Secure Burst Control Packet Scheme for Optical Burst Switching Networks

Yahaya Coulibaly *, Athman Ahmed Ibrahim Al-Kilany*, Muhammad Shafie Abd Latiff * George Rouskas, IEEE Fellow†
Satria Mandala * and Mohammad Abdur Razzaque §
* Faculty of Computing
Universiti Teknologi Malaysia, 81300 Johor Bahru, Malaysia
Email:coulibaly@utm.my, shafie@utm.my, satria@utm.my
† North Carolina State University Box 8206 890 Oval Drive Raleigh, NC 27695-8206
Email: rouskas@ncsu.edu
‡ King Abdulaziz University, Jeddah Abdullah Sulayman, Jeddah 22254 Kingdom of Saudi Arabia
§ Trinity College Dublin School of Computer Science
Email: razzaqum@tcd.ie

***Abstract*—Optical networks are the most adequate platform for the transport of ever increasing bandwidth-hungry applications and services (BwGAS). Additionally, these networks cope with the continuous growth of the number of Internet users. Optical Burst Switching (OBS) paradigm is expected to be the backbone infrastructure of near-future all-optical Internet. In OBS, data and control packet known as burst header packet (BHP) are sent out of band (i.e., control packets and data bursts are carried by different channels) and it is sent ahead of the data burst to reserve necessary network resources for the corresponding burst. After the elapse of a predetermined time known as offset time, the data burst is sent with the hope that, the control packet was able to make necessary reservations. Sending the BHP ahead of the burst exposes the burst to different security challenges, particularly data burst redirection and denial of service attacks. If the BHP is compromised the corresponding burst will definitely be compromised. Less efforts have been dedicated to investigate control packet security issues in OBS. In this paper, we propose and evaluate a solution to address Data Burst Redirection (DBR) Attack in OBS networks. The solution is designed based on Rivest-Shamir-Adleman (RSA) public-key encryption algorithm. We evaluated the algorithm via computer simulation. Evaluation metrics are burst loss ratio and throughput. The obtained results demonstrate that, the proposed algorithm has succeeded in protecting the network against DBR attacks reducing the number of compromised BHP. In the future, the authors will work on denial of service issues considering reliability aspects.**

I. Introduction

Exponential growth of the number of Internet users and bandwidth greedy applications are in continuous development [1, 2, 3], such as e-health, e-education, e-administration, IPTV, video conference, and others. Such development continues to push Telecos and scientific research community towards optical networks.

Three optical switching paradigms have been proposed in the literature to take advantage of WDM technology and to satisfy the requirements of bandwidth-greedy applications. These paradigms are Optical Circuit Switching (OCS) [4], Optical Burst Switching (OBS) [5] and Optical Packet Switching (OPS) [6]. Although OBS remains the promising paradigms and the most likely to be implemented in the near future, this paradigm still suffers from high burst loss due to burst contention at the core node in the absence of buffers. Burst contention occurs when two or more bursts contend for the same resource at the same time. Common solutions to bufferless OBS is the use fiber delay lines (FDLs) wavelength converters [7] and or deflection routing among other solutions. Another issue which is affects OBS performance and has not yet been deserved adequate consideration is security.

In OBS networks, each data burst (DB) is associated with a corresponding Burst Header Packet (BHP) which is sent ahead of the DB on different WDM channel. The BHPs task is to reserve required resources ahead of the the burst as well as DBs path information for path configuration [8]. If 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 arrive anyhow to an input port core node which no longer belongs to its corresponding BHP; it will be dropped or reach to unpredictable destination [9]. When the BHP arrives at the compromised core node, the attacker will start lunching abuse actions before the corresponding DB reaches the desired node. In such cases, the attacker injects a malicious BHP instead of the original BHP and initiates new relationship between the malicious BHP and the reserved DB; in the new BHP, the forwarding path of incoming DB is changed to a fake and non-desired destination [9, 10]. This attack is called Data Burst Redirection Attack as showing in Figure 1. In this paper we have developed a solution that tackles redirection issue in OBS. The solution is based on RSA algorithm and the obtained results demonstrate improved burst loss ratio and overall network throughput.

The rest of this paper is organized as follows: In Section II, we review Security issues in OBS. Section III elaborates algorithm design; Simulation environment are described in Section IV. Simulation results are analysed in Section V. Concluding remarks are described in Section VI.

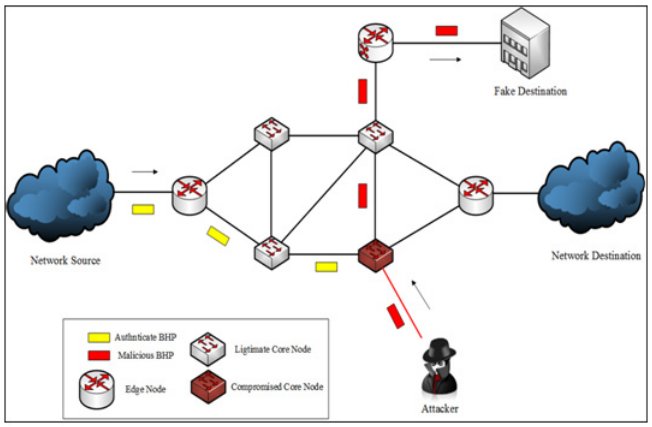

Fig. 1. Data burst redirection attack in obs networks

II. Security Issues in OBS

In this Section, we investigate security issues in OBS and review some of related works. Table I describes some of potential threats in OBS network such as traffic analysis, eavesdropping, spoofing, burst duplication attack and service disruption via Denial of Service (DoS).

From security threats described in Table I, OBS networks are mostly affected by traffic analysis or eavesdropping. In such threats, an attacker listens passively to the authentication protocol to capture information for illegal future use as discussed in [11]. This is an issue in OBS where a passive attacker can intercept BHPs and compromise corresponding data burst [12]. When BHP is the subject of an attack, the passive attacker is able to analyse and observe the carried traffic information from the compromised BHPs which exposes the transparent DBs containing critical information [12]. In OBS, passive attackers are difficult to detect; however, prevention methods can be used to counter attack the threat.

As explained earlier, in OBS, BHP carries arriving data burst information and it is sent before the burst. If an attacker is able to intercept the BHP and modifies its contents, the corresponding burst is redirected to a fake and unauthorised destination [9]. This attack normally occurs during offset time (the time between control packet processing time and data burst transmission). The attacker simply violates the one-to-one relationship between DB and its BHP by injecting a new malicious BHP for the same data burst [9, 10]. Consequently, the original BHP will be dropped and the transported legitimate data burst will be scheduled and forwarded through a new reserved path to a fake destination.

Land attack [13] is a kind of security in which the compromised node copies the BHP and transmits back to the source and to the intended destination. Due to the fact that the attack is on a split capable node, the data also gets split and reaches both intended and unintended nodes thereby wasting resources.

Another security issue in OBS is denial of service (DoS) attack. Similar to other communication networks, OBS networks are vulnerable to DoS because scheduling decisions are based on resource availability [9]. Therefore, when a core router receives a BHP, it changes the state of a free optical channel to a busy state. This is known as channel reservation [14], [13]. In case of no idle WDM channels, the incoming data burst is discard. Thus, an attacker can launch DoS attack to compromise the network by injecting huge numbers of malicious BHP with long offset time to specific target in the network. When malicious BHP arrives to the target node, the target node starts reserving new WDM channel for each malicious BHP [9] and [13]. Each reserved channel will be waiting for anonymous bursts which will never arrive [14] and [15]. The main purpose of DoS attack is to make the target node totally unavailable for proper data transmission. DoS attack is illustrated in Figure 2.

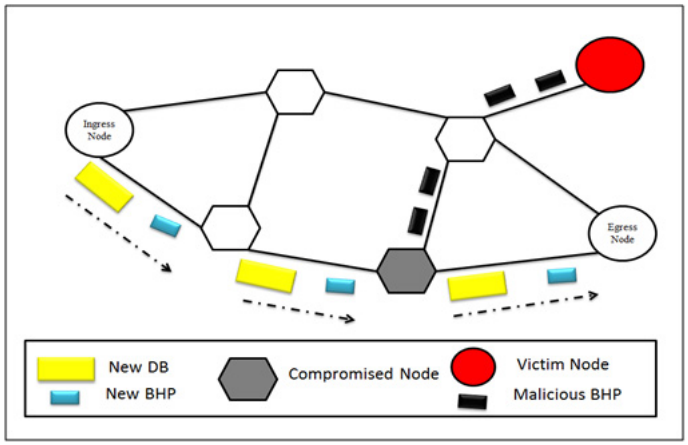

Fig. 2. DoS attack in OBS Network

In OBS, bursts are assembled and created at the Ingress node. Thus, bursts created are to be scheduled for particular channels at specified voids that fit the burst scheduled depending on voidfilling scheduling approaches. The authors in [16] observed that at times a particular node present at the intermediary could be compromised thus changing the value of the size of the assembled bursts at the BHP. The increased burst size value could push the egress node to check the value of the same during disassembly. Due to the attack, if the value is not comparable, the burst could be mistaken for another burst forcing the receiving node to ask for retransmission of the burst. This attack is known as burstification attack and it can happen at both edge and core nodes. For example, the attacker can compromise ingress node and create bursts of bigger sizes. This increases considerably burst reservation time. Increase in the burst reservation time not only affects propagation delay but it also affects burst latency. Increase in latency results in low throughput as it is inversely proportional to the latency.

III. The Proposed Security Measure

To design the proposed solution known as Control Packet Protection (CPPT-OBS), three cases were investigated. The three cases are: OBS network without security measures and without security attacks, OBS network under security attacks without security measures, and finally OBS network under security attacks with security measures. These scenarios are

TABLE I
SECURITY THREATS IN OBS NETWORKS

Threats	Descriptions	Remedy
Traffic Analysis	In this attack, information being communicated between the sources and destination is extracted	Power detection methods/Masking
Eavesdropping	It is similar to traffic analysis but differs the attack layer	Power detection methods/Optical Spectral Analysis Methods/Mutual authentication
Spoofing	In this attack, the attacker attempts to gain access to a system by using a false identity	Cryptographic methods
Burst Duplication Attack	Intermediate core router duplicates a control burst and modifies its contents to create new path between itself and an attacker	Digital signature/ Trusted node method
Service disruption (DoS)	It is a type of attack which prevents communication or Degrades the quality of service (QoS)	Prevention oriented Network Planning

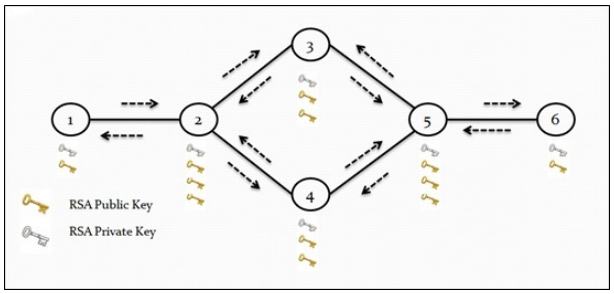

Fig. 3. Key Generation Illustration

largely explained in [17]. The technique proposed here is applicable to the third scenario.

Initially, we assume that all edge and core nodes of OBS networks are legitimate nodes. Under this consideration, each node is equipped with security measures such as confidentiality and authentication using RSA encryption algorithm. This process is called Self-Controlling. The RSA encryption is used to encrypt and decrypt burst control packets. The sender and receiver are point-to-point connected.

In the proposed mechanism, traffic transmission time is divided equally into time slots. At the beginning of each time slot, all OBS nodes start generating temporarily their own random pair keys (Private Key and Public Key) as illustrated in Figure 3. Then, each node multicasts its public key to its directly connected neighbours. While relevant sender and receiver nodes know the public key of each other, the private key of the node is preserved and kept secret from other OBS nodes. This ensures that the a node establish trusted communication with its neighbours.

Before the next timeslot starts, each node regenerates its new pair of keys randomly and double encrypts the public key with its old private key and with its old public key before broadcasting it to all connected neighbours. After sending its new encrypted public key, the old private and public keys of the nodes are revoked. When a receiver receives the encrypted key, the receiver decrypts the encrypted key with its old private key and then with the old public key of the sender. After the new public key is successfully received, decrypted, the old reserved public key of the sender is revoked and will never be used in the network.

When a node sends its public key and receives the public keys of its directly connected nodes, this node creates data set of neighbors public keys, which will be used frequently for creating secure traffic among them. The secure traffic is generated when the sender node encodes a generated BHP with its private key to prove that it is the source of the packet (Authentication). The encoded BHP will be encrypted again using the public key of the receiver to ensure the confidentiality of the encrypted BHP while in transition before reaching the receiver.

The process described earlier is known as Multi-layers security, multi-level security or defenc in depth security mechanism as discussed in [18]; this is because the BHP is encrypted twice before being sent to downstream nodes. So, the BHP is always sent as a cipher text through optical channel to the destination node.

When the BHP arrives at the destination node, the node decrypts it first using its private key to check the confidentiality of the received BHP. If the confidentiality is violated, the received BHP is dropped, otherwise the receiver node decodes the decrypted BHP using the public key of the sender to verify the authentication of the BHP. If the identity of the sender is not authenticated, the BHP is dropped. Else, the decoded BHP is received and allows the receiver read the contents of the BHP for further actions.

Although this mechanism ensures BHP security and reduces burst loss ratio as it will shown in Section IV, it is expected

that end-to-end delay will be increased. This limitation will be addressed in our future work. The detailed algorithm is described in Algorithm 1.

Algorithm 1 Secure BHP Mechanism

1: **Notations**:
2: $N[i]$: n^{th} node in the network. En_BHP : Encrypted Burst Header Packet. K_{TmpPub}: Temporary Public Key of a node. K_{TmpPrv}: Temporary Private key of a node. $Dc1\_BHP$: First decryption of BHP
3: $Dc2\_BHP$: Second decryption of BHP.
4: *stringlen* ← length of *string*
5: **while** K_{TmpPub}, K_{TmpPrv} not exist or expired **do**
6: Create new random $N[i].(K_{TmpPub}, K_{TmpPrv})$
7: Broadcast $N[i].K_{TmpPub}$ to $[1..t]$
8: Receive and Save $N[i].K_{TmpPub}$
9: **while** Not the End of Traffic **do**
10: Create BHP and Data Burst
11: Encrypt BHP
12: $En\_BHP = N[i+1].K_{TmpPub}$ $(N[i].K_{TmpPrv}(BHP))$
13: Send En_BHP to $N[i+1]$
14: Receiver decrypts BHP
15: $Dc1\_BHP$=N[i+1].K_TmpPrv(En_BHP)
16: **if** Decrypted $Dc1\_BHP$ compromised **then**
17: Drop En_BHP
18: Receiver performs second decryption
19: $Dc2\_BHP$=$N[i].K\_TmpPub(Dv1\_BHP)$
20: **if** $Dc2\_BHP$ not authentic **then**
21: Drop $Dc2\_BHP$
22: **else**
23: Receiver processes BHP
24: **if** $N[i+1]$ not the destination **then**
25: go to Line 11

IV. Simulation Environment

Simulation parameters, environment and results are elaborated in this Section. Simulation parameters are listed in Table II. All the simulations were carried out using NCTUns network Simulator and Emulator [19]. The algorithm was implemented on NSFNET topology shown in Figure 4; evaluation metrics are burst loss ratio and network throughput. Number of wavelengths, bandwidth and maximum queue size are Simulator constraints. Burst size of $10KB$ is based on the analysis of Jue et al., in [8].

Three scenarios were investigated:

- OBS network without Security Measures and without Attacks;
- OBS network under Security Attacks without Security Measures;
- OBS network under Security Attacks with Security Measures using the proposed technique.

Security attack is illustrated in Figure 5. The scenario is based on the 14 nodes NFS topology shown in Figure 4. In simulated network, 5 edge routers were used; each edge connects to one node (used as source and destination); thus a total of 5 sources and destinations were simulated. $PC19$ represents a source, $PC22$ represents an authenticate destination and $PC24$ is a fake destination. The normal traffic, i.e; the traffic between $PC19$ and $PC22$ passes through core nodes $(19, 18, 1, 2, 4, 5, 6, 7, 9, 13, 16, 22)$. The compromised core node is $Node13$. At this node traffic the attacker injects malicious BHP and redirect the traffic to $Node22$ instead of $Node16$ which is connected to the authenticated destination. Thus, the corresponding bursts will eventually be received by $PC24$ causing data lost at $Node13$ at the expense of $PC22$ the intended receiver of the data burst.

TABLE II
Simulation Parameters and Levels

Parameters	Levels
Simulation Topology	NSFNET
Bandwidth per wavelength (Gbps)Eavesdropping	1
Burst Size (KB)	10
Number of wavelengths	3
Maximum Queue length (KB)	60
Transport Layer Protocol	TCP and UDP

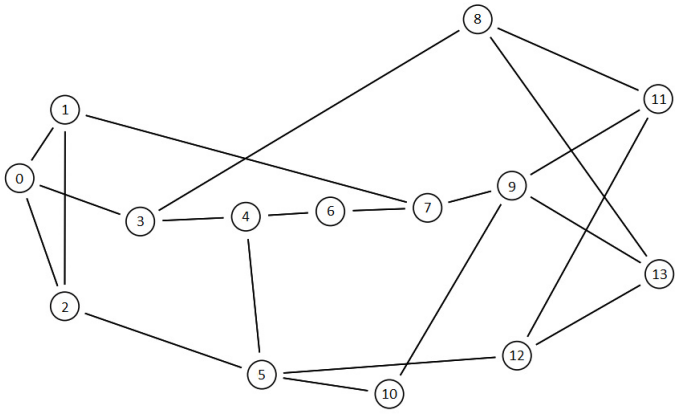

Fig. 4. Simulation Topology: NSFNET

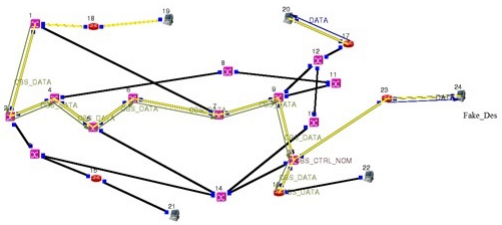

Fig. 5. Simulation Scenario

The results concern burst loss ratio and throughput which are analysed in Section V

V. Results Analysis

Figure 6 and Figure 7 illustrate the results of the three scenarios described earlier (i.e,. normal traffic, DBR Attack Effects in the absence of security measures and DBR attack in the presence of our proposed solution). The size of RSA key used in the evaluation is 512KB. From the results depicted in Figure 6, it can be observed that in the the normal traffic BLR increases as traffic increases. In the case of DBR attack without security measure, we notice rapid increase in BLR especially at low load as the attacker is able to modify and redirect captured BHPs resulting in considerable loss in the transmitted bursts; because these bursts could not be received by intended destinations.

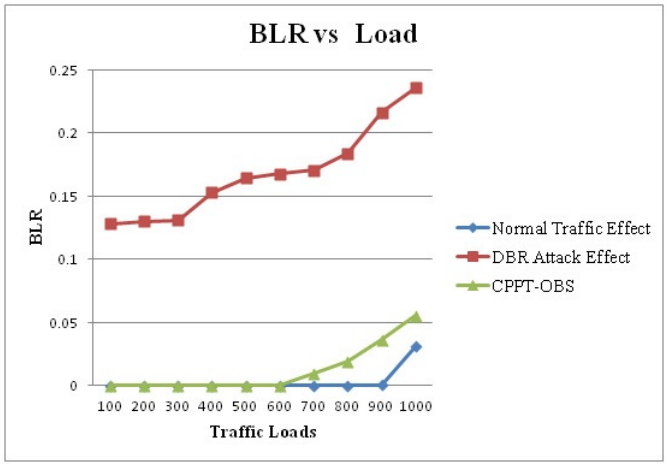

Fig. 6. Loss Results for the three Scenarios

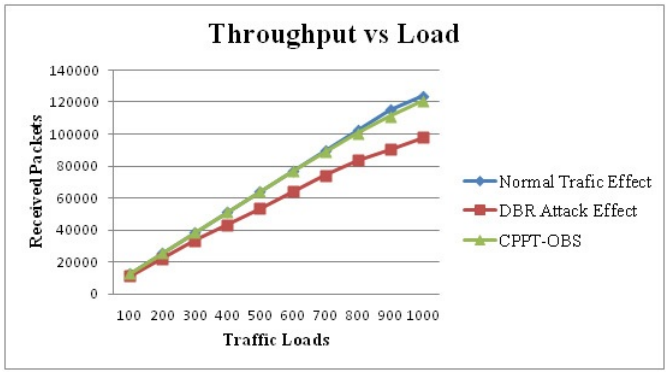

Fig. 7. Throughput Results for the three Scenarios

Figure 7 illustrates the number of received packets as traffic load varies. From the results, it is clear that throughput of non-secure OBS under DBR attack is low while with the application of the proposed solution, the throughput is improved which shows the potential of the solution to improve overall OBS network performance.

VI. Conclusions

In this paper, we have proposed and evaluated a security solution to counter measure security threats related to burst header packet in OBS networks. Three scenarios were investigated. Simulation results prove that, applying the proposed solution in an attack environment does reduce burst loss and increase overall network throughput. Thus, one can conclude that, devising efficient security for OBS network will contribute to making OBS a viable for future all-optical Internet. In the future, the authors will work on denial of service issues considering reliability aspects. It is expected that, end-to-end delay be increased due to the security measure proposed, thus; the technique can be enhanced to address the delay issue.

Acknowledgments

This research is supported by Ministry of Education Malaysia and Universiti Teknologi Malaysia (UTM) through Fundamental Research Grant (FRGS) Ref:4F324. and Q.J130000.2728.00K31 respectively.

References

[1] J. Wang, Z. Song, P. Lei, and R. Sheriff, "Design and evaluation of m-commerce applications," in *2005 Asia-Pacific Conference on Communications*. IEEE, 2005, pp. 745–749.

[2] B. Martini, V. Martini, F. Baroncelli, K. Torkman, and P. Castoldi, "Application-driven control of network resources in multiservice optical networks," *J. Opt. Commun. Netw.*, vol. 1, no. 2, pp. A270–A283, Jul 2009. [Online]. Available: http://jocn.osa.org

[3] J. Wang, R. V. Prasad, and I. Niemegeers, "In house high definition multimedia: An overview on quality-of-service requirements," *International Journal of Research and Reviews in Computer Science*, vol. 1, no. 1, 2010.

[4] A. Ghafoor, M. Guizani, and S. Sheikh, "Architecture of an all-optical circuit-switched multistage interconnection network," *Selected Areas in Communications, IEEE Journal on*, vol. 8, no. 8, pp. 1595–1607, 1990.

[5] C. Qiao and M. Yoo, "Optical burst switching (obs)–a new paradigm for an optical internetˆ{1}," *Journal of high speed networks*, vol. 8, no. 1, pp. 69–84, 1999.

[6] C. Guillemot, M. Renaud, P. Gambini, C. Janz, I. Andonovic, R. Bauknecht, B. Bostica, M. Burzio, F. Callegati, M. Casoni, D. Chiaroni, F. Clerot, S. L. Danielsen, F. Dorgeuille, A. Dupas, A. Franzen, P. B. Hansen, D. K. Hunter, A. Kloch, R. Krähenbühl, B. Lavigne, A. L. Corre, C. Raffaelli, M. Schilling, J.-C. Simon, and L. Zucchelli, "Transparent optical packet switching: The european acts keops project approach," *J. Lightwave Technol.*, vol. 16, no. 12, pp. 2117–2134, Dec 1998. [Online]. Available: http://jlt.osa.org

[7] B. Wang and N. Lella, "Dynamic contention resolution in optical burst switched networks with partial wavelength conversion and fiber delay lines," in *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, vol. 3, Nov 2004, pp. 1862–1866.

[8] J. P. Jue and V. M. Vokkarane, *Optical burst switched networks*. Springer, 2006.

[9] Y. Chen, P. K. Verma, and S. Kak, "Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks," *Security and Communication Networks*, vol. 2, no. 6, pp. 546–554, 2009.

[10] Y. Chen and P. K. Verma, "Secure optical burst switching framework and research directions," *Communications Magazine, IEEE*, vol. 46, no. 8, pp. 40–45, 2008.

[11] A. Kahate, *Cryptography and network security*. Tata McGraw-Hill Education, 2013.

[12] S. S. Chouhan and S. Sharma, "Identification of current attacks and their counter measures in optical burst switched (obs) network," *International Journal of Advanced Computer Research*, vol. 2, no. 1, 2012.

[13] N. Sreenath, K. Muthuraj, and P. Sivasubramanian, "Secure optical internet: Attack detection and prevention mechanism." IEEE, 2012, pp. 1009–1012.

[14] V. Shakhov, "Dods flooding attacks in obs networks," 2012.

[15] M. Sliti, M. Hamdi, and N. Boudriga, "A novel optical firewall architecture for burst switched networks," in *Transparent Optical Networks (ICTON), 2010 12th International Conference on*, June 2010, pp. 1–5.

[16] B. K. B. A. Terrance Frederick Fernandez and C. N. Sreenath, "Burstification threat in optical burst switched networks," 2014, pp. 1666–1670.

[17] A. A. I. A. Kilany, *Enhanced RSA Key Managment Mechanism for Control Packet Protection in Optical burst Swicthed Networks*, 2013.

[18] X. Yang, Z. Li, Z. Geng, and H. Zhang, "A multi-layer security model for internet of things," in *Internet of Things*. Springer, 2012, pp. 388–393.

[19] [Online]. Available: http://nsl.csie.nctu.edu.tw/nctuns.html