Bio-inspired Security Scheme for IoT Technology

Charles O. Muango
University of Shanghai for Science and Technology
Jun Gong Rd 516
Shanghai 200093, China

Jairus O. Malenje
University of Shanghai for Science and Technology
Jun Gong Rd 516
Shanghai 200093, China

Qu Shaojian
University of Shanghai for Science and Technology
Jun Gong Rd 516
Shanghai 200093, China

ABSTRACT

There is a general consensus among scholars and ICT practitioners that the evolution of technology in today's world has advanced [1] to a level where communication between individuals and abstract objects is possible under the framework of Internet of Things (IoT). However, due to security threats and constrained resources (such as memory, power and processing capacity), applying traditional approaches of security on these category of devices has become a challenge to ICT professionals in this era of cybersecurity. Therefore, this study proposes a flexible solution that can be used to classify IoT devices into operational domains, whereby a meta-heuristic Nature-Inspired Firefly algorithm is used to tune parameters for the various domains to prevent attacks from spilling all over the entire community of IoT devices. With this approach, no device shall be allowed to communicate outside its domain. The proposed technique is modeled on the behavior of the firefly that uses its light intensity to communicate to friends and frighten off impostors or enemies. Through iterative simulations done, we were able to achieve constant light intensity (attractiveness) with different bands. Our findings revealed a fast and improved convergence rate as compared to other nature inspired algorithms. Therefore, we recommend that these bands can be allocated to the various IoT domains. Limitations of the study and future directions are well addressed.

General Terms

Fire fly Algorithm, IoT, Security.

Keywords

IoT; Cyber-security; Firefly; Domain; Light-intensity

1. INTRODUCTION

As an emerging technology, Internet of Things (IoT) is already affecting how we run our daily affairs [2]. Phys-ical devices (such as fridges, food-warmers, television sets, watches, health wrist bands, car alarms) have been given 'life' by being equipped with sensors and inter-networking capability to facilitate seamless connectivi-ty. IoT enables physical objects to understand their im-mediate surroundings and perform tasks by having them communicate together, collate data and co-ordinate judgements. This has improved on efficiency since the sensors use existing networks to enable remote management. Their usage is expected to continue grow-ing exponentially in the coming years by an estimate of over 20 billion objects by 2026 [3]

Connected technologies and their application are useful to users, but they come with many inherent security challenges which were not foreseen with traditional network systems [4] while the rapid growth of the IoT-enabled devices effectively broadens the attack surface [5] [6]. With a growing worldwide demand, manufacturers are in a race against time to beat each other for a slice of the IoT market-share while paying less attention to security requirements of these devices [7]. Therefore, going for-ward, visibility and device access control may be a daunting task for the ICT professionals in the work place considering proliferation of these devices object [8]. Consequently, there is a need to keep abreast with the ever evolving technological IoT space with emphasis on security aspect of the players in the internet-works. For instance, the "Mirai" IoT malware that threatened to take over the internet by use of a Distributed Denial of Service Attack on connected devices has led to resurgence of new IoT botnets [9]. Some researchers have warned of an imminent botnet storm "cyber hurricane" in the horizon [10] [11] [12]. A malware by the name "Reaper" has gone a notch higher by abusing susceptibilities in IoT devices and recruiting them into a botnet web [13]. Recently, it was disclosed that a critical Bluetooth flaw had affected billions of devices, a case in point being the AI-based voice-activated personal assistants [14].

In spite of the growing application of IoT [15], there are glaring features that differ from legacy IT devices that make the security component in them a problem to both users, IT security personnel and researchers in general. Specifically, IoT devices have the following deficits: re-source inhibited, vastly connected, highly susceptible, diverse and across-the-board, acquired by others and finally they are not network safe [3]. In this paper a parameter tuning security solution for IoT devices is pro-posed. The suggested solution utilizes a bio-inspired approach and specifically the Firefly Algorithm for parameter tuning because fireflies exhibit similar behavioral properties in the way they adapt to their immediate environments vis-à-vis relationship with their neighbors. This is carried out by way of simulation and results are discussed thereafter in the text. The rest of the paper is organized as follows. In section 2, we give an overview of related works. Section 3 presents the Firefly Algorithm. Simulations and experimental results are shown in section 4. Finally, we conclude this paper concisely in section 5.

2. RELATED WORK

Many studies have been carried out on networks and data security but recently, focus has shifted to IoT devices due to its rapid technological maturity over the outdated IT standards. A study done by [16] proposed a novel model for averting catastrophes in IoT-based home automation by implementing Reed Solomon Codes for error detection and correction before any operation invoked by the user gets executed. The authors looked into mitigating attacks on the central system that control power usage in smart homes that pose high notch risk. Their proposed solution checks on errors that might have been induced in the wireless communication channels or in the data repository. A study done by [17] proposed an algorithmic approach to security de-sign for integrated IoT smart services. They explain that by integrating smart applications under IoT infrastructure it shall benefit users' access to heterogeneous services more securely. Further, they recommend application of the solution to different security levels in IoT smart environments that will deal with all security is-sues. However, this approaches cannot hold for vicious attacks such as Distributed Denial of Service (DDoS) attacks which users might not be able handle at the local level. In-spite of their effectiveness these counter measures will be resource intensive considering the limited resources in IoT devices.

Another study done by [7] looked into security issue by doing an analysis of IoT component life cycle focusing of induced vulnerability at every stage of development. They assert that, the intervention of third party solutions cannot be applied uniformly as this will increase the overall cost of the system. They further challenge researchers to develop security solutions that would be relevant across the IoT component life cycle. According to a survey done by [18] on IoT security attacks, many of the attack threats were already on standby just waiting for the adoption of the IoT devices. The authors classify the attacks in terms of efficiency and damage. Node injection attack is the most difficult to detect whereas internet worms are invented everyday due to detection limitation. They accentuate the need to have a light load and robust security solution that can optimally handle security issues in IoT. Our proposed solution aims at addressing the issues addressed by the above authors in terms of offering light load security solution that can be built into the devices at the production stage. If manufacturers can be compelled to enforce security at the time of production with view of the domains in IoT only then can we avert DDoS which are prevalent within this family.

The case study done by [19] on military conscious simulation and IoT security challenges recognized that perceiving and executing trust contrivances to protect services/people/objects in changing setups seems to be a challenging research direction. The authors point to the lack of design and implementation for trust mechanism in real networks. Their closing remarks on the paper highlight the fact that the ubiquitous nature of IoT makes it difficult to deal with security issues conclusively given the diverse user and application requirements. In [20] the authors propose the use of a game theoretic technique to deal with anomaly detection technique to single attacks in the system. Though it is a good start in dealing with attack signatures but still suffers the global threshold to deal with and accommodate all IoT devices due to their inadequate resources. Further still, the system can be overwhelmed especially where there are high false positive rates given the dynamic nature of real world attacks such as botnets.

[21] highlights a comparative analysis of the different attacks that target specific layers of the IoT environment and their counter measures. Their approach is categorized into application, processing, network and perception layers of the IoT. As much as they pointed out the measures to be taken under each category, they conclude by advocating for better extraordinary solutions to IoT security and privacy. A survey of security challenges to the IoT layered architecture and protocols used in running of IoT is done by [22]. The authors map out existing solutions to current problems and go ahead to propose block chain, a technique used for cryptocurrency as a robust solution to security issues in IoT. This is a very noble step in the right direction but given the de-merits of IoT devices the solution might not be effective in terms of power and memory resources required to update the current state of a device. [23] proposed an IoTChecker, a data-driven framework to semantically model IoT configurations to arrest security configuration anomalies and analyze IoT-specific threat vectors. In this concept, they have an automatic configuration analytics that describes dependencies in the complex IoT interactions through rules, reasoning and queries. The mechanism extracts configuration data scattered from online sources and populates it with suitable ontology concepts as per registered products. It then does critical security analyses of real-world home automation systems from different perspectives. Considering that threats are dynamic and at times skewed to particular brands of IoT devices, the proposed method might come short particularly where the attack is not on its listed ontology scenarios. The other problem that might arise is the current probing of these devices to an external anomalies database that will take off a lot of processing time and power from the devices.

[24] looked into device security in IoT convergence majoring on categorization of devices into domains as per the definition by various standards organizations such as the ITU-T (the International Telecommunication Un-ion Telecommunication Standardization Sector), the ISO/IEC JTC 1 (Special Working Group on Internet of Things) and one M2M (a global scale Partnership Project organized by 7 major standards organizations around the world (ETSI (Europe), TIA, ATIS (North America), ARIB, TTC (Japan), CCSA (China), and TTA (South Korea)) to develop the global IoT service platform's standard technology. The authors went ahead to summarize and categorize the various IoT device applications into key thematic areas as well as threats in each. They acknowledge the fact that the IoT constrains, especially the use of lightweight security protocol and low computing power, have led to exposure of the communication space to new cybersecurity threats. This can be attributed to increased openness and IoT device's specialty.

[23] underscores the fact that IoT devices interact and impact the environment with limited or no human mediation. Their network comprises of thousands of IoT devices using diverse protocols, having varying re-sources, complex interdependencies and diverse net-working and security requirements. The configuration data of IoT systems is mostly unstructured, lacking ma-chine interpretable semantics and thus, traditional analysis techniques cannot tackle the IoT-specific con-figuration challenges of scalability, interoperability and security. From literature, since the IoT devices have power, memory and processing power constrains, thus this division will better highlight management of these devices. Secondly, the separation of domains will better provide a level of dealing with attacks under each segment, such that should there be a global attack targeting a particular domain the rest are not disenfranchised. Since fireflies have the ability to scare off intruders we expect no infiltration of communication between the different groups as each shall be operating at a higher or lower fitness (attractiveness) level than the other thus further enhancing on the IoT security which was our main focus in this paper.

In [21] the authors reiterate that, there was no standard architecture and security strategies put in place for one architecture that would work for all attacks. Consequently, there is need for researchers to try and come up with solutions that can aide in attack avoidance. In a nutshell, they conclude by saying that it is mandatory to standardize IoT architecture. This study attempted to answer this question by optimizing variables using the Firefly algorithm to be able to create communication paths for the various domains in IoT as depicted by [24]. We present a nature-inspired parameter tuning algorithm for IoT security by modeling the holistic behavior of the firefly of attracting mating partners, sharing food and warding off enemies. Our solution takes into account the limitation of IoT devices especially less processing power, limited battery life and storage space. The subdivision of these domains would make it easier for management; in case of an attack on one domain, say by DDoS, it would not spill over to other units out-side that domain. The separation enhances security and privacy through shielding since they shall be operating on different access levels (Class).

3. FIRE FLY ALGORITHM

This is a nature-inspired meta-heuristic algorithm that was formulated by [25] in 2008; it has been used in recent years across many applications. About 2000 firefly species exist in the world, and they all can be characterized by radiation of short, rhythmic flashes. Uniqueness comes in the pattern of flashes. Bio-luminescence is the process by which the light is produced; basic roles of such flashes are to attract coupling partners and potential prey. This algorithm is motivated by the blinking light of fireflies in nature. It reflects a physical formula of light intensity of firefly found in nature and the main ideas of the firefly algorithm is interpreting light intensity characteristics as follows:

I. All fireflies are unisex and an attraction is between any two fireflies.

II. Attractiveness is proportional to light intensity. A firefly with lower light intensity will move toward the fireflies with higher light intensity, thus if none exists, the firefly will randomly explore the space.

III. The light intensity of a firefly is determined by fitness function.

IV. The light intensity of the firefly can as well be used as a defense mechanism

From literature the light intensity at a particular distance r from the light source obeys the inverse-square law. In other words, the light intensity I decreases as the distance r increases in terms of I ∝ 1/r2. Weakness of the light intensity can as well be a result of the air particles absorbing portions of it.

The pseudo code is presented below;

```
Begin
Define
light absorption coefficient γ initial attractiveness β0
    randomization parameter α
Objective function f (X ), X = (X1, ... , Xd)T
Generate initial population of fireflies Xi (i = 1, 2, ... , n)
Light intensity Ii at xi is determined by f (Xi)
while (t < MaxGeneration) for i = 1: n all n fireflies for j
    = 1 : i all n fireflies
if (Ij > Ii), Move firefly i towards j in d-dimension;
end if
Attractiveness varies with distance r via exp [−γ r2]
    Evaluate new solutions and update light intensity
    end for j
end for i
    find the current best
```

Light intensity I (r) varies according to the inverse square law, thus it can be presented as

$$I\ (r) = \frac{I_s}{r^2} \qquad (1)$$

for a given medium with a fixed light absorption coefficient γ, where Is is the intensity at the source with varying distance r. The final light intensity I can be computed as;

$$I\ (r) = \ I_0 e^{-yr^2} \qquad (2)$$

Since the firefly's attractiveness β is proportional to the light intensity seen by adjacent fireflies, the attractiveness β of a firefly is calculated by;

$$\beta = \beta_0\ e^{-yr^2} \qquad (3)$$

where r is the distance between any two fireflies, i and j at xi and xj respectively, which is the Cartesian distance, β0 is attractiveness at r = 0 and is the light absorption coefficient the environment.

$$x_i = \quad rand\ (Ub - Lb) + Lb \qquad (4)$$

Movement of the firefly i from its current position towards a more attractive (brighter) firefly j is calculated by;

$$X_i^{t+1} = \ X_i^t + \beta \exp\left[-yr_{ij}^2\right] \ + \alpha_t(rand - 1/2) \qquad (5)$$

where α is a significance factor of the randomization parameter and rand with uniform distribution U (0, 1) is a random number obtained from the uniform distribution and is a random generator.

The distance ri,j between any two fireflies I and j at xi and xj , respectively, is defined as the Cartesian distance,

$$r_{ij} = \left|\left|X_i - X_j\right|\right| = \sqrt{\sum_{k=1}^{d}\left(X_{ik} - X_{jk}\right)^2}$$

` (6)

where Xi,k is the k th component of the spatial coordinate Xi of the ith firefly

4. SIMULATIOM AND ANALYSIS

The objective of the proposed solution was to demonstrate the possibility of subdividing IoT devices into domain clusters while maintaining communication within the clusters thereby ensuring security with no spill over. To demonstrate the effectiveness of the proposed model, two kinds of comparisons are investigated in this research. The light intensity **I(r)** and the attractiveness **β** which basically control the movement and association of the fireflies into various clusters/groups. Guided by the above parameters we sought to find an optimum operational level where we can maintain the light intensity **I(r)** and the attractiveness **β** for seamless communication among the IoT devices.

The attraction and light absorption coefficient are two significant parameters. The values of those parameters determine the speed of convergence and the behavior of firefly algorithm. The behavior here we are looking at the component of the firefly that fends off intruders from joining a specific group while still being able to carry on with sharing of information within. We coded the Firefly Algorithm using python programming language to aide our simulation. The main objective was to come up with different bands that could be assigned to different IoT domains thus creating a sub-netting scenario.

Tuning was done on the **I(r)** and **β** variables over different test

runs to derive the global parameters that could support the applicability of the above algorithm in solving IoT security problem. In the simulations, the parameters, except when specified differently, were set to the following values: initially, 50 individuals are randomly generated in a population and the number of generations is equal to 100, **β**= 0.2 and **γ** =0.2. Results for this simulation is presented in

Fig. 1 above shows that the best fitness levels which is a parameter that dictates the light intensity / brightness diminishes with longer iterations. **γ** represents the gamma values that were being tuned while we maintained when **β=0.2** to depict the normal behavior of the firefly in their habitat. **γ** is the parameter that dictates the light intensity; thus by varying it we were able to see the interplay with **β=0.2**. This implies that, for longer distances the firefly would not be able to communicate with each other to achieve the core objective of food sharing or mating due to reduced light intensity. The variation of the light intensity also comes in handy at times as a security control measure to fend off intruders. However, with low light intensity over longer iterations, communication power could be lost among close groups, something we wanted to achieve while being able to ensure device security.

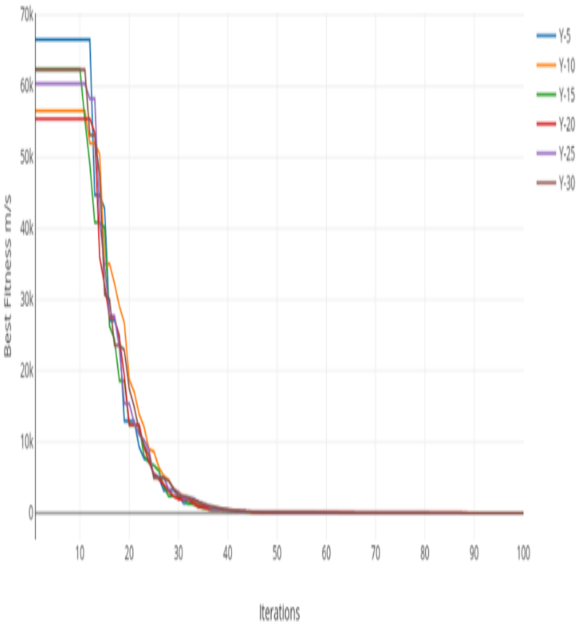

Fig. 1 Results before optimization of Variables

To achieve our objective of a bio-inspired approach to IoT security scheme, we opted to vary **β** and **γ** parameters. The result is presented below in Fig. 2.

From the test results shown in Fig.1, tuning only the **γ** and not the **β** did not achieve comprehensive results for us thus the decision to tune both β and γ parameters uniformly at an interval of 0.5. This was informed from our test runs that had very little impact on both values on both x and y axes. According to the results in Fig. 2, with increased runs of 200 iterations we were able to show that we can actually achieve longer communication distances without losing the light intensity I(r). Furthermore, with the different bands represented by the horizontal lines we can now allocate each to an IoT domain. This is backed by the firefly behavior of each cluster being able to shield themselves from interlopers. Taking this into account, IoT devices can be configured to mimic this rare natural characteristic of this intelligent small insects for security purposes.

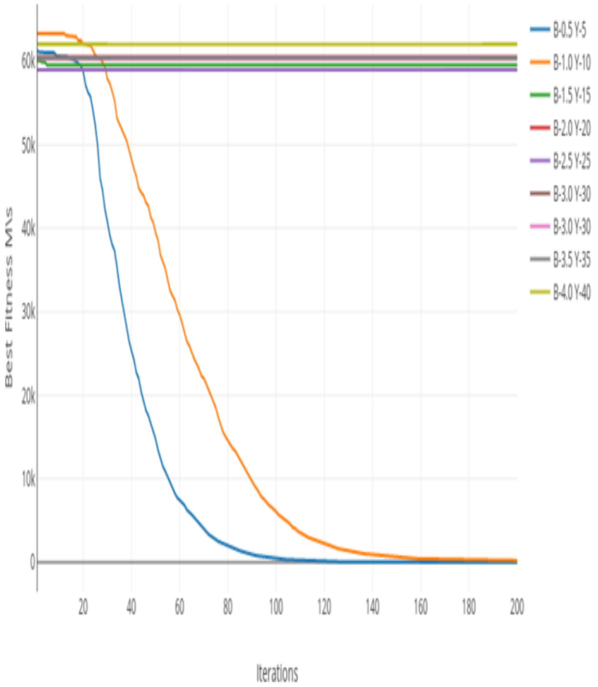

Fig. 2 Final result of Optimized values

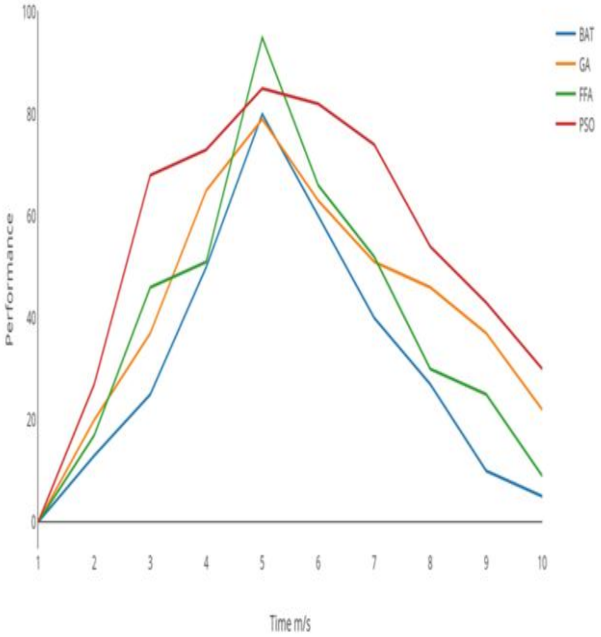

Fig. 3 Algorithm Performance Comparison

Further, as the results in Fig 2 show positive results (horizontal lines) creating different threshold or rather categories that can be allocated in for each service domain namely energy service domain, smart homes service domain, E-health service domain and any other that will arise. To further enhance our work, we compared the performance of the Firefly Algorithm with other selected bio-inspired algorithms for the following reasons: first, nature inspired methods are controlled by exploring the population to find the best fitness and then exploiting it, and secondly, they avoid sticking to local optima by a random solution either by a randomization parameter or mutation and crossover. The results of this comparison are shown in Fig. 3.

Fig.3 gives a comparison among well-known heuristic optimization algorithms, namely Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and BAT Algorithm (BAT) against the Firefly Algorithm (FFA). The 3 algorithms were implemented to solve the problem at hand with the same number of simulation runs (200). The average time taken to give a solution was collected for purposes of performance evaluation represented by the expression below:Performance = [Average time / Total time] X100%

Performance was a measure used to gauge how the various algorithms compare to each other in reaching the global optimum solution under same conditions. From Fig. 3, it can be noted that our nature-inspired algorithm of choice ranked above the rest in terms of finding the best fitness with regard to time. The focus of study was at 5m/s time line which was the point at which the algorithms reached their peaks in terms of convergence speed then descended afterwards. This is also important in that IoT devices due to their energy limitations, should be able to use less power during synchronization with peers. Though it should be noted that the time taken by each algorithm strictly relies on the implementation pattern, hardware and software.

5. CONCLUSION AND FUTURE WORK

We used the firefly algorithm, a nature-inspired meta-heuristic algorithm to optimize parameters for our domain regularization. The efficacy of the proposed method demands less processing and memory on the part of IoT devices; control will be decentralized within a domain thus communication can only take place with members of the same domain only. With the growing numbers of IoT devices it is imperative to enforce security within the environment of operation. The findings of the current study could help developers and standards organizations to address the IoT security paradox by applying separation of devices and allocating them communication standards deemed operationally fit. By mimicking the firefly behavioral characteristics which are almost similar to how IoT devices communicate and more especially repulsing of unwarranted connections, threats inherent in IoT devices can be dealt with effectively. Although this research has proposed a general way to deal with the problem of IoT security, it didn’t go further to show how the repulsion of indifferent connections can be achieved within the different domains. As future work, we will further study the characteristics of the light intensity that can be best suited to repel intruders at the same time allow for incorporation devices in the same domain. investigate more security. In addition, we shall work to build this architecture and test it in a real environment.

6. ACKNOWLEDGMENTS

Our thanks to all colleagues who contributed towards formulation and conceptualization of the idea.

7. REFERENCES

[1] Internet Society, "2017 Internet Society Global Internet Report - Paths to Our Digital Future," 2017.

[2] Olivier Flauzac , Carlos Gonzalez , and Florent Nolot , "New Security Architecture for IoT Network," in International Workshop on Big Data and Data Mining Challenges on IoT and Pervasive Systems, 2015.

[3] Pwnie Express, The IoT Security Gap. Boston: Pwnie Express, 2017.

[4] Jouini Mouna , Ben Arfa Rabai Latifa , and Khedri Ridha , "Multidimensional Approach Towards a Quantitative Assessment of Security Threats," in The 6th International Conference on Ambient Systems, Networks and Technologies(ANT 2015), 2015.

[5] Behrens Reinhard and Ahmed Ali , "A Security Architecture for The Internet of Things," KSII Transactions on Internet and Information Systems, vol. 11, no. 12, pp. 6092-6115, 2017.

[6] Vashi Shivangi , Ram Jyotsnamayee , and Modi Janit , "Internet of Things (IoT) A Vision, Architectural Elements, and Security Issues," in International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.

[7] Marconot Johan , Pebay-Peyroula Florian , and Hély David , "IoT Components LifeCycle based Security Analysis," in 2017 Euromicro Conference on Digital System Design, 2017.

[8] Express Pwnie, "Internet Of Evil Things," 2017.

[9] Wei Wang. (2017, October) https://thehackernews.com. [Online]. https://thehackernews.com/2017/10/iot-botnet-malware-attack.html

[10] Check Point Research. (2017, October) Check Point Research. [Online]. https://research.checkpoint.com/new-iot-botnet-storm-coming/

[11] Elisa Bertino and Islam Nayeem , "Botnets and internet of things security," Computer, pp. 76-79, February 2017.

[12] M. Antonakakis et al., "Understanding the mirai botnet," in USENIX Security Symposium, 2017.

[13] Greenberg Andy. (2017, October) WIRED. [Online]. https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/

[14] Khandelwal Swati. (2017, November) The Hacker News. [Online]. https://thehackernews.com/2017/11/amazon-alexa-hacking-bluetooth.html

[15] Kamal Aldein Mohammeda Zeinab and Sayed Ali Elmustafa , "Internet of Things Applications, Challenges and Related Future Technologies," World Scientific News, vol. 67, no. 2, pp. 126-148, 2017.

[16] Afzal Shah Idris , Amin Malik Faizan , and Arshid Ah Syed , "Enhancing Security in loT based Home Automation using Reed Solomon Codes," in IEEE WiSPNET 2016 conference, 2016.

[17] Jerald. A Vimal , Rabara. S Albert , and Premila Bai Daisy , "Algorithmic Approach to security Architecture for Integrated IoT Smart Services Environment," in World Congress on Computing and Communication Technologies (WCCCT), 2017.

[18] Deogirikar Jyoti and Vidhate Amarsinh , "Security Attacks inIoT: A Survey," in International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.

[19] Riahi Sfar Arbia , Chtourou Zied , and Challa Yacine , "A systemic and cognitive vision for IoT security: a case study of military live simulation and security challenges," in 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C), 2017.

[20] Sedjelmaci Hichem , Mohamed Senouci Sidi , and Taleb Tarik, "An Accurate Security Game for Low-Resource IoT Devices," in IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 66, NO. 10, OCTOBER 2017, 2017.

[21] Muhammad Ahemd Mian , Ali Shah Munam , and Wahid Abdul , "IoT Security: A Layered Approach for Attacks & Defenses," in International Conference on Communication Technologies (ComTech), 2017.

[22] Ahmad Khan Minhaj and Salah Khaled , "IoT Security: Review, Blockchain Solutions, and Open Challenges," Future Generation Computer Systems, no. FUTURE 3814, 2017.

[23] Mohsin Mujahid , Anwar Zahid , and Zaman Farhat , "IoTChecker: A data-driven framework for security analytics of Internet of Things configurations," computers & security , no. 70, pp. 199–223, 2017.

[24] Kim Hyun-Jin, Chang Hyun-Soo , Suh Jeong-Jun , and Shon Tae-shik , "A Study on Device Security in IoT Convergence," in 2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA), 2016.

[25] She Yang Xin, Nature Inspired Optimization Algorithms.: Elsevier Inc., 2014.