues to evolve beyond its traditional hierarchical design.

3. Security Analysis

There are some built in security mechanism in OSPF which are designed to strengthen the security of protocol. These measures help to mitigate some malicious attacks but fail to handle to more severe attacks [5]. OSPF LSA header detail has been given in Figure 1.

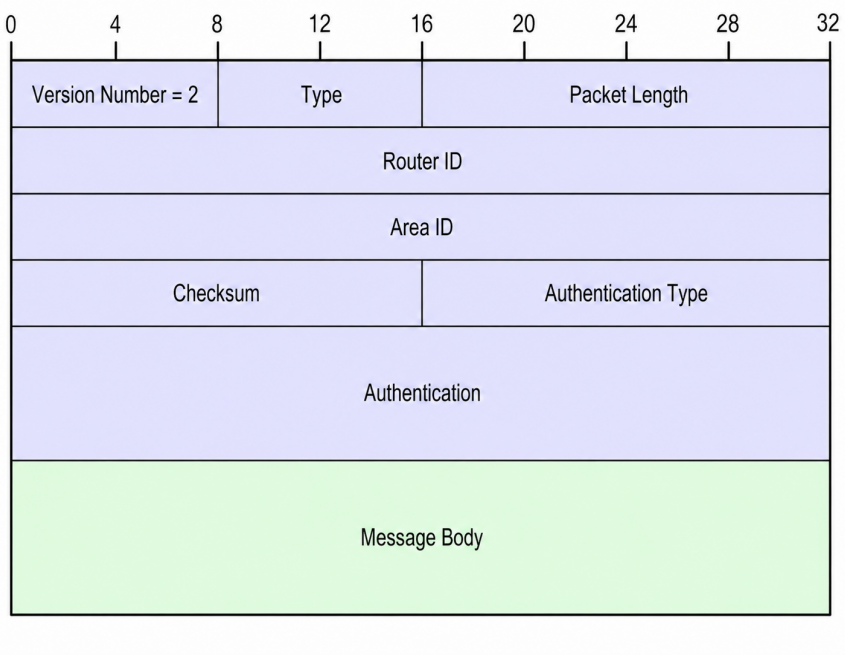


Figure 1: *OSPF LSA header.*

3.1. Authentication Mechanism

Authentication mechanism is embedded in every packet of OSPF routing protocol. Packet header of OSPF has an Authentication field which is 32-Bit in length. There is also an Authen Type field of 16-Bit. The Authen Type field identifies the type of the authentication used. These two fields are the basis of security mechanism in OSPF protocol. Authen Type field can have certain values which are defined by IANA [4]. These values indicate which type of authentication is used in the protocol. A value set to 0 is considered to be NULL authentication which means there will be no authentication mechanism between information exchanges. Encryption is considered one of the most secure authentication type in this particular case. In this a key is generated for all in routers a network. Every router in the network attaches this key with message whenever it wants to exchange routing information with neighboring routers [7]. MD5 has been used with one way hash function. The message generated after performing this operation is called message digest of 32-Bit. If for any reason this message is intercepted by an attacker, they can't see the contents of the message as it is encrypted. So the encrypted message is of no use to anyone until they get the appropriate key. No tampering can be done to the encrypted message, hence at the level of routing information exchange this mechanism can provide integrity of data.

3.2. Hierarchical Routing Mechanism

The size of routing table directly impacts the performance of routing protocol [2]. OSPF routing mechanism is designed in way that it can avoid the problem of large routing tables. The hierarchical design of this protocol ensures smart routing tables and computing resources making it more robust and secure. OSPF uses Autonomous system concept which divides network in different segments. Area Border Router (ABR) is the router

which communicates with other autonomous systems. Every Area is isolated to other area. In this way threat to a certain area do not propagate to other areas in the network. This scheme also reduces the routing table size. In this way hierarchical routing provides security to some extent.

3.3. Fight Back Mechanism of Fake LSA

Fake LSA can cause replay attacks. In this type of attack the adjacency can fail and in some cases can cause high CPU usage. To avoid these kind of attacks OSPF has some built mechanism [4]. LSA level sequence number can help to avoid this attack but not all replay attacks can be avoided with this scheme. The sequence number used in this scheme is per-LSA based. This sequence number increases when LSA is changed. In this way it can avoid replay attack as old LSA cannot be a part of routing information. The database description packets also include a sequence number. If the incorrect sequence number is received the database exchange process restarts. LSA sending has been shown in figure 2.

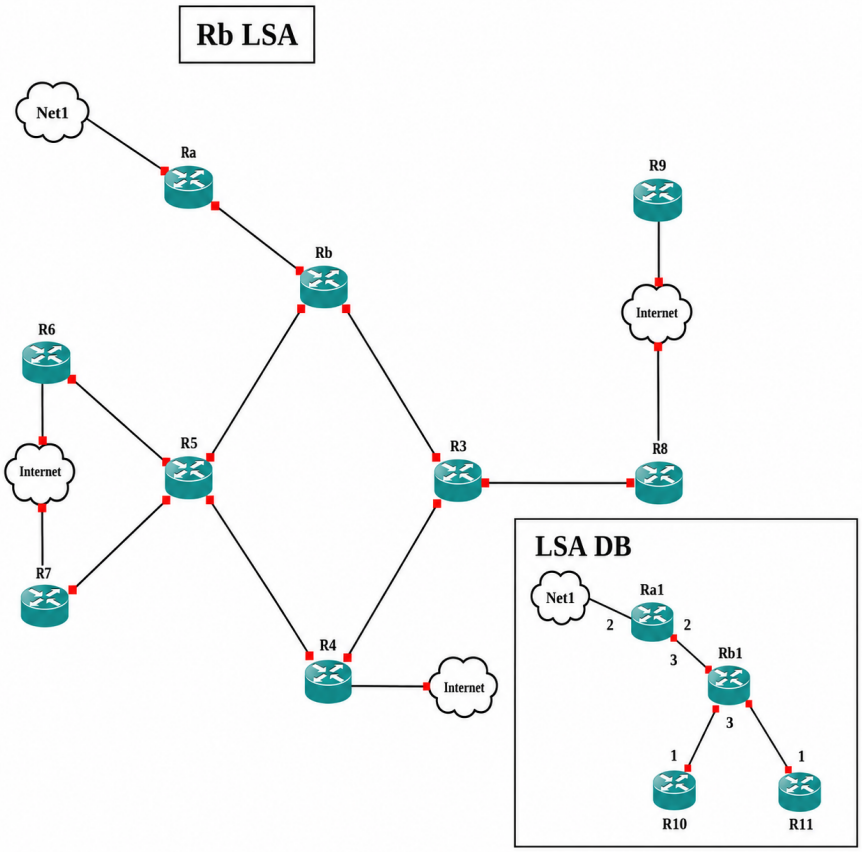


Figure 2: *An example of LSA sending.*

4. Vulnerability Analysis

OSPF protocol has some built in mechanism to handle security threats but still there are some vulnerabilities. Some of the vulnerabilities are identified.

4.1. Plain Text Password Vulnerability

Usually the authentication type is set to 0 which means there is no authentication. In this scenario routers exchange LSAs without any authentication configuration. At receiving end only checksum is calculated to verify the integrity of message if checksum is cleared the packet is forwarded. The forwarded LSA is stored in database of Link State. This configuration

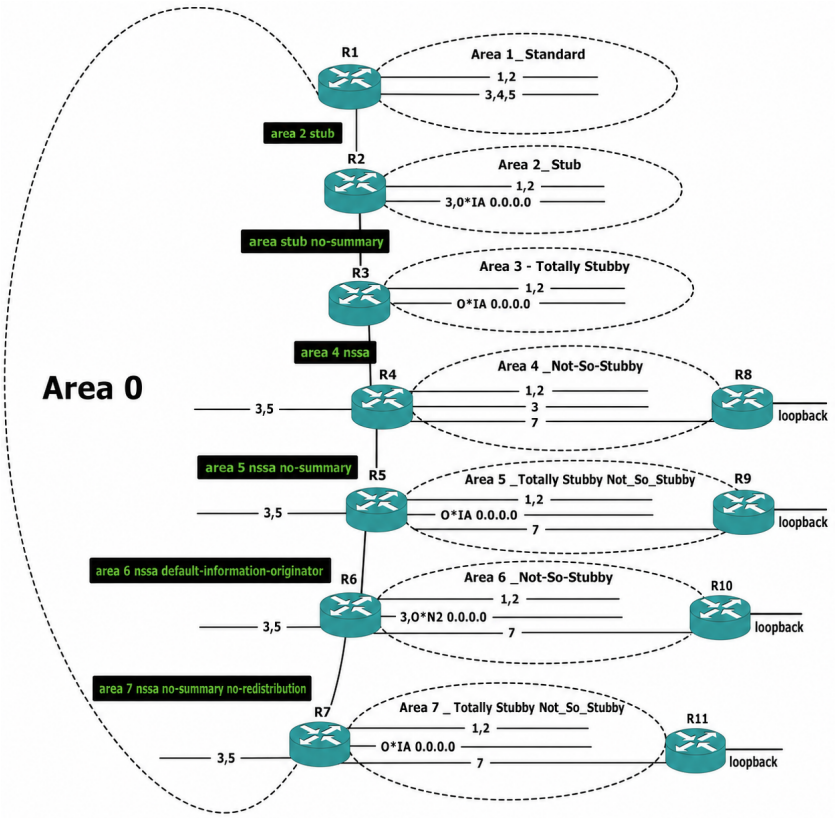


Figure 3: *OSPF areas.*

is considered to be unsecure. As LSA exchange can be attacked by a malicious user and if modified then wrong routing information will be stored in the Link-State Database. It will have a negative impact on the whole topology as wrong routes will be advertised [8].

If the authentication type field is set to 1, a simple password authentication is enabled. In this scenario a simple password is

stored in 64-Bit authentication field. This password along with the message is delivered to destination in plain text form. At the receiving end checksum is calculated and the password is checked. This configuration has a security perspective flaw. If the message is intercepted during transmission. The attacker can easily understand the password as it is sent in plain text form. The OSPF packet can be modified by the attacker and then can be retransmitted with the wrong information. This could lead to a routing disruption. When the authentication option is enabled it could stop some attacks but eavesdropping cannot be avoided with this configuration.

4.2. MaxAge Field Vulnerability

In OSPF LSA has a very crucial role in routing information exchange. The header of LSA has a very important field called LS age. It indicates the time when LSA is created and that time is modified in a fixed defined way. Whenever LSA passes from a router the value of this age field is modified. LS age field is not part of the MD5 digest because its value has to be updated on every router on its way from source to a destination.

If the LSA is intercept during transit from source to destination and attacker modifies this LS age field values then it could cause serious problems. If an attacker can modify the value of age field to MaxAge the LSA will be outdated prematurely. It will corrupt the link-State Database [9]. Once the database is corrupted the wrong route information will propagate to all neighboring routers and will cause a disruption. It is difficult to troubleshoot this kind of attack as it propagates seamlessly.

4.3. Sequence Number Vulnerability

LSA header has another important field called LS sequence number. Each LSA specifies its own unique number. It is a signed 32-bit integer field. The main purpose of this field is to identify the old and duplicate link state advertisements.



Figure 4: *Simulated topology.*

LS sequence numbers are linearly ordered. The most large sequence number will be representing most recent link state advertisement [10].

In case of an attack the LS sequence number field can be modified to an initial value. This type of situation caused a replay attack. External attacker can dissipate the router resources by directing malicious packets. This could also interrupt the adjacency relationship between OSPF neighbors. During the attack scenario router recalculates shortest path again and again and sudden changes happen in the routing table. Consequently, LSAs of the corresponding link are also modified which cause route flapping. Detail of OSPF areas has been shown in Figure 3.

5. Methods

The vulnerabilities identified in the previous section can be overcome by implementing some encryption techniques. The protection method for the simple password vulnerability is to implement encryption authentication to resolve the weakness of varying OSPF packets and producing new packets [4]. The latest encrypted serial number from the recent router must be kept by all connected and neighbor routers (static storage, to avoid loss after restart). The newest encrypted serial number of packet of OSPF should be higher or at least equal to stored encrypted serial number in router. Although the encrypted authentication susceptibility, Link State Update package header is communicated in the form of plain text which will create chances to unauthorized users to making amendments in the LSU (Link State Update) package.

Every router in the network finds its neighbors router through hello packet and interchange its information database. This is “forming an adjacency” and “synchronizing databases”. Routing database of every router combined with each other and form a distributed databases of routing. The LSA (link state advertisement) is flooded all over the network, time to time and when the changes followed in the information. Numerous copies of the same LSA may be received by the router but the most updated is kept and transmitted which is rely on the encrypted sequence number and age fields [11].

The sequence number is produced by the originating router which has initially produced it and boosted with each periodic propagation of the Link State message. Every LSA is aged at the forming router and the other neighbor routers through which it explorations. When the age of LSA extents to maximum age (MaxAge) at a router, it is eliminated from the database of router and propagated to the network for eradication the distributed routing database. As for as security concerns MD5 algorithm is not very sheltered because recent events have shown that it can also be deciphered. Therefore digital signature is suggested as a protection mechanisms for OSPF routing protocol. The prime idea behind the design of digital signatures is that LSA data of OSPF must be integrated with digital signature and recommended the usage of authentication algorithm within neighbor to neighbor to secure the distribution of all protocols [13].

Link state information engaged by initiator router and digital signature must be integrate with the data during transmission through OSPF overflowing. Such approach will deliver one end to another end reliability and endorsement for LSA data. Routers which are provided digital signatures are called “authenticated routers”, and incorporated with non-authenticated routers. A digital signature attached to an LSA by the source router provides verification verify that the data transmit from the advertising router. This procedure assure that that information has not been changed in transit by any unofficial user. If faulty router distribute the inaccurate routing data then the digital signature have a method to trace route the issue from its originating position.

This mechanism must be executed with some main components. It can provide sustenance for a digital signature algorithm in authenticated routers. This will be in confirmation to provide a signed version of all routing information LSA. This one also have a provision for new LSA Router Public Key [5]. Now, all typical functions of normal OSPF router can be performed by authenticated OSPF router. In accumulation of normal functionality, an authenticated OSPF router produce routing data with signed LSA, achieves information of signature algorithm and key, validates the received signature, and conducts information LSA of new key. Type-of-service (TOS) routing should be sustained by authenticated OSPF router. Particular link can be recognized by the fields which are LSA type, Link ID and Advertising router ID. Link ID for the confirmation of link and other ID is used for the confirmation of advertising router. Sequence number and checksum are two significant fields which recognize particular instance of LSA [14].

Router 1 Configurations

1. Interface Loopback 0
2. IP address 172.16.10.36 255.255.255.240
3. Interface Serial 0/0
4. IP address 192.16.64.1 255.255.255.0
5. IP OSPF message-digest-key 1 MD5 c1$c0
6. Router OSPF 10
7. Network 172.16.0.0 0.0.255.255 area 0
8. Network 192.16.64.0 0.0.0.255 area 0
9. Area 0 authentication message-digest

Figure 5: *Configuration of R1.*

The information which includes in the signature is hash algorithm, key size, key identifier, and signature algorithm with identification. MD5 and SHA are definite selections for the hash algorithm, RSA and DSA are used for the signature algorithm. The key identifier has the functionality to identify the production of multiple keys for the usage of signature creation. This can simplicity be transmission of a new key. The signature identification algorithm, size of key, and hashing algorithm provide wide range in areas of autonomous system which have access of multiple signature algorithms. With the help of this extensibility can be achieved if size of the key have inadequate security or the availability of the asymmetric cryptography algorithms.

LSA header has an age field which identifies the length of time spent by LSA in system. The router which has originally produced this LSA along with all other routers that transmit an LSA will enhance the age of LSA. Following field's checksum, age and the sequence number permits the confirmation of most updated LSA in the router. When an age of LSA kept in the database of any other router and reaches a set maximum age (MaxAge), it is eliminated from own database of router and propagated to the network to eradication the distributed routing database. (MaxAge) maximum age is considered more "recent" as compared to other age, each router accepted upon reaching this and cause the resultant LSA to be eradicated from local databases. This technique is used to eliminate the obsolete information from distributed routing tables and databases [2]. In case of failure of router then its LSA may extent MaxAge in different routers in area and will be eliminated. If the outdated LSA of router purged by itself from system in that case age will be precipitately adjust to MaxAge and propagate the LSA. Although this mechanism is pretty much optimal in working but this particular component of the protocol is rarely protected by digital signature scheme [15].

The signature normally does not have age field as this field must be updated by routers other than the originating router which produced original LSA. This is the most prime motive that the age field must not integrated in the checksum computation. The age field must be sheltered, in case of out of order router aged the neighbor router's LSA's (Age field value updated to MaxAge) this will disturb routing with the help of faulty router. In order to given protection to the age field, the signature must append the age field only when age field value comes to MaxAge. If the value field reaches to MAXAGE value only then there is a possibility to add age field in signed LSA.

6. Experiment with Results

A simulated network model is established in GNS3 simulator. According to infonetrics research, almost 75% enterprise networks use Cisco's in world [8]. Two Cisco-2500 series routers have been used in this simulated topology. All these routers have been directly connected with each other via serial links. OSPF protocol has been configured using MD5 algorithm in this topology. Network topology is shown in Figure 4.

6.1. Configuration of MD5 Algorithm

Router 1 has been configured with the OSPF configurations and MD5 algorithm for securing the transmission of packets from R1 to R2. These configuration need to be configured on both routers. Router 1 configuration detail, at line#1, 2 a loopback interface 0 has been created and assigned IP address 172.168.10.36. At line#3, 4, 5 configure the serial interface 0/0 and assign IP address 192.16.64.1 followed by a command to enable the authentication mechanism using

Router 2 Configurations

1. Interface Loopback 0
2. IP address 70.70.70.70 255.255.255.255
3. Interface Serial 0/0
4. IP address 192.16.64.2 255.255.255.0
5. IP OSPF message-digest-key 1 MD5 c1$c0
6. Clockrate 64000
7. Router OSPF 10
8. Network 192.16.64.0 0.0.0.255 area 0
9. Network 70.0.0.0 0.255.255.255 area 0
10. Area 0 authentication message-digest

Figure 6: *Configuration of R2.*

Algorithm 1 Verification of MD5 Authentication in OSPF

1: **Command:** `show ip ospf interface serial 0/0`
2: Serial0 is up; line protocol is up.
3: Internet address: `192.16.64.1/24`, Area 0.
4: Process ID: 10; Router ID: `172.16.10.36`; Network Type: `POINT_TO_POINT`; Cost: 64.
5: Transmit delay: 1 sec; State: `POINT_TO_POINT`.
6: Timer intervals: Hello = 10 sec, Dead = 40 sec, Wait = 40 sec, Retransmit = 5 sec.
7: Hello due in `00:00:05`.
8: Index: 2/2; flood queue length: 0.
9: Next: `0x0(0)/0x0(0)`.
10: Last flood scan length: 1; maximum: 1.
11: Last flood scan time: 0 msec; maximum: 4 msec.
12: Neighbor count: 1; adjacent neighbor count: 1.
13: Adjacent neighbor: `70.70.70.70`.
14: Suppress Hello for 0 neighbor(s).
15: **Message-digest authentication enabled.**
16: **Youngest key ID is 1.**

MD5 algorithm with password c1$c0 which is used for protecting the link from unauthorized access. This hashing algorithm is enables on both interfaces now. At line#6 configure the OSPF routing protocols on Router 1 (R1) using command router OSPF 10, here 10 is the autonomous number. At line#7, 8 enter the network address on which OSPF wants to be executed, so in this scenario OSPF run on the 172.16.0.0 networks which belongs to loopback address and 192.16.64.0 network which belongs to the WAN link with Area 0. At line#9 Area 0 is the back bone area in OSPF. Next command Area 0 authentication message-digest used for to secure the complete Area 0 using MD5 algorithm.

Router 2 configuration detail, at line#1, 2 loopback interface 0 has been created and assigned IP address 70.70.70.70. Then at line#3, 4, 5 configure the serial interface 0/0 and assign IP address 192.16.64.2 followed by a command to enable the authentication mechanism using MD5 algorithm with password c1$c0 which is used for protecting the link from unauthorized access. This hashing algorithm is enables on both interfaces At line#6 set the clock rate 64000 for router 2. At line#7 configure the OSPF routing protocols on Router 2 (R2) using command router OSPF 10, here 10 is the autonomous number. At line#8, 9 enter the network address on which OSPF wants to be executed, so in this scenario OSPF run on the 70.0.0.0 networks which belongs to loopback address and 192.16.64.0 network which belongs to the WAN link with Area 0. Here Area 0 is the back bone area in OSPF. Next command at line#10 Area 0 authentication message-digest used for to secure the complete Area 0 using MD5 algorithm.

Verification of MD5 algorithm is with the help of command give at line#1. Confirmation of MD5 algorithm enabling given at line#15, 16 in Alogrithm 1.

7. Conclusion

Routing information of all neighbors routers must be securely and accurately delivered which is usually circulated by the OSPF routing protocol. Digital signature techniques can be used to secure and protect the source integrity and authenticity. This research article elaborated a design in which digital signatures integrated with the LSA data. This design protects the routing database from internal and external invaders also secure interior causes of error, specially the contributors in the protocol which are supposed to be unsecure. Another concept of implementation of hashing algorithm MD5 using simulator GNS3 has been configured on routers using OSPF routing protocols. Router are presented to circulate the hashing algorithm to all other routers which are in the area of autonomous system through the flooding method of OSPF. A reliable authentication of binding among the router ID and public key. This authentication must be included in the OSPF Area 0. After implementation of all above techniques and mechanisms routing information is secure and has ability to protect from DOS (denial of Service) attacks. Somehow, still have some advance level attacks through which routing information may be modified and traceable.

Author Declarations

Author Contributions (CRediT): Atif Manzoor: Conceptualization, Methodology, Software, Investigation, Formal Analysis, Writing - Original Draft.

Funding: No external funding was received for this research.

Data Availability Statement: Not applicable

Acknowledgments: No acknowledgments are reported.

Conflicts of Interest: The author reports no conflicts of interest.

Ethics Statement: Not applicable

Declaration of Generative AI: An AI-assisted tool was used during manuscript preparation for language editing and formatting support. The author checked the revised content and remains responsible for the accuracy, integrity, and content of the manuscript.

References

[1] E. Kaffashi, A. M. Mousavi, H. R. Rahvard, S. H. Bojnordi, F. Khademsadegh, and S. Amirian, "A new attack on link-state database in Open Shortest Path First routing protocol," *Journal of Electrical and Electronic Engineering*, vol. 3, no. 2-1, pp. 39-45, 2014. doi: 10.11648/j.jeee.s.2015030201.19.

[2] S. L. Murphy and M. R. Badger, "Digital signature protection of the OSPF routing protocol," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, pp. 93-102, 1996. doi: 10.1109/NDSS.1996.492416.

[3] R. J. Perlman, "Network layer protocols with Byzantine robustness," Ph.D. dissertation, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, 1988.

[4] B. Kumar and J. Crowcroft, "Integrating security in inter-domain routing protocols," *ACM SIGCOMM Computer Communication Review*, vol. 23, no. 5, pp. 36-51, 1993. doi: 10.1145/165611.165615.

[5] G. G. Finn, *Reducing the Vulnerability of Dynamic Computer Networks*, ISI Research Report ISI/RR-88-201, Information Sciences Institute, University of Southern California, Marina del Rey, CA, USA, Jun. 1988.

[6] A. A. Vladimirov, K. V. Gavrilenko, J. N. Vizulis, and A. A. Mikhailovsky, *Hacking Exposed Cisco Networks: Cisco Security Secrets & Solutions*. New York, NY, USA: McGraw-Hill/Osborne, 2006.

[7] S. Waichal and B. B. Meshram, "Router attacks: Detection and defense mechanisms," *International Journal of Scientific & Technology Research*, vol. 2, no. 6, pp. 145-149, 2013.

[8] W. Odom, *CCNP ROUTE 642-902 Official Certification Guide*, 1st ed. Indianapolis, IN, USA: Cisco Press, 2010.

[9] G. Nakibly, E. Menahem, A. Waizel, and Y. Elovici, "Owning the routing table-Part II," presented at *Black Hat USA*, Las Vegas, NV, USA, 2013.

[10] Cisco Systems, "Configuring BGP," in *Cisco IOS IP Configuration Guide, Release 12.2*. Cisco Systems, 2006. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfbgp.html. Accessed: Feb. 8, 2019.

[11] F. Le, G. G. Xie, and H. Zhang, "Understanding route redistribution," in *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, pp. 81-92, 2007. doi: 10.1109/ICNP.2007.4375839.

[12] D. F. Asigbe, A. M. Mustapha, C. C. M. Agbesi, B. F. Ephraim, A. S. K. Bright, and S. Clement, "Performance analysis of Interior Gateway Routing Protocol (EIGRP) over Open Shortest Path First (OSPF) protocol," *International Journal of Scientific & Technology Research*, vol. 5, no. 9, pp. 111-117, 2016.

[13] S. Vissicchio, L. Vanbever, L. Cittadini, G. G. Xie, and O. Bonaventure, "Safe routing reconfigurations with route redistribution," in *Proceedings of IEEE INFOCOM*, pp. 199-207, 2014. doi: 10.1109/INFOCOM.2014.6847940.

[14] R. Graziani and A. Johnson, *Routing Protocols and Concepts: CCNA Exploration Companion Guide*. Indianapolis, IN, USA: Cisco Press, 2008, ch. 3, "Introduction to Dynamic Routing Protocols."

[15] S. G. Thorenoor, "Dynamic routing protocol implementation decision between EIGRP, OSPF and RIP based on technical background using OPNET Modeler," in *Proceedings of the 2nd International Conference on Computer and Network Technology (ICCNT)*, pp. 191-195, 2010. doi: 10.1109/ICCNT.2010.66.

[16] Z.-Z. Wei and F. Wang, "Achieving resilient routing through redistributing routing protocols," in *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 1-5, 2011. doi: 10.1109/ICC.2011.5962605.

[17] S. S. Samaan, "Performance evaluation of RIPng, EIGRPv6 and OSPFv3 for real-time applications," *Journal of Engineering*, vol. 24, no. 1, pp. 111-122, 2018. doi: 10.31026/j.eng.2018.01.08.

[18] S. A. Alabady, S. Hazim, and A. Amer, "Performance evaluation and comparison of dynamic routing protocols for suitability and reliability," *International Journal of Grid and Distributed Computing*, vol. 11, no. 7, pp. 41-52, 2018. doi: 10.14257/ijgdc.2018.11.7.05.

[19] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231-48246, 2018. doi: 10.1109/ACCESS.2018.2863036.

[20] S. Naseer and Y. Saleem, "Enhanced network intrusion detection using deep convolutional neural networks," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 10, pp. 5159-5178, 2018. doi: 10.3837/tiis.2018.10.028.

[21] A. Arsalan and R. A. Rehman, "Interest broadcasting and timing attack in IoV (IBTA-IoV): A novel architecture using Named Software Defined Network," *Computer Networks*, vol. 213, Art. no. 109121, 2022. doi: 10.1016/j.comnet.2022.109121.

[22] H. Sawalmeh, M. Malayshi, S. Ahmad, and A. Awad, "VPN remote access OSPF-based VPN security vulnerabilities and counter measurements," in *Proceedings of the 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 236-241, 2021. doi: 10.1109/3ICT53449.2021.9581512.

[23] X. Zhu, W. Bao, J. Zhang, Y. Jiang, and H. Ma, "Research and analysis on the vulnerability of OSPF routing protocol," *Journal of Cyber Security*, vol. 8, no. 2, pp. 42-53, 2023. doi: 10.19363/J.cnki.cn10-1380/tn.2023.03.04.

[24] X. Gomes, J. Fonseca, and R. Valadas, "Open Shortest Path First extension for the support of multiarea networks with arbitrary topologies," *IET Networks*, vol. 13, no. 3, pp. 241-248, 2024. doi: 10.1049/ntw2.12112.