Journal of Computer Science 10 (1): 128-137, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.128.137 Published Online 10 (1) 2014 (http://www.thescipub.com/jcs.toc)

AN APPROACH TO MITIGATE DENIAL OF SERVICE ATTACKS IN IEEE 802.11 NETWORKS

[1]Adriano Cesar Ribeiro, [1]Alex Roschildt Pinto, [1]Geraldo Francisco Donega Zafalon, [2]Daniel Fernando Pigatto, [2]Kalinka Castelo Branco and [1]Adriano Mauro Cansian

[1]Departamento de Ciências de Computação e Estatística (DCCE), Instituto de Biociências, Letras e Ciências Exatas (IBILCE), São Paulo State University (UNESP)-São José do Rio Preto-SP, Brazil
[2]Departamento de Sistemas de Computação (SSC), Instituto de Ciências Matemáticas e de Computação (ICMC), University of São Paulo (USP)-São Carlos-SP, Brazil

Received 2013-06-17; Revised 2013-10-15; Accepted 2013-11-12

ABSTRACT

Wireless networks are widely deployed and have many uses, for example in critical embedded systems. The applications of this kind of network meets the common needs of most embedded systems and addressing the particularities of each scenario, such as limitations of computing resources and energy supply. Problems such as denial of service attacks are common place and cause great inconvenience. Thus, this study presents simulations of denial of service attacks on 802.11 wireless networks using the network simulator OMNeT++. Furthermore, we present an approach to mitigate such attack, obtaining significant results for improving wireless networks.

Keywords: Computer Networks, Security, Denial of Service Attacks, Embedded Systems

1. INTRODUCTION

Embedded systems are systems equipped with a dedicated and customized processing among software and hardware, usually geared toward a specific goal, thus improving the investment, lodging, performance and box power consumption (Yu *et al*., 2010). Unlike general purpose computers, embedded systems perform a set of predefined tasks, commonly on a very specific requirements basis. Since these systems are dedicated to specific tasks, engineering techniques can optimize the final product design, reducing size, cost and computational resources. Therefore, embedded systems market share is on constantly growing (Lee *et al.*, 2013), since they have played many different roles in modern devices.

The communication among embedded systems shows the undeniable relevance of computer networks to their proper operation. Due to its wide dissemination and use in different places and also due to the growing demand for mobility, wireless communication has emerged as an essential tool for embedded systems. Among the existing standards of wireless communication protocols, stands out the IEEE 802.11 (Wi-Fi) (IEEE, 2007). It is the most commonly used standard nowadays and presents significative growth in applications and infrastructures of everyday life (Feng, 2012).

Malicious actions by which such systems are susceptible range from information theft by interference in communication, to illegitimate use or application of the controlled device. In order to have some acceptable security level to devices using embedded systems, it is necessary to detect and solve problems related to attacks targeting these ones. mongo the many attacks to which they are subject, one of the most used and that should be

Corresponding Author: Alex Roschildt Pinto, Departamento de Ciências de Computação e Estatística (DCCE), Instituto de Biociências, Letras e Ciências Exatas (IBILCE), São Paulo State University (UNESP)-São José do Rio Preto-SP, Brazil

highlighted, is the Denial of Service (DoS), which is an attempt to make a system or network resource unavailable (Sandstrom, 2011).

This study aims to present a study and analysis of an attack being uttered to a wireless network and to propose the means to mitigate it in an effective manner. In order to achieve this goal, our study used a simulated networking based on the OMNeT++ network simulator. It provides the necessary resources to design and to structure the network, as well as the means to assess the effectiveness of the attack and the applied countermeasures.

The study is organized as follows: Section 2 presents the related work. Section 3 addresses the problem, the attack analysis and mitigation proposed, as well parameters used in the simulations. Section 4 presents the case studies and results. Finally, section 5 shows conclusions and future work.

1.1. Related Works

Problems related to wireless network security have great attention to R&D community, mainly issues regarding denial of service. Malekzadeh *et al*. (2011) authors show the effects of a denial of service over a wireless network, through simulations using OMNeT++ network simulator. Furthermore, a comparison between simulated and actual attack data is developed, intending to show that the simulator validates the data and presents consistent results. In the simulated scenarios, the authors conducted several tests verifying the throughput and delay of generated network traffic using TCP and UDP segments. The results show a sudden fall to 0 bps throughput and important increase to delay, from 0 seconds to about 6 seconds over the time which the attack is performed. The study shows the amount of lost packets in the simulations was 37.90% when the attack was in effect. Whereas it is feasible to ompare the simulated model with the real model, so can be proved that the results obtained from attack mitigation, the main event discussed in this work, may also be considered feasible and consistent with what goes on in an actual attack.

Sandstrom (2011) proposed a technique for denial of service etection and mitigation, which is divided into three phases: Initialization, authentication and request. In the initialization stage, the authentication server chooses a private key for the station and calculates its corresponding public key. This step is performed before any further and is only required once. In the request phase, the station asks the Access Point (AP) to grant access to the desired network. The AP then sends to station a set of random numbers with the public key to be used for traffic exchange. At last, during authentication phase, the station sends a message containing a hash for the random number received from the AP using its public key, among other information, like password. The use of random numbers prevent the following denial of service attacks kinds: Flood, deauthentication and disassociation.

To prevent denial of service type deauthentication and disassociation, it is proposed in (Arockiam and Vani, 2012) a protocol based on factorization of very large prime numbers. Initially the station enerates two primes (p1 and n1) which are multiplied. The same procedure is performed by AP, enerating another two prime numbers (p2 and n2). In the authentication phase, these numbers exchange occurs between the station and the AP. If some of the stakeholders send deauthentication packets, it also sends coupled his number p1 and p2 to validate authenticity of the package deauthentication. The tests were performed using several different prime numbers lengths (p and q) from 64, 128, 256 and 512 bits. In all cases, the defense against this type of attack was satisfactory, meaning even with spoofing deauthentication packets; the AP was able to ignore the bogus request.

Considering a case of denial of service attack that uses frame control, (Malekzadeh *et al.*, 2012) propose a method that revokes the channel reservation asked by attacker. Sending a packet with a Request to Send (RS) too high, the AP admits that reservation and then broadcast a Clear to Send Packet (CSP) advising the channel reservation for window time requested. However, if the AP does not receive any packet shortly thereafter, then it revokes that channel reservation, featuring a denial of service. As a result, was achieved a throughput increase during the attack, which was raised from 0.3 to 0.6 packets per time frame.

The study presented in (Lee *et al*., 2009) rests upon unused bits in 802.11i frames protocol. Thus, random bits are inserted in authentication/association and deauthentication/disassociation frames, which are generated by the communication between stations by some sort of algorithm. All sent frames are set at this value and if a frame does not match the actual, that frame is rejected. The tests carried out using actual boxes that performed the exchange of data using File Transfer

Protocol (FTP). According to this study, some attacks had success for some settings of bits used for verification, but others not, mitigating analyzed attacks.

Soryal and Saadawi (2012), is proposed a detection method which is based on number of packets successfully sent by a station containing CTS number received for this same station. Each station probes channel and uses a method called Markov Chain, which is used to measure network throughput. Thus, is checked the throughput achieved calculating Markov Chain and the amount of CTS frames received. If this number of CTS frames is greater than the throughput achieved, then that node is identified as an attacker and its MAC address is saved.

The defense against attacks like frame control proposed by (Mynemi and Huang, 2010), is to use a method for generating and distributing keys, shown in 802.11f protocol. Next it generates a message authentication code using the generated key. Initially the AP seeks other APs over the channel and if none is found, it generates a number K, which will be sent over a TCP connection to other stations. Beyond that number K, is generated a sequence number S, which is based on the duration of channel reservation contained within in frames RTS/CTS. Results were obtained through simulations had allowed to observe which attacks were not successful. For instance, the value before the attack throughput was 28.4 Mbps using UDP protocol and, after attack mitigation, throughput was preserved at 27.6 Mbps allowing to conclude that the process was successful **Table 1**.

Due to fact that DoS attacks have been great demand and present a satisfactory efficiency, there are many ways to accomplish them. Thus, it is necessary to prevent several malicious activities, as presented on studies above. The purpose of this present work is to mitigate a DoS attack type that has characteristic of flooding a station with transmitting requests.

2. MATERIALS AND METHODS

Considering wireless networks, there are two situations which the stations have problems when probing the channel to the start the transmission. The first consideration is related to hidden terminal problem, where due to fading the hosts cannot detect the transmission of the others, resulting in collisions (Kurose and Ross, 2012) **Fig. 1**.

For problems like this, there is a scheme in IEEE 802.11 protocol which includes a channel reservation to be used as a frame control called Request to Send (RTS). When a station intends to send information, it listens the channel to check if it is idle. Due to the hidden terminal problem, it can be possible that other station has been started a transmission and the busy channel was not detected. Thus, when the channel is detected idle, the station waits a slot of time Distributed Inter Frame Spacing (DIFS) before sending a RTS frame. This RTS frame takes the estimated time duration, in microseconds, which the station will use the channel to transmit the information. Once Access Point (AP) receives the frame, it will send another frame called CTS by broadcast to the neighboring stations warning that the channel will be busy by the required time.

The attack model described in the present woks uses flood to send information with RTS frame. This technique sends a huge amount of RTS frames in a short time to a server, causing congestion. In this case, the consequence is the wireless channel reservation congestion using RTS frame. Thus, the full control of the channel occurs, denying service to other host in the wireless network.

The algorithm modeled for the attack used in this work consists to start in a defined time in the simulator sets. In the following, the attacker listens if the channel is idle and if this is confirmed, a controller loop starts sending packets Internet Control Message Protocol (ICMP) to their destination, according to the time interval between these jackets, until the time limit to the end of the attack. The algorithm is showed in the **Fig. 2** and it details how a denial of service attack is performed in the simulations.

According to the type of the attack performed, we have developed a mitigation model. This model consists of receiving a RTS frame with duration of time changed to high value and send a CTS frame to reserve the channel to the attacker. In the following, when the packet ICMP with the information is received, a verification of the transmission time obtained is much smaller than the required, the connection is finished. The algorithm illustrated in the **Fig. 3** describes how the mitigation is performed.

The protocol used in the simulations is the 802.11b and the wireless network topology is the type of infrastructure. The proposed topology is illustrated in the **Fig. 4**.

Topology illustrated in the **Fig. 4** é generic and it can be extended to desired number of hosts, APs and attackers. Nevertheless, the model proposed in this work is only with one attacker, thus characterizing a DoS attack.

To perform the simulation some parameters must be set. Theses parameters were obtained though real tests and simulations previously performed. In the **Table 2** are showed the parameters used in the simulations.

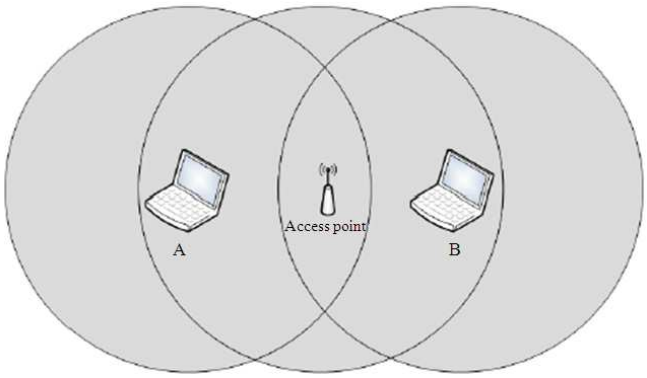

Fig. 1. The hidden terminal problem

```
if channel is idle, do
      waits for SIFS (Short Interframe Space) interval
      sends a RTS frame with an altered duration
      obtains a CTS frame from the AP freeing the channel
      sends a ICMP package to the destination
if final of attack is true, stop
```

Fig. 2. Model of the denial of service attack used

```
receives RTS frame
sends CTS with reserved time
calculates correct time
if reserved time >> calculated time
      cancels connection
```

Fig. 3. Proposed model of mitigation

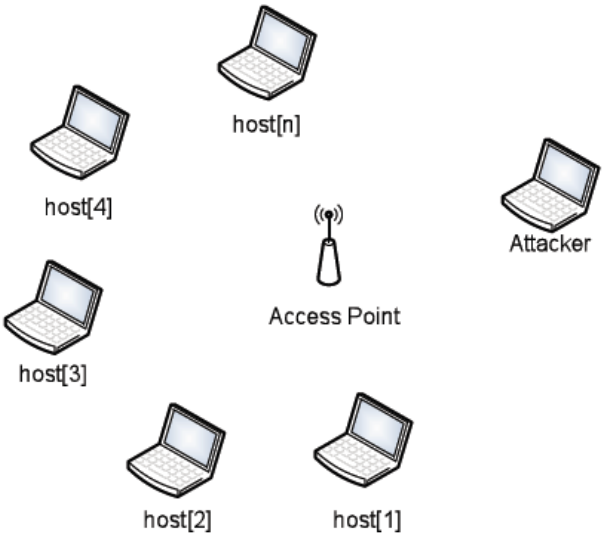

Fig. 4. The topology used in case studies

3. RESULTS AND DISCUSSION

To collect the results there are functions from the simulator modules, which obtain the time when packets are sent for each host and the time to packets arrive to destination. Furthermore, it is presented the drop percentage of the packets, which increases with DoS attack and returns to the normal when it uses the mitigation model proposed.

The performed simulations were based on scenarios, which are composed by following evaluation data: Normal traffic (only legitimate hosts), network behavior under DoS attack and network behavior using the mitigation model. Each test set described a particular scenario and, thus, there are some variations of these scenarios with 2, 4, 8, 16, 32, 64, 128 legitimate hosts, respectively.

The metric used to analyses the network behavior was the throughput. This is a well know metric when an evaluation of a network is needed. The value of this measurement can be obtained using equation illustrated in **Fig. 5**.

As observed in **Fig. 5**, size means the length of the packet (in bytes) sent and time-to-arrive is the time this packet spent to arrive to destination.

The results of simulations with normal traffic and with traffic under DoS attack are showed in **Fig. 6-12**.

The throughput variation presented in the **Fig. 6** is small, due to the reduced number of simulated hosts on wireless network. The average variation of throughput without an attacker is 57.28 Bps. Nevertheless, it can be easily realized that throughput variation starts from the beginning of the DoS attack, where throughput reaches almost 0 Bps for approximately 5 seconds.

The throughput variation illustrated in the **Fig. 7** to normal traffic is similar to the simulation with 2 hosts, in **Fig. 6**, maintaining the average throughput around 57, 53 Bps. When the attack starts, the medium is busy for about 5 seconds until the network can be reestablished. In this case, the average throughput was 26.84 Bps. In the simulation using mitigation occurs a significant decrease of the throughput, however it does not reach 0 and its interval is short. In this case of mitigation, the average throughput is 56.64 Bps, close to simulation of normal traffic.

In the **Fig. 8** is showed a greater variation of throughput due to the increase of the number of hosts in the wireless network. Thus, congestion on the network occurs, but the average throughput is kept in 50.03 Bps. With the beginning of DoS attack the throughputc reaches almost 0 for 4 seconds. In this case, the average throughput is 29.67 Bps. When the mitigation strategy starts, a slightly decrease occurs, but the average throughput simulation with attack and mitigation is 49.38 Bps.

In the **Fig. 9** can be noticed that the throughput of wireless network has less variation. This case occurs because the simulations on networks with more than 16 hosts have their sent ICMP packet interval increased of 1 second, instead of 100 milliseconds of the previous simulations. Thus, the network throughput keeps uniform with an verge of 54.49 Bps. In the simulation with DoS attack, the throughput reaches 0 for some seconds, maintaining average throughput around 35.61 Bps. This last average is greater than the averages of the previous simulations because the traffic interval is greater too. The simulation with mitigation shows results with throughput almost without variation and its average is 54.61 Bps.

In the **Fig. 10** is presented the normal traffic in a simulation with 32 hosts. The variation keeps in a short interval with a throughput average of 55.51 Bps. In the simulation of attack the throughput variation is kept until the DoS attack starts and then it decreases abruptly, with throughput average reaching 41.06 Bps. As the interval adopted to packet change increases, the amount of measures decreases and therefore, although the graphic is very similar to the simulations with 2 **Fig. 6-7** hosts, causing a variation of throughput average. When the mitigation is simulated for this set of 32 hosts, a brief decrease happens and the average throughput is 54.23 Bps. The mitigation model brings satisfactory results, because the average throughput is very close to that obtained with the simulation without an attacker.

In the **Fig. 11** is resented the simulation results for 64 hosts. The throughput variation for normal traffic slightly increases and number of measures is also greater, resulting in an average throughput equal to 55.99 Bps. The simulation of DoS attack brings the throughput to almost 0, decreasing the average throughput to 47.93 Bps. In the simulation of mitigation, the throughput decreases slightly for a few seconds, but it does not reach 0. This fact concerns to the increasing of the number of nodes in the network. The average throughput does not reach zero and it maintains the average of 54.05 Bps, i.e., closed to the obtained average without attacker action.

There is a wide throughput variation of the simulation with 128 hosts when we compare with the previous simulations. The average throughput for this simulation without an attacker is 51.22 Bps.

```
throughput = size / time_to_arrive
```

Fig. 5. Throughput calculation

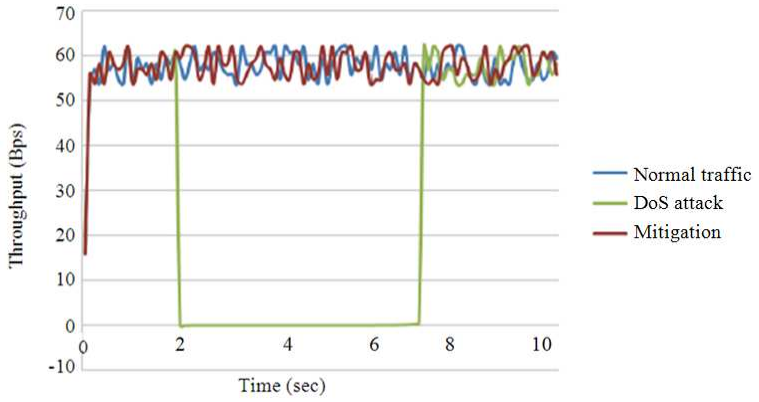

Fig. 6. Simulations with 2 legitimate hosts

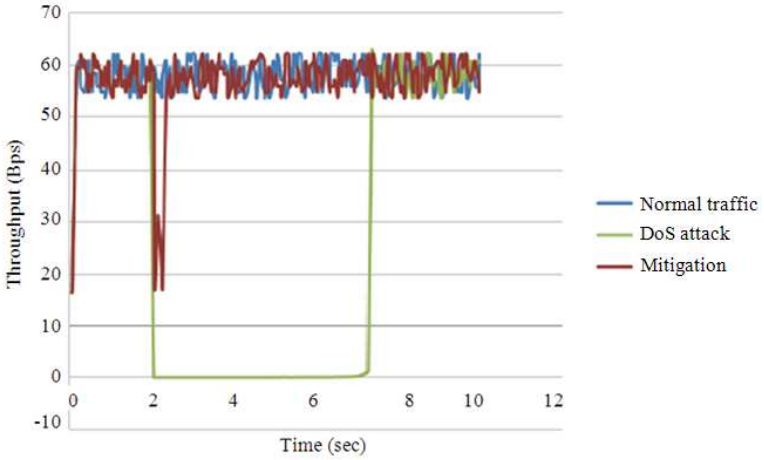

Fig. 7. Simulations with 4 legitimate hosts

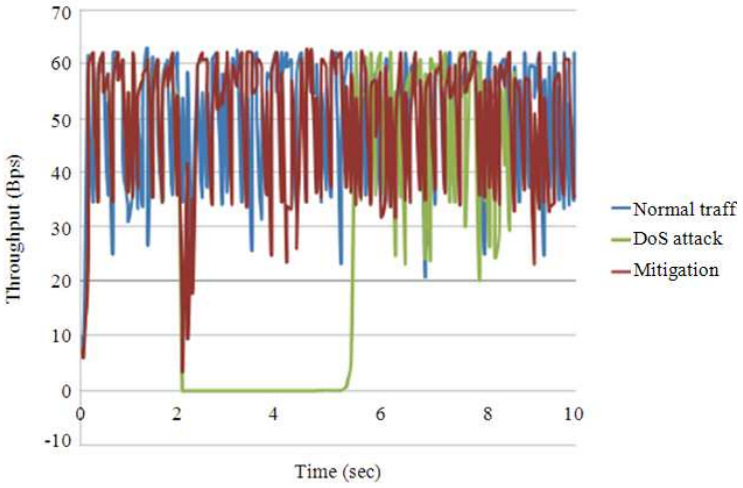

Fig. 8. Simulation with 8 legitimate hosts

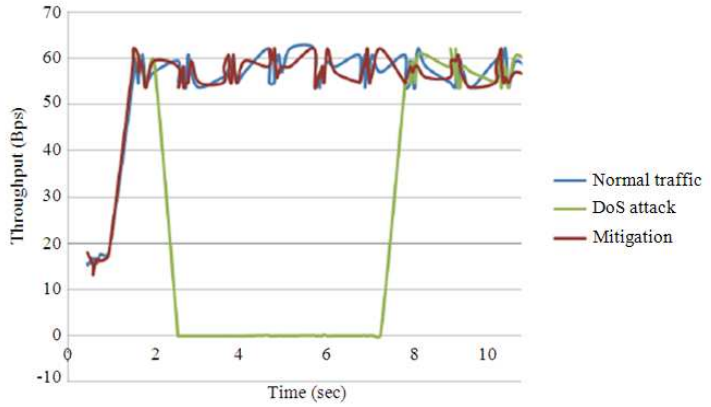

Fig. 9. Simulations with 16 legitimate hosts

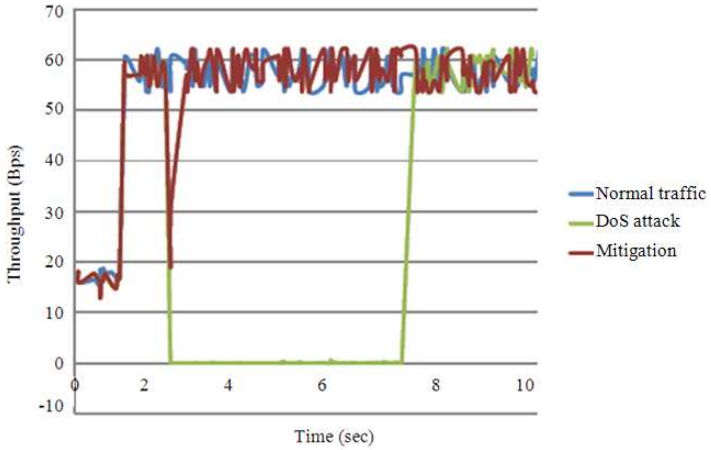

Fig. 10. Simulations with 32 legitimate hosts

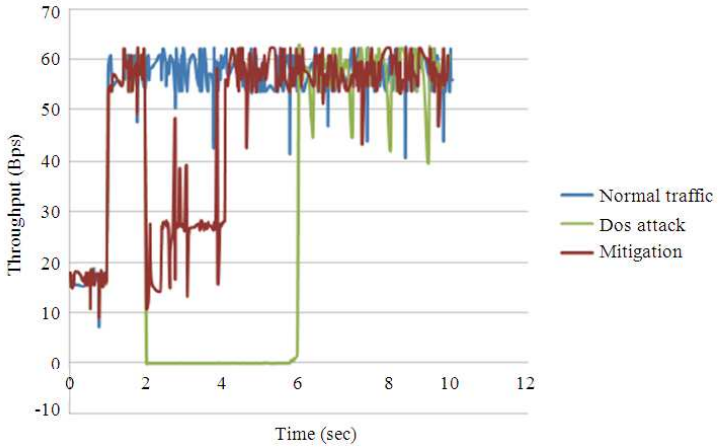

Fig. 11. Simulation with 64 legitimate hosts

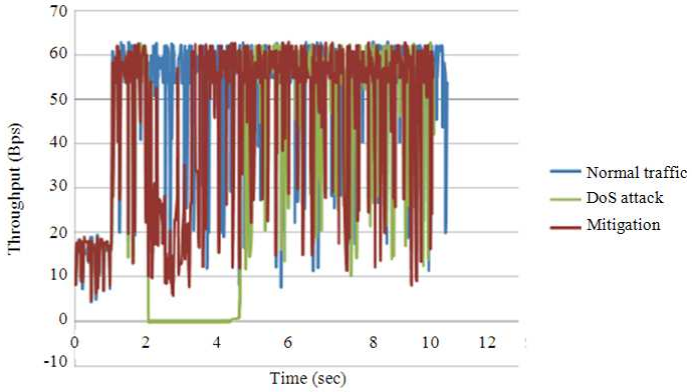

Fig. 12. Simulations with 128 legitimate hosts

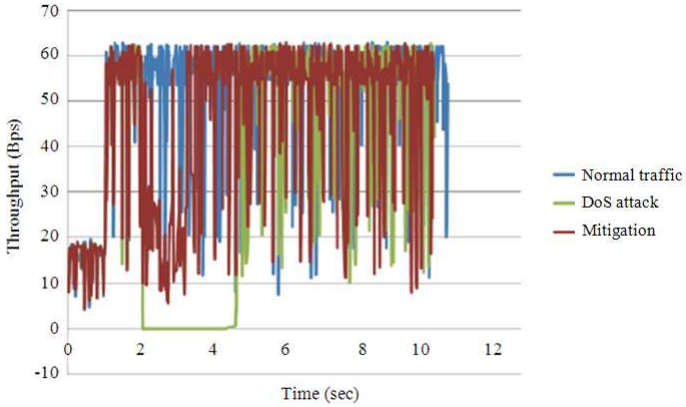

Fig. 13. Average throughput with different scenarios

Table 1. Related works approach

Paper	Approach	Results
Malekzadeh *et al*. (2011)	Assessing denial of service RTS /CTS in simulations and in real scenario	Sudden drop in throughput, increase in delay of packets from 0 to 6 seconds and packet loss rate of 37.9%
Sandstrom (2011)	Divided into phases, which consist in the generation, exchange and authentication by public key.	Detects DoS attacks in authentication and reduces DoS flood during the authentication phase and the probe request.
Nguyen *et al*. (2008)	Performs factoring of very large prime numbers.	Even for prime numbers with varying bit, the model was successful, ignoring deauthentication attacks.
Negi and Rajeswaran (2005)	Repealing the channel reservation, request if not sent any useful package within a time interval	Obtained results in that the network throughput in a testing scenarios rise of 0.3 to 0. 6 packets per time nterval.
Lee *et al*. (2009)	Makes use of unused bits in the header to generate random numbers.	For use of 5 bits or more random numbers, mitigation occurs as expected.
Soryal and Saadawi (2012)	Uses Markov chain to obtain a more accurate throughput With this, a CTS frames received by the host. If this ratio is greater than CTS the result of the Markov chain, the DoS attack is detected.	The tests showed that the model was successful at detecting the check is made of the quantity and attacker MAC address.
Mynemi and Huang (2010)	A approach is used for generation and distribution of keys. To supplement is generated based on a sequence number requested in the RTS frame time.	Tests showed that the network throughput with UDP traffic value was 28.4 Mbps and the mitigation model, the value of the throughput was27.6 Mbps

Table 2. Parameters used for the simulations

Adopted standard	802.11b
Simulation time	10 sec
ICMP packet sizes	56 bytes
Interval of sending ICMP packets	100 milliseconds for 2, 4 and 8 hosts scenarios
Interval of sending ICMP packets	1 second for 16, 32, 64 and 128 hosts scenarios
Start of the attack	2 sec
Final of the attack	2,3 sec
Interval for sending ICMP packets from the attacker	5 milliseconds

Table 3. Parameters used for the simulations

	Drop (%)		
Scenario	Normal traffic	DoS attack	Mitigation
2 hosts	0	26,65	0
4 hosts	0	31	0
8 hosts	0	25,64	0
16 hosts	0	20,67	0
32 hosts	0	27	0
64 hosts	0	6,89	0
128 hosts	0	12,59	0

When the attack starts the network flow falls down and the average throughput reaches 45.93 Bps. As similar as **Fig. 11**, in the simulation of mitigation the **Fig. 12** has a slightly decrease of its throughput, but it does not reach zero. In the context of mitigation, the average throughput is 50.20 Bps, also near from the results of simulation without attacker.

According to the results presented previously, is clear that the Denial of Service attacks are troubling. The network throughput almost reaches zero when the attack is performed and the network takes some time after the attack to operate normal again. Then, with the proposed mitigation strategy we can notice a great improvement of the network behavior. The amount of packets in the network, the time interval among them and the number of hosts are factors which affect the throughput.

For a better visualization of the network throughput scenarios, in the **Fig. 13** are showed a bar graphic with the average throughput for each scenario: Normal traffic, traffic under attack and traffic with mitigation.

As it can be seen in the **Fig. 13**, is clear the network. During the simulation time, the network throughput decreases considerably, although the time attack has been short. In general, denial of service attacks might last minutes or hours.

Another way to evaluate the negative impact on the network is the number of packets dropped. In the **Table 3** are showed the percentages of the packets dropped in the tested scenarios, previously described.

For the tests with normal traffic there is no packet dropped. When the denial of service attack starts, the number of packets dropped increases a lot. With the use of mitigation model the percentage of packets dropped returns to zero, as it was before the DoS attack.

4. CONCLUSION

In critical embedded systems, is very important a well done communication among the nodes. Due to the sensitivity of wireless networks, the malicious activities may cause a lot of damage to the system, pecially to perform works.

The problem described in this work shows the damage caused by a DoS attack on a network. With the proposed mitigation model was possible minimize this damage. Besides that, the simulations were performed with different amount of nodes, starting with few nodes until many nodes, where the traffic congestion occurs frequently.

When we anal yes the related works, we notice there are many ways to mitigate DoS attacks. Due to the lack of authentication of packets and frames, the attackers are able to perform their DoS attacks more easily. Some works present many strategies to authenticate these packets and frames which impove tha network flow.

In this study, we propose a simple, but efficient approach. The results showed that the method we used is efficient and may be useful in wireless network security and consequently in critical embedded systems. As future works, new simulation with new scenarios may be developed. Besides that, we guess to be interesting to

perform tests with different attack strategies, allowing the study of new mitigation techniques.

5. ACKNOWLEDGEMENT

We thank to INCT-SEC and our institutions for the support to the development of this study.

6. REFERENCES

Arockiam, L. and B. Vani, 2012. Security algorithms to prevent Denial of Service (DoS) attacks in WLAN. Int. J. Wireless Commun. Netw. Technol., 2: 1-7.

Feng, P., 2012. Wireless LAN security issues and solutions. Proceedings of the IEEE Symposium on Robotics and Applications, Jun. 3-5, IEEE Xplore Press, Kuala Lumpur, pp: 921-924. DOI: 10.1109/ISRA.2012.6219343

IEEE, 2007. IEEE Standard 802.11. Local na metropolitan barea networks-specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. pp: 1232-1232.

Kurose, J.F. and K.W. Ross, 2012. Computer Networking: A Top-down Approach. 6th Edn., Pearson Education, ISBN-10: 0133128091, pp: 864.

Lee, D.H., H.P. In, L. Keun, P. Sooyong and M. Hinchey, 2013. Sustainable embedded software life-cycle planning. IEEE Soft., 30: 72-80. DOI: 10.1109/MS.2012.75

Lee, Y.S., H.T. Chien and W.N. Tsai, 2009. Using random bit authentication to defend IEEE 802.11 DoS Attacks. J. Inform. Sci. Eng., 25: 1485-1500.

Malekzadeh, M., A.A.A. Ghani and S. Subramaniam, 2012. A new security model to prevent denial-of-service attacks and violation of availability in wireless networks. Int. J. Commun. Syst., 25: 903-925. DOI: 10.1002/dac.1296

Malekzadeh, M., A.A.A. Ghani, S. Subramaniam and J.M. Desa, 2011. Reliability of omnet++ in wireless networks dos attacks: Simulation Vs testbed. Int. J. Netw. Security, 13: 13-21.

Mynemi, S. and D. Huang, 2010. IEEE 802.11 Wireless LAN control frame protection. Proceedings of the 7th IEEE Consumer Communications and Networking Conference, Jan. 9-12, IEEE Xplore Press, Las Vegas, NV., pp: 9-12. DOI: 10.1109/CCNC.2010.5421585

Negi, R. and A. Rajeswaran, 2005. DoS analysis of reservation based MAC protocols. Communications.

Nguyen, T., D. Nguyen, D.H.M. Tran, B.N. Vu and H. Mittal *et al*., 2008. Solution for defending against deauthentication/disassociation attacks on 802.11 networks. Networks.

Sandstrom, H., 2011. A Survey of the Denial of Service Problem. In: Reducing the Denial of Service Attacks in WLANs, Singh, R. and T.P. Sharma, (Eds.), Detecting and World Congress Information Communication Technologies, pp: 968-973.

Soryal, J. and T. Saadawi, 2012. IEEE 802.11 denial of service attack detection in manet. Proceedigns of the Telecommunications Symposium, Apr. 18-20, IEEE Xplore Press, London, pp: 1-8. DOI: 10.1109/WTS.2012.6266083

Yu, Y., G. Shi, J. Wang and J. Zhang, 2010. The Practice and exploration on the education mode for embedded systems major. Proceedings of the International Conference on Education and Management Technology, Nov. 2-4, IEEE Xplore Press, Cairo, pp: 367-370. DOI: 10.1109/ICEMT.2010.5657637