An Intelligent Security Approach using Game Theory to Detect DoS Attacks in IoT

Farzaneh Yazdankhah
Department of computer, Safashahr Branch,
Islamic Azad University, Safashahr, Iran

Ali Reza Honarvar
Department of computer, Safashahr Branch,
Islamic Azad University, Safashahr, Iran

***Abstract*—The Internet of Things (IoT) is a new concept in the world of Information and Communication Technology (ICT). The structure of this global network is highly interconnected and presents a new category of challenges from the security, trust, and privacy perspectives. The data transfer problems through the Denial-of-Service (DoS) attacks simply occur in this network and lead to service slow down or system crash. At the present time, traditional techniques are being widely used to confront the denial-of-service attacks in the Internet of Things and unfortunately, smart techniques have been less studied and exploited. In this research, a security solution on the basis of game theory is proposed to detect the denial-of-service attacks and prevent the problems in the services of the network of the Internet of Things. In order to scrutinize the performance of the suggested method in the network, this method was simulated using the NS2 simulator. The simulation results confirmed that the game-theory strategies in the proposed method outperformed the existing methods. Furthermore, in order to verify the acquired findings, a comparative evaluation was exhibited according to the three factors of operational throughput, latency, and energy consumption.**

***Keywords*—Internet of Things (IoT); network security; attack detection**

I. INTRODUCTION

Although the Internet of Things has been highlighted as one of the modern technologies in recent years, its applications have not been completely analyzed yet. This technology initially emerged as the radio frequencies for communications. Afterward, along with the advancements of wireless devices, smart sensors, and microcontrollers, it could improve the machine-to-machine communications and provide a platform for the communications between humans and things [1], [3]. The Internet of Things is generally founded on wireless technologies [5]. Since in the near future, a massive volume of information will be transmitted and received using the interconnected devices and management systems [4], different concerns will be brought in, particularly on the security issues. Given the rapid growth of this technology and joining of different things to this network, and also, the communication with each other, new challenges have arisen in various security issues, such as confidentiality, identity recognition, privacy, integration, etc. Moreover, the problems resulting from transferring and processing unwanted data have caused new user concerns and legal issues [2]. So far, a variety of methods have been presented to create security in the Internet of Things, including light and safe operating systems, scalable procedures for the alternate control, and new detection and blocking solutions for the raised threats. However, due to the existence of threats in different aspects and methods, establishing security in the Internet of Things is a complex and difficult task, requiring various smart mechanisms.

The threats and attacks against the security of the Internet of Things can be investigated from different aspects [7]. From one perspective, attacks can be categorized into two active and inactive groups, and from another perspective, they can be classified as the destructive and non-destructive groups [8]. However, the pivotal point is that the attacks to networks, regardless of their type, can cause irreparable damages to users, devices, things, and their communications. One of the main attacks used by attackers are the denial-of-service attacks, which are performed to disrupt the services and the network communications, and mostly lead to network disruption.

It should be indicated that the traditional security solutions have many defects and shortcomings. Two principal weaknesses of the traditional methods in the intrusion detection systems are as follows [6]:

1) From a technical viewpoint, they are highly complicated.

2) They rely on the temporary methods, based on trial and error.

The main drawback of the traditional security solutions is the lack of a specific framework, for decision-making about the quantity and the type of attacks [9]. In this context, smart security methods can provide us with suitable facilities to overcome this disadvantage.

In confronting problems, smart methods can apply the mathematical frameworks to analyze and model the problems. The solutions based on game theory have been described as an appropriate tool to tackle the security problems and different threats in the network [10], [11]. Game theory can be exploited to solve those problems, where several players with different motivations and purposes compete with each other [12]. Moreover, it is capable to analyze diverse scenarios (i.e. more than one hundred thousand scenarios) before making any decision, and choose the best solution.

The purpose of the present paper is to provide a smart security solution for detecting the denial-of-service attacks in the services of the network of the Internet of Things, using game theory. Then, through simulating the suggested solution using the NS2 software, the results will be compared with the existing methods. Next, the important factors at the time of the

denial-of-service attacks (including energy consumption, latency, and operational throughput) will be investigated. From an innovation perspective, the research contributions are as follows:

- Classifying and evaluating the denial-of-service attacks in wireless networks.
- Acquiring a suitable equilibrium, on the basis of the Nash equilibrium, in order to achieve a security balance in the Internet of Things.
- Presenting a smart method for attack detection based on game theory.

II. Related Work

The intrusion detection systems are amongst the network security issues, in which game theory has been more broadly applied. It logically originates from the fact that the traditional IDSs are based on the decision-making theory. As explained in Chapter One, game theory appears to be more suitable over the traditional decision-making theory for the sake of security problems.

In [13], the theoretical game-theory approaches, compared to IDS, were explained for different game models and in particular, two chapters of this book (9 and 10) were devoted to this topic. In [14], the entire Section 5 is considered the theoretical approaches of the game theory, over the IDS.

In [15], a multi-stage dynamic game model was adopted to study the intrusion detection problem in a mobile ad-hoc network. A method was proposed in [16], which models the configuration problem of the policy-based IDS, as a dynamic random game. In [17], a random game model was considered for the insider attack problem. A game method was suggested in [18] to study the problem of intrusion detection in wireless ad-hoc networks.

In [19], the problem of destructive signals was investigated in a scenario, called a MIMO Gaussian Rayleigh-fading channel. The interaction between the destructive signal generator and the transmitter-receiver pair was modeled as a zero-sum game, in which the attacker attempts to minimize the mutual information between the transmitted and received signals, while the defenders attempt to maximize it.

In [20], a method was exhibited to confront the denial-of-service attacks on the Internet based on a game theory, in which an attacker in the Internet attempts to transform the main page in a specific server. A random game method between the network manager and the attacker was suggested, where in each time step, the two players choose their actions and the game is transferred into a new state, according to the probabilities, depending on the chosen actions. The authors, through the simulations, showed that the game accepts several Nash equilibriums.

All the conducted studies and the presented games indicated that the resources required by the network may be the target of attacks. In [21], the authors considered a non-cooperative multi-person game on a graph with two types of players, which includes a set of attackers and a defender, which respectively indicate the viruses and the system security software. Each attacker selects one node for contamination and the defender selects a simple path (or edge) for protection.

Detection techniques are less efficient in terms of the energy and implementation costs [22], [23]. A vast majority of detection methods fail to individually confront the denial-of-service attacks [24]. Proactive counteractions can be mainly classified into two categories of software and software/hardware proactive counteractions [25]. The so-far performed studies have disclosed that the software proactive counteractions are more efficient over the other techniques, since unlike others, they do not use some costly algorithms for defense. However, the detection-based counteractions are known as the efficient solutions for the active attacks, such as the constant, deceptive, and random attacks [26].

III. Evaluation of Attacks in Wireless Sensor Networks

This section describes the evaluation of attacks in wireless sensor networks. Understanding the behavior of these attacks will be useful for the development of counteractions. Implementation of the attacks for evaluation is carried out based on the modeling, described in the previous section. The modeling process in the previous section presented a clear understanding of the things, involved in signal attacks as well as their interaction. In this section, in order to assess their effect, the attacks will be evaluated, under different traffic conditions and with various numbers of the destructive nodes in the network. In terms of the activity type, the denial-of-service attacks on wireless sensor networks can be categorized as follows [26], [27]:

- Constant attacks.
- Deceptive attacks.
- Random attacks.
- Reactive attacks.

IV. Simulation Details

All attacks were implemented using the NS2 simulator. The parameters set during the simulation are shown in Table 1. These parameters are considered according to the IEEE 802.15.4 radio model. The simulation of attacks was done under the following hypothesis:

The simulation was accomplished with variable time intervals of the traffic, which is beneficial for measuring the performance of attacks under different traffic conditions. The traffic time interval varied from 0 to 10000 milliseconds. In these simulations, the number of destructive nodes or the attacked nodes in the network was considered variable. Table 2 shows the result in different time intervals. Simulations have been done in four different conditions as follows:

- WSN with constant attack.
- WSN with deceptive attack.
- WSN with random attack.
- WSN with reaction attack.

TABLE I. SIMULATION PARMETERS

Parameters	Setting
Network Interface Type	Wireless : 802.15.4
Radio Propagation Model	Two-Ray Ground
Antenna	Omni antenna
Channel Type	Wireless channel
Link Layer	LL
Interface Queue	Priority Queue
Buffer size of IFq	50
MAC	802.15.4
Routing Protocol	Ad-hoc routing
Energy Model	Energy Model
Initial Energy	0
Idle Power	31mW
Receiving Power	35mW
Transmission Power	31mW
Sleep Power	15µW
Number of nodes	20
Node Placement	Random
Number of simulation run	50

TABLE II. COMPARISON OF ENERGY CONSUMPTION OF ATTACKS AT DIFFERENT TIME INTERVALS

	Energy consumption(Joule)			
Time (ms)	Constant_ Attack	Random_ Attack	Deceiver_ Attack	Reaction_ Attack
0-2000	50.2000 26.8667 51.3111	22.7222 40.5000 37.1667	32.5222 54.7444 36.9667	41.8000 42.8000 44.8000
2001-4000	43.5333 43.5333 40.2000	31.6111 26.0556 37.1667	49.1889 42.5222 39.1889	46.8000 42.8000 47.8000
4001-6000	34.6444 65.7556 65.7556	22.7222 72.7222 49.3889	35.8556 45.8556 98.0778	57.0222 52.9111 66.2444
6001-8000	80.2000 46.8667 56.8667	64.9444 67.1667 83.8333	75.8556 59.1889 53.6333	87.3556 81.8000 72.9111
8001-10000	73.5333 69.0889 57.9778	63.8333 66.0556 57.1667	81.4111 46.9667 73.6333	90.6889 96.2444 78.4667
>10000	52.4222 96.8667 69.0889 44.6444	96.0556 57.1667 33.8333 84.9444	58.0778 42.5222 68.0778 20.3000	86.2444 106.2444 78.4667 98.4667

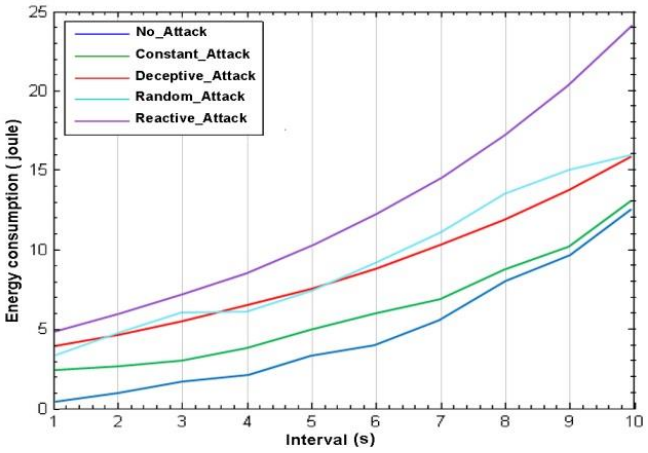

Fig. 1. Comparison of energy consumption of attacks in different interval.

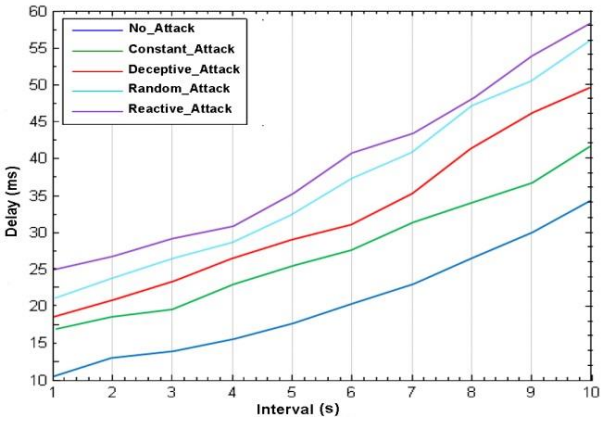

Fig. 2. Comparison of delay for send/receive packets in network after different attacks in different interval.

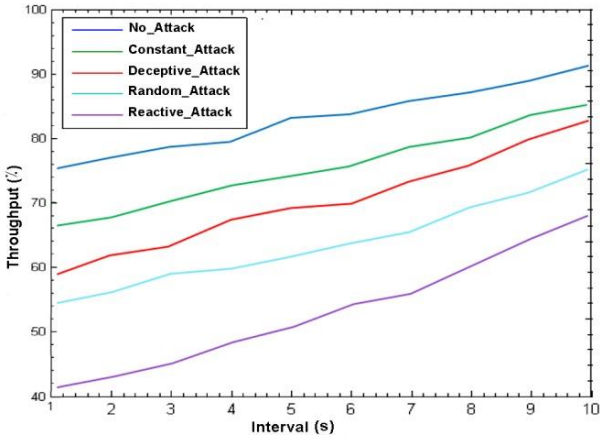

Fig. 3. Comparison of throughput of network after different attacks in different interval.

Fig. 1, 2 and 3 exhibit the analyses of the reactive, random, deceptive, and constant attacks, compared to the no-attack condition, by considering different time intervals in the sensor network. The analysis was performed by measuring three parameters of the sensor network. The operational throughput, latency, and energy consumption are, respectively, shown in Fig. 1, 2 and 3.

V. GAME THEORY MODEL

The signal game can be regarded as a game between two players (i.e. the destructive signal transmitter and the node (transmitter/receiver)), for which the equations can be made according to their performance and objective. The transmitter of the destructive signal is a player, which prevents the users' communication with each other through blocking the communication channels in the wireless network, and makes it impossible to transmit/receive data in the target channels. The node is a player, whose purpose is to efficiently utilize the network channels in order to increase the operational throughput of the whole network. Furthermore, the game can be modeled as a game between the destructive signal generator node and the observer node, in which the observer nodes are responsible for attach detection. In addition to the above strategic parameters, the following ones were also taken into account in the game:

- G_d : Gain, obtained from the attack detection.
- t : Time, required for periodic monitoring.
- A_D : Attack duration.
- P_c and P_p : Attack detection costs, using continuous and periodic monitoring.
- G_a : Attacker's gain for a successful attack.
- P_{cj} , P_{dj} and P_{rej} : Attack costs for constant, deceptive, and reactive destructive signal generators.
- T_s : Sleeping duration for the destructive signal generator node.
- T_i : Time interval, for producing packages and destructive signals.

A. Nash Equilibrium

In this section, the Nash equilibrium will be investigated for a signal game occurring in the network, in which none of the players has an independent motivation for changing the strategy.

In the game, every player attempts to maximize its final gain. Considering the number of strategies in the game on one side, and the possibility of occurring simultaneous attacks with different strategies on the other side, it can be concluded that achieving a deterministic Nash equilibrium will be very difficult. Therefore, achievement of a nash equilibrium can be examined through the probability. Hence, by using a combination of strategies and the probability distribution on the set of strategies, achieving the maximum gain in the final result will become feasible. Thus, m is considered as the probability of continuous monitoring in the channel and 1-m as the probability of periodic monitoring. If the time interval for constant and random attacks is extremely short, it will become nearly equal to constant attacks (i.e. like deceptive attacks).

$$m^* = \frac{G_a - P_T}{G_a(1 - t)} \qquad P_T = P_{rej} + P_{cj} + P_{dj} \tag{1}$$

$$j^* = \frac{G_d - M}{G_d A_D} \qquad M = P_p + P_c \tag{2}$$

B. Simulation Results

At this stage, the NS2 discrete event simulator was employed to implement the game theory strategies in order to confront the attacks. The parameters adjusted during the simulations are displayed in Table 1. The idle power, reception power, transmission power, and sleep power were considered according to the IEEE 802.15.4 radio model.

Fig. 4, 5 and 6, respectively, show the comparative evaluation for the no-attack condition, the suggested game-theory method, and the optimal detection strategy. At this stage, three parameters (including average energy consumption, latency, and operational throughput) were evaluated at different traffic time intervals.

Fig. 4 displays the average energy consumption in different conditions. The obtained results demonstrated that at the time of attacks, the suggested solution works more optimally over the optimal strategy and reduces the energy consumption. The main reason for representing the energy efficiency is that the detection mechanism of the game theory is based on the cross-layer detection, which helps to detect the attacks earlier and lower the energy consumption.

The main reason for representing the energy efficiency is that the detection mechanism of the game theory is based on the cross-layer detection, which helps to detect the attacks earlier and lower the energy consumption [28]. Another advantage of the game theory solution over the optimal strategy solution is that it attempts to achieve equilibrium and this helps to maintain the cooperation among the involved nodes. This cooperation can effectively assist to improve the energy consumption. Fig. 5 and 6 presented the average delay and the average operational throughput in the network, respectively.

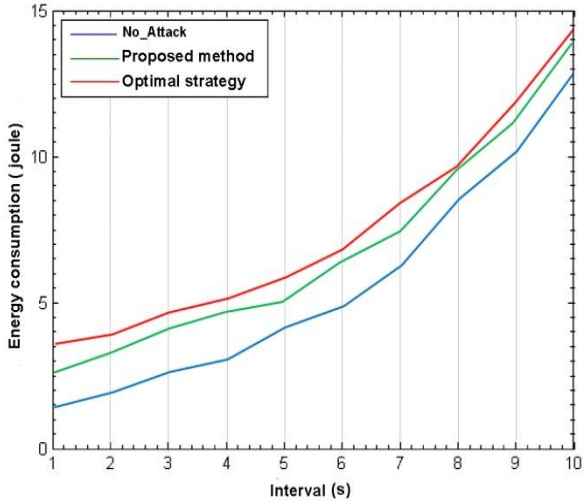

Fig. 4. Comparison of energy consumption between proposed strategies and optimal solution in variable traffic mode.

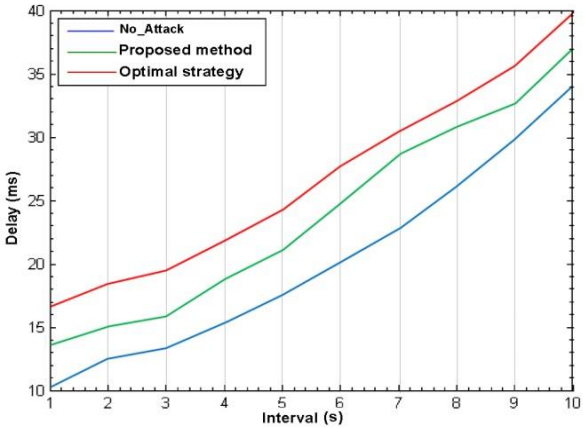

Fig. 5. Comparison of delay in network after attack between proposed strategies and optimal solution in variable traffic mode.

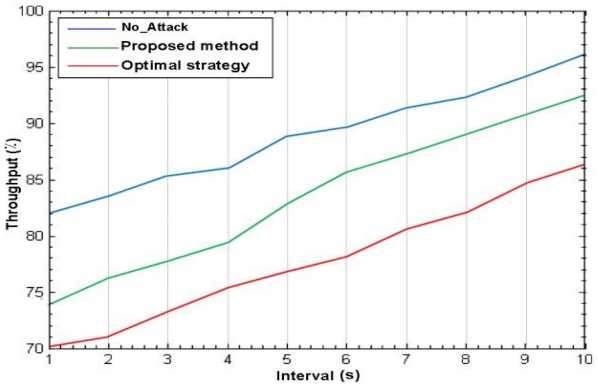

Fig. 6. Comparison of throughput between proposed strategies and optimal solution in variable traffic mode.

VI. Conclusions

Security threats are increasingly being developed due to the expansion of the networks connected to the Internet of Things as well as the lack of suitable mechanisms for counteractions. Wireless sensor networks are seriously vulnerable to attacks, and their ability of resistance against the attacks is one of the critical challenges in the development of these networks. Security in all levels of the Internet of Things is in correlation with its performance. Two main weaknesses of the traditional intrusion detection systems are as follows: 1) from a technical perspective, they are highly complicated; and 2) they rely on the temporary methods based on trial and error. Smart solutions have shown that although they have their own specific complexities, they are faster in speed and much more optimal in performance. The results obtained in this paper, which is based on the game theory, confirmed that smart methods can have better performance compared to the other strategies in terms of energy consumption (25-30%), latency, and operational throughput (10-15%).

Acknowledgment

This work has been sponsored by Islamic Azad University Safashahr/Iran to research and development operational program for the project “Improvement of Security in Internet of Things”. I am grateful to all of those with whom I have had the pleasure to work with this and other related projects.

References

[1] M. Abomhara, and G.M. Køien, “Security and privacy in the Internet of Things: Current status and open issues”, International Conference in Privacy and Security in Mobile Systems (PRISMS), 2014, pp. 1-8. DOI: 10.1109/PRISMS.2014.6970594

[2] D. Bandyopadhyay, and J. Sen, “Internet of things: Applications and challenges in technology and standardization”,Wireless Personal Communications, 2011, 58(1), pp. 49-69. DOI: 10.1007/s11277-011-0288-5

G. Gan, Z. Lu, and J. Jiang, “Internet of things security analysis”, International Conference of Internet Technology and Applications ,2011, pp. 1-4. DOI: 10.1109/ITAP.2011.6006307

[3] A.I. Abubakar, H. Chiroma, S.A.Muaz, and L.B.Ila, “A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems”, Procedia Computer Science, 2015, pp. 221-227. DOI: 10.1016/j.procs.2015.08.443

[4] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, “A survey of game theory as applied to network security”, In System Sciences (HICSS), 2010 43rd Hawaii International Conference, 2010, pp. 1-10. DOI: 10.1109/HICSS.2010.35

[5] M. Li, I. Koutsopoulos, and R. Poovendran, “Optimal jamming attacks and network defense policies in wireless sensor networks”, In INFOCOM 2007. 26th IEEE International Conference on Computer Communications, 2007, pp. 1307-1315.

[6] S. Mousavi , A. Mosavi , A.R. Varkonyi-Koczy ” A Load Balancing Algorithm for Resource Allocation in Cloud Computing”, Recent Advances in Technology Research and Education. INTER-ACADEMIA 2017. Advances in Intelligent Systems and Computing, 2017, vol 660. pp. 289-296. DOI: 10.1007/978-3-319-67459-9_36

[7] J.P. Hubaux, and L. Buttyan, “Security and cooperation in wireless networks”, The Economist. ISBN: 0521873711 9780521873710,(2017)

[8] A.D. Wood, J.A. Stankovic, and G. Zhou, “DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks. In Sensor, Mesh and Ad Hoc Communications and Networks”, 2007 SECON'07. 4th Annual IEEE Communications Society Conference, 2007, pp. 60-69. DOI: 10.1109/SAHCN.2007.4292818

[9] M. Tambe, M. Jain, J.A. Pita, and A.X. Jiang, “Game theory for security: Key algorithmic principles, deployed systems, lessons learned. In Communication, Control, and Computing (Allerton)”, 2012 50th Annual Allerton Conference, 2012, pp. 1822-1829.

[10] S.M. Mousavi, G. Fazekas, “Dynamic resource allocation using combinatorial methods in Cloud: A case study”, 16th international conference CogInfoCom 2017, IEEE Conference, 2017, pp. 221-232.

[11] T. Alpcan, and T. Basar, “A game theoretic analysis of intrusion detection in access control systems”, In Decision and Control, 2004. CDC. 43rd IEEE Conference, 2004, pp. 1568-1573. DOI: 10.1109/CDC.2004.1430267

[12] S. Mousavi, A. Mosavi , A.R. Varkonyi-Koczy, and G. Fazekas. “A novel algorithm for dynamic resource allocation in Cloud Computing”, Journal Acta Polytechnica Hungarica, March 2017, 14(3), pp. 80-101.

[13] T. Alpcan, and T. Başar, “Network security: A decision and game-theoretic approach”, Cambridge University Press, Book, 2010.

[14] Y.W. Law, M. Palaniswami, L.V. Hoesel. J. Doumen, P. Hartel, and P. Havinga, “Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols”. ACM Transactions on Sensor Networks (TOSN), 2009, pp. 6-13. DOI: 10.1145/1102219.1102234

[15] S. Sanyal, A. Shelat, and A. Gupta, “New Frontiers of Network Security:The Threat Within”, In Information Technology for Real World Problems (VCON), 2010 Second Vaagdevi International Conference on IEEE, 2010, pp.63-66. IEEE. DOI: 10.1109/VCON.2010.19

[16] L. Chen, and J. Leneutre, “A game theoretical framework on intrusion detection in heterogeneous networks”, IEEE Transactions on Information Forensics and Security, 4(2), 2009, pp.165-178. DOI: 10.1109/T IFS.2009.2019154

[17] M. Fallah, “A puzzle-based defense strategy against flooding attacks using game theory”, IEEE transactions on dependable and secure computing, 7(1), 2010, pp. 5-19. DOI: 10.1109/TDSC.2008.13

[18] S. Beckery, J. Seibert, D. Zage, C. Nita-Rotaru, and R. Statey, “Applying game theory to analyze attacks and defenses in virtual coordinate systems”, In Dependable Systems and Networks (DSN), 2011 IEEE/IFIP 41st International Conference, 2011, pp. 133-144.

[19] R. Muraleedharan, and L.A. Osadciw, “Jamming attack detection and countermeasures in wireless sensor network using ant system”, In Defense and Security Symposium, 2006, pp. 624-631.

[20] A.D. Wood, J.A. Stankovic, and S.H. Son, “JAM: A jammed-area mapping service for sensor networks”, In Real-Time Systems Symposium IEEE, 2003, pp.286-297. DOI: 10.1109/REAL.2003.1253275.

[21] M. Cagalj, S. Capkun, and J.P. Hubaux, “Wormhole-based antijamming techniques in sensor networks”, Transactions on Mobile Computing, 6(1), 2007, pp. 130-138. DOI: 10.1109/TMC.2007.250674.

[22] A. Mpitziopoulos, D. Gavalas, G. Pantziou, and C. Konstantopoulos, ”Defending wireless sensor networks from jamming attacks”, 18th International Symposium of Indoor and Mobile Radio Communications, 2007, pp.1-5. DOI: 10.1109/PIMRC.2007.4394775

[23] S. Mousavi, G. Fazekas, "Increasing QoS in SaaS for low Internet speed connections in cloud", The 9th International Conference on Applied Informatics, Eger, 2014, pp. 195-200. DOI: 10.14794/ICAI.9.2014. 1.195.

[24] W. Xu, T. Wood, W. Trappe, and Y. Zhang, " Channel surfing and spatial retreats: defenses against wireless denial of service", 3rd ACM workshop on Wireless security, 2004, pp. 80-89. DOI: 10.1145/102364 6.1023661.

[25] H. Wei, X. CHunhe, W. Haiquan, Z. Cheng, and J. Yi, "A game theoretical attack-defense model oriented to network security risk assessment", In Computer Science and Software Engineering, International Conference on IEEE, 2008, pp. 1097-1103. DOI: 10.1109/ CSSE.2008.1651.

[26] G. Zhou, T. He, J.A. Stankovic, and T. Abdelzaher, "RID: Radio interference detection in wireless sensor networks", In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 2005, pp. 891-901. DOI: 10.1109/INFCOM. 2005.1498319.

[27] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, " JAID: An algorithm for data fusion and avoidance on sensor networks", Pervasive and Mobile Computing, 5(2), 2009, pp. 135-147. DOI: 10.101 6/j.pmcj.2008.06.001.

[28] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks", Transactions on Mobile Computing, 9(8), 2010, pp. 1119-1133. DOI: 10.1109/TMC.2010.75