Volume 2, Issue 2, December 2018

ISSN 2587-1943

IJIEA

INTERNATIONAL JOURNAL OF INNOVATIVE ENGINEERING APPLICATIONS

International Journal of Innovative Engineering Applications is published June and December.

Adress for the manuscripts and correspondence:

Uluslararası Yenilikçi Mühendislik Uygulamaları Dergisi
Fırat Üniversitesi Kampüsü Teknoloji Fakültesi Merkez –Elazığ
Tel: +90 424 237 0000/ Ext.7655
e-mail: ijieatr@gmail.com

ISSN: 2587-1943

Elazığ-2018

ISSN 2587-1943

FAILURE ANALYSIS OF A SUPERHEATER PIPE BASED ON MICROSTRUCTURE / MECHANICAL PROPERTIES STUDY

R. Bakhtiari, M. Ahmadian, A. Olfati, M. Derhambakhsh

Original scientific paper

The fundamental role of superheater pipes in turbines is to produce superheated steam and direct it to the turbine. These parts are subjected to damage due to the creep, corrosion and oxidation resulting from combustion exhaust. In this research, the affecting factors of failure in a plantain superheater pipe was investigated. Wet chemistry and SEM/EDS analysis were used to investigate the combustion exhaust deposits and a scanning electron microscope (SEM) was used to study the fracture surfaces in order to determine the mechanisms of the fracture. The results showed that exposure of the superheater pipes at temperatures higher than the standard limits caused strength reduction and occurrence of plastic deformation. Furthermore, the combustion exhaust deposits, caused reduction in heat transfer, in addition to severe corrosion as well as cavity formation due to the presence of hydrogen were the main reasons of the pipes failure.

Keywords: *Combustion deposits; Failure analysis; Superheater pipes; Thermal power plant*

1 Introduction

Stationary power generators are one of the most important industries in the country. Many of these generators are steam types which are supplied by fossil fuels. Industrial boiler systems are one of the main parts of a power plant, producing steam for the process units and supplying it to generate electricity. Any factor which leads to shut down of boilers is considerable from an economic aspect. Therefore, preventing these factors is essential. One of the problems that continually results in overhaul of power plants is failure of the boiler pipes. In drum boilers, output steam at higher temperatures, which is called dry steam or superheated steam, has more energy. The process of producing superheated steam takes place in superheaters which are composed of parallel pipes placed in the path of hot gases produced from combustion exhaust. The heat of combustion exhaust is transfered from the outside into the pipes. Then, the saturated steam is converted to superheated steam which is transfered to the higher pressure parts of the turbine [1]. Superheated steam is important according to the following:

- Condensation of steam is impossible due to the heat loss, which is helpful where the steam has to travel long paths.

– The superheated steam prevents corrosion and damage of the turbine blades.

The damage of boiler pipes that causes shut down of a power plant for a while is one of the fundamental problems of steam power plants. Repair processes lead to heavy expenses for the steam power plants in the country. Superheater pipes are repaired and replaced periodically, but the possibility of tubal rupture in times shorter than the deadline time highlights the importance of this issue. Several factors are reported about the failure of superheater pipes. Exposure of metals to high temperatures can reduce the strength and at higher temperatures, the possibility of creep increases. Measuring instruments cannot gather detailed information about the characteristics of the fluid and boiler. However, radiation heat transfer of the pipes could be studied using fluid dynamic modeling techniques. In this method, critical points of the pipe can be identified that shows that pipe bending is the most likely damage mode due to the effects of overheating [2]. Software analysis on pollutants exhausted from combustion shows that the pollutants can increase the pipe temperature. These pollutants are deposited on the surface of superheater pipes causing an increase in temperature and corrosion rate. High temperature corrosion has different mechanisms and therefore different prevention and protection strategies such as thermal barrier coatings.

Tarshizi et al. [3] reported a case study on a superheater pipe and its failure. In this case, an evaluation of pipe lifetime was performed using computational methods with an emphasis on creep lifetime reduction. Kahrom et al. [4] also focused on the joints between the superheater pipe and header output. Microstructural studies on damaged areas using simulation software showed that thermal stresses, due to excessive heat, had a considerable effect on the properties of the joints between pipes and header. Afterward Nemati et al. [5] investigated the wall thickness reduction of pipes under high temperature and pressure in a power plant boiler. The results attempted to predict the time of replacement before failure or breakdown and determining the mechanism of thickness reduction. For this purpose, thickness measurements using the ultrasonic method were carried out on superheater and re-heater pipes during periodic maintenance intervals. The results led to identification of critical points susceptible to failure. Using this method, making proper decisions about replacement of the pipes was possible properly.

In this research, failure analysis of a failed superheater pipe was carried out using SEM/EDS analysis and wet chemistry analysis, and the fracture surfaces were also studied using a scanning electron microscope (SEM).

2 Experimental method

In order to investigate the causes of failure, some samples of failed superheater pipes from the Bistoon heat power plant were studied. The samples for testing were prepared from different parts of the pipes. One of the samples was from an undamaged pipe. In the first stage, the chemical compositions of an original pipe and a damaged pipe were determined using spectrometry analysis. Then the deposits formed on the damaged pipes were removed and their chemical composition was determined using wet chemistry analysis. Hardness testing was carried out according to Vickers, Brinell and Rockwell B methods and the related standards. These measurements were done on different parts of the damaged pipes and hardness profiles were obtained as a function of the distance from the failure region. The ultrasonic method was used to determine the thickness reduction at some parts of the superheater pipes. Scanning electron microscopy (SEM) was used to study the microstructures. Furthermore, an SEM/EDS analysis was used for phase analysis. The SEM and SEM/EDS analysis were also used to study the fracture surfaces.

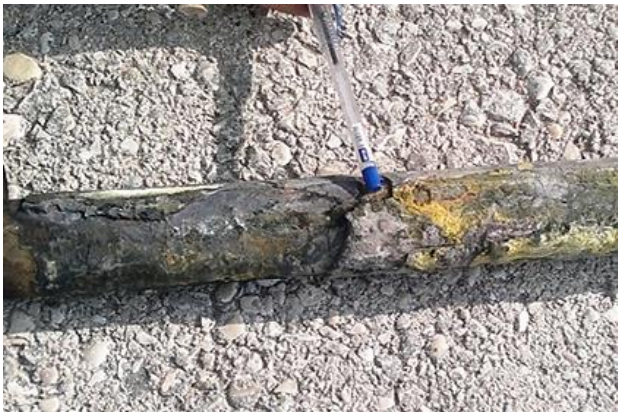


Figure 1. Combustion deposits on the outer surface of the damaged superheater pipe.

Table 1. Chemical composition of the pipe at different conditions (wt.%)

	S	Cu	Co	Al	Ni	Mo	Cr	Mn	Si	C	Fe
As-received sample	0.003	0.01	-	0.04	0.04	0.65	0.92	0.68	0.31	0.17	Base
Damaged sample	0.011	0.06	0.003	0.095	0.074	0.55	0.87	0.44	0.14	0.25	Base
Standard sample (SA-335 P 12)	0.025	-	-	-	-	0.44-0.65	0.8-1.25	0.30-0.61	0.50	0.05-0.15	Base

3 Results and discussion

3.1 Visual study

The damaged pipes were studied visually. The observation showed that the whole outer surface of the pipe was covered with a thick and continuous layer which was the deposits of combustion exhaust (Fig. 1). Formation of the deposits on the outer surface of the pipe increased the working temperature of the pipe which resulted in severe hot corrosion and oxidation. Therefore, the pipe was exposed to damage under higher internal pressure and higher working temperature than the design. The deposited layer thickness was determined to be 6 mm which was high enough to cause damage.

3.2 Chemical analysis of the damaged pipe

Chemical composition of the original pipe and damaged pipe, determined using spectrometry analysis, is shown in Table 1. The chemical composition of the original pipe was generally consistent with ASTM SA-335 P12 steel which specifies ferritic low alloy steel for seamless superheater pipes. These pipes are known as plantain superheater pipes used in the steam power plants. Table 1 also shows that the content of some of the elements in the chemical composition of the damaged pipe are increased or decreased, compared to those of the original pipe. For example, the content of some elements such as sulfur, cobalt, nickel and carbon are increased. The service conditions of the pipes and particularly high temperature can cause changes in the weight percentage of elements just on the pipe surface, which can affect surface properties of the pipes. Therefore, the differences can be generally due to the different production lots for the damaged and original parts. For example, sulfur, which can be transferred to the surface of superheater pipes via the boiler fossil fuels, can cause a reduction in the pipe strength. Carbon, which can form intermetallic compounds, increases the probability of the brittle fracture in the pipes. Furthermore, reduction of Mo and Cr in the damaged pipe, decreases the corrosion resistance at the high temperatures.

3.3 Hardness

In order to determine the hardness variation in the damaged area of the pipe, a hardness profile was plotted (Fig. 2). The results showed that the hardness of damaged area was the highest value but this value was not high enough to cause brittle behavior. Cold working at the fractured area at the service conditions can be the reason for slightly higher hardness of this area.

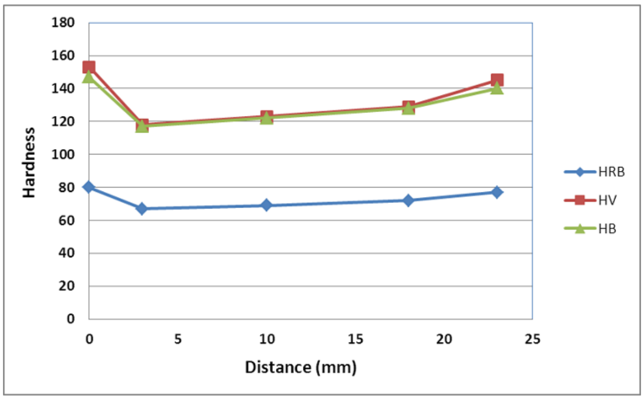


Figure 2. Hardness profile as a function of distance from the fracture area of the damaged pipe.

3.4 Corrosion on the inner surface of the pipe

Inner surfaces of the superheater pipes are in contact with hot and high pressure steam. Therefore, oxidation occurs on the inner surface of the pipe and thickness reduction will result due to the pressure and flow of the steam. This can be a factor in superheater pipe failures. Fig. 3 shows the inner surface of the damaged superheater pipe which contains layered oxidation. These oxidations are visible at the surface and their thickness can show the oxidation volume. Studies have shown that these layers could be iron oxide that formed with the presence of oxygen under favorable thermodynamic conditions. The related reaction is the following:

$$2Fe+H_2O+O_2 \rightarrow Fe_2O_3+2H\uparrow \quad (1)$$

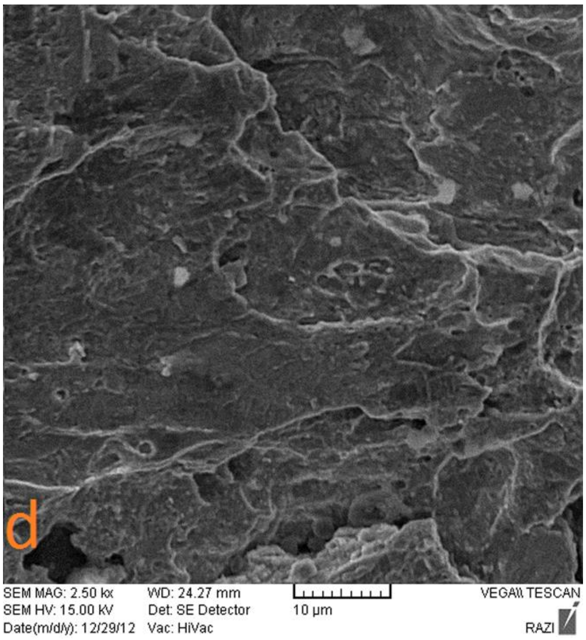


Figure 3. SEM micrograph of inner surface of the damaged pipe containing layered iron oxide.

For further study, the internal diameter of a new and damaged pipe of a similar lot was measured. Fig. 4 shows the comparison of the thickness reduction for the pipes. Results showed that the internal diameter of the damaged pipe increased by 2 mm and its thickness was reduced.

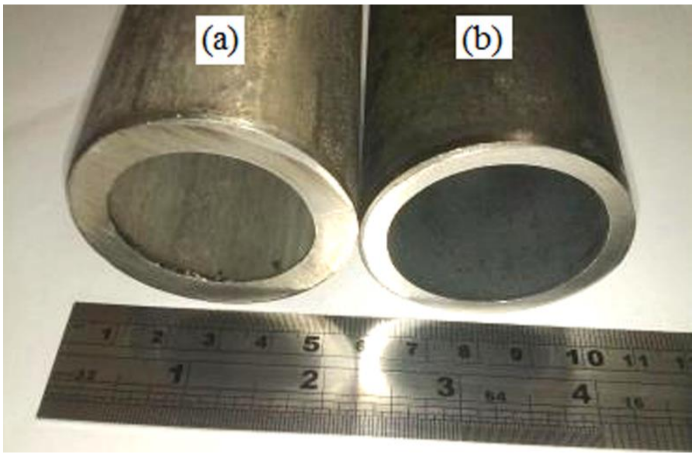


Figure 4. Comparison of thickness reduction between the (a) original and (b) damaged pipes.

3.5 Thickness measurement of the damaged pipe

In order to determine the thickness reduction of the damaged pipe, ultrasonic thickness measurement was used. The results showed that the damaged pipe thickness was reduced compared to the standard thickness of the original pipe of a similar lot (6 mm). The thickness was non-symmetrical as 5.70 mm on one side and 4.78 mm on the other side of the damaged pipe. The maximum thickness reduction was at an area where corrosive agents made of boiler fossil fuels caused deposition and therefore excessive corrosion.

3.6 Corrosion on the outer surface of the pipe

Wet chemistry analysis was used to determine the chemical composition of the deposits on the outer surface of the pipe. The results showed that the deposits were mostly organic compounds (96.85% organic+3.15% inorganic). Table 2 shows analysis of the chemical composition of inorganic material. The fuel of power plants is generally Mazut in winter which causes the deposition rate to increase. Another fuel used in power plants is natural gas mostly used in the warm seasons. Gas combusts more easily than Mazut and therefore has a higher oxidation rate. Therefore, the risk of damage when using gas as the fuel is higher than the Mazut.

The presence of sulfur and iron in the analysis (Table 2) shows that inorganic deposits on the outer surface of the damaged pipe includes sulfide compounds formed due to the presence of sulfur sources in the environment. Higher content of sulfur in the analysis compared to other elements confirms this. On the other hand, the presence of elemental sulfur in the environment is a factor to increase the penetration of hydrogen in the steel. An oxide layer, formed on the outer surface due to corrosion, reduces the cooling effect of the steam and causes the temperature of the pipe to increase, and therefore reduces the life time. The presence of various metal impurities such as sodium, nickel and vanadium and non-metallic impurities such as sulfur and nitrogen in the form of organic compounds in the liquid fuels causes various problems. These metals in the combustion gases could be absorbed on the pipe surface which can cause failure due to the oxidation and reaction with the pipe alloy. As a result of this reaction, complex compounds are formed with low melting points.

Table 2. Chemical composition of inorganic material on outer surface of the damaged pipe (wt.%)

Ni	Fe	S	Cr	Fe
4.4	0.077	36	6.76	0.0036

According to Table 2, the compounds also contain nickel and chromium. There are several sources of nickel to be deposited on the outer surface of the pipe such as boiler fuel in the combustion chamber and the burner nozzle. These nozzles are generally made of nickel-based superalloys, which could release nickel to be deposited on the adjacent pipes. Line scan analysis of nickel across the fracture area on the outer surface of the pipe is shown in Fig. 5. This profile indicates a high content of nickel in the surface deposits.

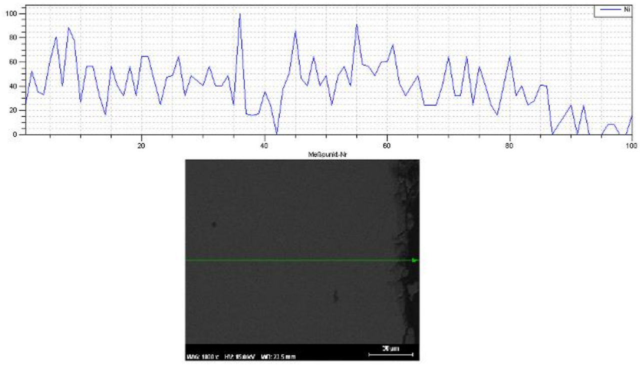
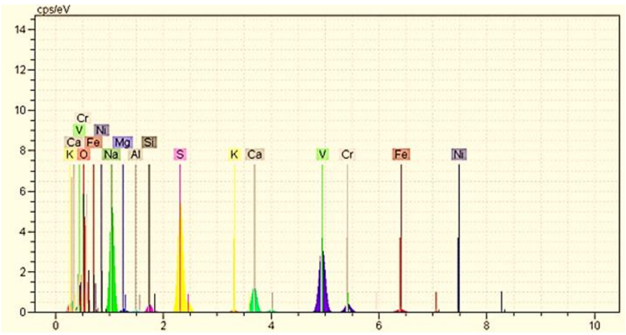


Figure 5. Line scan analysis of nickel across the fracture area on the outer surface of the pipe.

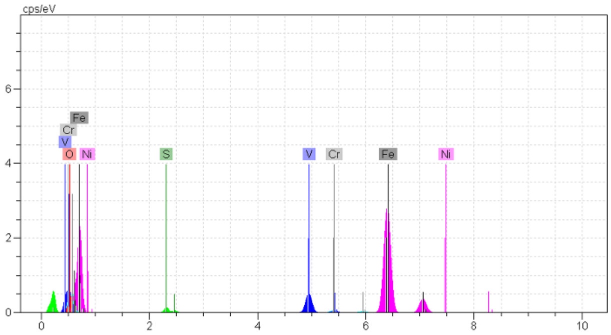
The most harmful elements in fossil fuels are vanadium, sodium and sulfur. These elements can form low melting point (249-677oC) complexes. The resulting liquid dissolves iron oxide, and this molten layer facilitates oxygen transport and oxidation of the pipe outer surface. The SEM/EDS analysis of dark green deposits on the outer surface is shown in Fig. 6. Due to the high percentage of vanadium in the deposits and also the presence of sulfur and sodium, the formation of Na2SO4 and its combination with V2O5, which leads to formation of sodium vanadate complexes, is probable. These complexes have low melting points and cause adhesion of ash particles on the pipe outer surface and therefore reduction of heat transfer.

Analysis of yellow-green deposits (Fig. 7) showed that the content of elemental vanadium was the highest. Some vanadate complexes is known as the most corrosive compounds. Furthermore, the content of sulfur is considerable (according to Fig. 7), and sulfur compounds have an important role on the corrosion of the pipe. Therefore, combustion deposits could be considered as one of the most important factors of failure in the superheater pipes. The results of all analyses showed the content of calcium of 2-4% which caused high strength scale deposits to form on the outer surface of the pipes.



O	Na	S	Mg	Al	Si
52.15	15.42	16.81	2.38	0.38	1.03
V	Cr	Fe	Ni	Ca	K
5.09	-	0.79	1.00	3.10	1.84

Figure 6. SEM/EDS analysis of dark green deposits on outer surface of the damaged pipe (wt.%).



O	Na	S	Mg	Al	Si
4.30	-	0.85	-	-	-
V	Cr	Fe	Ni	Ca	K
6.19	1.17	87.48	0.01	-	-

Figure 7. SEM/EDS analysis of yellow-green deposits on outer surface of the damaged pipe (wt.%).

3.7 Fracture surface studies

In this study, fracture of superheater pipes was observed to occur at the knee bends in some cases (Fig. 8). Due to the high heat concentration at knee bends, severe deformation and rupture occurs. Therefore, these parts are among the most frequently fractured areas in the boiler. Being in direct contact with flame and hot corrosion and oxidation, as well as deposits from fossil fuel combustion exhaust, causes thickness reduction of the pipe and finally a sudden failure.

In other damaged samples, the failure occurred next to the knee bends. According to Fig. 9, these damaged pipes have sharp edges. In this case, plastic yielding at high temperatures can result in opening up the pipe and forming sharp edges. Also, the fracture mechanism can be crack nucleation at the parts which lost their thickness and then a rapid crack growth and final fracture. The rapid growth of cracks can be due to sudden increase of pressure in the pipes.

In this study, some of the damaged pipes had relatively brittle fracture in which the pipe has been cut in half and no plastic deformation was visible. In this case, sudden increase of pressure in the pipes was the main reason for the failure.

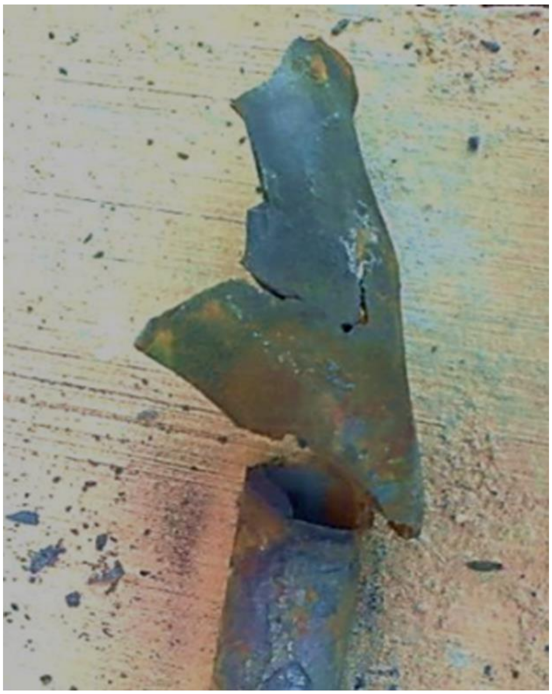


Figure 8. Fracture of a superheater pipe at the knee bends.

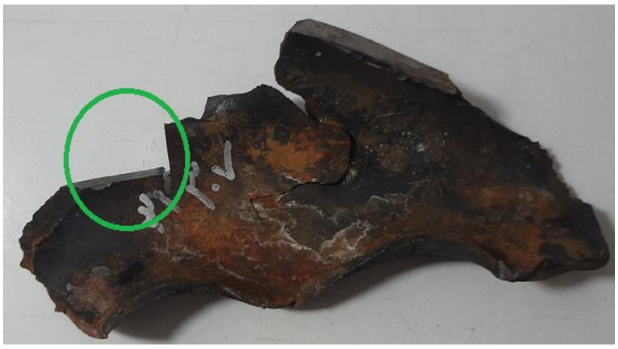


Figure 9. Fracture of a superheater pipe next to the knee bends (Highlighted area is the location used for SEM studies).

An SEM micrograph of the fractured area at a knee bend (Fig. 8) is shown in Fig. 10. According to this figure, growth of deposits because of exposure at high temperatures caused formation of cavities at the fracture surface. In steels, hydrogen damage takes place generally in the presence of atomic hydrogen. In humid atmospheres and at high temperatures, corrosion and electrolysis reactions can lead to atomic hydrogen formation via the reduction of hydrogen ions. Some of these atomic hydrogen form molecular hydrogen again and the others penetrate into the steel structure. The penetrated hydrogen atoms gather in grain boundaries and form cavities. Furthermore, some dimples are visible in Fig. 10. The dimples can show relatively ductile fracture. As discussed before, the plastic deformation caused formation of sharp edges at the damaged pipe.

Fossil fuel combustion deposits on the outer surface of pipe surfaces can lead to hot corrosion and severe oxidation. In Fig. 11.a, the deposits, which can be mainly sulfur-riched, are accumulated and have cavities. In Fig. 11.b, vanadium-riched deposits, with higher hardness in comparison with those of Fig. 11.a, can be detected which have a melting point at about 600°C.

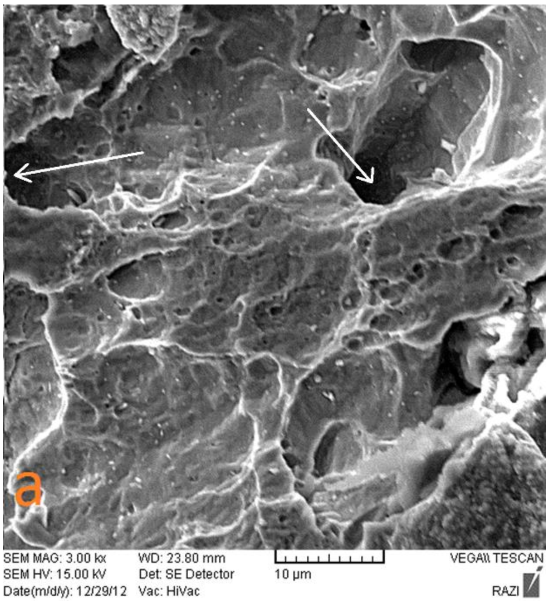


Figure 10. SEM micrograph of the fractured area at a knee bend including cavities (indicated as white arrows).

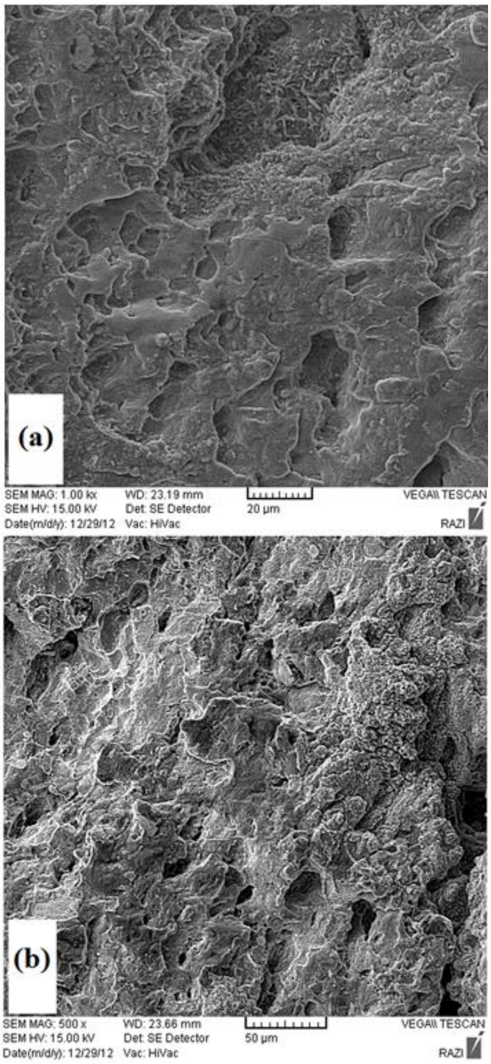


Figure 11. SEM micrograph of (a) fossil fuel deposits and (b) hard oxide layer on the outer surface of the damaged pipe.

1Cr-0.5Mo steels are used in boiler pipes which working temperature is 510 to 540°C. 2.25Cr-Mo steels, which have a higher oxidation resistance and creep strength compared to 1Cr-0.5Mo steels, are good choices to use at temperatures up to 650°C in environments without hydrogen and at temperatures up to 480°C in environments contained hydrogen. Since the standard temperature limit for using ASTM SA-335 P12 steel pipes (the steel used in this study) is 500°C, being exposed to higher temperatures could be critical. One of the damage mechanisms in superheater pipes is microstructural changes occurred at high working temperatures. These changes includes changes in structure, size and the spacing distances of carbides, compositional changes of ferrite and variation of solid solution strengthening. Creep is an important failure mechanisms in boilers and specially in their superheater pipes. Carbides are the main source of creep cavities. At high temperatures, conversion of carbides is the following:

$$M_3C \rightarrow M_3C + M_2C \rightarrow M_3C + M_2C + M_7C_3 \rightarrow M_3C + M_2C + M_7C_3 + M_{23}C_6 \quad (2)$$

These carbides cause the grain boundaries to become serrated. These grain boundaries are unstable and cause strength reduction at service conditions. At high temperatures and under high stresses, cavities could be formed at these carbides. Generally, grain boundary carbides could be main factor of creep fracture [6,7].

4 Conclusions

Failure analysis of a superheater pipe was carried out using microstructural analysis and hardness measurements. The results showed that corrosion and the related deposits on the pipe surface, as well as cavity formation due to the hydrogen absorption were the main mechanisms of the pipe failure. The evidences were the following:

- Working temperature was higher than the permitted limit of the steel which caused strength reduction and occurrence of plastic deformation.
- Reduction of pipe thickness resulted in decrease of pipe strength especially at the knee bends and excessive heat applied to the knee bends increased the rate of microstructural changes.
- Deposits had a major role in the pipe corrosion and its thickness reduction. Vanadium and sulfur elements had the greatest content in the deposits.
- SEM micrographs showed cavities at the fracture surfaces. The presence of hydrogen could be the source of cavity formation.

To prevent and control the damages in the studied pipes, the following is recommended:

- Controlling the boiler temperature to prevent unwanted temperature rise during service.
- Selecting appropriate steel for service conditions of the boiler.
- Lowering oxide deposits inside the pipe using proper acid washing.
- Using fuels with appropriate composition to control the content of undesirable elements such as sulfur.
- Using sandblast to clean the outer surfaces of the pipes.

Acknowledgments

The authors would like to acknowledge Bisotun Electricity Production Management Company for supplying the specimens of this research.

5 References

[1] Lee NH, Kim S, Choe BH, Yoon KB, Kwon D. Failure analysis of a boiler tube in USC coal power plant. Eng Fail Anal 2009;16:2031-5.

[2] Rahimi M, Khoshhal A, Shariati M. CFD modeling of a boiler’s pipes rupture. Appl Therm Eng 2006;26:2200-492.

[3] Jones DRH. Creep failures of overheated boiler, superheater and reformer tubes. Eng Fail Anal 2004;11:873-93.

[4] Thielsch H, Smoske R, Cone F, Husband J. Failure analysis of superheater outlet header. Adv Mater Process 2000;157:43-4.

[5] Port RD, Herro HM. The NALCO guide to boiler failure analysis. 2nd ed. McGraw- Hill Inc; 2011.

[6] Davis JR. Refractory metalls and alloys. ASM specialty handbook: Heat-resistant materials; 1997.

[7] Viswanatan R. Damage mechanisms and life assessment of high temperature components. Metals Park, Ohio: ASM International; 1995.

Authors’ addresses

R. Bakhtiari, Ph.D. in Materials Engineeing
Razi University
Department of Materials and Textile Engineering, Faculty of Engineering, Razi University, Kermanshah, Iran.
r.bakhtiari@razi.ac.ir, bakhtiari.r@gmail.com

M. Ahmadian, M.Sc. in Materials Engineeing
Azad University
Department of Materials Engineering, Azad University, Kermanshah, Iran.
m.ahmadian@fnpcc.com

A. Olfati, M.Sc. in Materials Engineeing
Azad University
Department of Materials Engineering, Azad University, Kermanshah, Iran.
abbasolfati@yahoo.com

M. Derhambakhsh, M.Sc. in Materials Engineeing
Azad University
Department of Materials Engineering, Azad University, Kermanshah, Iran.
benjaminder@gmail.com

ISSN 2587-1943

SMART SECURITY OF IOT AGAINST DDOS ATTACKS

Ahmet Efe 1, Esra Aksöz 2, Neslihan Hanecioğlu 3, Şeyma Nur Yalman 4

Original scientific paper

Since the internet, which is pervasive in every area of our lives, is so inevitable that the number of intelligent systems and devices, which are interconnected, have increased day by day through e-government, industry 4.0 and smart city applications. These devices have led to the emergence of the 'Internet of Things' (IoT) concept to the extent that intelligent systems became widespread. In addition to facilitating the life and functionality of these devices, we also need to take some safety precautions to prevent failures, difficulties and denial of service. In order to take the necessary precautions, we need to know functionality and capability of devices and risks, vulnerabilities and threats as well. We have conducted a survey on taking all kinds of security precautions against DDoS attacks, to contribute to increase the security level of these intelligent devices.

Keywords: *Internet of Things, intelligent systems, E-government, Security of IoT.*

1 Introduction

The keywords start with 'smart' are very popular in nowadays like smart cities, smart watches, etc. All of them are related with Internet of Thing (IoT) technology. Communication of these devices provided via the internet. Also, intelligent transportation will access a web of interconnected data from GPS location to weather and traffic updates via the internet. Also, the traffic lights will light up according to the intensity of the road through the data they get from the internet. These situations will make human life much easier. But these will bring security problems. Because of these operations, a very large amount of data will be generated, and these data will need to be protected. If there is an illegal access to information and attacks in the system of the smart house, it will cause physical disruptions. Because of these situations, all data in IoT need to be protected.

While traditional ransom software enters computers and encrypts files, IoT ransom software can take control of systems used in the real world. Many of the practical advantages of IOT technology are ransom operators who use their own advantage, can cut off electricity, stop vehicles, and even prevent production lines from functioning. These methods, which are much more likely to create more damage, will also increase the amount of ransom money that attackers are willing to give back to their IoT device. If there is a place where such extra ransom could be obtained, the attackers will not be idle.

Some experts think that such an attack can be solved by simply resetting the IoT device, turning it on and off, or starting it all over again. But IoT is not the irreversible effect of traditional ransom software, which makes ransom attacks terrible. This time the dangerous situation is the timing of the attack. Many complex IOT schemes are already in use, which can lead to catastrophic failure to reach critical systems for even a second.

As IoT is increasingly integrated into more critical systems, the inability to reuse the locked systems in time can cause serious harm to the individual and the public. Examples of these critical systems are cardiac pacemakers to power plants. How long do you wait to pay when a relative or your heart rate is disabled by ransom software?

Let's give another example. When intelligent vehicles become widespread, locking only 3 for a short time is enough to overturn the traffic of an entire city. Even worse: think that the subway signaling system does not work for just 1 minute. How many lives get in danger?

Examples of IoT repatriation attacks are also shown. Pen Test Partners, a UK based company, for example, took a smart thermostat with ransom software and ran the thermostat at full power as long as the required money was not paid. This, of course, was just a test. Later, other security companies and software groups, smart homes, intelligent offices, connected and autonomous devices showed how worn-out smart devices could be captured by ransom software.

All elements that make up smart cities, from traffic lights to bus stops or even roads, need to be defended against the pirates because they are interconnected. Developed cyber security methods complicate the work of hackers, but those who manage smart cities should always be on the alert. In this article, we will talk about what we need to do to ensure that the software that forms smart cities is not hacked by data thieves.

IoT security must be cleared from the beginning in the face of all these "demonstrations". In the past few weeks, DDoS attacks were made with 145 thousand IOT compatible cameras (web cameras, security cameras, etc.) captured by cyber hijackers.

2 Problems with IoT in general

There are many risks and threats arising from IoT vulnerabilities. As a simple example can be given from printers that have IoT capabilities. Recently, as seen in the attack on the DNS provider Dyn, probably IoT (objects of the Internet) powered by using botnet DDoS attacks will keep on happening in 2017. by 2016, all an IOT botnet (Mirai) by targeting the Internet one of the big DNS server can be interrupted for hours.

In this case in the hands of almost any person who is the most powerful government actors are prepared for a worldwide communications network. The only way the growth of the phenomenon of IOT botnet security issue being considered to have produced a lot of devices. Patch is written in millions of existing sensitive IOT device, but the patch process was so complex that users prefer to skip the process of patch.

Printer devices found in every office may seem innocent and innocuous at first. However, the writers form one of the most important networks in the office. There is extensive networking between printers and computers in intensive offices, and this poses a high risk for cyber-attacks. Efficient document processing and superior security are now more important to every office. This situation will require more stringent measures, especially in the era of the Internet of Things (IOT).

IoT technologies, which have come to our minds frequently in recent times, are taking place in different areas of our lives day by day. IOT networks can create a variety of usability by connecting many devices at home and in offices. But these technologies and devices add to the business life, as well as threats to data security. Unless security precautions are taken regarding the use of connected devices over the Internet, the possibility of infiltration of important data out of the office is increasing.

Connected devices that do not have sufficient cyber security can lead to malicious aliens entering offices' operating systems. This has the potential to make office networks and infrastructures suddenly vulnerable to cyber-attacks. Canon, the technology company, lists the most serious problems with printer devices used over IOT networks as follows:

- Employees can get someone else's documents from the printer,
- If the printer settings are not checked for security,
- Unauthorized change of documents to be transmitted over the network,
- Monitoring network traffic of cyber hackers leaking into networks via IOT devices,
- Ability to digitally copy documents on un-passworded printers.

2.1 Problems with Intelligent Home Systems

Smart home systems, from heating to lighting in many ways more comfortable and makes the home life easier while increasing energy efficiency also reduces the cost. Other solutions in this area smart alarms and locks increase our security. Smart home assistants such as Google Home and Amazon Echo, though not yet widespread in our country, ensure that all devices in the house communicate and communicate with each other. According to Gartner, in 2020, 25 billion objects in the world will be in contact with each other, and smart home devices will be most of these devices. When you say that, you can think that an extremely comfortable future is waiting for us. But let's look at the empty side of the glass. How safe are these smart home systems that make our lives easier? In this week's article, I've put together the security risks of smart home systems and the simple measures that can be taken.

According to a study conducted in the US in 2016, 47 percent of people do not prefer to use smart devices in their homes yet because they are not sure of their safety. If we go from popular examples again; Amazon Echo and Google Home's voice recording features keep users nervous. In an incident in 2017, the police requested Amazon's Echo records in the house but were confronted by Amazon's objection. Subsequently, the defendant had submitted his own request to be used in his defense. According to another study in 2016, your camera and microphone can be hacked through security vulnerability on Android-based smart TVs. With a malicious application installed on the TV, hackers accessing the device can access other connected devices at home via TV.

Another scary detail on smart home systems is about the WiFi network. Because a WiFi network with security weakness means easy access to the entire system in your home. The best part of smart home technologies is to integrate complex processes and make them manageable from one place. However, the security levels of 3rd party integrations are not yet at the desired level, and this situation makes the smart home systems vulnerable to attacks. Security processes, on the other hand, have become complicated by cyber-hackers' efforts to take home network routers to attack criminals to attack smart home devices. The report, which was shared by Trend Micro in 2017, carried out more than 1.8 million cyber-attacks in the first 6 months of 2017 through home network routers from all over the world. In 8 percent of these attacks, hackers access a home device, run malware remotely, and use confidential information like a password. Other types of attacks; the transmission of content transmitted through the affected devices to the attackers. If we collect the safe risks of smart home systems, we see that the following 3 headings come to the fore: Remaining long time to vulnerable networks, changing passwords and changing the number of home devices, as well as occasional software updates / software updates.

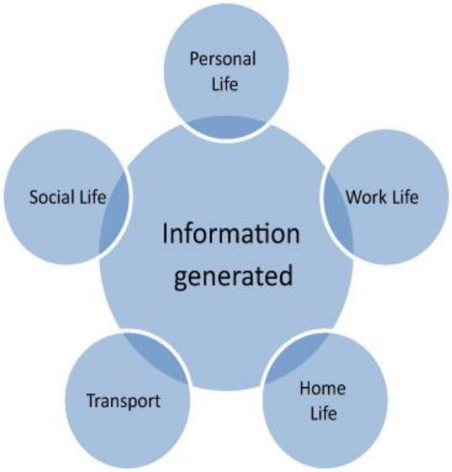
As the dangers and attacks in the cyber world increase, security companies also increase and enrich their proactive approach and solutions. Malicious software is also evolving as hackers implement the encryption method to start using cloud services as a weapon. According to the 2018 Annual Cyber Security Report, which was prepared by Cisco this year, more and more investments will be given to vehicles using artificial intelligence and machine learning to reduce the lifespan of cyber attackers. Cisco researchers, over a period of 12 months, they observed a more than 3-fold increase in the use of encrypted network communications for the malware samples examined.

2.2 Problems with Smart City Applications

All the elements of the smart cities of the future, such as public vehicles, public transport vehicles, traffic lights, street lamps, etc., exchange data with each other online. The city environment created by these intelligent systems can be quite attractive for data thieves. The city of Glasgow has invested € 24 million in smart street lamps and traffic monitoring sensors to facilitate the lives of pedestrians and cyclists. Similarly, the city of Bristol has created a city operating system to collect and interpret data on environmental pollution that threatens community health. It uses. While such cities often use these systems on their main streets, they aim to create a smart city and facilitate the lives of people of the city by spreading them all over the city. However, it is imperative to consider the chaotic conditions that may be caused by a data thief infiltrating the traffic monitoring sensors or the city operating system. Leading security researchers state that open, sensitive data exchanges, such as smart cities, may be more vulnerable to hackers than to computers and smartphones.

The security research company IO Active Labs warned those who governed smart cities by stating that many cities do not plan against cyber-attacks, even though cities have plans against natural disasters such as floods and earthquakes. Intelligent strategies should be developed against cyber-attacks since a human-centered disaster can lead to great devastations.

IO Active Labs, found that 200,000 traffic control sensors from Washington to Melbourne could easily infiltrate pirates. Pirates could exploit these vulnerabilities to manipulate traffic signals or change electronic road signs, such as speed limits, to fatal accidents. Data thieves who exploit vulnerabilities in intelligent systems, such as security systems that can be easily captured, face detection camera systems, can cause large-scale crimes to be committed. Looking at these examples, we can say that a system that is more vulnerable to pirates than a special system would be more attractive. But since all systems are connected in intelligent cities, infiltration of any of the systems with the domino effect can cause a great mess. Therefore, security strategy should be handled and at the same time, all security vulnerabilities for each system should be minimized or even eliminated.



3 Literature Review

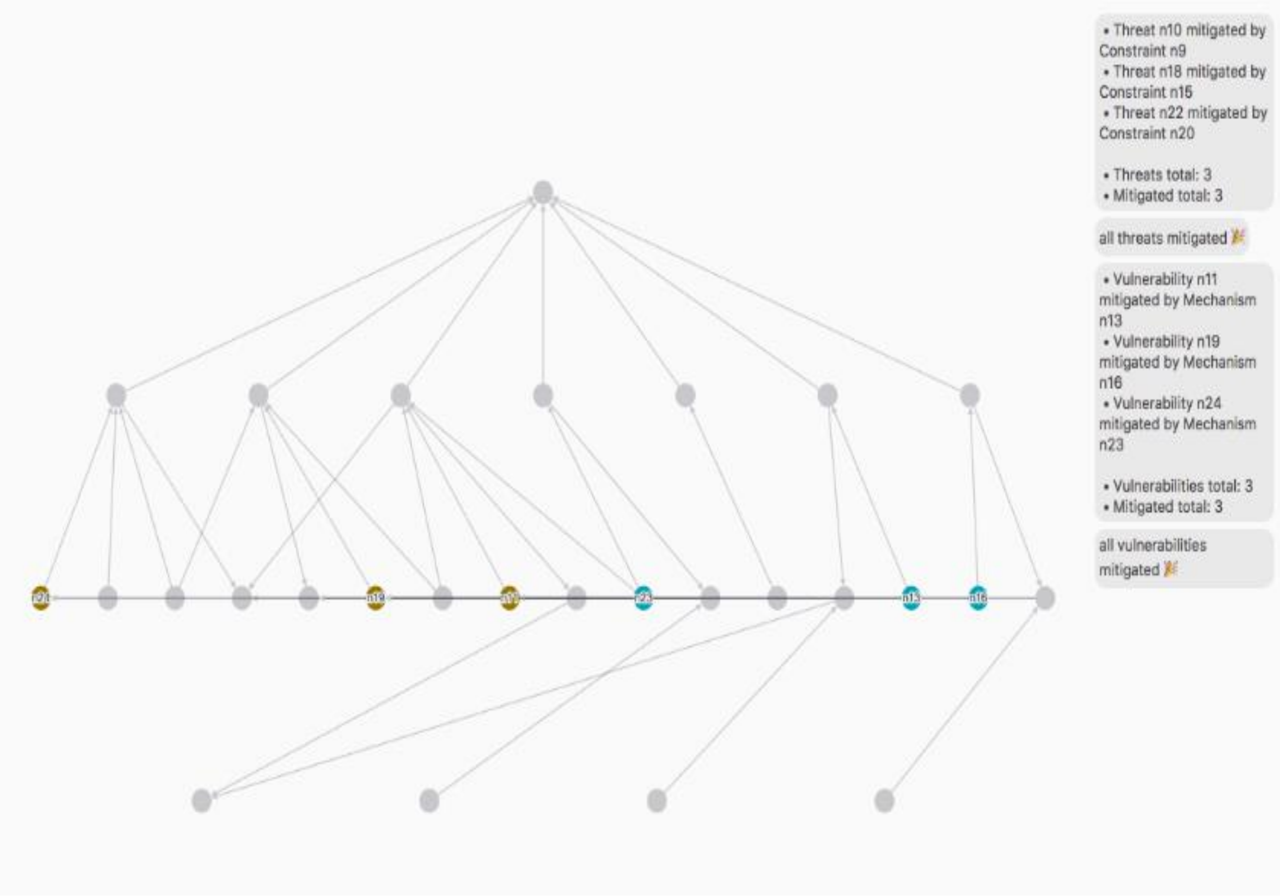
As seen in figure 1, a lot of data is being generated. The collections of that data store such as on the device or on a cloud aggregator. This situation causes some risks such as attacks to the stored data. For preventing this issue, several best practices papers published for IOT security best practices recently. The Broadband Internet Technical Advisory Group (BITAG) generated the report about IoT devices based on consumer [1]. The US Department of Homeland Security (DHS) published a document, ignoring things such as personal privacy [2]. The Federal Trade Commission (FTC) released suggestions that stress confidentiality concerns such as notice, data minimization, choice and data safety [3].

Another academic study presents a set of well-investigated Internet of Things (IoT) security guidelines [4].We considered suggestions from all these sources when preparing our article. According to the above studies, to ensure security at IOT devices, devices must be secured, network must be secured, and the overall IOT system must be secured. These headings will be detailed in the security part together with their subheadings.

The following project launched in 2016 in Github. This project is about authentication/authorization feature for Android based Over the Air Firmware update. By using some cryptographic techniques, it developed an algorithm that requires client (android) authentication and authorization before it can go ahead with the OAD update [5].

Another study about IoT security is The Secure IoT Home Gateway [6] in Github. This project improved an innovative solution for safe home gateway.

Some people do a graphical security analysis tool for IoT networks [7] in Github. The name of the project is apparatus software tool. The screenshots of the project is in the Figure 2. We can see all threats and vulnerabilities detailed in this figure.



• Threat n10 mitigated by Constraint n9
• Threat n18 mitigated by Constraint n15
• Threat n22 mitigated by Constraint n20

• Threats total: 3
• Mitigated total: 3

all threats mitigated 🎉

• Vulnerability n11 mitigated by Mechanism n13
• Vulnerability n19 mitigated by Mechanism n16
• Vulnerability n24 mitigated by Mechanism n23

• Vulnerabilities total: 3
• Mitigated total: 3

all vulnerabilities mitigated 🎉

Figure 2. A graphical security analysis

4 IoT Devices Architecture

IoT devices mainly consist of three layers:

- Application Layer
- Network Layer
- Perceptron Layer

Perceptron Layer Attacks:

In perception layer, IOT devices have a strong relationship with sensors, Radio-Frequency Identification (RFID), wireless sensor networks (WSN).

5 IoT Attacks

IoT devices architecture is potentially open to a huge number of attacks. Attacks may be performed at different levels [8]:

• At network level, the hacker has only access to the device through the network or through the applications offered by the IoT solution provider (eavesdropping).

• At device level, the hacker has also access directly to the device, and can perform additional attacks, i.e. invasive or semi-invasive attacks.

• At chip level, the hacker can physically perform attacks on chips located in the device (e.g. reverse engineering).

5.1 Distributed Denial of Service Attacks on IoT Devices

Distributed Denial of Service (DDoS) attacks are defined as a system consisting of many distributed structures is attacking the target. Commonly DDoS attacks are evaluated by considering three layer which are Perception, Network and Application Layer [9] [10]. In table 1 indicates what kind of attacks happens in these layers.

At perception layer RFID is main technology for reading data from sensor without human interaction and touch.

a) Jamming: In this electromagnetic jamming is done to prevent tags from communicating with reader.

b) Kill Command Attack: This kind of attack deactivates communication by using command tag easily.

Table 1. Attacks for different layers

Layer Name	Attacks Name
Perception Layer	Node Capture Fake Node Malicious Data DoS Attack Timing Attack Routing Threads Replay Attack Side Channel Attack
Network Layer	Man in the Middle Attacks DoS Attacks Exploit Attacks Sybil Attacks
Application Layer	Data Access Permission Authentication Software Vulnerabilities Data Aggregation Distortion Data Protection

A new command tag can be protected by password, but anyone can apply a brute force attack and crack it because of limited memory and processing.

The most popular attack on network layer is DoS attacks. On the other hand, on application layer, software vulnerabilities are open to attacks.

5.2 Botnet Attack on IoT Devices

Normally, DDOS attacks with viruses turned into zombies, laptop and desktop computer is via a botnet consisting of. However, this time the hackers have seized the Internet devices of objects: Biggest attacks are on smart phones, smart watches, fitness bracelets, boiler thermostats; smart was made with the Internet of objects, such as lamps

As shown in Figure 3, Botnet attacks are that many computers are managed from a single point in the direction of evil intent.

Malicious hackers set up a community of thousands of zombies and perform botnet attacks via a kind of virus-infected access programs. A Botnet-possessed attacker can easily manage all the computers on his network from any part of the world.

The Botnet attack, which is seen as a dense entry of users, is no different to the normal visitor in the server's eyes. However, when too many user’s login and logout to a web site continuously, the server will have to respond to too many requests, and after a while the web site may close because the service band is full [11].

Botnet attacks forms the basis of DDoS attacks. More than one request is simultaneously sent to the target system via the botnet tool to perform DDoS attacks.

5.3 Statistics for Botnet-Aided DDoS Attacks on IOT Implementation

If we need to talk about the quarter results of 2017:

- In the fourth quarter of 2017, DDoS attacks were carried out on target systems in 84 countries.
- The rate of attacks targeting China is over half of all attacks (51.84%).
- The most attacks were occurred against South Korea, China and USA. However, in terms of the number of botnet C & C servers, Russia has come to the fore.
- The longest DDoS attack of Q4 lasted 146 hours in 2017. If we look at previous periods, the longest attack of 2017 (277 hours) was recorded in Q2.
- SYS DDoS is the most popular attack method; the less common method is ICMP DDoS.

Now, we can see the graphs related to the results:

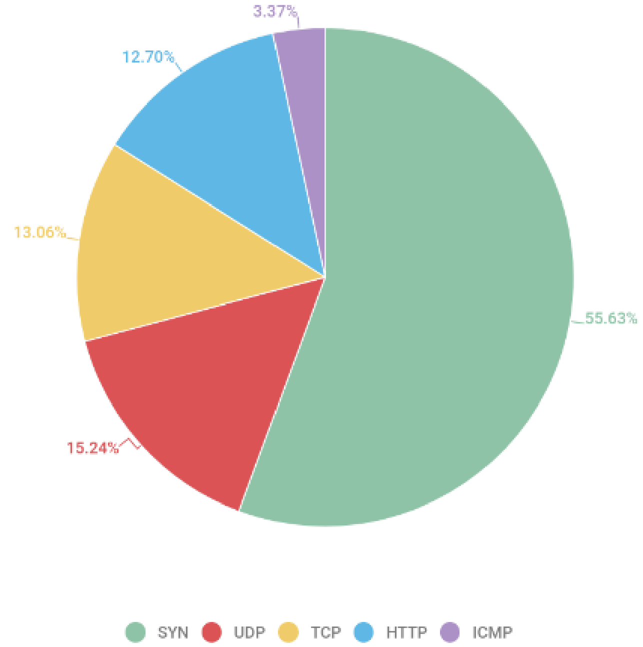


Figure 3. Dispersion of DDoS-attack according to communication protocols - [12]

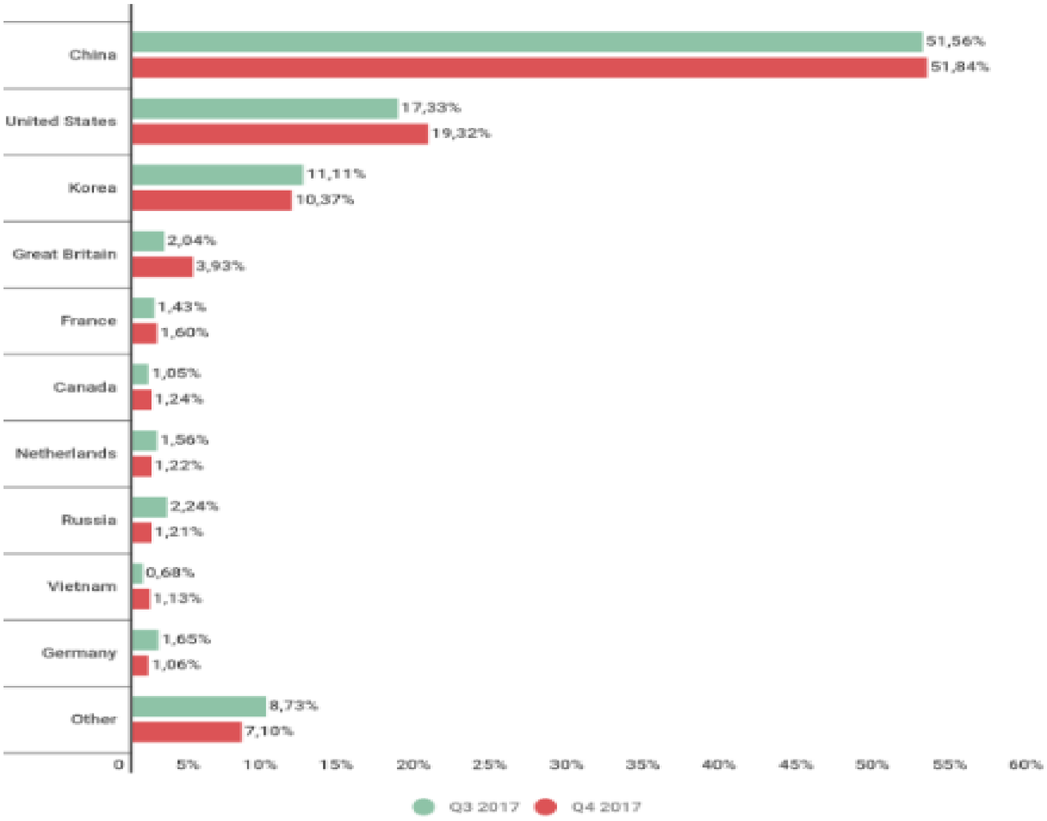


Figure 4. Dispersion of DDoS-attack according to country - [12]

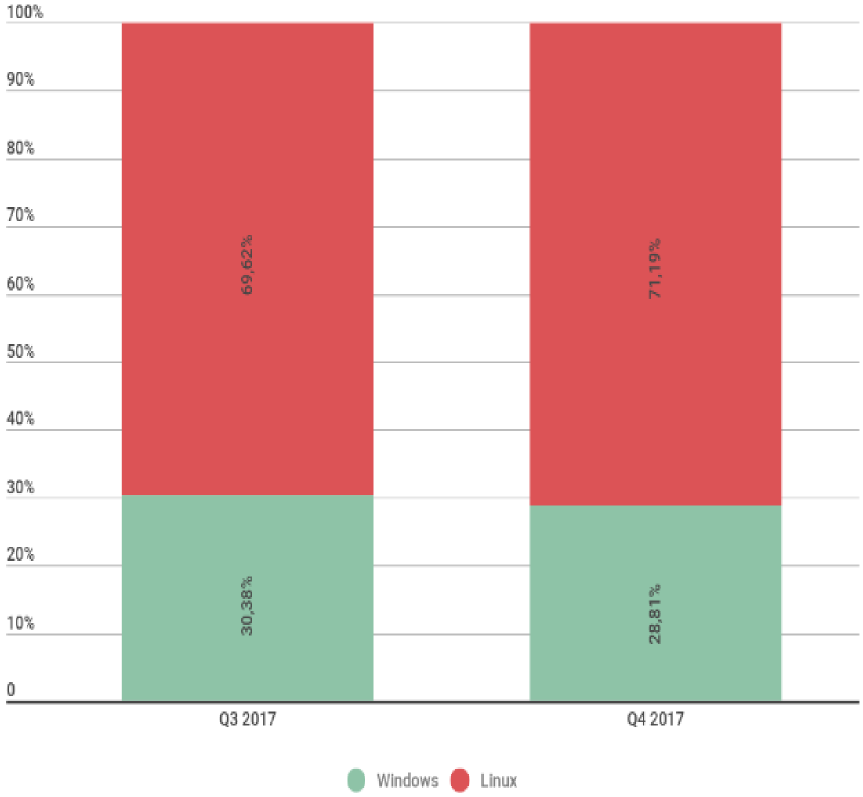


Figure 5. Windows vs Linux-essential botnet attacks – [12]

6 Security of the IoT Devices

We examined the attacks of the IoT devices. In this part, we will examine the security of these devices. This section is separated into three subtitles: security of IoT devices, security of IoT networks and security the full IoT system and is examined each of them detailed.

6.1 Durable hardware

Some these computers may run unsupervised. The IoT system contains a lot of devices. The supervision of these hundreds of computers is very difficult. For this reason, IoT devices takes a lot of attacks as we stated before. For preventing this situation, it is kept these computers isolated thus only a few specific people must be access the system.

6.2 Updating/patching

The computers must be updated in the IOT. New computers are being developed as new cyber attacks. However, no manufacturer 20 years life expectancy is an RFID tag cannot protect future cyber attacks. No firmware will be released after 10 years cannot be prepared to block the malware. That's why we can't protect the internet of objects of the software update.

6.3 Testing

It is the most important that IoT devices pass the testing for the security. But the static testing is not suitable for finding vulnerabilities, because it doesn’t find vulnerabilities in processors or memory. For this reason, dynamic testing is necessary for finding these vulnerabilities of these components in IoT.

6.4 Data from removed devices

When the devices are growing old and the user decides to remove of them from the system, these devices must be removing without exposing the data. That is, the data or information in the removed system must be protected.

7 Securing Networks

7.1 Identity

Easy predictable credentials must not use in the IoT system. The computers must not use default username/password information, because once predicted many computer hacks.

7.2 Cryptographic and safe protocols

Even though a computer identity are safe, that is despite user selects strong password and username, contact between devices might be listened. In the IoT there are many protocols, including LoRaWAN, NFC, Sigfox, Bluetooth, Wi-Fi, 6LoWPAN, Neul, Z-Wave, Zigbee etc. According to these protocols, a computer may have necessary to use powerful.

7.3 Separation of the network

For the security of the IoT system, divide the network into segments using IP address ranges etc. These sub networks are used in firewall security to specify one or more source and destination interfaces on the platform.

7.4 Security the full IoT system

The main concept of IoT is to connect objects via Internet; I mean that the devices communicate with each other through the internet. IoT devices ensure services that are explorable by other IoT devices. For preventing the attacks in the internet, only authorized clients should discover the device.

8 Conclusion

Everything in smart homes is connected to the central access point router. Whether your home is fully connected or managed by a single smart device, the first place you need to start improving security is the router. For this, you first need to make your choice of router correctly. The second simple but important setting is to set a new password by changing your router password.

Security must be one of the main criteria in choosing the right device. Some smart device providers can encrypt through the cloud to reduce risks. To avoid the vulnerability, I recommend you choose smart devices that use business applications that work with business partners. If you already have smart home devices, you should learn the features well. For example, if you have features that you do not want / you do not want to change the settings menu, you can personalize the device.

According to the 2015 “Norton Cyber Security Inside Report”, 33 percent of smartphone users do not have a device password. Since smart devices can be controlled via smartphones, your smartphone can be the key entry point to access other devices in your home and the entire system. If your unsecured phone gets in the hands of malicious people, they can interfere with your smart home system as they wish. To do this, first put a password on your smartphone. Another important and necessary step is to install security software on your computer or mobile devices. Because regardless of the security level, all devices can be vulnerable to external attacks.

Managers should take responsibilities to understand the systems they receive while creating intelligent cities and establish transparent relationships with the companies they support from the establishment stage to the maintenance. In addition, every smart city should have trained cyber security emergency response teams against possible cyber-attacks and bad consequences. Not being able to know how to react to the attacks can cause great turmoil, stopping in the usual city life flow. Therefore, serious cyber security strategies should be created. But threats can be re-energized against changing strategies such as bacteria gaining antibiotic resistance. In other words, it is usual to face a new security threat against each improved security strategy. Therefore, security measures should be constantly updated and monitored. In other words, those who want to be protected against attacks should always be a few steps ahead of the pirates.

DDoS attacks can be used easily to IOT infrastructure collapses. For an attack to the diameter, and worst-case scenario; the cities’ or companies’ IT team, for DDoS attacks must develop an effective strategy to prevention. Thanks to the devices used in the form of solutions overprovisioned normal DDoS attacks that exceed your bandwidth, you can manage. For example, a 20 Gbps regular user traffic 1-Gbps bandwidth DDoS attack that uses a device that you can use to have your plan and potential bandwidth is received here by your service provider. If your service provider has to offer the real attack is more bandwidth to work with cloud-based DDoS a considerably increased "scrubber" you may need a hybrid cloud containing.

Segmentation is important for complex smart city IOT networks. For example, the user Smart transport network services, web pages, like other smart energy networks must be a logical way. This helps in isolating segmentation attack and malicious software from a network to another IOT network when switching to the threats the region advanced to be identified. Still, in this way, smart city may be divided into network security zones, and that internal traffic and restricted data and monitoring of devices and resources helps to prevent unauthorized access, use or disclosure.

This type of segmentation is smart city-wide board of IOT equipment only when necessary to communicate with devices and systems and only in designated protocols makes it possible to this communication. In this way, you can also let your internal network is part of a DDoS attack of or the becoming.

To sum up, the attacks of the IoT devices are many. In this article, we examined the Botnet attacks and DDoS attacks and the security of the IoT system in general. For protecting the system for these attacks, emphasized measures must be taken in the security section.

9 References

[1] BITAG, "Internet of Things (IoT) Security and Privacy Recommendations," A Uniform Agreement Report, November 2016. https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[2] HC, "strategic principles for securing the internet of things," U.S. Department of Homeland Security, November 15,2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[3] FTC, " Internet of Things: Privacy and Security in a Connected World," *Federal Trade Commission,* 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[4] "Internet of Things (IOT) security best practices," *IEEE Internet Technology Policy Community White Paper,* February 2017.

[5] WIND, "Security for Internet of Things," https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[6] "Secure Home Gateway & Registry Idea," https://github.com/CIRALabs/Secure-IoT-Home-Gateway

[7] "ASTo - Apparatus Software Tool," https://or3stis.github.io/apparatus/

[8] Vault, "IOT Security Solutions," [Online]. Available: https://www.insidesecure.com/content/download/1064/13249/file/IoT%20SecuritySolutions%20White%20Paper.pdf. [Accessed April 2018].

[9] N. Mukrimah, A. Amiza, Y. Naimah and B. L. Ong , "Internet Of Things(IoT) : Taxonomy of Security Attacks," in *International Conference on Electronic Design(ICED),* Phuket, 2016.

[10] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in *Ninth International Conference on Computational Intelligence and Security*, Nanning Guangxi, 2013.

[11] Techopedia, "Botnet Attack," Techopedia, [Online]. Available: https://www.techopedia.com/definition/29948/botnet-attack. [Accessed March 2018].

[12] Securelist, "DDoS attacks in Q4 2017," KasperskyLab, [Online]. Available: https://securelist.com/ddos-attacks-in-q4-2017/83729/. [Accessed March 2018].

Authors' addresses

Ahmet Efe 1, PhD, CISA, CRISC, PMP
İnternal Auditor at Ankara Development Agency,
Part Time Lecturer at Yıldırım Beyazıt Universiy
Ankara/Turkey E-mail: icsiacag@gmail.com

Esra Aksöz 2, MSc Candidate
Yıldırım Beyazıt University, Department of
Computer Science, Ankara/Turkey E-mail:
esra.aksoz06@gmail.com

Neslihan Hanecioğlu 3, MSc Candidate
Yıldırım Beyazıt University, Department of
Computer Science, Ankara/Turkey E-mail:
neslihanecioglu@gmail.com

Şeyma Nur Yalman 4, MSc Candidate
Yıldırım Beyazıt University, Department of
Computer Science, Ankara/Turkey E-mail:
seymanur.ylmn@gmail.com

ISSN 2587-1943

CONTOUR SURFACES IN THE (2+1)-DIMENSIONAL SINE-POISSON MODEL

Haci Mehmet Baskonus 1, Hasan Bulut 2, Sibel Sehriban Atas 3

Original scientific paper

This paper apply the modified exp(-Omega(xi))-expansion function method to the (2+1)-dimensional Sine-Poisson equation. Many complex soliton solutions are successfully constructed. 2D and 3D figures along with contour surfaces by using several computational programs such as Mathematica and Matlab are plotted. Finally, at the end of manuscript, general conclusion about these novel findings which they are differ from existing results are given.

Keywords: *Complex function solution, Exponential function solution, Modified exp(-Omega(xi))-expansion function approach, Sine-Poisson equation.*

1 Introduction

Solving nonlinear evolution equations (NEEs) and seeking explicit and exact solutions of NEEs has become one of the most exciting and extremely active domains in nonlinear theory. Especially, solitons, as an important concept of analytical solutions of nonlinear partial differential equations fields, have attracted attention of scientist from all over the world during three last decades. During these years, it has been submitted many works to the literature related with the numerical solutions of NEEs together with analytical, exact, travelling, and approximate solutions. Moreover, in real world problems, Fuzzy approaches for risk analysis and evaluation in multi-criteria decision making problems. Furthermore, multi-criteria decision-making methods have been used in the selection of personnel in daily life problems and many others with mathematical aspects [1-27, 31-44].

The main aim of this paper, using modified exp(-Omega(xi))-expansion function method (MEFM) is to find new soliton solutions to the (2+1)-dimensional Sine-Poisson equation defined as [28]

$$u_{tt}-u_{xx}-u_{yy}+m^2\sin(u)=0, \tag{1}$$

where m is real constant and non-zero.

2 General Facts of MEFM

Let’s consider the partial differential equation:

$$P(u_x,u_t,u_{xx},u_{tx},\cdots)=0, \tag{2}$$

where, $u=u(x,t)$ is an unknown function, P is a polynomial in $u(x,t)$ and its derivative in which highest order derivatives and nonlinear terms are involved and the subscripts stand for the partial derivatives. The basic phases of method are expressed as follows:

Step 1: Let’s consider the following travelling transformation defined by

$$u(x,y,t)=U(\xi),\ \xi=kx+ly-wt, \tag{3}$$

By using Eq(3), we can convert Eq.(2) into nonlinear ordinary differential equation (NODE) defined by;

$$N(U,U',U'',\cdots)=0. \tag{4}$$

where N is a polynomial of U and its derivatives and the superscripts indicate the ordinary derivatives with respect to ξ.

Step 2: Suppose the travelling wave solution of Eq.(4) can be rewritten as following manner;

$$U(\xi)=\frac{\sum_{i=0}^{N}A_i\left[\mathrm{e}^{-\Omega(\xi)}\right]^i}{\sum_{j=0}^{M}B_j\left[\mathrm{e}^{-\Omega(\xi)}\right]^j}, \tag{5}$$

where $A_i,B_j,(0\le i\le N,0\le j\le M)$ are constants to be determined later, such that $A_N\neq 0, B_M\neq 0,$ and $\Omega=\Omega(\xi)$ verifies the following ordinary differential equation;

$$\Omega'(\xi)=\exp(-\Omega(\xi))+\mu\exp(\Omega(\xi))+\lambda. \tag{6}$$

Eq. (6) has the following solution families [9,29,30]:

Family-1: When $\mu\neq 0,\ \lambda^2-4\mu>0,$

$$\Omega(\xi)=\ln\left(\frac{-\sqrt{\lambda^2-4\mu}}{2\mu}\tanh\left(\frac{\sqrt{\lambda^2-4\mu}}{2}(\xi+E)\right)-\frac{\lambda}{2\mu}\right), \tag{7}$$

Family-2: When $\mu\neq 0,\ \lambda^2-4\mu<0,$

$$\Omega(\xi)=\ln\left(\frac{\sqrt{-\lambda^2+4\mu}}{2\mu}\tan\left(\frac{\sqrt{-\lambda^2+4\mu}}{2}(\xi+E)\right)-\frac{\lambda}{2\mu}\right), \tag{8}$$

Family-3: When $\mu=0,\ \lambda\neq 0,$ and $\lambda^2-4\mu>0,$

$$\Omega(\xi)=-\ln\left(\frac{\lambda}{\exp(\lambda(\xi+E))-1}\right), \tag{9}$$

Family-4: When $\mu\neq 0,\ \lambda\neq 0,$ and $\lambda^2-4\mu=0,$

$$\Omega(\xi) = \ln\left(-\frac{2\lambda(\xi+E)+4}{\lambda^2(\xi+E)}\right), \tag{10}$$

Family-5: When $\mu = 0,\ \lambda = 0,$ and $\lambda^2 - 4\mu = 0,$

$$\Omega(\xi) = \ln(\xi+E), \tag{11}$$

being $A_0, A_1, A_2, \cdots A_N, B_0, B_1, B_2, \cdots B_M, E, \lambda, \mu$ are constants to be determined later. The positive integer N and M can be determined by considering the homogeneous balance between the highest order derivatives and the nonlinear terms occurring in Eq. (8).

Step 3: Setting Eq.(5) and Eq.(6) into Eq. (4), we get a polynomial of $\exp(-\Omega(\xi))$. We equate all the coefficients of same power of $\exp(-\Omega(\xi))$ to zero. This procedure yields a system of equations whichever can be solved to find $A_0, A_1, A_2, \cdots A_N$, $B_0, B_1, B_2, \cdots B_M, E, \lambda, \mu$ with the aid of computer programs. Substituting the values of $A_0, A_1, A_2, \cdots A_N, B_0, B_1, B_2, \cdots B_M, E, \lambda, \mu$ in Eq. (9), the general solutions of Eq. (4) complete the determination of the solution of Eq. (2).

3 Application of MEFM

This section apply the MEFM to the Eq.(1) for obtaining some new complex soliton solutions.

Example-1 When we apply Eq.(3) to the Eq.(1), we obtain the following nonlinear ordinary differential equation;

$$\left(w^2-k^2-l^2\right)U'' + m^2\sin(U) = 0. \tag{12}$$

In Eq.(12), when we use $\sin(U) = \left(e^{iU} - e^{-iU}\right)/2i$, we can find the following equality;

$$2\left(w^2-k^2-l^2\right)ie^{iU}U'' + m^2e^{2iU} - m^2 = 0. \tag{13}$$

If we use $V = e^{iU}$, we reach the following equality;

$$\begin{aligned}&2\left(w^2-k^2-l^2\right)V''V - 2\left(w^2-k^2-l^2\right)(V')^2\\ &+m^2V^3 - m^2V = 0.\end{aligned} \tag{14}$$

Balance principle between $V''V$ and V^3;

$$N = M + 2. \tag{15}$$

By using this relationship, we can attain some new soliton solutions for Eq.(1) as follows:

Case 1: By getting $M = 1$ and $N = 3$, after then, we can write follows;

$$V = \frac{A_0 + A_1\,e^{-\Omega} + A_2\,e^{-2\Omega} + A_3\,e^{-3\Omega}}{B_0 + B_1\,e^{-\Omega}}, \tag{16}$$

$$\begin{aligned}V' &= \frac{\left[A_1\,e^{-\Omega}(-\Omega') + A_2\,e^{-2\Omega}(-2\Omega') + A_3\,e^{-3\Omega}(-3\Omega')\right]\left[B_0 + B_1\,e^{-\Omega}\right]}{\left[B_0 + B_1\,e^{-\Omega}\right]^2}\\ &\quad-\frac{\left[A_0 + A_1\,e^{-\Omega} + A_2\,e^{-2\Omega} + A_3\,e^{-3\Omega}\right]\left[B_1\,e^{-\Omega}(-\Omega')\right]}{\left[B_0 + B_1\,e^{-\Omega}\right]^2} = \frac{\Upsilon}{\Psi},\end{aligned} \tag{17}$$

$$V'' = \frac{\Upsilon'\Psi - \Upsilon\Psi'}{\Psi^2},$$

$\vdots,$

where $A_3 \neq 0$ and $B_1 \neq 0$. Substituting Eqs.(16,17) in Eq.(14), we get an equation including $\exp(-\Omega(\xi))$ and it has various powers. Therefore, we have a system of algebraic equations from the coefficients of polynomial of $\exp(-\Omega(\xi))$. Solving this system of equations, it yields us the following coefficients;

Case 1.1: When

$$A_0 = -\frac{1}{12}\lambda\left(-4A_1 + \lambda A_2\right), B_0 = \frac{\lambda\left(-4A_1 + \lambda A_2\right)}{4\left(A_1 - \lambda A_2\right)}B_1,$$

$$A_3 = \frac{4\left(-A_1 + \lambda A_2\right)}{3\lambda^2}, \mu = \frac{1}{4}\lambda^2\left(1 + \frac{3B_1}{-A_1 + \lambda A_2}\right),$$

$$m = \frac{i\sqrt{3}\sqrt{-k^2 - l^2 + w^2}\,\lambda\sqrt{B_1}}{\sqrt{-A_1 + \lambda A_2}},$$

we find the following soliton solutions under the *Family-1* condition as

$$u_1 = -i\ln\left[-\frac{\left(3\sqrt{B_1} + \sqrt{3}\sqrt{A_1 - \lambda A_2}\tanh\left(\frac{\sqrt{3}\lambda\sqrt{B_1}}{2\sqrt{A_1 - \lambda A_2}}(E + kx + ly - wt)\right)\right)^2}{3\left(\sqrt{A_1 - \lambda A_2} + \sqrt{3}\sqrt{B_1}\tanh\left(\frac{\sqrt{3}\lambda\sqrt{B_1}}{2\sqrt{A_1 - \lambda A_2}}(E + kx + ly - wt)\right)\right)^2}\right]. \tag{18}$$

For better understanding of physical meaning of Eq.(18), 2D and 3D figures along with contour graphs may be observed in Figures (1) and (2) for suitable values of parameters as follows;

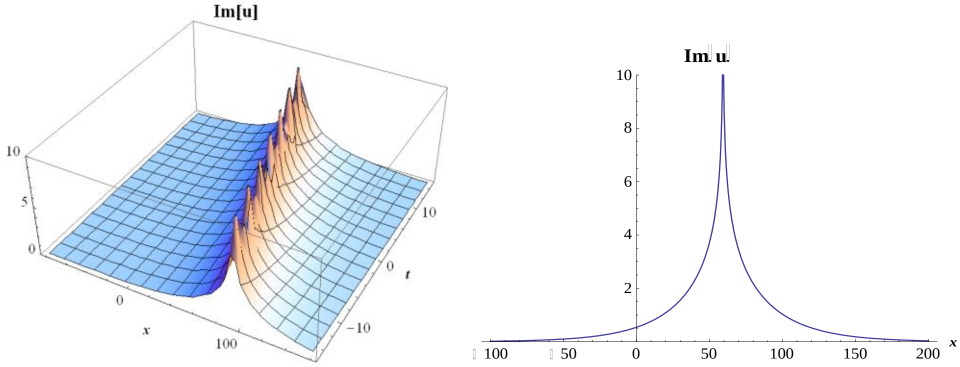


Figure 1. The 2D and 3D surfaces of Eq.(18)

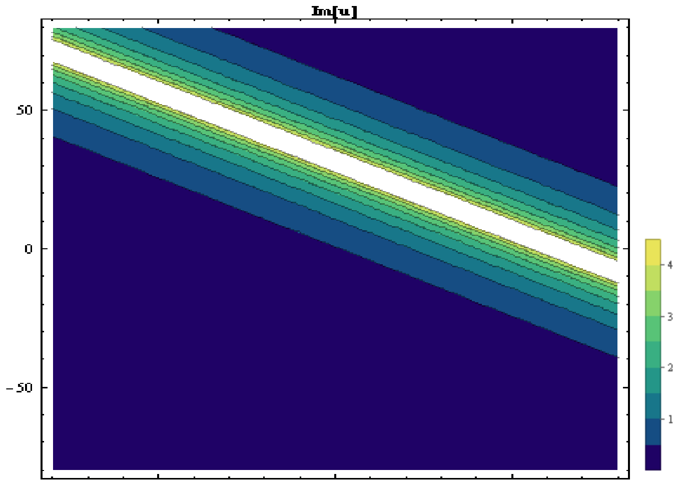


Figure 2. The contour surfaces of Eq.(18)

Case1.2. If

$$A_0=-\frac{1}{12}\lambda\left(-4A_1+\lambda A_2\right),B_0=\frac{\lambda\left(-4A_1+\lambda A_2\right)}{4\left(A_1-\lambda A_2\right)}B_1,$$

$$A_3=\frac{4\left(-A_1+\lambda A_2\right)}{3\lambda^2},\mu=\frac{1}{4}\lambda^2\left(1+\frac{3B_1}{-A_1+\lambda A_2}\right),$$

$$m=\frac{i\sqrt{3}\sqrt{-k^2-l^2+w^2}\lambda\sqrt{B_1}}{\sqrt{-A_1+\lambda A_2}},$$

we find the following another new soliton solutions under the *Family-2* condition as

$$u_2=i\ln\left(3\right)-i\ln\left[\frac{\left(\left(3\sqrt{B_1}+\sqrt{-3A_1+3\lambda A_2}\tan\left(\frac{\sqrt{3}\lambda\sqrt{B_1}}{2\sqrt{-A_1+\lambda A_2}}\left(E+kx+ly-wt\right)\right)\right)\right)^2}{\left(\left(\sqrt{-A_1+\lambda A_2}-\sqrt{3B_1}\tan\left(\frac{\sqrt{3}\lambda\sqrt{B_1}}{2\sqrt{-A_1+\lambda A_2}}\left(E+kx+ly-wt\right)\right)\right)\right)^2}\right]. \tag{19}$$

For Eq.(19), 2D and 3D figures along with contour graphs may be observed in Figures (3) and (4) for suitable values of parameters as follows;

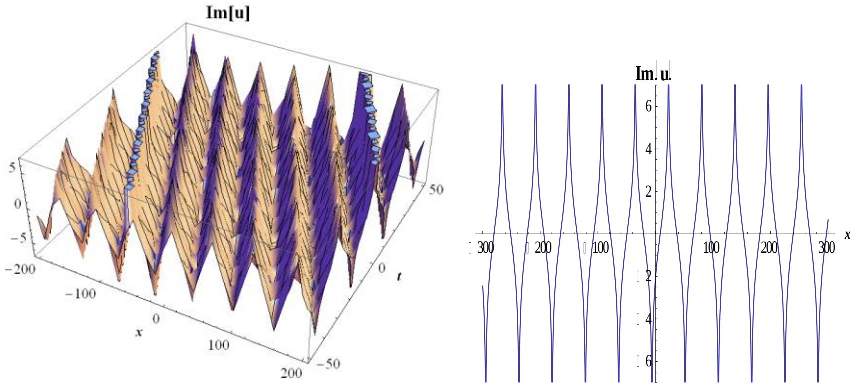


Figure 3. The 2D and 3D surfaces of Eq.(19)

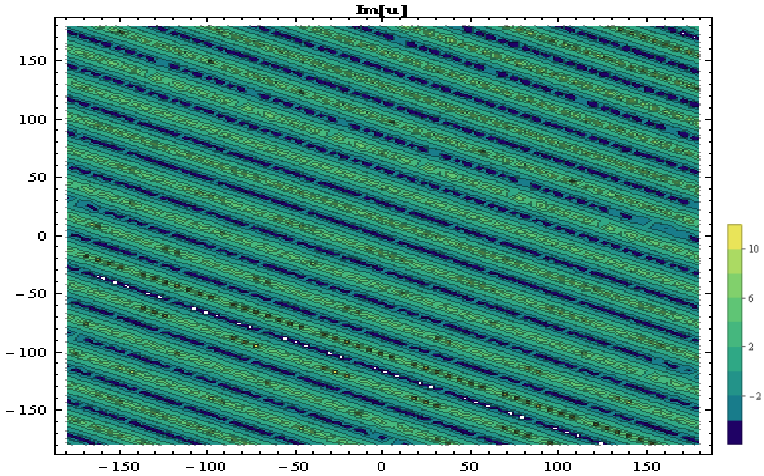


Figure 4. The contour surfaces of Eq.(19)

Case1.3. If

$$A_0 = B_0\left(-1+\frac{\mu A_3}{B_1}\right), A_1 = \mu A_3 - \frac{1}{B_1}2\sqrt{A_3}B_0\sqrt{\mu A_3 - B_1} - B_1,$$

$$\lambda = -\frac{2\sqrt{\mu A_3 - B_1}}{\sqrt{A_3}},\ A_2 = -2\sqrt{A_3}\sqrt{\mu A_3 - B_1} + \frac{B_0 A_3}{B_1},$$

$$l = \frac{\sqrt{m^2 A_3 + 4\left(-k^2 + w^2\right)B_1}}{2\sqrt{B_1}},$$

we obtain the following another new complex singular soliton solutions under the Family-1 condition as

$$u_3 = -i\ln\left[\begin{array}{l}\dfrac{\mu A_3}{B_1} - 1 - \dfrac{4\mu\sqrt{A_3}\sqrt{\mu A_3 - B_1}}{\kappa - \varpi B_1 \tanh\left(\dfrac{1}{2}\varpi\left(E + kx - tw + yl\right)\right)} \\ + \dfrac{4A_3\mu^2}{B_1}\left[\dfrac{2\sqrt{\mu A_3 - B_1}}{\sqrt{A_3}} - \varpi\tanh\left(\dfrac{1}{2}\varpi\left(E + kx - tw + yl\right)\right)\right]^{-2}\end{array}\right], \tag{20}$$

$$\varpi = \sqrt{-4\mu + \frac{4\left(\mu A_3 - B_1\right)}{A_3}}, \kappa = \frac{2\sqrt{\mu A_3 - B_1}}{\sqrt{A_3}}B_1,$$

For Eq.(20), 2D and 3D figures along with contour graphs may be observed in Figures (5) and (6) for suitable values of parameters as follows;

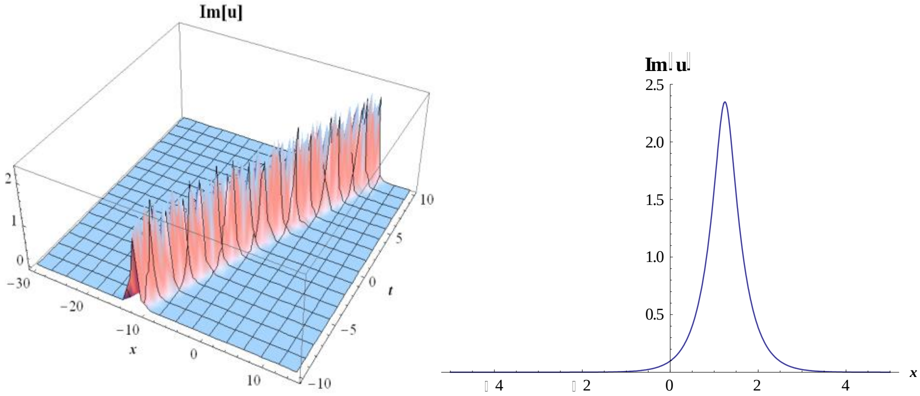


Figure 5. The 2D and 3D surfaces of Eq.(20)

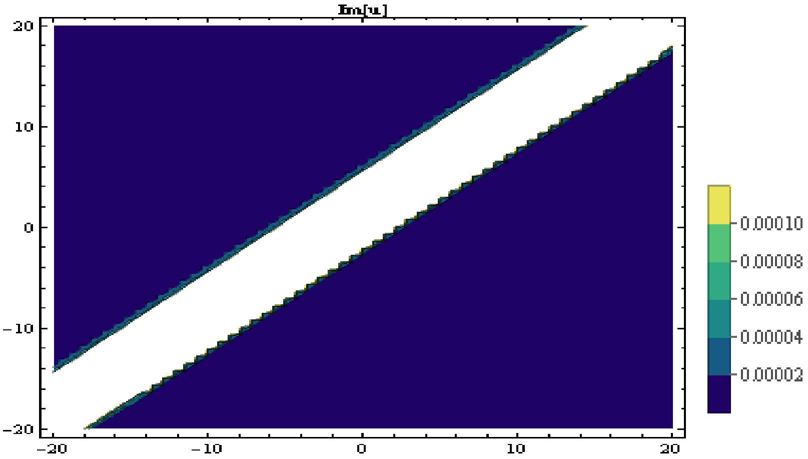


Figure 6. The contour surfaces of Eq.(20)

4 Conclusion

In this paper, we have applied MEFM to the Eq.(1). Then, we found some new complex soliton solutions such as hyperbolic and trigonometric functions. With the help of several computational computer programming, we have also plotted two and three-surfaces of results along with contour surfaces. All Figures (1-6), it can be observed that these surfaces have symbolized the physical properties of model considered in this paper. Comparising with papers presented in literature [28], it can be viewed that these soliton solutions are entirely new constructed by using MEFM. To the best of our knowledge, the application of MEFM to the Eq.(1) has not been submitted before.

Acknowledgements

Authors want to thanks for the reviewer for their valuable contributes.

5 References

[1] Ciancio, A., Baskonus, H.M., Sulaiman, T.A., Bulut, H., New Structural Dynamics of Isolated Waves Via the Coupled Nonlinear Maccari's System with Complex Structure, *Indian Journal of Physics*, 92(10), 1281–1290, 2018.

[2] Ilhan, O.A., Sulaiman, T.A., Bulut, H., Baskonus, H.M., On the new wave Solutions to a Nonlinear Model Arising in Plasma Physics, *European Physical Journal Plus*, 133(27), 1-6, 2018.

[3] Yokus, A., Baskonus, H.M., Sulaiman, T.A., Bulut, H., Numerical simulation and solutions of the two-component second order KdV evolutionary system, *Numerical Methods for Partial Differential Equations*, 34(1), 211-227, 2017

[4] Bulut, H., Sulaiman, T.A., Baskonus, H.M., Akturk, T., Complex Acoustic Gravity Wave Behaviors to Some Mathematical Models Arising in Fluid Dynamics and Nonlinear Dispersive Media, *Optical and Quantum Electronics,* 50(1), 1-19 2018.

[5] Bulut, H., Sulaiman, T.A., Baskonus, H.M., Yazgan, T., Novel Hyperbolic Behaviors to Some Important Models Arising in Quantum Science, *Optical and Quantum Electronics*, 49(349), 1-16, 2017.

[6] Baskonus, H.M., Sulaiman, T.A., Bulut, H., Akturk, T., Investigations of dark, bright, combined dark-bright optical and other soliton solutions in the complex cubic nonlinear Schrödinger equation with -potential, *Superlattices and Microstructures*, 115, 19-29, 2018.

[7] Şenel, M., Şenel, B., Havle, C.A., Risk Analysis of Ports in Maritime Industry in Turkey Using FMEA Based Intuitionistic Fuzzy Topsis Approach, *ITM Web of Conferences*, 22(01018), 1-10, 2018.

[8] Cattani, C., Sulaiman, T.A., Baskonus, H.M., Bulut, H., On the soliton solutions to the Nizhnik-Novikov-Veselov and the Drinfel'd-Sokolov systems, *Optical and Quantum Electronics*, 50(3), 138, 2018.

[9] Bulut, H., Yel, G., Baskonus, H.M., Novel Structure to the Coupled Nonlinear Maccari's System by Using Modified Trial Equation Method, *Advanced Mathematical Models and Applications*, 7(2), 14-19, 2017.

[10] Araci, S., Ozer, O., Extended q-Dedekind-type Daehee-Changhee sums associated with extended q-Euler polynomials, *Advances in Difference Equations*, 2015(1), 272-276, 2015.

[11] Ozer, O., Pekin, A., An Algorithm For Explicit Form of Fundamental Units of Certain Real Quadratic Fields and Perion Eight, *European Journal of Pure and Applied Mathematics*, 8(3), 343- 356, 2015.

[12] Şenel, B., Şenel, M., Risk Analysis: Fault Tree Analysis Application on Traffic Accidents Occured in Turkey, *Anadolu University Journal of Social Science*,13(3), 65-84, 2013.

[13] Şenel, B., Şenel, M., An Analysis of Technology Acceptance in Turkey Using Fuzzy Logic and Structural Equation Modeling, *Journal of Business Research* 3(4), 34-48, 2011.

[14] Şenel, B., Şenel, M., Aydemir, G., Use and Comparison of Topsis and Electre Methods in Personnel Selection, *ITM Web of Conference,* 22(01021), 1-10, 2018.

[15] Ozer, O., Omran, S., On The Generalized C*-Valued Metric Spaces Related With Banach Fixed Point Theory, *International Journal of Advanced and Applied Sciences*, 4(2), 35-37, 2017.

[16] Şenel, B., Şenel, M., Aydemir, G., Multi Criteria Decision Making Method Topsis with Personnel Selection, *Journal of Researches On Economy Management*, 13, 19-70, 2017.

[17] Baskonus, H.M., New acoustic wave behaviors to the Davey–Stewartson equation with power-law nonlinearity arising in fluid dynamics, *Nonlinear Dynamics*, 86(1), 177–183, 2016.

[18] Ozer, O., A Note On Structure of Certain Real Quadratic Number Fields, *Iranian Journal of Science and Technology*, 41(3), 759–769, 2017.

[19] Seyedi, S.H., Saray, B.N., Nobari, M.R.H., Using interpolation scaling functions based on Galerkin method for solving non-Newtonian fluid flow between two vertical flat plates, *Applied Mathematics and Computation*, 269, 488-496, 2015.

[20] Seyedi, S.H., Saray, B.N., Ramazani, A., On the multiscale simulation of squeezing nanofluid flow by a high precision scheme, *Powder Technology*, 2018.

[21] C.Cattani, A. Ciancio, On the fractal distribution of primes and prime-indexed primes by the binary image analysis, *Physica A*, 460, 222–229, 2016.

[22] Sulaiman, T.A., Yokus, A., Gulluoglu, N., Baskonus, H.M., Bulut, H., Regarding the Numerical and Stability Analysis of the Sharma-Tosso-Olver Equation, *ITM Web of Conferences*, 22(01036), 1-9, 2018.

[23] Akturk, T., Sulaiman, T.A., Baskonus, H.M., Bulut, H., Complex Acoustic Gravity Wave Behaviors to a Mathematical Model Arising in Nonlinear Mathematical Physics, *ITM Web of Conferences* 22(01032), 1-6, 2018.

[24] C.Cattani, Sulaiman, T.A., Baskonus, H.M., H.Bulut, Solitons in an inhomogeneous Murnaghan's rod, *European Physical Journal Plus*, 133(228), 1-12, 2018.

[25] Bulut, H., Yel, G., Baskonus, H.M., An Application Of Improved Bernoulli Sub-Equation Function Method To The Nonlinear Time-Fractional Burgers Equation, *Turkish Journal of Mathematics and Computer Science*, 5, 1-17, 2016.

[26] Yel, G., Baskonus, H.M., Bulut, H., Novel archetypes of new coupled Konno–Oono equation by using sine–Gordon expansion method, *Optical and Quantum Electronics*, 49(285), 1-10, 2017.

[27] Ünlükal, C., Şenel, M., Şenel, B., Risk Assessment with Failure Mode and Effect Analysis and Gray Relational Analysis Method in Plastic Enjection Prosess, *ITM Web of Conferences,* 22(01023), 1-10, 2018.

[28] Su, K.L., Xie, Y.X., Solving (2+1)-dimensional sine-Poisson equation by a modified variable separated ordinary differential equation method, *Chinese Physics B*, 19, 100302(10), 1-10, 2010.

[29] Bulut, H., Sulaiman, T.A., Baskonus, H.M., Rezazadeh, H., Eslami, M., Mirzazadeh, M., Optical solitons and other solutions to the conformable space-time fractional Fokas-Lenells equation, *Optik: International Journal for Light and Electron Optics*, 172, 20-27, 2018.

[30] Sulaiman, T.A., Bulut, H., Yokus, A., Baskonus, H.M., On the Exact and Numerical Solutions to the Coupled Boussinesq Equation Arising in Ocean Engineering, *Indian Journal of Physics*, https://doi.org/10.1007/s12648-018-1322-1, 2018.

[31] Baskonus, H.M., Askin, M., Travelling wave simulations to the modified Zakharov-Kuzentsov model arising in plasma physics, *6th International Youth Science Forum "LITTERIS ET ARTIBUS", Computer Science and Engineering,* Lviv/Ukraine, 24–26 November 2016.

[32] Dusunceli, F., Solutions for the Drinfeld-Sokolov Equation Using an IBSEFM Method, *MSU Journal of Science*, 6(1), 505-510, 2018.

[33] Askin, M., Salti, M., Aydogdu, O., Cosmology via thermodynamics of polytropic gas, *Modern Physics Letters A*, 32(32), 1750177, 2017.

[34] Dusunceli, F., Celik, E., Numerical Solution For High-Order Linear Complex Differential Equations with Variable Coefficients, *Numerical Methods for Partial Differential Equations*, DOI: 10.1002/num.22222, 2017.

[35] Duran, S., Askin, M., Sulaiman, T.A., New soliton properties to the ill-posed Boussinesq equation arising in nonlinear physical science, *An International Journal of Optimization and Control: Theories and Applications*, 7(3), 240-247, 2017.

[36] Dusunceli, F., Celik, E., Numerical Solution for High-Order Linear Complex Differential Equations By Hermite Polynomials, *Iğdır University Journal of the Institute of Science and Technology*, 7(4), 189-201, 2017.

[37] Askin, M., Yilmaz, A., The Calculation of Correlation Time (τ) for T 1 Spin–Lattice and T 2 Spin–Spin Relaxation Times in Agar Solutions, *Spectroscopy letters*, 37(2), 217-224, 2004.

[38] Dusunceli, F., Celik, E., Fibonacci matrix Polynomial Method For Linear Complex Differential Equations, *Asian Journal of Mathematics and Computer Research*, 15(3): 229-238, 2017.

[39] Askin, M., Zengin, B., Korunur, S., Kor,H. Koylu, M.Z., The examination of a variety of different ions added to the crown ether derivatives with high field NMR spectrometer, *Russian Journal of Physical Chemistry B*, 11(3), 391-394, 2017.

[40] Dusunceli, F., Celik, E., An Effective Tool: Numerical Solutions by Legendre Polynomials for High-Order Linear Complex Differential Equations, *British Journal of Applied Science & Technology*, 8(4), 348-355, 2015.

[41] Yokus, A., Sulaiman, T.A., Gulluoglu, M.T., Bulut, H., Stability Analysis, Numerical and Exact Solutions of the (1+1)-Dimensional NDMBBM Equation, *ITM Web of Conferences*, 22(01064), 1-10, 2018.

[42] Kaymaz, K., Zengin, B., Askin, M., Taskaya, S., Investigation Of Mechanical Stresses On Sandwich Composite Layers According To The Pressure By Making Use of Ansys Software, *Gümüşhane University Journal of Science and Technology Institute*, 79-93, 2018.

[43] Askin, M., Effect of the Transition Metal Elements on the Relaxation Times in the Agar Solutions, *Asian Journal of Chemistry*, 19(4), 3191-3196, 2017.

[44] Zengin, B., Yaraneri, H., Korunur, S., Investigation of energy relaxation in 1-D nonlinear lattices by wavelets, *European Physical Journal B*, 85(11), 388, 2012.

Authors' addresses

Haci Mehmet Baskonus 1,
Department of Mathematics, Faculty of Education,
Harran University, Sanliurfa, Turkey
hmbaskonus@gmail.com

Hasan Bulut 2,
Department of Mathematics, Faculty of Science,
Firat University, Elazig, Turkey
hbulut@firat.edu.tr

Sibel Sehriban Atas 3,
Department of Mathematics, Faculty of Science,
Firat University, Elazig, Turkey
suzundag90@gmail.com

ISSN 2587-1943

KAN GRUPLARI VE STRES DÜZEYİ ARASINDAKİ İLİŞKİLER

Mevlüt Alataş 1

Original scientific paper

Bu çalışmada, insanların kan grupları ile duygusal yapıları arasında nasıl bir bağ bulunduğunu belirlemek amacıyla stres değişkeni ele alınmış ve kan grupları ve stres düzeyi arasındaki ilişkilerin belirlenmesi hedeflenmiştir. Genel stres düzeyleri (GSD) ve patolojik stres düzeyleri (PSD)'ni ölçmek amacıyla hazırlanan anket, her kan grubundan (A, B, AB, O) 20 farklı kişiye uygulanmıştır. Uygulama sonucunda, toplam GSD değerinin toplam PSD değerinden düşük olduğu ve hem PSD hem de GSD değerlerinin kan grupları düzeyinde sıralamasının AB > O > B > A şeklinde olduğu görülmüştür. Cinsiyet bakımından ise kadınların hem PSD hem GSD açısından erkeklere oranla daha stresli oldukları belirlenmiştir.

Anahtar Kelimeler: *Kan Grupları, Stres, İlişki, Elazığ, Türkiye.*

RELATIONSHIPS BETWEEN BLOOD GROUPS AND STRESS LEVELS

In this study, stress variables have been discussed to determine what kind of relationship existing between blood groups and emotional structures of people and it has aimed to designate the relationship between blood groups and stress levels. The questionnaire prepared to measure general stress levels (GSD) and pathological stress levels (PSD) has applied to 20 different individuals from each blood group (A, B, AB, O). As a result of the application, it has been observed that total GSD value has been lower than PSD value, and both PSD and GSD have been ranked at blood group level as AB > O > B > A. In terms of gender, it has been indicated that women are more stressed than men in the sense of PSD and GSD.

Keywords*: Blood Groups, Stress, Relationship, Elazığ, Turkey.*

1 Giriş

İnsan vücudunun belki de en önemli maddesi, olmazsa olmazı kandır. Çünkü vücudumuzun % 7-8'ini oluşturan kan; A, B, AB ve O olmak üzere dört gruptan oluşur. Bazen bir damla kan, insanların hayatında köklü değişiklikler oluşturabilir. İnsanların yaşamlarında önemli değişiklikler oluşturan etkenlerden bir diğeri ise strestir. Stres, kişinin üzerinde hissettiği baskı ve gerginlik durumudur (URL, 1). Bu gerginliğe gerek yaşam değişikliklerinden gerekse çevresel olaylardan kaynaklanan birçok etken sebep olabilir. Stres yaratabilecek büyük yaşam değişiklikleri arasında; taşınma, yeni bir okula başlama ya da okul değiştirme, yeni bir işe ya da yeni bir yaşam tarzına geçiş, evlenme, hamilelik, boşanma, ayrılık, bir yakının ölümü, işten atılma, iflas ve kronik hastalıklar sayılabilir. Stres yaratabilecek bazı çevresel olaylar ise zaman baskısı, yarışma ya da rekabet, maddi sorunlar, gürültü ve hayal kırıklıkları olarak sıralanabilir. Tüm bu sebeplerden, duygusal, düşünsel, davranışsal ve bedensel olarak varlığını hissettiğimiz stresin, etki derecesi ise kişiden kişiye göre değişmektedir (URL, 1). Etki derecesindeki farklılıkların acaba kan grupları ile bir ilişkisi var mıdır? Şimdiye kadar kan gruplarının; kişilik özellikleri (URL, 3, URL, 4; URL, 5), beslenme ve spor tercihleri (URL, 2; URL, 6) arasındaki ilişkileri inceleyen birkaç çalışma yapılmış olmasına rağmen insan psikolojisi ile ilişkisini ele alan herhangi bir çalışma yapılmamıştır. Bu çalışmada, insanların kan grupları ile duygusal yapıları arasında nasıl bir bağ bulunduğunu belirlemek amacıyla günlük yaşamımızın bir parçası olan stres değişkeni ele alınmış ve kan grupları ve stres düzeyi arasındaki ilişkilerin belirlenmesi hedeflenmiştir.

2 Materyal ve Metod

Çalışmada uygulanacak anketin maddelerinin hazırlanması için stres ile ilgili kitap, dergi ve makaleler okunup incelenmiştir. İncelenen eserlerden esinlenerek anket maddeleri oluşturulmuştur (Ek 1). Oluşturulan anketler 80 adet çoğaltılarak, Elazığ il merkezinin farklı kesimlerinde, farklı yaş gruplarından (15-57 yaş) bireylere (Öğretmen, öğrenci, doktor, polis, serbest meslek) uygulanmıştır. Anket maddelerinin puan değerleri (Hiçbir zaman 0, Ara sıra 1, Sık sık 2, Her zaman 3) belirlenmiştir. Yine uygulanan anketlerin madde sayılarıyla bağlantılı olarak belirlenen ölçekler doğrultusunda (Genel Stres Düzeyi için: 0-10 düşük, 10-20 orta, 20-30 yüksek; Patolojik stres düzeyi için: 0-15 düşük, 15-30 orta, 30-45 yüksek) değerlendirilmesi yapılmıştır.

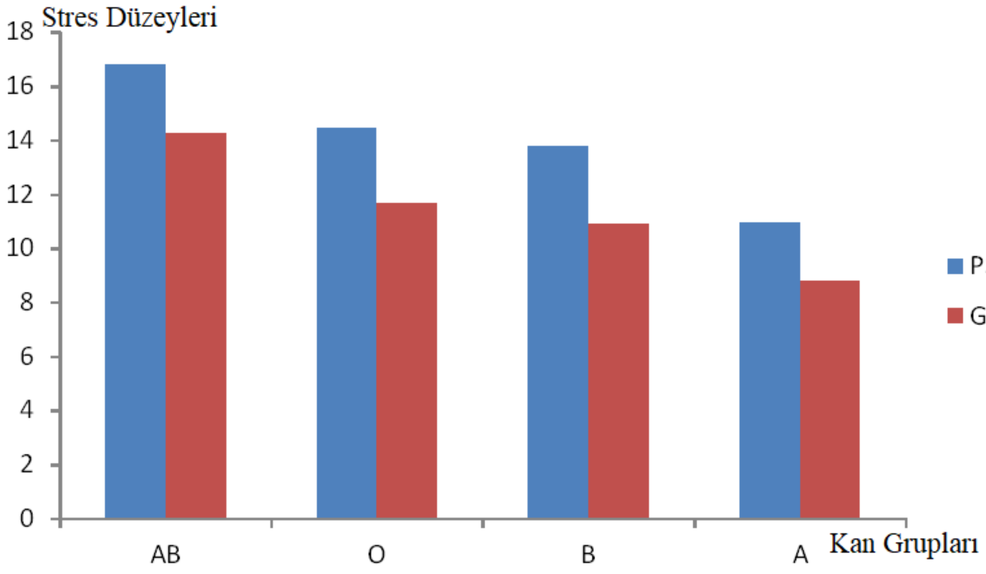
3 Bulgular ve Sonuç

Her kan grubuna ait 20 olmak üzere, toplamda 80 anket formunun değerlendirilmesi sonucunda kan gruplarına ait genel stres düzeyleri (GSD) ve patolojik stres düzeyleri (PSD) aşağıdaki gibidir (Tablo 1, Şekil 1). Bu verilerden kan gruplarının hem PSD hem de GSD sıralaması AB > O > B > A şeklinde olduğu görülmektedir.

Kan gruplarına ait tablolar detaylı incelendiğinde, AB, B ve O gruplarının orta dereceli, A grubunun ise düşük dereceli GSD'ne sahip olduğu görülmektedir. Orta dereceli GSD'ne sahip grupları kendi içerisinde değerlendirdiğimizde AB'nin ilk sırada, O'ın ikinci, B'nin ise üçüncü sırada olduğu görülür.

Tablo 1. Kan gruplarına ait GSD ve PSD değerleri

Kişi Sayısı		GSD	PSD		GSD	PSD		GSD	PSD		GSD	PSD
1	A	5	13	B	12	13	AB	4	5	O	17	16
2	A	10	14	B	6	12	AB	12	14	O	14	16
3	A	7	2	B	11	18	AB	12	12	O	13	17
4	A	10	10	B	21	25	AB	27	18	O	9	10
5	A	18	20	B	8	10	AB	27	17	O	9	17
6	A	8	14	B	5	1	AB	15	20	O	18	20
7	A	13	20	B	8	13	AB	12	22	O	15	17
8	A	7	8	B	9	11	AB	21	29	O	22	10
9	A	9	9	B	12	8	AB	14	10	O	14	19
10	A	18	19	B	9	20	AB	14	15	O	9	17
11	A	11	14	B	11	15	AB	25	30	O	8	11
12	A	4	4	B	9	10	AB	18	21	O	3	8
13	A	7	9	B	15	19	AB	20	28	O	10	11
14	A	12	11	B	15	18	AB	2	7	O	10	12
15	A	2	7	B	8	5	AB	11	28	O	9	9
16	A	6	8	B	14	14	AB	7	8	O	9	8
17	A	6	10	B	17	16	AB	5	8	O	19	25
18	A	3	6	B	8	10	AB	15	17	O	11	17
19	A	10	7	B	10	23	AB	12	15	O	4	13
20	A	10	14	B	10	15	AB	12	12	O	11	16
Ortalama		8,8	10,95		10,9	13,8		14,25	16,8		11,7	14,45



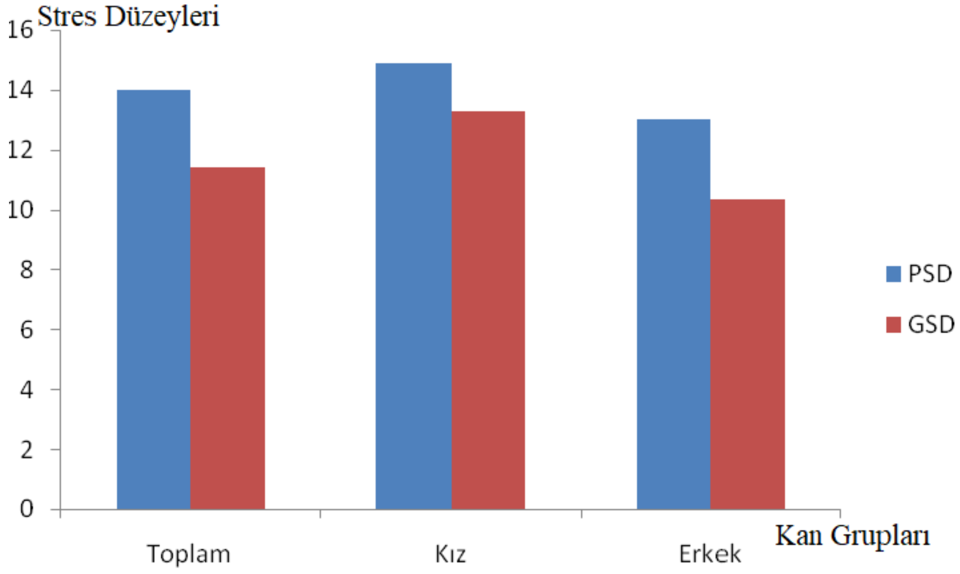
Şekil 1. Kan gruplarına ait GSD ve PSD değerleri.

Patolojik stres düzeyi açısından kan gruplarını değerlendirdiğimizde ise AB'nin orta, A, B ve O'ın ise düşük stres derecesine sahip olduğu görülmektedir. Düşük dereceli PSD'ye sahip A, B ve O kan gruplarını kendi içerisinde değerlendirdiğimizde O'ın ilk sırada, B'nin ikinci, A'nın ise üçüncü sırada olduğu görülür.

Tüm gruplar ortak olarak değerlendirildiğinde, toplam GSD 11,41 değerinde orta dereceli stres düzeyine sahipken, toplam PSD 14 değerinde olup düşük dereceli stres düzeyine sahiptir.

Yine tüm gruplar ortak olarak değerlendirilip cinsiyet farkına göre bir gruplama ve değerlendirme yaptığımızda ise, kadın ve erkeklerin orta dereceli GSD'ne sahip oldukları ve değerlerinin ise kadınlar için 13,3 erkekler için 10,3 olduğu görülür. PSD açısından değerlendirildiğinde ise kadın ve erkeklerin düşük dereceli PSD'ye sahip oldukları ve değerlerinin ise kadınlar için 14,9 erkekler için 13 olduğu görülmektedir (Şekil 2). Gerek GSD ve gerekse PSD değerlerinde, kadınlara ait değerlerin yüksek çıkmasını günlük yaşamda üstlendikleri görev ve sorumluluklarının fazlalığı ile yorumlayabiliriz.

Kan grupları ile stres düzeyi arasındaki ilişkileri inceleyen bu çalışmada, insanların sahip oldukları kan grupları ile duygusal yapıları arasındaki bağlantı ortaya konulmuştur. Yine yapılan bu çalışma ile daha önce herhangi bir çalışma yapılmamış bu alanda bilimsel bir açık giderilmiştir. Ayrıca bu çalışmanın yapılacak çalışmalara taban oluşturacağı, bölge veya ülke genelinde ileride yapılacak diğer çalışmalara büyük katkılar sağlayacağını umuyoruz.



Şekil 2 Bireylerin kan gruplarına ait GSD ve PSD değerleri.

Teşekkür

Testlerin uygulanma aşamasındaki yardımlarından dolayı, Mert Hüseyin Kılıç ve Ayşe Güler'e teşekkür ederim.

4 Kaynaklar

[1] URL, 1. Boğaziçi Üniversitesi Öğrenci Rehberlik ve Psikolojik Danışmanlık Merkezi. Website: http://www.burem.boun.edu.tr/?q=node/50 [11.12.2018].

[2] URL, 2.Kan grupları ve Beslenme İlişkisi. Website: http://beslenmebulteni.com/beslenme/?p=1117 [09.12.2018].

[3] URL, 3. Kişiliğiniz kan grubunu belirtiyor. Website: http://www.hurriyet.com.tr/saglik/6995595.asp [10.12.2018].

[4] URL, 4. Kan Grubuna Göre Karakter Özellikleri Website: http://www.bilgiustam.com/kan-grubuna-gore-karakter-ozellikleri/ [15.12.2018].

[5] URL, 5. Kan grupları ve Kişilik Özellikleri. Website: http://www.mynet.com/haber/foto-analiz/kan-gruplari-ve-kisilik-ozellikleri-1565510-2 [18.12.2018].

[6] URL, 6. Website: http://www.sporpartnerim.com/aktiviite-haberlerii/1328-kan-gruplarina-gore-beslenme-ve-spor-tavsiyeleri.html [20.01.2015].

Authors' addresses

M. Alataş . Ph.D. in Biomedical Engineeing
Munzur University
Department of Biomedical Engineering, Faculty of Engineering
mevlutalatas@hotmail.com

ISSN 2587-1943

DIFFERENCE SCHEMES METHODS FOR THE FRACTIONAL ORDER DIFFERENTIAL EQUATION SENSE OF CAPUTO DERIVATIVE

Mahmut Modanli 1

Original scientific paper

This study gives numerical solution of the fractional order partial differential equation defined by Caputo fractional derivative. Laplace transform method is used for the exact solution of this equation depend on intial-boundary value problem. The difference schemes are constructed for this equation. The stability of this difference schemes is proved. Error analysis is performed by comparing the exact solution with the approximate solution. The effectiveness of the method is shown from the error analysis table.

Keywords: *Caputo derivative, Difference scheme method ,Fractional order differential equation, Laplace method, Stability estimates*.

1 Introduction

Partial differential equation is very important for the many fields. The numerical and the exact solutions of this differential equations have many various methods. In [7,10], the authors studied high-order linear complex differential equations. Fractional order differential equation has many applications in engineering, physic, finance, physics and seismology [1-3]. The Atangana-Baleanu (AB) derivative was applied successfully in modelling of various real phenomena such as [4-6]. Some methods were applied the fractional and partial differential equation in [13,14]. Modanli applied two different method for fractional telegraph differential equation depend on nonlocal initial conditions [12].

In [8], the authors worked to implicit difference approximation for the time fractional heat equation with the nonlocal condition. Finally, Sarboland gave numerical solution of time fractional partial differential equations using multiquadric quasi-interpolation [9].

In this article, we consider fractional order differential equation defined by Caputo derivative to obtain numerical results. Then, the stability inequality is showed by the given the initial conditions. We examine the following fractional order differential equation

$$\begin{cases} {}_0^C D_t^\alpha u(t,x) + \frac{\partial u(t,x)}{\partial x} + u(t,x), \\ -\frac{\partial^2 u(t,x)}{\partial x^2} = f(t,x), \\ 0 < x < L,\ \ 0 < t < T, \\ u(0,x) = r_1(x),\ \ 0 \le t \le T, \\ u(t,X_L) = u(t,X_R) = 0,\ X_L \le x \le X_R, \\ 0 < \alpha \le 1. \end{cases} \qquad (1)$$

Now, we shall recall some basic definitions and properties of fractional calculus theory for fractional order differential equation.

Defination 1.1 The Caputo fractional derivative $D_t^\alpha u(t,x)$ of order α with respect to time is defined as: as:

$$\frac{\partial^\alpha u(t,x)}{\partial t^\alpha} = D_t^\alpha u(t,x) =$$

$$\frac{1}{\Gamma(n-\alpha)} \int_0^t \frac{1}{(t-p)^{\alpha-n+1}} \frac{\partial^\alpha u(p,x)}{\partial p^\alpha} dp, \qquad (2)$$

$$(n-1 < \alpha < n),$$

and for $\alpha = n \in N$ defined as:

$$D_t^\alpha u(t,x) = \frac{\partial^\alpha u(t,x)}{\partial t^\alpha} = \frac{\partial^n u(t,x)}{\partial t^n}.$$

2 Constructed difference schemes and its stability

We consider a rectangular domain $w^h \times w^\tau$ for the difference scheme method. For this method, suppose that $h = \frac{L}{M}$ for x-axis and $\tau = \frac{T}{N}$ for t −axis as grid mess, then we get

$$x_n = X_L + nh,\ n = 1,2,\ldots,M,\ \ t_k = k\tau, k = 1,2,\ldots,N..$$

We write the original differential equation (1) at the point $(x_n,\ t_k) \in w^h \times w^\tau$ as

$${}_0^C D_t^\alpha u(\,t_k, x_n) + \frac{\partial u(\,t_k, x_n)}{\partial x} + u(\,t_k, x_n),$$

$$-\frac{\partial^2 u(\,t_k, x_n)}{\partial x^2} = f(\,t_k, x_n),$$

Now, we shall give the following definition for construct the difference scheme method.

Definition 2.1 First-order approach method for the calculation of the problem (2) given by the formula:

$$D_t^\alpha u(t_k, x_n) = D_t^\alpha u_n^k$$

$$\cong g_{\alpha,\tau} \sum_{j=1}^{k} w_j^{(\alpha)} (u_n^{k-j+1} - u_n^{k-j}), \tag{3}$$

where $g_{\alpha,\tau} = \frac{1}{\Gamma(2-\alpha)\tau^\alpha}$ and $w_j^{(\alpha)} = (j+1)^{1-\alpha} - j^{1-\alpha}$. Using the last values, one has the following approximation

$$\frac{\partial^\alpha u(t_k, x_n)}{\partial x^\alpha} = g_{\alpha,\tau}$$

$$\times \left[w_1 u_n^k - w_k u_n^0 + \sum_{j=1}^{k-1} (w_{k-j+1} - w_{k-j}) u_n^j\right]. \tag{4}$$

Applying Taylor expansion with respect to x, the first and second order difference schemes are obtained as the following form

$$u_x(t_k, x_n) \cong \frac{u_{n+1}^k - u_{n-1}^k}{2h}, \tag{5.a}$$

$$u_{xx}(t_k, x_n) \cong \frac{u_{n+1}^k - 2u_n^k + u_{n-1}^k}{h^2}. \tag{5.b}$$

Using the formula (3), (5.a) and (5.b) the difference schemes formula for the equation (1), we obtain

$$\begin{cases} g_{\alpha,\tau}(u_n^{k+1} - u_n^k) \\ +g_{\alpha,\tau} \sum_{j=1}^{k} w_j^{(\alpha)} (u_n^{k-j+1} - u_n^{k-j}) \\ +u_n^k + \frac{u_{n+1}^k - u_{n-1}^k}{2h} - \frac{u_{n+1}^k - 2u_n^k + u_{n-1}^k}{h^2} \\ \qquad = f(t_k, x_n) = f_n^k, \\ 1 \le k \le N-1, \ 1 \le n \le M-1, \\ u_n^0 = r_1(x_n), \ 0 \le n \le M, \\ u_0^k = u_M^k = 0, \ 0 \le k \le N. \end{cases} \tag{6}$$

Here $g_{\alpha,\tau} = \frac{1}{\Gamma(2-\alpha)\tau^\alpha}$ and $w_j^{(\alpha)} = (j+1)^{1-\alpha} - j^{1-\alpha}$.

We can rewrite the formula (6) as the following form

$$\begin{cases} \left(-\frac{1}{h^2} + \frac{1}{2h}\right) u_{n+1}^k + \left(-\frac{1}{h^2} + \frac{1}{2h}\right) u_{n-1}^k \\ +g_{\alpha,\tau} \sum_{j=1}^{k} w_j^{(\alpha)} (u_n^{k-j+1} - u_n^{k-j}) \\ +\left(-g_{\alpha,\tau} + \frac{2}{h^2} + 1\right) u_n^k + g_{\alpha,\tau} u_n^{k+1} = f_n^k, \\ 1 \le k \le N-1, \ 1 \le n \le M-1, \\ u_n^0 = r_1(x_n), \ 0 \le n \le M, \\ u_0^k = u_M^k = 0, \ 0 \le k \le N. \end{cases} \tag{7}$$

The formula (7) can be written in matrix form,

$$\begin{cases} Au_{n+1} + Bu_n + Cu_{n-1} = D\varphi_n, \\ u_0 = u_M = \vec{0}, \ 1 \le n \le M-1, \end{cases} \tag{8}$$

where $\varphi_n = f_n^k$, A, B, C and D are $(N+1) \times (N+1)$ matrices.

Using the modified Gauss-Elimination method, the formula (8) can be convert into the difference scheme as the following form

$$u_n = \alpha_{n+1} u_{n+1} + \beta_{n+1}, \ n = M-1, \dots, 2,1,0. \tag{9}$$

From the formulas (8) and (9), the following fair formulas can be obtain easily

$$\begin{cases} \alpha_{n+1} = -(B + A\alpha_n)^{-1} A, \\ \beta_{n+1} = (B + A\alpha_n)^{-1} (D\varphi_n - A\beta_n), \\ 1 \le n \le M-1, \end{cases} \tag{10}$$

Now, we shall the stability estimates theorem for the formula (8)

Theorem 2. 1 If $-g_{\alpha,\tau} + \frac{2}{h^2} + 1 + g_{\alpha,\tau}(2^{1-\alpha} - 1) > 0$, for $0 < \alpha \le 1$, then, the stability estimates are satisfied for the formula (8)

Proof. Using the formulas (9), (10) and the methods [8,11], the proof theorem is clear.

3 Numerical results

Example 3.1 We consider the following fractional order differential equation defined by the Caputo derivative

$$\begin{cases} {}_{0}^{C}D_t^{\alpha}u(t,x)+\frac{\partial u(t,x)}{\partial x}+u(t,x) \\ -\frac{\partial^2 u(t,x)}{\partial x^2}=f(t,x), \\ f(t,x)=x(1-x)(\cos\left(x+t+\frac{\alpha\pi}{2}\right) \\ +(3-2x^2)\cos(x+t) \\ -(x^2-x)\sin(x+t) \\ 0<x<1,\ \ 0<t<1, \\ u(0,x)=x(1-x)cosx,\ \ 0\leq x\leq 1 \\ u(t,0)=u(t,1)=0,\ \ 0\leq t\leq 1, \\ 0<\alpha\leq 1. \end{cases} \qquad (11)$$

The exact solution of the formula (11) is obtained $u(t,x)=x(1-x)cos(x+t)$ by using Laplace transform method. We have used a procedure of modified Gauss elimination method for difference equation (6). We calculate the maximum norm for the error analysis using by

$$\in=\max_{\substack{n=0,1,\ldots,M \\ k=0,1,2,\ldots,N}}|u(t,x)-u(t_k,x_n)|,$$

where $u(t_k,x_n)$ is the approximate solution and $u(t,x)$ is the exact solution. Thus, the Table 1. gives error analysis for the difference scheme method.

Table 1. Error Analysis

$\tau=\frac{1}{N}, h=\frac{1}{M}$			
The difference scheme (11)			
$N=5, M=25$	$N=10, M$ $=100$	$N=20, M$ $=400$	$N=25, M$ $=625$
0.0531	0.0405	0.0370	0.0366

Tablo 1. Error analysis are calculated for the variable values $0<t<1$, $0<x<1$ and $\alpha=0.5$ of the approximation solution by helping the difference formula (6).

Remark 3.1 From Table 1., we see that the numerical results are consistent and stabile for $\tau=h^2$ which is the condition of Theorem 3.1.

4 Conclusion

In this paper,the first order difference schemes for the equation (1) are constructed. Stability inequalities are proved for given difference schemes. Approximate solutions for numerical experiment are found by the difference-method. Error analysis is performed by comparing the exact solution with the approximate solution. The effectiveness of the method was seen from the error analysis table. MATLAB program is used for all numerical calculations.

References

[1] Celik, C. and Duman,M. Crank-Nicholson method for the fractional equation with the Riezs fractional derivative. Journal of computational physics, 231:1743-1750, 2012.

[2] Gorial, I.I. , Numerical methods for fractional reaction-dispersion equation with Riesz space fractional derivative. Eng. and Tech. Journal, 29:709-715, 2011.

[3] Jafari, H. and Gejii, V.D., Solving linear and nonlinear fractional diffusion and wave equations by adomian decomposition. Appl. Math. and Comput., 180:488-497, 2006.

[4] Atangana, A. and Koca I. Chaos in a simple nonlinear system with Atangana--Baleanu derivatives with fractional order. Chaos, Solitons & Fractals, 89, 447-454.

[5] Alkahtani, R.T., Chua's circuit model with Atangana--Baleanu derivative with fractional order. Chaos, Solitons & Fractals, 89, 547-551, 2016.

[6] Owolabi,K.M and Atangana, A., Chaotic behaviour in system of noninteger-order ordinary differential equations. Chaos, Solitons & Fractals, 115, 362-370, 2018.

[7] Dusunceli, F. and Celik, E., Fibonacci matrix Polynomial Method For LinearComplex Differential Equations, Asian Journal of Mathematics and Computer Research, 15(3): 229-238, 2017.

[8] Karatay, İ., Bayramoğlu, Ş. R., and Şahin, A., Implicit difference approximation for the time fractional heat equation with the nonlocal condition. Applied Numerical Mathematics, 61(12), 1281-1288, 2011.

[9] Sarboland, M., Numerical solution of time fractional partial differential equations using multiquadric quasi-interpolation scheme. European Journal of Computational Mechanics, 1-20, (2018).

[10] Dusunceli, F. and Celik, E., An Effective Tool: Numerical Solutions by Legendre Polynomials for High-Order Linear Complex Differential Equations, British Journal of Applied Science & Technology, . 8(4): 348-355, 2015.

[11] Modanli, M, ve Akgül, A., Numerical solution of fractional telegraph differential equations by theta-method: The European Physical Journal Special Topics, 226.16-18: 3693-3703, 2017.

[12] Modanli, M., Two numerical methods for fractional partial differential equation with nonlocal boundary value problem: Advances in Difference Equations, 2018(1), 333, 2018.

[13] Dusunceli, F., Solutions for the Drinfeld-Sokolov Equation Using an IBSEFM Method, MSU Journal of Science, 6(1), 505-510. DOI : 10.18586/msufbd.403217, 2018.

[14] Dusunceli, F. and Celik, E., Numerical Solution For High-Order LinearComplex Differential Equations with Variable Coefficients, Numerical Methods for Partial Differential Equations, DOI: 10.1002/num.22222, 2017.

Authors’ addresses

Mahmut Modanli, PhD
Harran University
Faculty of Arts and Sciences
Depart of the mathematics
Sanliurfa, Turkey
mmodanli@harran.edu.tr

ISSN 2587-1943

GENITAL STRUCTURES OF TWO SPECIES OF THE GENUS *SCYMBALIUM* ERICHSON, 1839 (COLEOPTERA, STAPHYLINIDAE, PAEDERINAE)

İnanç Özgen 1, Eduard A. Khachikov 2

scientific note

Descriptions of the internal structures of the genitalia of *Scymbalium anale* (Nordmann, 1837) and *S. persimile* (Cameron, 1940) are presented in this paper. The structure of endophallus and genital structures of females of both species are homotypic.

Key words: *Staphylinidae, Paederinae, Scymbalium, genitalia.*

1 Introduction

In this paper, description of the morphology is presented on the internal structures of the genitalia (endofallus, spermatheca and vagina) of males and females of two species - *Scymbalium anale* (Nordmann, 1837) and *S. persimile* Cameron, 1940. Detailed studies have not been done on the genitalia of these species up to now.

These data can be used in taxonomy and systematics.

2 Material and Method

Specimens were mounted on a cardboard plate (glued with water-soluble glue) and pinned onto an insect pin. Genitalia were placed on a plastic plate in Hoyer's medium or in a container with an aqueous solution of glycerol, and pin up one pin with the corresponding specimens. Part of the preparations was made with endofallus fully straightened, and in some – only partially.

Terminologies of describing genitalia (partially) and of their preparation were derived from Khachikov and Shavrin 2010.

The abbreviations in the text and illustrations are given below:

ventral-distal titititillator – vdt

apical projection – ap

medio-lateral chamber –mlch

dorsal chamber– dch

lateral chamber– lch

vagina – vag

sex gland – sg

spermatheca – sp

Places of storage of the materials are marked as follows:

cEKh – private collection of Khachikov E. (Rostov-on-Don, Russia).

3 Results

Genus Scymbalium Erichson, 1839

Type species Achenium anale Nordmann, 1837

Scymbalium anale (Nordmann, 1837: 153)

Material: 2♂, 2♀, Russia. Rostov region., vill. Bagaevskaya, 20.VI.2009. leg. Khachikov E. (cEKh).

Distribution: Europe, Algeria, Middle East, Turkey, Kazakhstan, Turkmenistan (Schülke & Smetana, 2015).

Genitalia. Male. Endofallus is short as a whole and extended distally. The ventral side of endofallus: large ventral-distal titillator (vdt) is situated in its distal part. Medio-lateral chambers (mlch) adjacent to ventral-distal titillator (vdt) laterally, on each side. The dorsal side: apical projection (ap) is located in its apical part. Dorsal chamber (dch) is in the proximal part. The lateral side: lateral chambers (lch) are situated in its middle part on each side.

Female. Vagina is sacciform, with transverse grooves. Spermatheca (sp) is curved and sclerotized. Sex gland (sg) is elongated, slightly curved. (Figure: 1 – 4)

***Scymbalium persimile* Cameron, 1940: 251**

Material: 2♂, 2♀. Russıa, Daghestan, Makhachkala city, N of suburb, Karaman-2, 16.VI.2009, leg. Iljina E. (cEKh).

Distribution: Iraq and South European Territory of Russia (Anlaş et al., 2012).

Genitalia. Male. Endofallus is short as a whole, wider in the distal part. Apical projection (ap) is situated in its apical-dorsal part. Dorsal chamber (dch) is in the proximal part dorsally. On the ventral side, large ventral-distal titillator (vdt) is located in its distal part. Medio-lateral chambers (mlch) are adjacent to ventral-distal titillator (vdt) laterally, on each side. Lateral chambers (lch) are located in the middle part of endofallus on each lateral side.

Female. Vagina is baggy, with transverse grooves. Spermatheca (sp) is curved and sclerotized. Sex gland (sg) is elongated, slightly curved. (Figure: 5-7)

3 Comparison

The structure of endofallus and genital structures of females of both species are homotypic, likely. The main differences are in some particulars at the level of species. For example, in *Scymbalium persimile* the ventral-distal titillator is larger than for *S. anale*. Thus, as presented, the structure of the genitalia of these species accentuated their taxonomic status.

Acknowledgements

The authors are sincere grateful to Kasatkin D.G. and Shmatko V.Yu. (Russia, Rostov-on-Don) for making illustrations and Ilyina E.V. (Russia, Makhachkala) for given material.

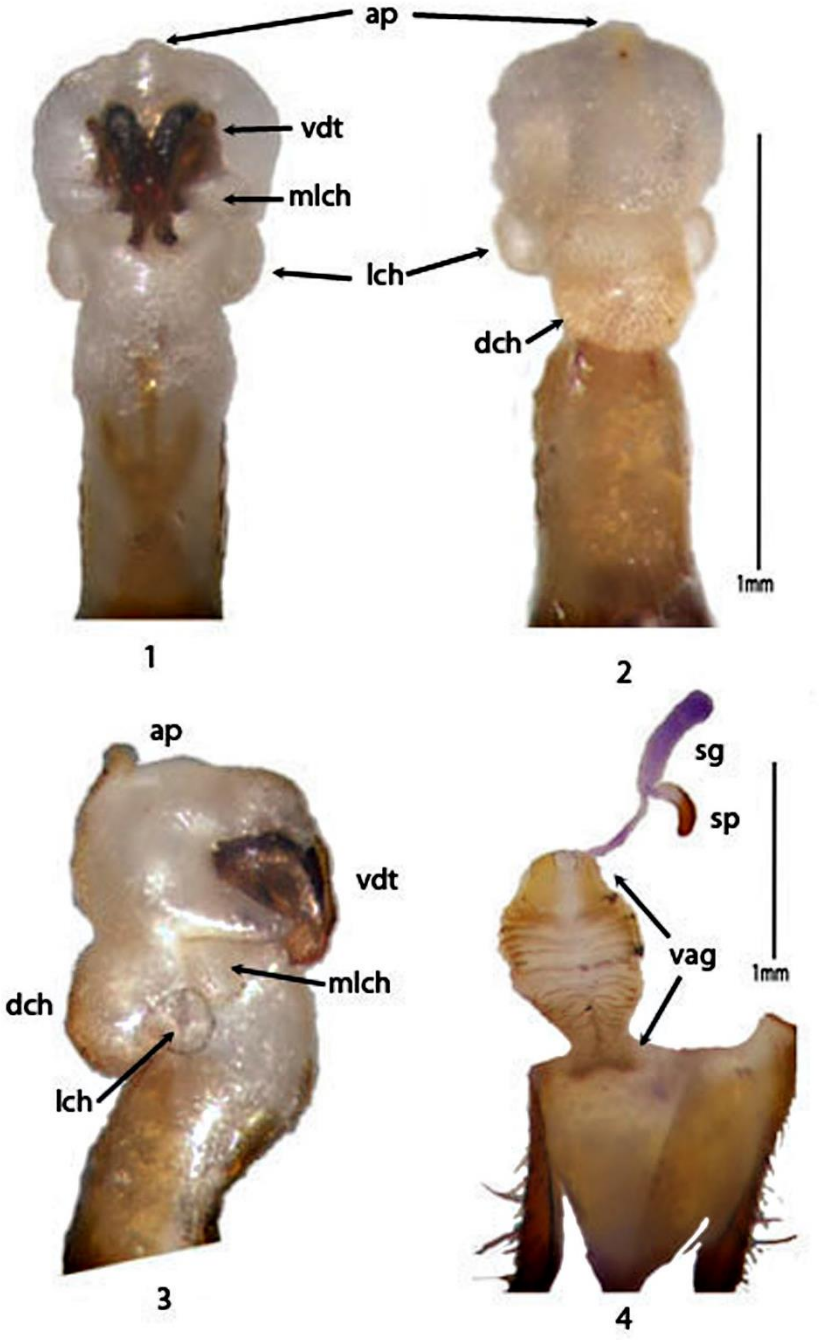


Figure 1-4: Genitalia morphology of *Scymbalium anale* (Nordmann, 1837)

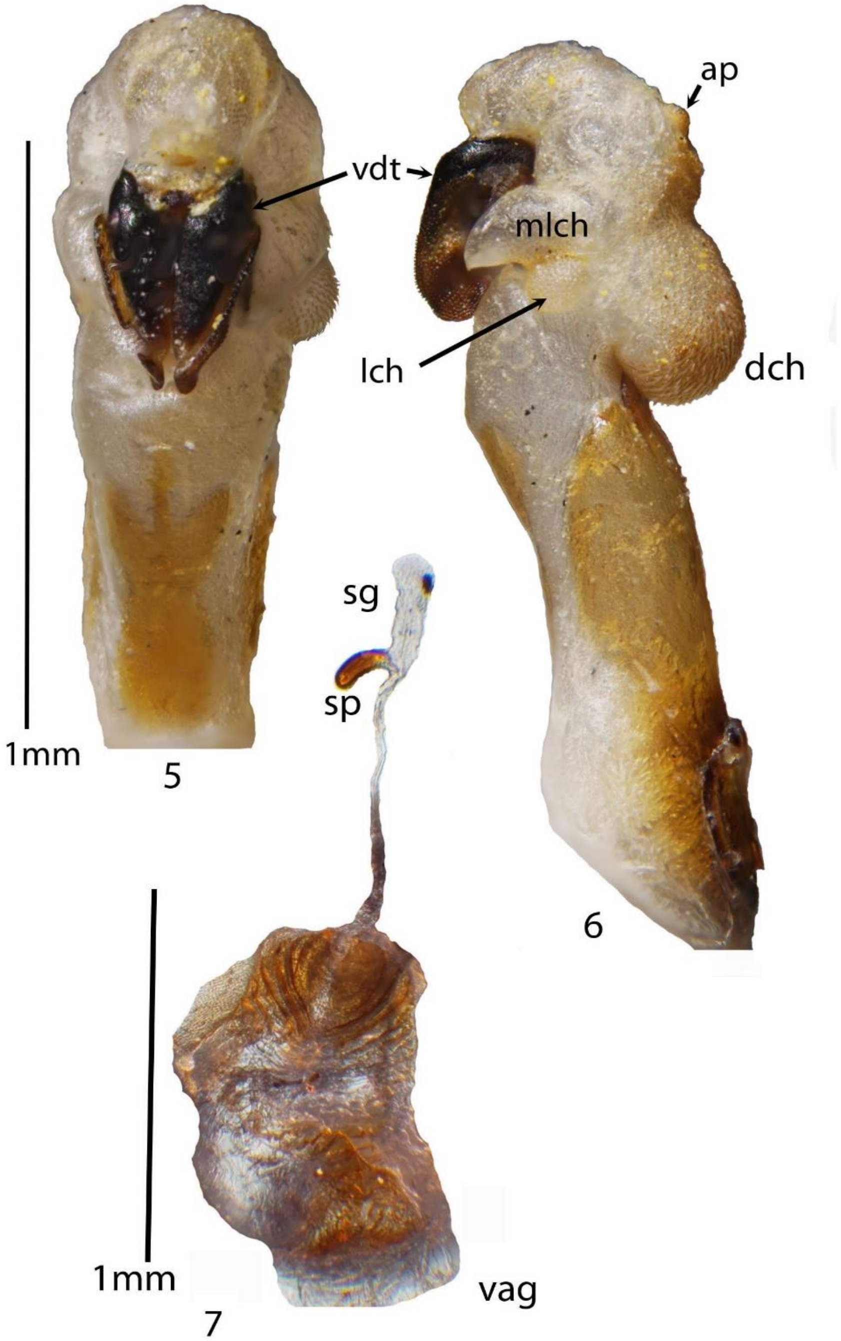


Figure 5-7: Genitalia morphology of *Scymbalium persimilis* Cameron, 1940

References

[1].Anlaş S., E. A. Khachikov & Iljina E. V. 2011. New records on the distribution of some species of the subfamily Paederinae (Staphylinidae, Coleoptera) from Asia and Europe. *Acta Zoologica Bulgarica* 63 (2) 205-207.

[2].Khachikov E.A., Shavrin A.V. 2010. Genital structures of some East Palaearctic species of the subtribe Staphylinina Latreille, 1802 (Coleoptera, Staphylinidae). *Euroasian Entomological Journal*. 9(4): 631–640.

[3].Schülke, M. & Smetana, A. 2015. Staphylinidae, pp. 304-1134. – In: Löbl I. & Löbl D. (eds), Catalogue of Palaearctic Coleoptera. Volume 2. Hydrophiloidea – Staphylinoidea. Revised and updated edition. Leiden: Brill: xxvi + 1702 pp.

Authors' addresses

İnanç Özgen 1, PhD
Fırat University,
Bioengineering Department,
Elazığ, Turkey
inancozgen@gmail.com

Eduard A. Khachikov 2, PhD*
Rostov branch of Russian Entomological Society,
Alexandrovsky spusk, 59,
Rostov-on-Don Russia.

ISSN 2587-1943

ADDITIONAL NOTES ON THE SOME APHROPHORID SPITTLEBUGS OF EASTERN ANATOLIA (HEMIPTERA: CERCOPOIDEA: APHROPHORIDAE)*

İnanç Özgen 1, Aykut Topdemir 2, Fariba Mozaffarian 3

scientific note

The study was carried out to determine Aphrophoridae species in Eastern Anatolia in 2018. Five species were collected by sweeping net on herbs. The collected specimens were identified as: *Aphrophora salicina* (Goeze, 1778), *Lepyronia coleoptrata* (Linnaeus, 1758), *Paraphilaenus notatus* (Mulsant & Rey, 1855), *Philaenus spumarius* (Linnaeus, 1758) and *Neophilaenus campestris* (Fallén, 1805). The species *P. spumarius* and *L. coleoptrata* were the most abundant species and the others were rather rare. The species of family Aphrophoridae are xylem feeders so they are considered as candidates for transmitting bacteria *Xylella fastidiosa*. Therefore, the role of the identified species in the agricultural ecosystems in the collecting sites needs to be studied.

Key words: *Hemiptera, Aphrophoridae, Fauna, Eastern Anatolia*

1 Introduction

The Aphrophoridae or spittlebugs are a family of insects belonging to the order Hemiptera. Nymphs of Aphrophoridae secrete a frothy saliva-like mass, which gives the name “spittlebugs” for insects in the superfamily. The species of family Aphrophoridae are xylem feeders so they are considered as candidates for transmitting bacteria *Xylella fastidiosa.* In this study were carried out to determine of Aphrophorid fauna in Eastern Anatolia of Turkey.

2 Material and Method

In this study, These species were collected in the herbs in May to August 2018 in Elazığ and Tunceli provinces. Specimens have been photographed witby a Olympus SZX 51 model stereo binocular microscope.

3 Results

Aphrophora salicina (Goeze, 1778)

Material examined: Elazığ, Günbağı village, Pagan location, 21.VI.2018, 3 exs., Arındık village, 28.VI.2018, 2 exs., Totally: 5 exs.

Note: The species is mostly associated with *Salix* species (Mozaffarian et al., 2015).

Lepyronia coleoptrata (Linnaeus, 1758),

Material examined: : Elazığ, Günbağı village, 19.V.2018, 15 exs., Arındık village, 28.VI.2018, 22 exs. **Totally**: 37 exs.

Neophilaenus campestris (Fallén, 1805)

Material examined: Elazığ, Aşağı Çakmak village, 18.V.2018, 3 exs.

Note: *N. campestris* prefer mostly grasslands, *Neophilaenus campestris* Fallén showed harbour the bacterium in their body (Elbeaino et al.,2014; Moussa et al., 2017).

Paraphilaenus notatus (Mulsant & Rey, 1855),

Material examined: Elazığ, Aşağı çakmak village, 18.V.2018, 6 exs.

Note: It was determined to potential vector of *Xylella fastidiosa.* This specimen was distributed to French mainland, South Russia, Ukraine, Eastern Palearctic, Near East. It is commonly found that in Poacea herbs (Anonymous, 2018)

Philaenus spumarius (Linnaeus, 1758)

Material examined: Elazığ, Günbağı village, 19.VI.2018, 22 exs.,Arındık village, 28.V.2018, 10 exs.,, Tunceli, Pertek, Akdemir, 12.06.2018, 12 exs. Totally: 44 exs.

Note: The most economically important species of this family in Turkey is *Philaenus spumarius* (L.), which is very widely distributed and found very abundantly (Lodos and Kalkandelen, 1981). *Philaenus spumarius* L. (Aphrophoridae) has so far been proven to transmit the CoDiRO strain (Saponari et al., 2014)

The majority of the species obtained by this study is the first record in terms of the locations. Because the vast majority of these species are *Xylella fastidiosa*'s vector, they are pests that need to be carefully considered.

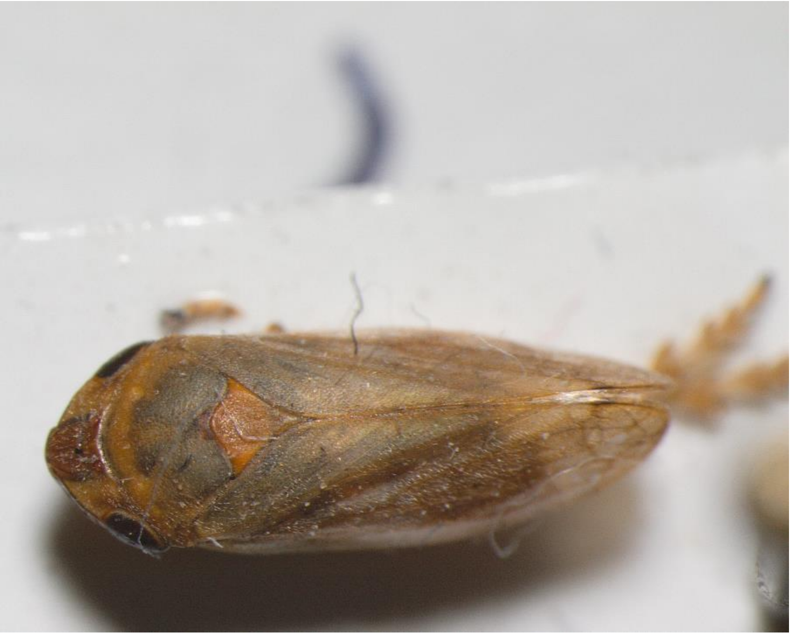


Figure 1. Habitus of Neophilaenus campestris (Fallén, 1805)

Abstract of this study was presented in Eurasian SciEnTech International conference in Ankara.

References

[1].Anonymous, 2015. Scientific Opinion on the risk to plant health posed by *Xylella fastidiosa* in the EU territory, with the identification and evaluation of risk reduction options. EFSA Journal. 13 (1): 3989.

[2].Elbeaino,T.,Yaseen,T., Valentini,F., Bemmoussai. E., Mazzoni V., D'onghia, A.M., 2014. Identification of three potential insect vectors of *Xylella fastidiosa* in Southern Italy Phytopathologia Mediterra 23: 328-332.

[3].Lodos, N. and A. Kalkandelen., 1981. Preliminary list of Auchenorrhyncha with notes on distribution and importance

[4].Moussa, I.E.B., Valentini, F., Mazzoni, V., Speranza, S., Lorusso, D., Digiaro, M., Varvaro, L. and A. M. D'ohghia, 2017. Seasonal distribution of *Philaenus spumarius* and *Neophilaenus campestris* in Apulian olives groves. European conference on *Xylella fastidiosa*: finding answers to a global problem. Palma de Mallorca, poster

[5].Mozaffarian, F., and M. Wilson., 2015. The aphrophorid spittlebugs of Iran (Hemiptera: Cercopoidae: Aphrophoridae).Zootaxa4052(4):442-456.

[6].Saponari M., Boscia D. ,Nigro F. Martelli G. P., 2013. Identification of DNA sequences related to Xylella fastidiosa in oleander, almond and olive trees exhibiting leaf scorchsymptomsin Apulia (Southern Italy). Journal of Plant Pathology, 95 -668

Authors' addresses

İnanç Özgen PhD
Fırat University,
Bioengineering Department,
Elazığ, Turkey
inancozgen@gmail.com

Aykut Topdemir PhD
Fırat University,
Bioengineering Department,
Elazığ, Turkey

Fariba Mozaffarian PhD
Insect Taxonomy Research Department,
Iranian Research Institute of Plant Protection,
Agricultural Research,
Education and Extension Organization,
Tehran, Iran.