International Science and Technology Journal
المجلة الدولية للعلوم والتقنية

Volume 36 العدد
Part 1 المجلد

http://www.doi.org/10.62341/atae1916

Received	2024/12/02	تم استلام الورقة العلمية في
Accepted	2025/01/10	تم قبول الورقة العلمية في
Published	2025/01/16	تم نشر الورقة العلمية في

Enhanced RSA Key Management Mechanism for Control Packet Protection in Optical Burst Switching Networks

Athman Ahmed Alkilany[a]

[a] Department of Information Technology, Higher Institute of Science and Technology - Tamzaoua El Shati, Libya
otmanutm@gmail.com

Abstract

Optical Burst Switch (OBS) network is a typical technology currently proposed, as an infrastructure to deal with most highly demanded communication services. OBS architecture consists of Data Burst (DB) as a payload and Burst Header Packet (BHP) as a control packet. BHP carries important information about path reservation and its corresponding DB. However, the information security (Privacy, Reliability, Confidentiality, Integrity, Availability, Authentication, and Authorization) of OBS network communication has been represented as the current issues, which affect the network performance in terms of data loss and data transmission delay. This paper focuses on security weaknesses of BHP transmission in OBS network against Data Burst Redirection (DBR) Attack. The current paper was conducted to develop a protection mechanism to ensure the confidentiality and authentication of BHP. In OBS, RSA public-key encryption algorithm has been enhanced and integrated. Moreover, the Self-Controlling key distribution technique has been implemented to ensure a high security level of key transmission between each pair of OBS nodes. Three different OBS environments have been designed and implemented. These environments were established on the bases of three different concepts; OBS Topology without Security Measures and without Security Attacks, OBS Topology under Security Attacks without Security Measures, and OBS Topology under Security Attacks with Security Measures. The obtained results are based on Burst Loss Ratio, Throughputs, and Average Delay Ratio. Such a result has successfully proved the trustworthiness and efficiency of Control Packet Protection Technique (CPPT-OBS) to prevent DBR attack.

Keywords: OBS , DB, BHP, DBR, RSA, CPPT

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 36 العدد
Part 1 المجلد
المجلة الدولية للعلوم والتقنية
International Science and Technology Journal
ISTJ
http://www.doi.org/10.62341/atae1916

آلية إدارة مفتاح RSA المحسّنة لحماية حزم التحكم في شبكات تبديل الاندفاع البصري

* عثمان احمد الكيلاني
قسم تقنية المعلومات، المعهد العالي للعلوم والتقنية – تامزاوة الشاطئ، ليبيا

الملخص

تعد شبكة تبديل الاندفاع البصري (OBS) تقنية نموذجية مقترحة حاليًا كبنية تحتية للتعامل مع خدمات الاتصالات الأكثر طلبًا. تتكون بنية OBS من Data Burst (DB) كحمولة صافية وBurst Header Packet (BHP) كحزمة تحكم. تحمل BHP معلومات مهمة حول حجز المسار وقاعدة بياناتها المقابلة. ومع ذلك، فإن أمن المعلومات (الخصوصية والموثوقية والسرية والنزاهة والتوافر والمصادقة والتفويض) لاتصالات شبكة OBS قد تم تمثيلها على أنها المشكلات الحالية التي تؤثر على أداء الشبكة من حيث فقدان البيانات وتأخير نقل البيانات. تركز هذه الورقة على نقاط الضعف الأمنية في نقل BHP في شبكة OBS ضد هجوم إعادة توجيه انفجار البيانات (DBR). تم إجراء الورقة الحالية لتطوير آلية حماية لضمان سرية ومصادقة BHP. في OBS، تم تحسين خوارزمية تشفير المفتاح العام RSA ودمجها. علاوة على ذلك، تم تنفيذ تقنية التوزيع الرئيسية للتحكم الذاتي لضمان مستوى أمان عالٍ لنقل المفتاح بين كل زوج من عقد OBS. تم تصميم وتنفيذ ثلاث بيئات OBS مختلفة. تم إنشاء هذه البيئات على أساس ثلاثة مفاهيم مختلفة؛ طوبولوجيا OBS بدون إجراءات أمنية وبدون هجمات أمنية، وطوبولوجيا OBS ضمن الهجمات الأمنية بدون إجراءات أمنية، وطوبولوجيا OBS ضمن الهجمات الأمنية مع الإجراءات الأمنية. تستند النتائج التي تم الحصول عليها إلى نسبة خسارة الاندفاع، والإنتاجية، ومتوسط نسبة التأخير. أثبتت هذه النتيجة بنجاح مصداقية وكفاءة تقنية حماية حزمة التحكم (CPPT–OBS) لمنع هجوم DBR

الكلمات المفتاحية: OBS – التبديل البصري للانفجار، DB – انفجار البيانات، BHP – حزمة رأس الاندفاع، DBR – إعادة توجيه انفجار البيانات، RSA – خوارزمية التشفير، CPPT – تقنية حماية حزم التحكم

http://www.doi.org/10.62341/atae1916

Introduction

The optical network has the ability to overcome most of the existing issues in the electronic network. One such issue is the traffic load with high capacity which is not available in the electronic network. Some advantages of the optical network are its ability to carry lots of data with high capacities and transmitting the data rapidly through the channels[1][2]. On the other hand, an optical network is prone with several defects. There are many issues that prevent it to be a totally end-to-end optical network which be utilized for connecting to the Internet. For example, the network equipments are characterized with high capital cost, and an optical network provides bufferless of handling the traffic. Consequently, the optical network represents the next generation of the core area of the Internet[1].

Historically, the optical network has undergone many generation stages. This project concerns on the Optical Burst Switching (OBS) networks. OBS represents the next generation of optical networks switching technologies. An optical burst switching network consists of optical burst switching nodes that are interconnected via optical fiber links. Each fiber link is capable of supporting multiple wavelength channels using Wavelength Division Multiplexing (WDM)[1][2]. The edge nodes in an OBS network are responsible for assembling and disassembling packets into burst, and scheduling the bursts for transmission on outgoing wavelength channels. The core nodes are primarily responsible for switching bursts from input to output ports [3][4].

Problem Background

The sensitive information in OBS networks is stored in Data Burst (DB) which carries a collection of different packets, and its corresponding Burst Header Packet (BHP) which known as Control Packet Header is forwarded ahead for resources reservations on the selected path[3][1]. The BHP contains traffic information, burst length, offset-time between BHP and its followed DB. The two main concerned approaches in OBS network are packet lost and packet delay issues [3][4]. Moreover, the security weaknesses are new opened issues in OBS area with respect to the main security elements (Confidentiality, Integrity, and Availability)[5].

In OBS networks, each DB is associated with its corresponding BHP, which is sent ahead of the DB on different WDM channel. The BHP's task is making a proper reservation for its corresponding DB, as well as DB's path information for path configuration [6]. If

http://www.doi.org/10.62341/atae1916

the scheduling request is rejected at one OBS core node, then; there will never be validation of optical path setting-up for the arriving DB.

Since, the DB will be arrived to an input port core node, which no longer belongs to its corresponding BHP; it will be dropped or reach to unpredictable destination [7][8].

In other case, when the authenticated BHP arrives to the compromised core node, the attacker will start lunching abusive actions before the corresponding DB reaches to this node. If an attacker injects his malicious BHP instead of an authentic BHP during an Offset-time between DB and its authentic BHP, and associates a new relationship between malicious BHP and reserved DB; then forwarding path of incoming DB has changed to a fake destination by following a new associated malicious BHP [7][8]. This attack is called Data Burst Redirection Attack as showing in Figure 1.

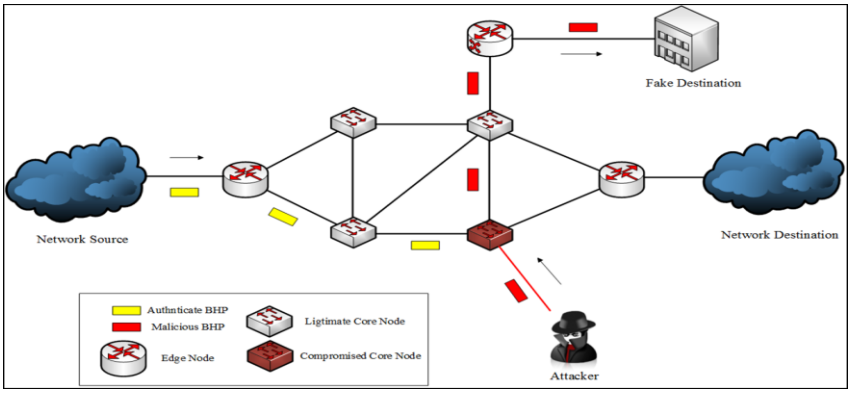

Figure 1: Data Burst Redirection Attack Scenario [9]

The main proposed solution to mitigate Data Burst Redirection attack is RSA public-key encryption algorithm [10][11][12][13]. But the public key distribution management is more complicated in OBS network. The complexity is related to generating a Trusted Third Party (TTP) which must be individually connected to all OBS nodes, and the ability to securely update all distributed keys to the entire participants in OBS network[13][14]. Additionally, the encoding and decoding processing time increases End-to-End delay depending on burst length. Because, long burst length takes more processing time to be encrypted and decrypted in each OBS node. However, when BHP length is small; BHP takes shorter time to be encrypted and decrypted [13].

http://www.doi.org/10.62341/atae1916

Regarding key management issue in OBS network, public key distribution process will be very weak against Man-in-the-middle Attack [15][16][17]. In such attack, attacker can fraud between any two connected OBS nodes by creating two malicious public keys. One public key between one node and himself, and another public key between himself and the next connected OBS node. So, the attacker can control the traffic flow between these two nodes by passively exposing the encrypted BHP and actively making some alterations on the encrypted BHP as well [18].

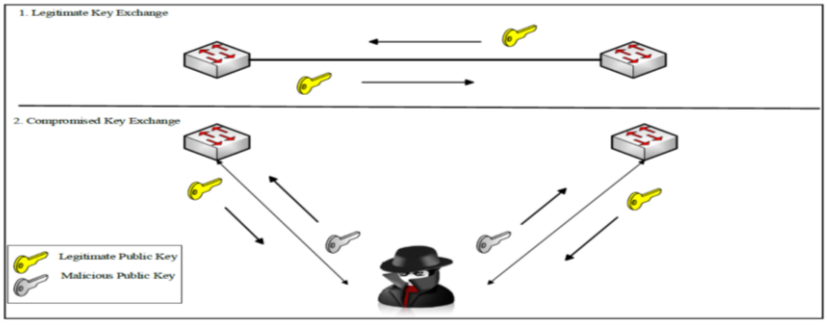

Figure 2. Man-in-the-middle Attack Scenario [18]

Thus, the secret public key exchange technique should be implemented to ensure that encrypted BHP travels across OBS nodes securely, and more difficult for Man-in-the-middle attack to compromise and expose the traffic information [5]. Due to vital value of BHP in OBS network, this project proposes a new security technique to protect BHP against DBR attack in OBS network. A special public key management mechanism will be used for that purpose.

Experimental Work.

Generally, the analysis phase is quite important for generating a new or developing an existing technique. Based on this concept, this phase explains OBS network environment, security issues related to establishing and forwarding data bursts and their BHPs. Additionally, several passive attack actions are launched against the established OBS network to show security vulnerabilities of this network. There are several requirements to analyze and implementing the OBS network as following:

http://www.doi.org/10.62341/atae1916

Table 1: The Necessary Parameters for OBS Network Configuration

No	Parameters	Assigned Values
1	NSF Network Topology	14 Core Nodes, 4 Edge Nodes
2	IP networks	2 Senders, 2 Receivers
3	Optical Fibers	25 Links
4	Traffic Load Trace Files	10 Files
5	Protocols	TCP and UDP
6	TCP Port Numbers	8800, 10051,10050,3353
7	UDP Port Numbers	3000,5000
8	Maximum Bandwidth Length	1000Mbps
9	Transmission Delay Time	1 ms
10	3 Optical Channels	1 Control Packet, 2 Data Burst
11	Control Packet Processing Time	2 ns
12	Switching Time	20 ns
13	Burst Timeout Send	10 ms
14	Burst Size	10000 Bytes
15	Maximum Queue Length	60000 Bytes
16	RSA (256–512) bit Processing time	(1-100 ms),(100-500 ms)
17	RSA (256-512) bit Lifetime	1- 2 hours
18	break RSA (256-512) keys time	(1-2s),(1-2h)

By using these parameters, the topology is generated, the network configuration is established, and trace files are created as traffic sources. The results of this analysis are going to be discussed later.

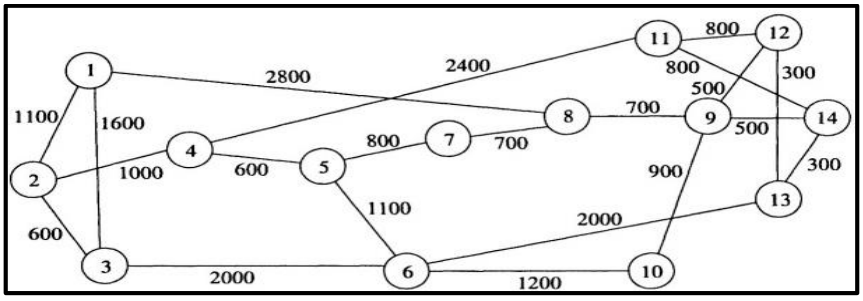

Figure 3.NSF network with 14 Nodes [2]

Implementation of the Control Packet Protection Scheme

In this stage, the new control packet protection scheme will be implemented when all the previous phases are successfully done. Initially, the implementation phase will begin with the installation of Fedora Linux operating system, and successful installation of NCTUns 6.0 simulator[6], and establishing the NSF OBS Network Topology which contains 14 core nodes and 4 edge nodes, and setting-up all required parameters to configure the OBS environment. Additionally, the traffic trace files will be generated by our own Traffic Generator software. These trace files contain the

http://www.doi.org/10.62341/atae1916

variant number of packets with fixed packet size (1024 byte) which are limited based on traffic load size. The traffic load sizes range is allocated as (100, 200, 300… 900, 1000) in bytes. Consequently, the trace files will be integrated with the established OBS topology into NCTUns simulator to generate the network traffics.

Since the OBS network environment is established and lunched successfully, the three main scenarios will be designed. Firstly, OBS Topology without Security Measures and without Security Attacks Scenario. In this scenario, the unsecure OBS network simulation will be launched and the obtained results will be recorded as the ordinary results.

Secondly, OBS Topology under Security Attacks without Security Measures Scenario. In this scenario, several passive attack actions will be launched against the unsecure OBS network to achieve some abuse actions. The abuse actions will affect the network traffic by compromising to controlling the BHPs traffics. This controlling affects the network throughputs with increasing number of dropped packets. The obtained results of compromised OBS network will be recorded as well.

Thirdly, OBS Topology under Security Attacks with Security Measures Scenario. In this scenario, the OBS mitigation scenario will be performed for protecting the BHPs transmissions between each two connected nodes. The protection mechanism will be fulfilled by integrating or injecting our proposed technique in every node in the generated OBS topology. In this case, the OBS network is being more secure. Then, the previous passive attacks will be applied again against the secure OBS network and the obtained results will be recorded as well. Finally, all the recorded results will be analyzed and evaluated in the next phase.

Designing of CPPT-OBS

In the first stage of CPPT-OBS, RSA key management process needs to be enhanced by applying Self-Controlling Key Management Mechanism. Because, OBS network is lacking yet for any key management controlling center such as Trusted Third Party (TTP), Key Distribution Center (KDC), Certification Authority (CA) [14[16][19][20]. In this mechanism, the traffic transmission time will be divided equally and frequently into time slots as shown in Figure 4. At the beginning of each time slot, all OBS nodes start generating temporarily their own random pair keys (Private Key, Public Key) as showing in Figure 5. Then, each node should

http://www.doi.org/10.62341/atae1916

multicast only its public key to all connected neighbor's trough available resources or interfaces. Because, the received public key should be known only among borders (sender and receiver) nodes, and the node's private key must be preserved and kept as a secret key from other OBS nodes. On other word, only the node's neighbors are able to establishing the trusted relationships and generating the secure paths with this node.

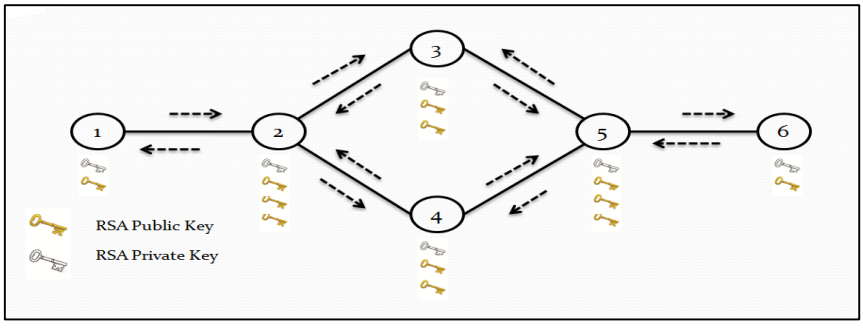

Figure 4. Self-Controlling Key Management Mechanism [21]

Before the second slot time is started, each node should start regenerating its new pair keys randomly. In addition, before multicasting for the new public key to all connected neighbors, sender node encrypts its new public key by its old private key first, then with sender's old public key. The new encrypted public key should be multicoated to all connected neighbors. After sending sender's new encrypted public key, the sender's old private and public keys should be revoked. When a receiver receives the encrypted key, the receiver decrypts the encrypted key with the receiver's old private key and then with sender's old public key. After the new public key is successful received, decrypted and reserved, the old reserved public key of the sender should be revoked and never to be used anymore.

In the second stage of CPPT-OBS, the enhanced RSA encryption algorithm will be integrated with OBS environment as showing in Figure 4. When one node sends its public key and receives all public keys of border nodes in OBS network, this node creates the data collection of neighbor's public keys, which are used frequently for creating secure traffics among them. The secure traffic is generated when the sender node encodes a generated BHP via sender's private key to prove that this packet is coming from sender node (Authentication). The encoded BHP will be encrypted again by using receiver's public key to ensure the confidentiality of the

http://www.doi.org/10.62341/atae1916

encrypted BHP while is been transmitted through a control channel and reached to the receiver. On other word, the generated BHP is encrypted twice before being sending; firstly, with sender's private key and secondly with receiver's public key. This process is called Multi-layers Security mechanism. So, the encrypted BHP should be sent in cipher text format through the optical channel to the receiver OBS node.

Since the encrypted BHP is reached to the receiver node, the receiver will start decrypting back the encrypted BHP. Firstly, the receiver will decrypt the encrypted BHP via receiver's private key to check the confidentiality of the received BHP. If it is compromised, this BHP will be dropped. Else, the receiver node will decode the decrypted BHP via a sender's public key, which is previously kept in receiver site and verifies the authentication of this BHP. If the sender's identity is not authenticated, this BHP will be dropped. Else, the decoded BHP is appeared in the plaintext form again which makes the receiver node able to start reading the carried information and start processing.

Additionally, the sender or receiver node will be decided by their transmission situations. In OBS network, the optical routers and switches are able to send and receive different burst control packets with different signaling and reservation of optical channels. In other words, the OBS node is called a Sender in case of sending OBS traffics, and the exact OBS node will be converted to be a Receiver situation in case of receiving OBS traffics. The Figure 4 illustrates the flowchart of CPPT-OBS for creating a trusted BHP transmission between each two connected OBS nodes.

Developing of CPPT-OBS

As described in the literature review, the OBS network security is weak against DBR attack. Therefore, CPPT-OBS comes to prevent this kind of attack by adapting designed RSA encryption algorithm with enhanced key management. Technically, the researcher started with enhancing the key management processes in RSA which will be later adaptive with OBS environment in NCTUns simulator. Firstly, the researcher developed a public RSAPro class in C++ programming language as showing in Algorithm 1. As shown in figure 5.

http://www.doi.org/10.62341/atae1916

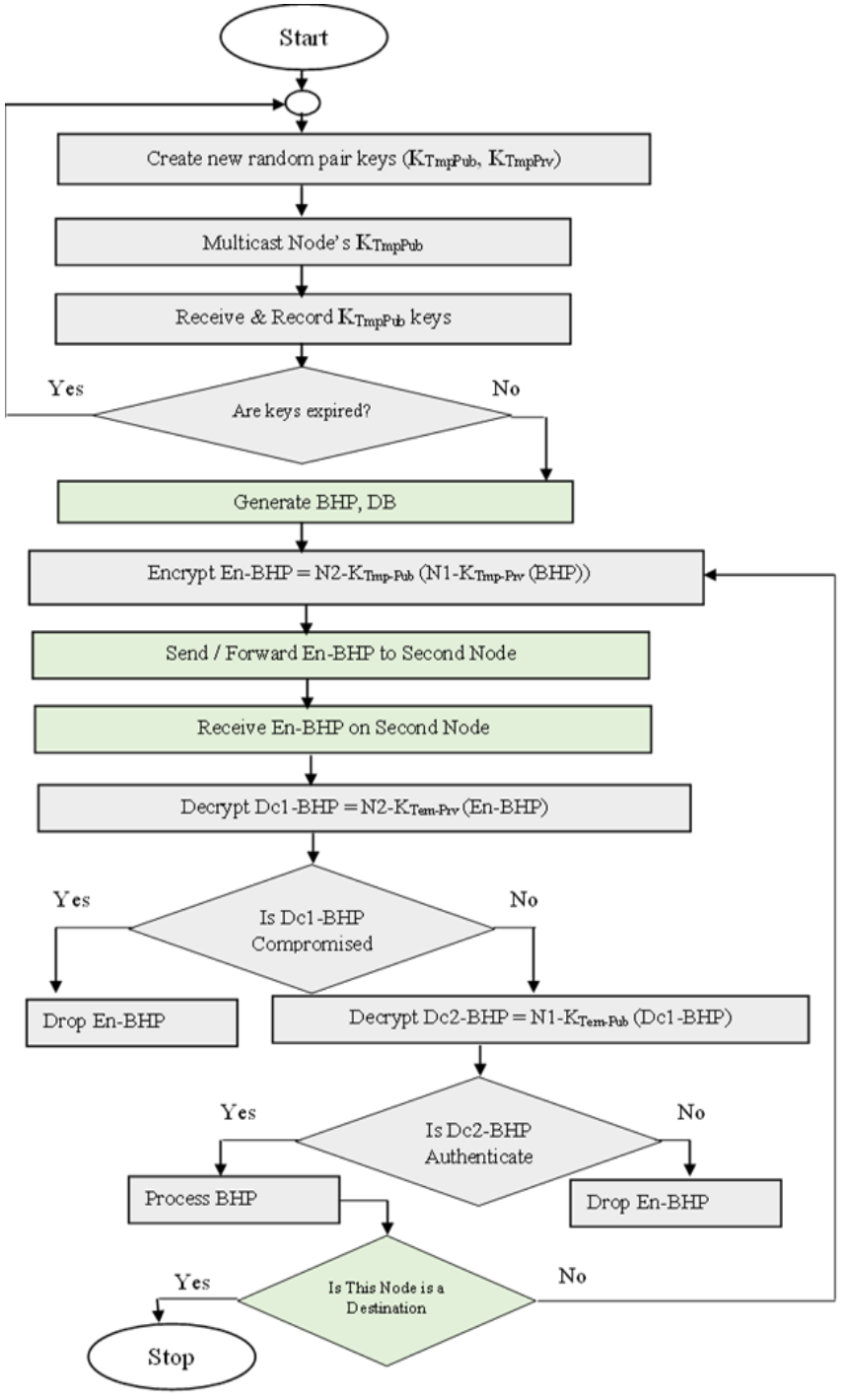

Figure 5. Workflow of CPPT-OBS

http://www.doi.org/10.62341/atae1916

At the beginning, the RSAPro class is functionally developing a group of objects with a list of keys for each object. Each object can save object's pair keys and other public keys of all connected nodes. Each pair keys are generated randomly by finding out a variant of the two big prime numbers. Thus, the RSAPro class generates and assigns different pair keys to all objects frequently for every 5 second.

In key distribution process, the RSAPro class controls the key multicasting technique. Every object has relationships with all connected object. Therefore, the RSAPro class gives orders to all objects for start sending their public keys to their connected objects, and every object keeps all received public keys for encryption and decryption processes. Consequently, the Self-Controlling key management mechanism is being developed and designed successfully.

Results and Discussion

The results of the three main scenarios are analyzed, investigated, compared, and evaluated in terms of the Burst Loss Ratio and Throughputs and Average Delay Ratio. These scenarios were established on the basis of three different concepts. These concepts include OBS Topology without Security Measures and without Security Attacks, OBS Topology under Security Attacks without Security Measures, and OBS Topology under Security Attacks with Security Measures.

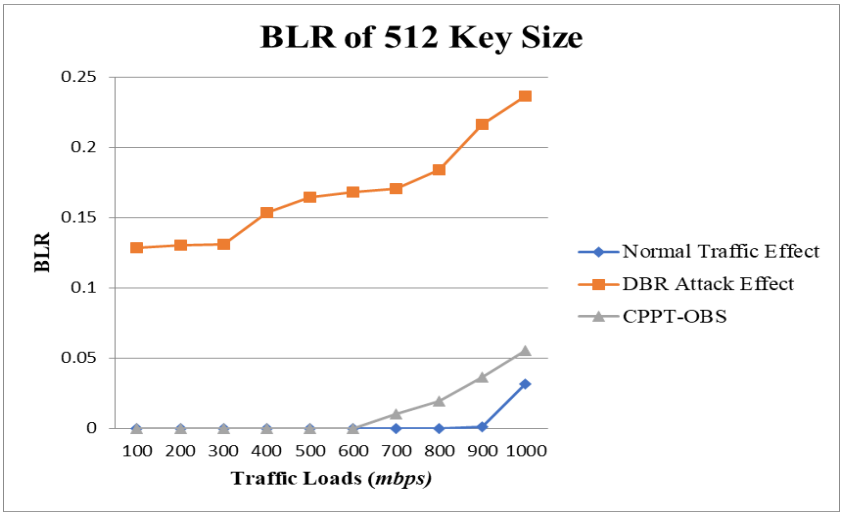

Figure 6. BLR with 512 Key Size

http://www.doi.org/10.62341/atae1916

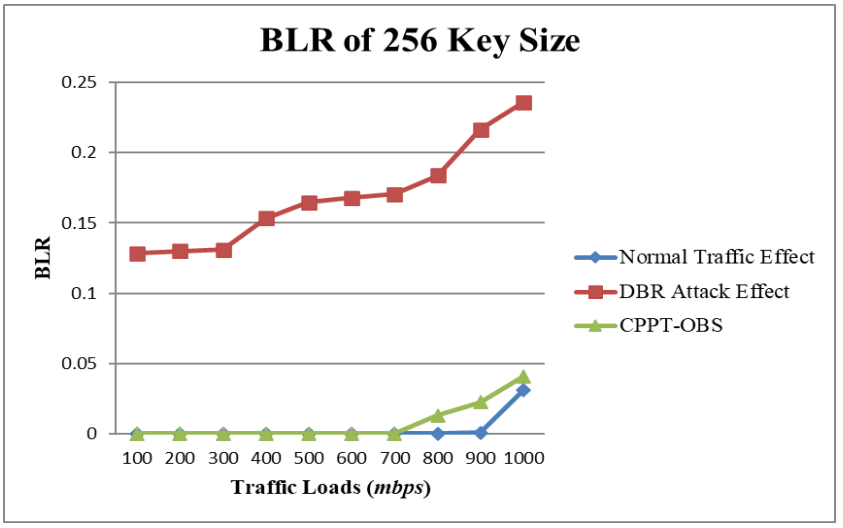

Figure 7. BLR with 256 Key Size

Figure 6 and Figure 7 are showing the Burst Loss Rate (BLR) in variant of OBS traffic loads. BLR is based on three different OBS environments (Normal Traffic Effects, DBR Attack Effects, and CPPT-OBS with 512 and 256 key sizes Effects). Regarding the literature review, the network traffics are affected by increasing of traffic loads, bursts congestions, increasing of packets delay in assembly queue, and etc. All these issues are out of scope for this research. In Figures (7, 8), the normal OBS traffic shows that BLR is lowly increasing by increasing traffic loads. On the other side, DBR attack effect is highly impacting to unsecure OBS traffic. In low traffic loads, the generated BHP is forward ahead of its corresponding DB with a long-offset time. So, the DBR attacker takes advantage of this situation. The DBR attacker got more time to modify and redirecting captured BHPs since the offset time is long. Consequently, the unsecure OBS environment with load traffic loads is a vulnerable against DBR attack.

The BLR is increased in medium and high traffic loads. Because, the offset time between a BHP and its corresponding DB is shorter than offset time in the low traffic load. Thus, the traffic congestions may happen when the DBR attacker attempts to redirect BHPs traffics. Because, the incoming BHPs with short offset time cannot be delayed while compromised BHPs are being modified. Then, the delayed BHPs will be dropped and their corresponding DBs are dropped as well. Moreover, every redirected BHP will change its corresponding DB path for reaching to a fake destination. Thus, all

http://www.doi.org/10.62341/atae1916

the aggregated packets that hold in redirected DB will be considered as dropped packets. Because, all these packets are not reached to their legitimated destinations. Consequently, the BLR is increased based on number of dropped packets in network traffics. These results proved that DBR attack is able to maliciously affect network traffics on unsecure OBS environment.

Regarding the results of CPPT-OBS implementation, the BLR is being low rate. In low and medium traffic load, the DBR attacker attempts to redirect BHPs traffic during their long-offset time but to no avail. Because, the path information of every captured BHP is encoded by random large keys. So that, the DBR attacker will release a captured BHP since the path information are not available. On the other side, BLR is increased in high traffic load. This increasing is according to delay of end-to-end transmission time. Because, the bottleneck will be established on compromised OBS node when DBR attacker attempts to redirect BHPs traffics. The bottleneck causes traffic congestion which increases a rate of dropped bursts in network traffic.

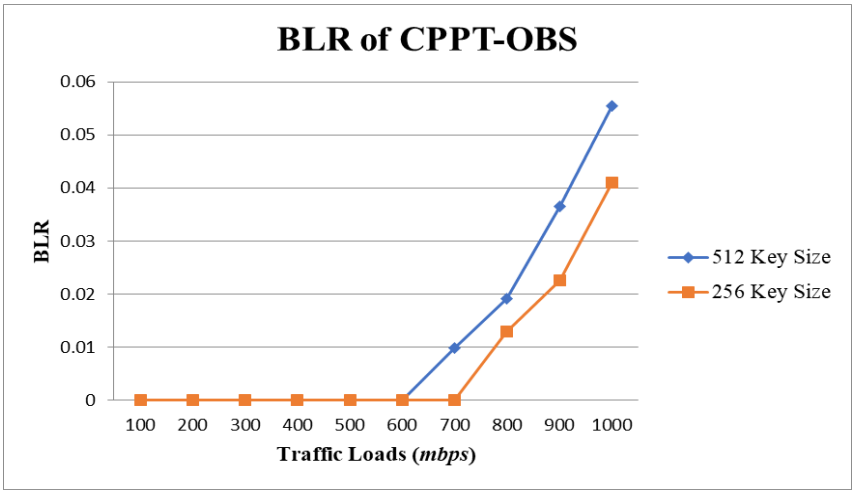

Figure 8: BLR of CPPT-OBS

By comparing the results of CPPT-OBS in Figure 8 with two different key sizes, the PLR is being low in 256 key size. Because, the encryption and decryption processing time with 512 key size consuming longer time than encryption and decryption processes with 256 key size. Since a protected BHP is delayed in every core node, the corresponding DB may be dropped when it is being arrived to next hope before its BHP in high traffic loads. On the

http://www.doi.org/10.62341/atae1916

other hand, the protection level is increased by increasing key size. Because, DBR attack may spend longer time to break 512 key size rather than 256 key size. Consequently, the protection process is affected by the key size.

Throughputs Results Analyzing

In this section, the implementation results of the three scenarios are showed and discussed based on the number of received packets (Throughputs) as following:

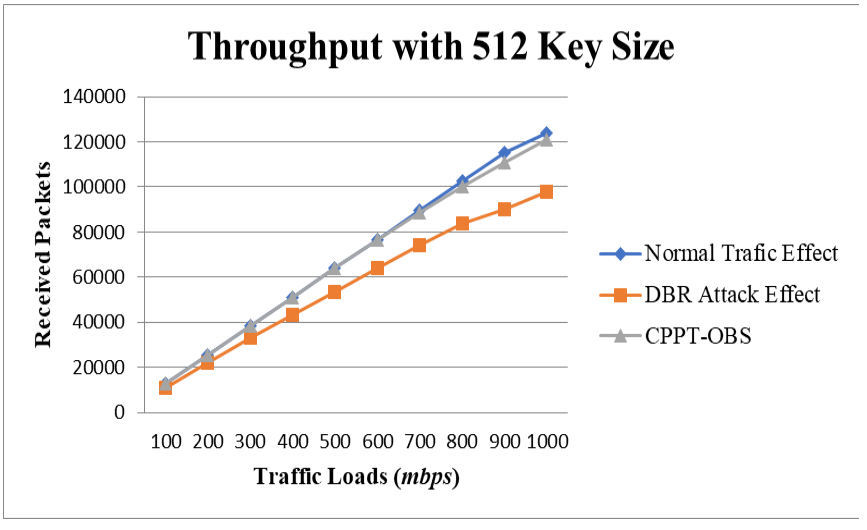

Figure 9: Throughput with 512 Key Size

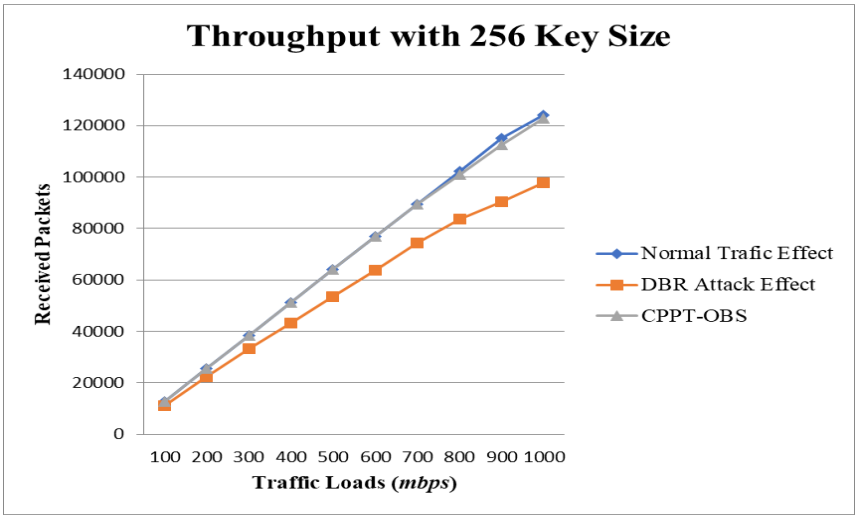

Figure 10: Throughput with 256 Key Size

http://www.doi.org/10.62341/atae1916

Figure 9 and Figure 10 are showing the number of received packets in variant OBS environment (Normal OBS Traffic effects, DBR Attack effects, and CPPT-OBS with 512 and 256 Key Size effects). The throughput of unsecure OBS under DBR attack is low. Each increasing of traffic loads causes decreasing in the number of received packets. All dropped and redirected packets are considered as packets loss. So that, the rates of dropped packets in medium and high traffic load are high.

On the other hand, CPPT-OBS prevents throughput from being decreased in low and medium traffic loads. But, the number of dropped packets is increased in high traffic loads. Because, the delaying of bottleneck core node and the shorting to offset time during encryption and decryption time consuming are decreasing throughputs with high traffic loads.

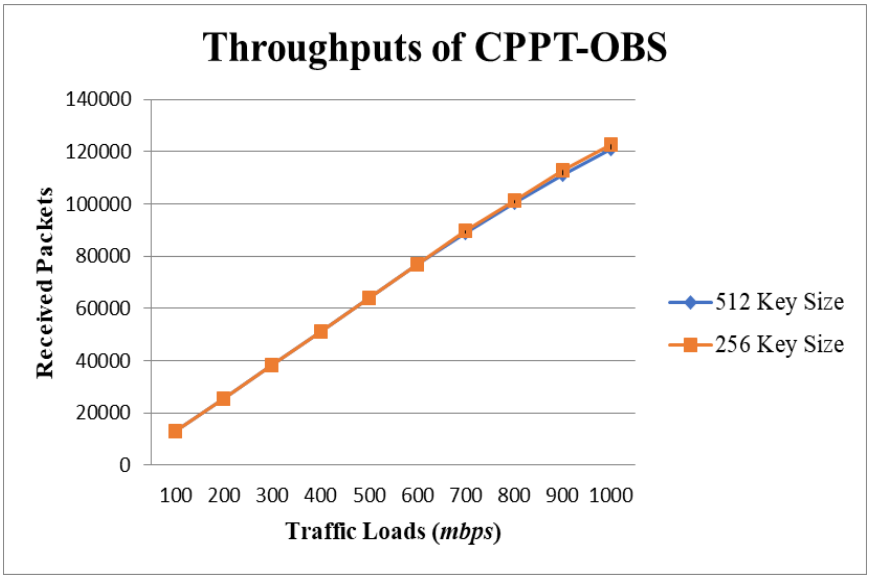

Figure 11: Throughput of CPPT-OBS.

Figure 11 is illustrating the throughputs effects for implementation of CPPT-OBS with two different key sizes. The number of received packets is decreased with 512 key size, and it is increased more with 256 key size. Because, the large key size consumes much time than small key size during encryption and decryption processes in each OBS node as discussed above. Consequently, the shortening of offset time between a protected BHP and its corresponding DB is a main factor of dropping OBS traffics.

http://www.doi.org/10.62341/atae1916

Average Delay Results Analyzing

In this section, the average delay for implementation results of the three main scenarios are displayed and investigated as following:

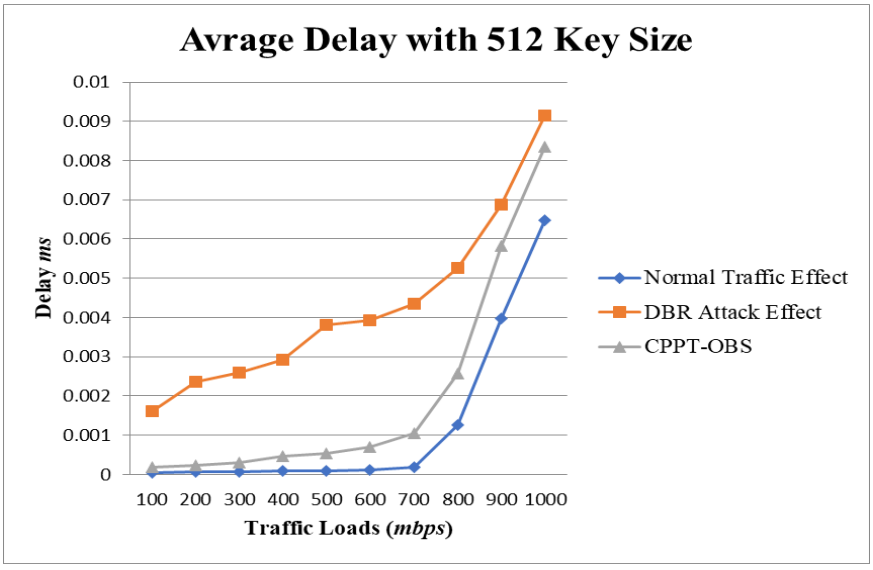

Figure 12: Average Delay with 512 Key Size

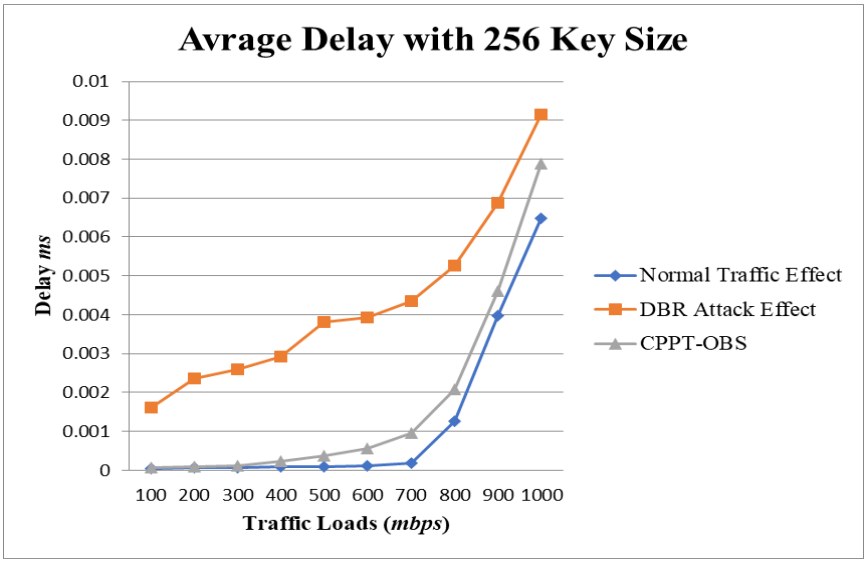

Figure 13: Average Delay with 256 Key Size

Figure 12 and 13 describe the average of end-to-end transmission delay based on Normal OBS Traffic effects, DBR Attack effect, and CPPT-OBS with 512 and 256 Key Size effects. BDR attack causes

http://www.doi.org/10.62341/atae1916

increasing of delay rate more than average delay of normal OBS traffic. Since DBR attack takes advantage of long offset time in low traffic loads, the offset time is decreasing in high traffic load. So, the bottleneck of traffic will be established on a compromised node. The redirected traffics are also considered as delayed traffics. Because, the legitimate destination will be waiting for some incoming traffic until it reached to time out.

The CPPT-OBS prevents DBR attack with low delay average. Because, every encryption and decryption processes of BHP are consuming some processing times. These consuming causes a delay during BHP offset time. Since BHP transmits ahead with short offset time in high traffic load, secure BHP may be delayed after its corresponding DB. Because, this time consuming is depending on two main factors (key block size, hope count in routing path). Regarding to hope count, the processing time of every encoding and decoding are affected by key block size.

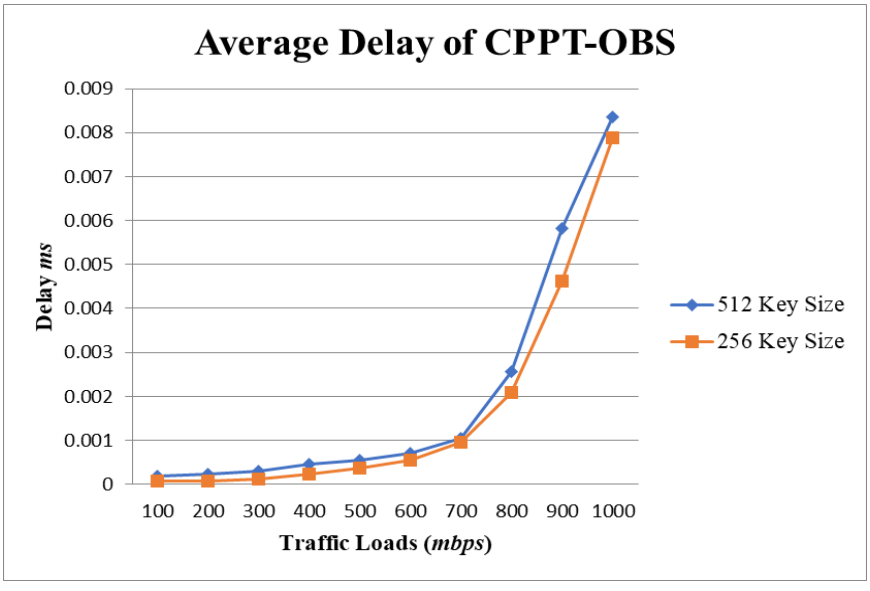

Figure 14: Average Delay of CPPT-OBS

In RSA encryption algorithm, data (that needs to be encoded or decoded) is divided in several blocks based on key block size. Thus, every increasing on key block size means consuming more processing time. Consequently, the result in Figure 14 proves that CPPT-OBS with 256 key size causes less delay average than a CPPT-OBS with 512 key size.

http://www.doi.org/10.62341/atae1916

Evaluation of CPPT-OBS

This evaluation presents experimented ideas according to previous results (BLR, Throughputs, and Average Delay Ratio). These ideas are observed and constructed during the implementation process and discussion phase. The security vulnerabilities of OBS network are considered as main issues in this environment. Because, the transparent network traffics may give opportunities for DBR attacker to change traffic directions to a fake destination. The network traffics may contain some critical information. Consequently, the data confidentiality and authentication of these traffics can be easily compromised. However, the obtained results showed that CPPT-OBS is able to protect OBS traffic from being attack. CPPT-OBS provides secure BHPs transmissions between every two connected OBS nodes by establishing robust relationship between them. The advantage of this technique is self-controlling for each node. Frequently, every node is able to generate own two pair keys randomly. Securely, every node sends node's new public key to all connected neighbors. Protecting BHP's path information from being attack by complex encryption and decryption processes. Additionally, CPPT-OBS is able to prevent a BHP from any DBR malicious actions. If DBR attacker attempted to modify BHP path information, CPPT-OBS will drop captured BHP when decode BHP info is verified with negative situation. If DBR attacker tried to add malicious BHP and drop a legitimate BHP, CPPT-OBS will drop a malicious BHP since next hope will verify the confidentiality of malicious BHP and authentication of sender with negative situation. Consequently, CPPT-OBS can be considered as an efficiency protection mechanism for preventing DBR attack in OBS network.

On the other side, CPPT-OBS is not free from flaws. Each key generating process is taking a long time to find two random prime numbers with specific key size. Therefore, each node needs to generate random keys which cost more delay time. However, physically we expect that each OBS node device can be adaptive with its key generating process. Because, every node will achieve its processes alone in separate manner with variant hardware specifications. Moreover, every generated BHP transmission consumes more processing time for encryption and decryption operations in each hope in its routing path.

http://www.doi.org/10.62341/atae1916

Conclusion

The main objective of this research is enhancing OBS security weaknesses of BHPs traffic transmission. So, the security improvement is achieved with providing high security level in terms of BHP's confidentiality and BHP's sender authentication. RSA enhancement was successfully done by developing a key control mechanism called Self-controlling technique. This technique provided a secure key exchanging between objects. Every object is able to generate its pair keys securely and randomly. Every object can establish trusted communication channels among all connected neighbors by frequently exchanging object's public key with all neighbors' public keys. Thus, every object can control itself successfully.

The enhanced RSA with Self-controlling technique was successfully integrated with OBS environment to improve a security level in OBS network. This adaption was established to provide a Control Packet Protection Technique (CPPT-OBS) against Data Burst Redirection (DBR) Attack. CPPT-OBS was successfully implemented to provide a confidentiality of BHP and an authentication of each sender. Consequently, the CPPT-OBS improves OBS security quality in terms of preventing DBR attack malicious action during BHP transmissions.

The CPPT-OBS performance was successfully recorded and discussed based on Burst Loss Ratio and throughputs and Average Delay Ratio. These results show that CPPT-OBS is able to prevent DBR attack. The advantage of CPPT-OBS is efficiency to support some OBS security countermeasures to overcome several security weaknesses with high throughputs and low burst loss. The scalability of CPPT-OBS approved that is can be adaptive with any size of OBS topology. On the other hand, the disadvantage of CPPT-OBS is consuming more time and causing Burst delay. This defect is regarding to key size and number of check points. Each increasing of key size causes more transmission delay time and check points number as well. Consequently, CPPT-OBS can be considered as a good protection technique of BHP in OBS network.

Future Works

Further studies need to be extensively done for key management with OBS environment. Finding out some improvements to the Self-controlling key management technique or establishing and

http://www.doi.org/10.62341/atae1916

developing a Trusted Third Party (TTP) in OBS environment is needed.

References

[1]-Vokkarane, V. M., Jue, J.P. ; Sitaraman, S.. (2002). Burst segmentation: an approach for reducing packet loss in optical burst switched networks. Communications, 2002. ICC 2002. IEEE International Conference.

[2]-Vokkarane.V. M; Jason P. JUE; (2005). Optical Burst Switching Network. B. Mukherjee. United States of America, Springer Science Business Media.

[3]-Vinod M.Vokkarane, K. H., and Jason P.Jue (2002). Threshold-Based Burst Assembly Policies for QoS Support in Optical Burst-Switched Networks. Optical Networking and Communications, Nasir Ghani. K. M. Sivalingam 123(136).

[4]-Al-Shargabi, M. A. and Abid .A (2007). The impact of OBS burst aggregation on VBR performance. Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference .

[5]-Subramanian, P. S. and Muthuraj K. (2011). Threats in Optical Burst Switched Network. International Journal of Computer Technology and Application 2(3): 510-514.

[6]-Shie-Yuan Wang, C.-L. H., and Chih-Che Lin (2009). The GUI User Manual for the NCTUns 6.0 Network Simulator and Emulator. Taiwan 4: 166.

[7]-S. Chakraborty, A. K. Turuk and B. Sahoo, "OBS network blocking probability prediction using ensemble technique," 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC), Gunupur Odisha, India, 2020, pp. 1-6

[8]-Liu, Susu & Liao, Xun & Shi, Heyuan. (2021). A PSO-SVM for Burst Header Packet Flooding Attacks Detection in Optical Burst Switching Networks. Photonics.

[9]-Muthuraj, K. and Sreenath. N. (2012). Secure Optical Internet: An Attack on OBS node in a TCP over OBS network. International Journal

[10]- Jiezhao, P. and W. Qi (2008). Research and Implementation of RSA Algorithm in Java. Management of e-Commerce and e-Government, 2008. ICMECG '08. International Conference

http://www.doi.org/10.62341/atae1916

[11]- Wang, S. and G. Liu (2011). File Encryption and Decryption System Based on RSA Algorithm. Computational and Information Sciences (ICCIS), 2011 International Conference.

[12]- Xin, Z. and Xiaofei. T (2011). Research and implementation of RSA algorithm for encryption and decryption. Strategic Technology (IFOST), 2011 6th International Forum.

[13]- Xuewen, T. and L. Yunfei (2012). Parallel Analysis of an Improved RSA Algorithm. Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference.

[14]- Stallings, W. (2010). Cryptography and Network Security: Principles and Practice. D. S. holds, Prentice Hall: 744 pages.

[15]- M. Sliti, M. Hamdi and N. Boudriga, "A novel optical firewall architecture for Burst Switched networks," 2010 12th International Conference on Transparent Optical Networks, Munich, Germany, 2010

[16]- Forouzan, B. A. and Mukhopadhyay .D. (2011). Cryptography and network security. McGraw-Hill Education (India) Pvt Limited, Tata Mcgraw Hill Education Private Ltd.

[17]- Chen. Y, Pramode K. Verma , Subhash Kak. (2009). Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks. Security and Communication Networks

[18]- Sharma, S . Chouhan S. (2012). Identification of current attacks and their counter measures in Optical Burst Switched (OBS) network. International Journal of Advanced Computer Research

[19]- Muthuraj, K. and Sreenath, N. (2012). "Secure Optical Internet: A Novel Attack Prevention Mechanism for an OBS node in TCP/OBS Networks." prevention 3(12).

[20]- B. A.M, A. G and V. J. B, "Secured Header Authentication Design using Time Competent HMAC for Optical Burst Switched Networks," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021

[21]- Kesar, Palak & Sandhu, Mandeep. (2019). Security Issues and the Energy Consumption in the Optical Burst Switched Networks. International Journal of Trend in Scientific Research and Development.