KONFERENCJA RADIOKOMUNIKACJI
I TELEINFORMATYKI
KRiT 2023

StegoBackoff: Tworzenie kanału skrytego z użyciem procedury backoff w sieciach standardu IEEE 802.11

StegoBackoff: Creating a Covert Channel Using Backoff Procedure in IEEE 802.11 Networks

Geovani Teca[1]; Marek Natkaniec[2];

[1] AGH University of Krakow, Krakow, teca@agh.edu.pl
[2] AGH University of Krakow, Krakow, natkanie@agh.edu.pl

Streszczenie: Kanał skrytej komunikacji to technika służąca do ukrywania tajnych wiadomości wewnątrz jawnej transmisji, stosowana do zapewnienia bezpiecznej komunikacji w niezaufanych środowiskach. W artykule przedstawiono nowy kanał skrytej komunikacji oparty na procedurze backoff sieci standardu IEEE 802.11. Artykuł opisuje implementację i dostarcza metryki do oceny wydajności pracy. Wyniki pokazują, że rozmiar ramki oraz liczba stacji w sieci bezprzewodowej bezpośrednio wpływają na wydajność proponowanego skrytego kanału.

Abstract: A covert channel is a technique used to conceal secret messages within an explicit transmission, applied to secure communication in untrusted environments. This paper presents a novel covert channel based on the backoff procedure in the 802.11 networks. The paper describes the implementation and provides metrics for evaluating its performance. The results reveal that the payload size and the number of stations competing for access to the wireless channel directly impact the covert channel's performance.

Słowa kluczowe: kanały skryte, mechanizm Backoff, sieci standardu IEEE 802.11, steganografia sieciowa

Keywords: covert channels, Backoff mechanism, IEEE 802.11 networks, network steganography

1. INTRODUCTION

IEEE 802.11 is a set of standards for Wireless Local Area Networks (WLANs) developed by the Institute of Electrical and Electronics Engineers (IEEE) and Commonly known as Wi-Fi [1]. Many features contributed to 802.11 networks being quickly adopted and becoming an immediate solution for connecting devices and the Internet. Devices that support the 802.11 standards are easily portable (e.g. laptops, wearable devices, and cell phones). Wi-Fi is simple to set up, either by configuring an Access Point (AP) or pressing the button on a device to start a hotspot, and it can be installed in places where there is no support to have wired network infrastructure. Finally, extending the network range means adding a few more APs allowing users mobility across the network with seemingly connectivity interruption.

Devices in the IEEE 802.11 network share the transmission medium. A device equipped with 802.11 radio, monitoring the channel, can detect when transmission occurs by measuring the channel signal energy levels. The IEEE 802.11 implements packet encryption to prevent the data from being exposed in the channel. However, over time, vulnerabilities in IEEE 802.11 encryption protocols have been discovered [2][3], posing security risks to networks and their users. Therefore, IEEE 802.11 network researchers must focus on developing mechanisms that allow users to send data without raising awareness that transmission is occurring.

Steganography, an ancient practice, has been adopted into the IEEE 802.11 network to enable users to send secret messages that go undetected through the shared channel. This is achieved by creating covert channels that decouple the encrypted data frame from the intended data. The explicit data frame serves as a cover or envelope for the secret message, allowing it to be transmitted without detection.

The paper introduces a novel covert channel based on the IEEE 802.11 backoff procedure and presents its implementation and associated metrics. The article makes several contributions to the field of IEEE 802.11 network steganography. Firstly, it presents a new approach to covert channel implementation using the backoff mechanism. Secondly, it highlights the significant impact of frame size, number of stations, and offered load on the covert channel's throughput, delay, and efficiency. Lastly, the paper reports experimental results for the 802.11ax extension, which enables achieving a noteworthy throughput for the covert channel.

The organization of the research paper is as follows: Section 2 presents the related works. It shortly discusses the existing covert channels for IEEE 802.11 networks. Section 3 describes the exponential backoff mechanism used to create the covert channel. Section 4 explains the covert channel concept and operation. Section 5 presents the simulation results. Finally, Section 6 concludes the paper.

2. RELATED RESEARCHES

The IEEE 802.11 standard implementation provides numerous opportunities for creating covert channels. One approach involves utilizing fields that allow custom values. For example, a study presented in [4] demonstrates two covert channels that can be implemented in the 802.11 MAC header. In the first covert channel, the secret message is inserted in the first 8 bits of the Sequence Control field. In the second covert channel, the secret

message is inserted in the Initial Vector (IV) field for a frame encrypted with WEP. Another study [5] presents a covert channel that inserts the secret message in the 2-bit field Protocol Version of the 802.11 MAC header. This covert channel exploits the fact that the standard specifies 00 as the default value, leaving the remaining three combinations (01, 10, 11) unused. Furthermore, the paper [6] describes a covert channel in 802.11e that uses the reserved bit combinations of three subfields (QoS, CF-Pollable, and CF-Poll Request) of QoS capability in the Association Request to signal the start and finish of the covert communication, and when the covert channel is established the covert message is inserted in the TXOP (Transmission Opportunity) and TID (Traffic Identifier) fields.

Another technique for creating a covert channel involves encoding the secret message in the time difference between consecutive transmissions. One example of this approach is the Covert DCF [7], which manipulates the backoff values in the Distributed Coordinated Function (DCF) to encode secret messages. To implement Covert DCF, the sender shares with the receiver a codebook that maps a 3-bit key to a random backoff value. The sender then selects the backoff slot that matches the desired secret message from the codebook and sends the packet after the selected backoff time. Covert-DCF implementation using an Off-The-Shelf wireless card is described in [8]. The paper [9] proposes a ternary timing covert channel. This method involves the sender and receiver monitoring the wireless channel to determine the free time intervals, which are then statistically analyzed to determine the free time interval distribution of the channel. The sender and receiver use this information to conceal and decode secret messages. After that, the sender selects a slot s from a given subset to encode the secret data and ensures that the sum of waiting times between consecutive transmissions equals the slot s. The study [10] presents an 802.11 covert channel that utilizes the interarrival times of either the Beacon frames or the Probe Request frames to encode the message. The method involves changing the generation interval of the frames based on the bit combination that the sender intends to transmit. For instance, to encode the bit sequence of 001, the sender can use a generation interval of $5ms$ for the first frame and $10ms$ for the second frame.

Moreover, another technique to conceal secret data involves manipulating the physical layer during the modulation process. One such method is based on the constellation shaping modulation technique, as described in [11], [12]. In this approach, the hidden message is concealed as a distorted constellation that results from hardware and channel imperfections or noise.

In contrast to the existing 802.11 covert channels, such as the one presented in [7], which also manipulates the random backoff value, the proposed covert channel in this paper does not require the sender to control random backoff slots, which maintains the fairness aspect of the procedure. Instead, it analyzes the impact of frame size and offered load, enabling the sender to adapt these parameters better to conceal more covert messages. Additionally, we examine the influence of external traffic, up to 20 stations sharing the transmission channel, and utilizing the latest 802.11ax amendment.

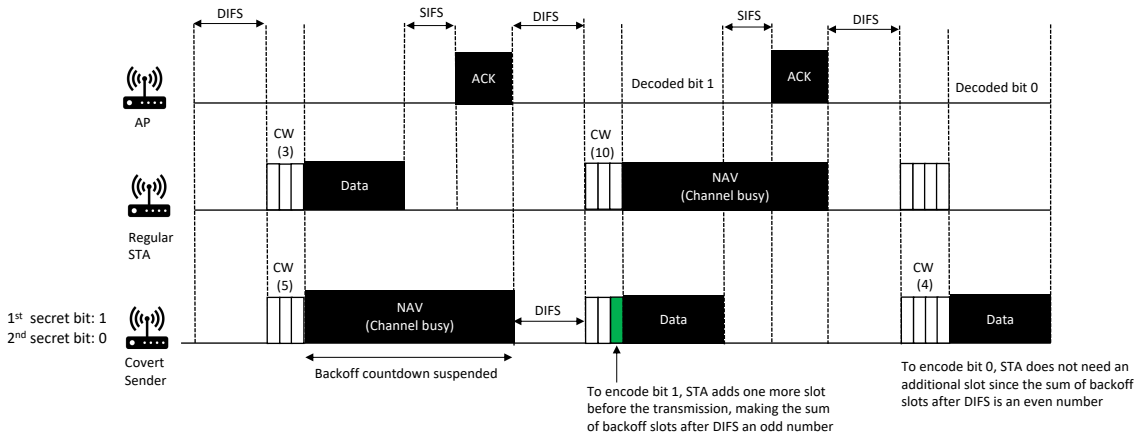
3. IEEE 802.11 BACKOFF PROCEDURE

The IEEE 802.11 standards require the Distributed Coordination Function (DCF) to enable asynchronous channel access for devices sharing the transmission medium [13]. DCF employs two methods of carrier sensing: physical and virtual. A station measures the channel signal energy in physical carrier sensing to determine whether it falls below a predefined threshold. Virtual carrier sensing, on the other hand, relies on the Network Allocation Vector (NAV) of the station, which provides information about the duration of other transmissions on the channel. The DCF procedure enables asynchronous channel access for devices sharing the transmission medium. In DCF, a station that wants to send a frame must first sense the channel. If the channel is busy due to ongoing transmission by another station, the sender waits until the end of the current transmission plus a specific time known as DCF Inter Frame Space (DIFS). After DIFS, the station selects a random integer backoff slot from 0 to a value of CW (Contention Window), calculated according to formula 1. Initially, every station sets CW to CW_{min}, but upon collision, it doubles until it reaches CW_{max}. However, after every successful transmission attempt or reaching CW_{max}, the CW is reset to CW_{min}. The countdown continues until the station's backoff slot reaches zero, at which point the station has won the competition to access the channel. During this time, other stations set the duration of the ongoing transmission in their Network Allocation Vector (NAV) and suspend their backoff countdown. The time interval between frames belonging to the same transmission (such as Data and ACK frames) is called Short Inter Frame Space (SIFS). After a transmission plus a DIFS period ends, the stations whose backoff has not reached zero resume their backoff countdown. The station that wins the competition for access to the channel gets a new backoff slot. The random exponential backoff algorithm used in DCF is designed to minimize the wait time for accessing the channel while reducing the probability of collisions.

$$CW = 2^x - 1 \tag{1}$$

4. STEGOBACKOFF CONCEPT AND OPERATION

The backoff procedure allows stations to determine the number of time slots that have elapsed before a transmission can start, using the DIFS and the remaining backoff time. By exploiting this property, a covert channel can be created by encoding a secret message in the parity of the backoff slot. The bit 0 corresponds to an even backoff slot, while an odd backoff slot is used for transmitting a bit 1. This covert channel has a bandwidth of one bit per frame, and any node on the channel can be the recipient, whether it is a station or an AP. The receiver monitors the channel and counts the number of slots passed from the DIFS until the frame is transmitted. Subtracting the DIFS from the frame arrival time gives the number of backoff slots the sender waited before transmitting the data. Based on the parity of this number, the receiver can decode the transmitted bit as a 0 or 1. The covert channel is highly resistant to steganalysis because it does not modify how backoff values are generated. If necessary, one extra slot is added to ensure the correct slot parity based on the secret message to be delivered.



Rysunek 1: StegoBackoff operation

Algorithm 1: Sender procedure

$backoff \leftarrow random(0, CW)$;
$covert\_bit \leftarrow message[i]$;
if *covert_bit is 0* **then**
  if *backoff is odd* **then**
    $backoff \leftarrow backoff + 1$;
  end
else
  if *backoff is even* **then**
    $backoff \leftarrow backoff + 1$;
  end
end

Rysunek 2: Pseudocode for the stegobackoff sender

Algorithm 2: Receiver procedure

$DIFS \leftarrow SIFS + 2 * Slot\_time$;
$slots\_lapsed \leftarrow (DIFS - frame\_arrival\_time)/Slot\_time$;
if *slots_lapsed is even* **then**
  decode bit 0;
else
  decode bit 1;
end

Rysunek 3: Pseudocode for the stegobackoff receiver

To illustrate how covert channels operate in practice, consider Fig. 1, where a covert sender has a queue of secret messages consisting of two bits, with the first being 1 and the second being 0. After DIFS, the sender draws a random backoff of 5 slots and begins the countdown. Meanwhile, another regular station also has a frame to transmit and competes for access to the channel. It draws a lower backoff of 3 slots and wins the competition, causing the covert station to suspend its backoff countdown and wait until the regular station's transmission is complete. After the regular station's transmission and another DIFS interval, the covert station resumes its backoff countdown with only two slots remaining. When the backoff countdown reaches zero, the covert station waits for one more slot, making the total number of slots after DIFS odd since it intends to send bit 1. The covert stations draw a new backoff of four when the first secret data transmission finishes. After DIFS, it wins the competition as it has a lower backoff than the regular stations and sends the frame without delay since the total number of slots passed after DIFS is even, and it intends to send a bit 0. The sender and receiver algorithms are presented in Fig.2 and Fig.3.

5. STEGOBACKOFF PERFORMANCE EVALUATION

5.1 Simulation Environment

The covert channel has been implemented in the ns-3 network simulator [14], a powerful discrete-event network simulator used to model and simulate various types of networks. This open-source simulator is written in C++ and Python and provides many features, including support for simulating 802.11 networks. Table 1 shows the main parameters set during the simulation. In all figures, the error of each simulation point for the 95% confidence interval did not exceed ± 2%.

Tabela 1: Simulation Parameters

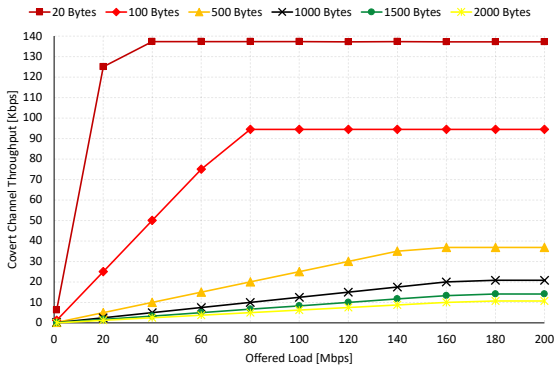
Parameter	*Value*
IEEE specification	802.11ax
Transport protocol	UDP
Channel band	2.4 [GHz]
Channel width	40 [MHz]
Guard interval	400 [μs]
Time slot	9 [μs]
SIFS	16 [μs]
DIFS	34 [μs]
Time slot	9 [μs]
MCS index	9
Mobility model	Constant
RTS/CTS	Disabled
Number of Tx and Rx antennas	1

5.2 First Scenario - Non-Competitive Channel Access

The isolated scenario involves only the covert STA and the AP, with no other STAs present. In this scenario, the covert STA generates UDP traffic, and the experiment involves increasing the offered load while maintaining a

constant frame size. The experiment is repeated with varying frame sizes to assess the impact of frame size on the throughput of the covert channel as the offered load increases.

Fig. 4 displays the simulated results of the isolated scenario. The findings indicate that the payload size directly impacts the covert channel throughput. As the figure shows, smaller payload sizes generate higher covert throughput values, while larger payload sizes result in lower throughput values. This is due to the fact that a smaller payload occupies the channel for a shorter duration, providing the covert stations with more transmission opportunities within the overall transmission time. Furthermore, our observations indicate that the payload size impacts the network saturation threshold. In particular, the network reaches its saturation point for small payload sizes with less offered load, while larger payload sizes require more load to achieve saturation. This can be attributed to heavier payloads demanding the station to send frames more quickly to reach a point where the additional offered load does not affect the network throughput.

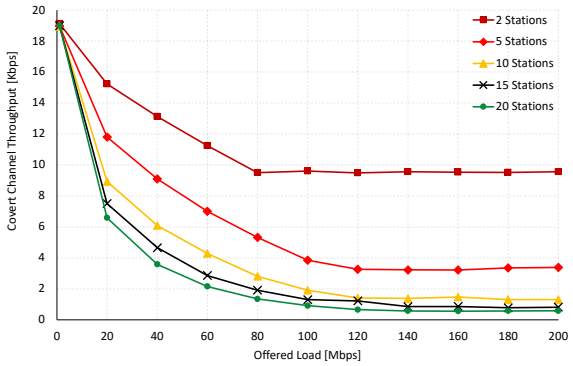


Rysunek 4: Offered load vs. covert channel throughput for different payload sizes, with 1 STA and 1 AP

5.3 Second Scenario - Contention-Based Channel Access

In this scenario, we introduce additional regular stations to the network, gradually increasing the network's density. The covert STA maintains a constant frame size of 1024 bytes and offers a load of 200 Mbps. The experiment aims to investigate the effect of increasing traffic generated by additional stations on the performance of the covert channel, including throughput, delay, and frame efficiency, which is the ratio of frames received over frames sent in percentage.

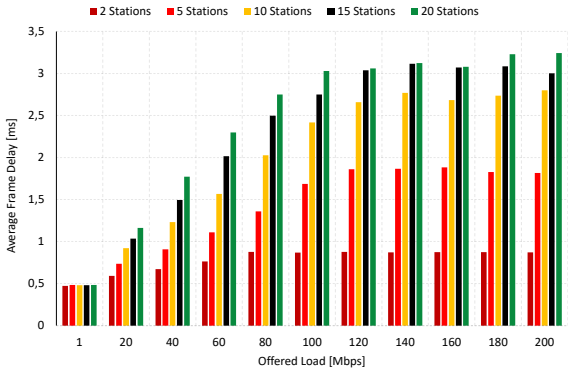
The simulation results in Fig. 5 show the impact of adding 1, 5, 10, 15, and 20 more stations to the network. It is observed that when the external traffic is low, at 1 Mbps, the covert channel is not affected and achieves approximately 19 Kbps throughput for all five experiments. This can be attributed to the fact that the covert station generates much higher traffic (200 Mbps) than 1 Mbps and, thus, do not face significant interference. However, as the offered load increases, the impact of external traffic becomes noticeable, and the covert throughput starts to decay. This is due to the increased competition for channel access, as more data is to be sent by external stations. Furthermore, it is observed that after adding 15 stations, the throughput values are close, suggesting that adding more stations beyond this point will have a minimal impact on the already decayed network throughput.



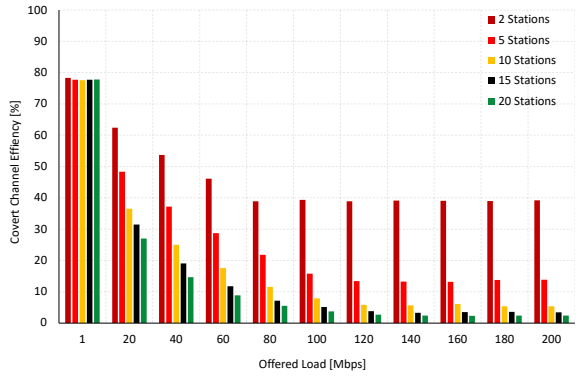
Rysunek 5: Regular stations offered load vs. covert channel throughput

Fig. 6 illustrates the impact of external stations on the delay of the covert channel. The results show that the delay increases proportionally to the offered load from the regular stations. As the offered load increases, the delay extends due to congestion. When traffic is high, more collisions occur, and the receiving queue at the AP increases, causing processing delays. Therefore, the delay experienced by the covert channel is directly proportional to the amount of offered load. Overall, in the worst-case scenario, with 20 stations generating 200 Mbps of traffic, the covert channel delay is below 3,5 ms, regarded as an excellent outcome.

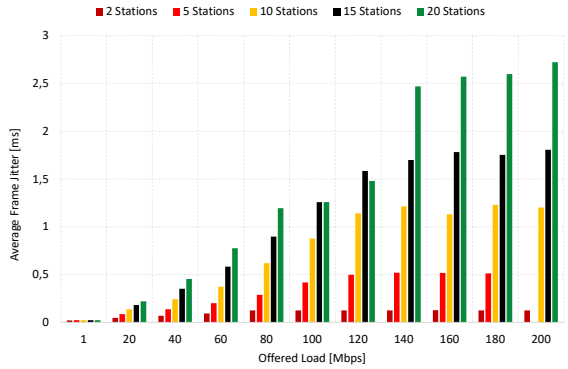
The efficiency of the covert channel is highly dependent on the offered load, as demonstrated by the results presented in Fig. 8. This figure displays the percentage of frames successfully delivered to AP and the percentage lost depending on the number of stations. The efficiency of the covert channel is inversely proportional to the offered load, as observed. At a low offered load of 1 Mbps, over 80% of frames are successfully delivered. However, as the amount of traffic increases, there is a significant reduction in efficiency. For instance, in scenarios with 10, 15, and 20 stations, the efficiency drops below 40% when the offered load reaches 20 Mbps. As the offered load increases, the increase in frame collisions becomes more evident. This decrease in efficiency is mainly due to the increase in frame collisions, which is intensified by the number of stations.



Rysunek 6: Regular stations offered load vs. covert channel delay



Rysunek 7: Regular stations offered load vs. covert channel efficiency



Rysunek 8: Regular stations offered load vs. covert channel efficiency

6. CONCLUSION

This paper presents a novel covert channel based on a backoff mechanism. The backoff mechanism employed by the covert station ensures the encoding of bits 0 and 1 in even and odd remaining backoff slots, respectively. The simulation results demonstrate that the covert channel's throughput, delay, and efficiency are directly influenced by the frame size, number of stations, and their offered load. Our findings indicate that the covert channel is highly effective for small payload applications, even in dense networks with low data traffic.

LITERATURA

[1] IEEE Standard for Information Technology. 2021. "Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2020". IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016): 1-4379.

[2] Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne. 2012. "Vulnerabilities of Wireless Security protocols (WEP and WPA2)". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1 (2) : 34-38.

[3] Kemal Bicakci, Bulent Tavli. "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks". Computer Standards & Interfaces 31 (5) : 931-941.

[4] Lilia Frikha, Zouheir Trabelsi, Wassim El-Hajj. 2008. "Implementation of a Covert Channel in the 802.11 Header". International Wireless Communications and Mobile Computing Conference, Crete, Greece : 594-599.

[5] Goncalves Ricardo. Tummala Murali. Mceachen John. 2012. "Analysis of a MAC Layer Covert Channel in 802.11 Networks". International Journal on Advances in Telecommunications 5(3&4) : 131-140

[6] Hong Zhao. 2014. "Covert channels in 802.11e wireless networks". Wireless Telecommunications Symposium, Washington, DC, USA : 1-5.

[7] Russell Holloway, Raheem Beyah. 2011. "Covert DCF: A DCF-Based Covert Timing Channel in 802.11 Networks". IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, Spain : 570-579.

[8] Sakthi V. Radhakrishnan, A. Selcuk Uluagac, Raheem Beyah. 2013. "Realizing an 802.11-based covert timing channel using off-the-shelf wireless cards". IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA : 722-728.

[9] F. Tahmasbi, N. Moghim and M. Mahdavi, "Ternary timing covert channel in wireless 802.11," 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Rasht, Iran, 2015, pp. 73-78, doi: 10.1109/ISCISC.2015.7387901.

[10] T. O. Walker and K. D. Fairbanks, "An off-the-shelf, low detectability, low data rate, timing-based covert channel for IEEE 802.11 wireless networks," 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2017, pp. 835-840, doi: 10.1109/CCNC.2017.7983242.

[11] Grzesiak Krystian, Zbigniew Piotrowski, and Jan M. Kelner. 2021. "A Wireless Covert Channel Based on Dirty Constellation with Phase Drift". Electronics 10(6) : 647. https://doi.org/10.3390/electronics10060647

[12] Pengcheng Cao, Weiwei Liu, Guangjie Liu, Xiaopeng Ji, Jiangtao Zhai, Yuewei Dai, "A Wireless Covert Channel Based on Constellation Shaping Modulation", Security and Communication Networks, vol. 2018, Article ID 1214681, 15 pages, 2018. https://doi.org/10.1155/2018/1214681

[13] Natkaniec Marek, and Andrzej R. Pach. "An analysis of the backoff mechanism used in IEEE 802.11 networks." Proceedings ISCC 2000. Fifth IEEE Symposium on Computers and Communications (2000): 444-449.

[14] https://www.nsnam.org