

Multiplayer reputation-based coalition game model (MRCGM) with dominant strategy analysis for detecting malicious attacks in wireless sensor networks

Amara S. A. L. G. Gopala Gupta *

Department of Computer Science and Engineering

Koneru Lakshmaiah Education Foundation

Vaddeswaram

AP

India

Syam Prasad Gudapati [†]

Department of Computer Science and Engineering

Sri Vasavi Institue of Engineering & Technology

Nandamuru

AP

India

Praveen Tumuluru [§]

Department of Computer Science and Engineering

Koneru Lakshmaiah Education Foundation

Vaddeswaram

AP

India

Abstract

Wireless Sensor Networks (WSNs) are turning into an essential portion of our lives. Devoid of assuring WSNs security (WS), there remain no broad implementations of WSNs. Because of sensor nodes' constrained capacities concerning computation, communication, and energy, giving protection to WSNs remains competitive. Indeed, the procedure of applying WS remains adaptable and vibrant that develops consistently. Attack-defend's crux in WS could be conveyed by collaborative schemes of interdependency when Game

* E-mail: amara_gupta@yahoo.com (Corresponding Author)

[†] E-mail: syamprasad.gudapati@gmail.com

[§] E-mail: praveenluru@gmail.com

Theory (GT) could be employed to consider communications amidst schemes of logical decision-makers. Hence, learning WS alongside GT possesses greater logic. This study proffers a Multiplayer Reputation-based Coalition Game Model (MRCGM) for seeking the false data injection amidst the nodes. An attacker attempts to sustain an ideal level of belief by correlating the identifications within the network (NW) to initiate a victorious transfer. Concurrently, the attacker should acquire a few charges for sustaining the trustability of its identifications. This proffered procedure employs this notion and turns the attack expensive by fixing a global threshold for nodes or identifications to be trustable and functional within the NW. Additionally, the beneficial function of the attacker and defender is as well described. The MRCGM has been correlated with 2 advanced methodologies like security-aware routing scheme employing repeated game (SARSRGM) paradigm and a Game-based Fuzzy Q-learning (GBFQL) scheme concerning diverse criteria. Consequently, the proffered MRCGM attains 124 kbps of Packet Drop Rate, 76.14% of energy efficiency, 96.1% of detection accuracy, 25.45% of energy consumption, and 102.45 ms of routing latency.

Subject Classification: 68M18.

Keywords: Malicious identification, Wireless sensor networks, Game theory, Reputation, Coalitional model, False data injection.

1. Introduction

Wireless Sensor Networks (WSNs) possess self-reliant Sensor Nodes (SNs) dispensed in the space that remain effortlessly deployable in hostile situations for surveilling environmental situations like noise, temperature, and pressure [1]. The network (NW) having RNs can be called multi-hop NWs. WSN gives a gateway (GW) that functions as an interface between the end-user for processing the data transferred by the SNs. These NW types have a few constraints [2]. Since the nodes remain broadly spread, WSNs will be open to diverse malicious attacks (MAs) like the malicious node (MN) could effortlessly penetrate the NW and the opponent node concealed as one of the NW nodes, misleading the rest of the nodes that exist within the NW and the NW crowding [3].

Because of the presence of an abundance of nodes in WSN, a protection should be provided at disparate levels that remain intricate [4]. The present study gives needful techniques for securing communication in WSN. Owing to the great range of disposition versatility, the WSN's implementations remain massive and could be widely classified into the surveilling and tracing classes [5].

Tracing implementations encompasses objects, animals, humans, vehicles, and armed forces opponent tracing [23].

For acquiring a pragmatic and possible WSN and because of the NW's procedure nature, Game Theory (GT) remains considered an alluring and appropriate base for achieving the model objective. The GT defines the players' conduct in a game [8]. According to this, sensors administer their procedures concerning power resources dedicated to sensing and interacting amidst themselves and with a global controller thereby the designated job can be finished efficiently as liked.

The Cooperative GT (CoGT) gives diagnostic tools for learning the logical players' conduct while these players collaborate and regard entire players' usefulness [9]. The Non-Cooperative GT (NCGT) as well encompasses an extensive scale of implementations within WSN. Notice that the NCGT remains chiefly concentrated upon every user's independent benefit instead of the entire NW's benefit [24]. This study's inspiration ensures applying WSNs security (WS) procedure remains an adaptable and vibrant procedure, which develops consistently.

The inputs of this study include:

- The proffered procedure performs as a decision support system (DSS) that vivaciously updates the trust values (TVs) amidst nodes and gives a quantifiable architecture and conceptual foundation for optimizing an NW protector in contemplating decisions precisely and efficiently.
- This procedure employs solely positive trust suggestions. When so ever a victorious communication betwixt nodes occurs, a positive TV will be designated to the node giving the services.
- To authenticate a victorious transfer, the nodes will be haphazardly requested to generate a few indisputable transfer pieces of evidence for creating this procedure strong and extra impervious opposing false trust updating requisitions.

2. Related Works

This segment addresses several MN identification paradigms in WSNs, and the procedure will be coherently described for detecting the disadvantages.

The study [12] introduces a new Artificial Noise Generation (ANG) scheme centered upon GT for enhancing the protection opposing privacy attacks within WSNs. ANS involves presenting intrusions in the spectrum for concealing the actual data.

The study [13] focuses on exploiting GT for identifying strong decentralized trust administration capable of enduring MNs forwarding untrue scores (US).

The study [14] highlights a clustering strategy within clustered WSNs for splitting the nodes into 3 kinds – malignant, skeptical, and usual nodes. The game's Nash equilibrium (NE) betwixt the usual and SNd has been confirmed to be present.

The study [15] uses the GT approach to design and reduce jamming attacks within WSN. A correlative assessment has been performed between the established optimized protection architecture – GT solution (GTS) and optimum strategy (OS) analyzed in the study.

The study [17] puts forth the Game of WSNs (GWSN). This remains an incomplete data game established with the employment of NCGT bearing the presumption that entire players remain logical.

The study [22] suggests a collaborative Game-based Fuzzy Q-learning (GBFQL) scheme for WSN.

The study [19] contemplates a security-aware routing scheme employing repeated game (SARSRG) paradigm in Mobile Ad-hoc NW optimizing secure routing.

The study [20] introduces a new technique called the self-improved sea lion optimization (SISLO).

In spite of the considerable studies upon the ID in the literature, no one deals with the issue in heterogeneous environments (HE). Inspired by this observance, the present study provides to the prevailing literature by giving the game-theoretic architecture of the NW ID issue in HE comprising of targets having disparate protection benefits. By classifying the consequential equilibrium procedure, we additionally infer the minimal surveillance resource requisite and the OS of the defender end in these HE.

3. Proffered Methodology

The present study has been intended to concentrate upon the GT paradigm for the building of a defense scheme for enhancing protection within WSN. Figure 1 illustrates the comprehensive framework for the proffered malignant identification methodology. At first, the WSN topology has been built by selecting the CHs amidst the NW ensued by building the FDI MA paradigm in the clinical framework. Subsequent to building, the Multiplayer Reputation-based CL Game Model (MRCGM) assists in identifying MNs that comprise reputation mechanism (RM),

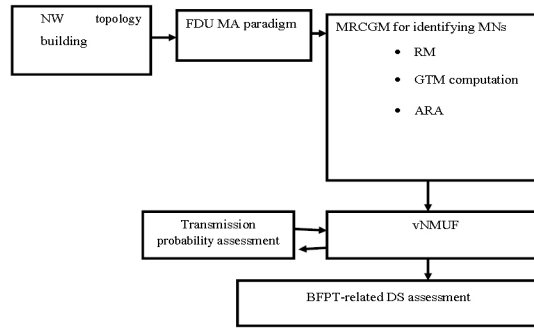


Figure 1

Comprehensive system framework to identify MA in WSN

global trust matrix (GTM) computation for threshold seeking, and attacker reward assessment (ARA) procedure.

The von Neumann-Morgenstern utility function (vNMUF) has been embraced to compute the utility function (UF) for the attacker as well as the defender. Lastly, the dominant strategy (DS) has been assessed employing Brouwer fixed-point theorem (BFPT) that, therefore, optimizes its anticipated utility above entire feasible real schemes.

3.1 NW paradigm

WSNs interact wirelessly by employing radio. In the radio communication system, the signal reception's indicator level can be indicated as RSSI (Received Signal Strength Indicator). This employs a 2.4 GHz band having a rough distance of up to fifty meters [21] and reinforces mesh topology.

The cluster has been shaped in order that every sensor by itself chooses to be designated as a GW with a few distinct feasibilities. A CH possesses a solo GW to a sink. This GW might or might not be a cluster member. CH sends GW Selection Message (GSM) to the chosen GW, and, subsequently, there remains feasibility to comprehend to what chosen node the GW remains connected. The GW SN disperses the transferred sensor readings (SRs) to each CH by determining what part of these SRs should transfer a CH h centered upon the workload (WL) of h . Furthermore, the EC amidst the CH as well remain nicely stabilized, so the CH quitting can be lessened consecutively lessening the cluster reformation.

$$E_{cl} = IE_{elec}(k-1) + l_{amp} E \sum_{k=0}^n d^2 \text{ to CH}$$

3.3 *Malignant identification employing GT paradigm*

The game paradigm stimulates the communication of the attacker and defender, weighs the test outcomes and identification efficacy out of intrusion identifier (the rate of identification's correct and incorrect), and sums up the NE for aiding identification for making logical reply decision lastly.

3.4 *MRCGM*

If a user employs the sensor NW (SNW) out of a cluster node, he/she remains a legal and authorized user and has particular rights given out of the system as per its protection policy.

3.5 *RM*

There remain N nodes within the Nw , for whatsoever $CL \ C \in 2^{N_6}$, that employed the feature function (FF) in designing a CL game (CG). The function assists in computing the independent nodes' PO like they could notice combining the CL as a logical decision because rationality remains a chief presumption in the GT.

The maximum admitting probability (MAP) can be provided as:

$$A_i(C) = \max_j C \left\{ \frac{\sum_{i \in C} P_{ij}}{|C|} \right\} C = \{i \in C, i \neq j, P_{i,j} \neq 0$$

The FF proffered will be,

$$v_t(C) = \begin{cases} 0, & \text{if } |C| = 1 \\ \alpha S_t(C) + \beta A_t(C) + \gamma D_t(C), & \text{if } |C| \geq 1 \end{cases}$$

Those weight criteria α , β , and γ could be employed for giving variableness for the nodes' FF. There remains no fixed nearby quantity for a specific node owing to the wireless settings' motile nature. For whatsoever node $i \in C$, $|C| > 1$, the independent PO share remains:

$$x_t(i) = \frac{1}{|C|} (\alpha S_t(C) + \beta A_t(C) + \gamma D_t(C))$$

The core mentions the total members' sum PO of the CL that should be above the solo PO's value of whatsoever independent node. This could be summed up as,

$$\sum_{i \in C} x_t(i) \geq v_t(C)$$

Table 1
Notations portrayal

Notation	Description
N	No. of nodes in the NW
C	Nodes' CL
G_i	Nodes within the node i's TR
$v_i(C)$	Protection FF for CL C
$S_i(C)$	SRt for the CL C
$T_i(C)$	CL C's TR
$P_{i,j}$	Collaboration of node i with node j probability
$A_i(C)$	Maximum admitting probability for CL C
$x_i(i)$	Node i's PO share
$\alpha, \beta, \text{ and } \gamma$	Weight
q_L, q_N, q_U	LT, neutral, and UT values accordingly
σ, λ	RV's rate of increment and decrement accordingly

If a node transmits its TR, it obtains an increase, and when this flops, the contrary takes place. A novel node, which links the NW, could be designated as a neutral reputation q_N . Entire reputations will be valid for a duration T_v . The Table 1 exhibits the Notations portrayal

3.6 GTM computation

Subsequent to computing the reputation, the trust matrix (TM) paradigm emerges for discerning what quantity FD has been instilled. The Trust Association's (TA) globality from node-a to node-b in the feature c_i exhibits the disparity betwixt this TA and entire TAs within the NW in which the trustee remains the node-b.

This could be exhibited as:

$$g_i(a, b) = 1 - \sum_{j=1}^n \frac{|\varphi_1(p_j, b) - \varphi_1(a, b)|}{2(n-1)}$$

When the value g_i remains one, the TR remains global in the feature c_i . This refers to the entire nodes within the NW possessing similar trust within node-b as the node-a. With the conception of weighted mean, innately, the array's GbT could be determined by,

$$t_s = \frac{\sum_{j \in S} t_j^2}{\sum_{j \in S} t_j}$$

In this, it is assured that an array's GT would be predominated by the nodes with high GT value. This would consistently remain between the

GT's minimal and maximal values of the members of the array S . The FT t_i of a node i could be prejudiced by the GT t_{si} of trust designation of the array si as per the expression, and, thus, the node i 's altered GT could be mentioned by,

$$\begin{aligned}
 t_i &= [t_i^p, t_{si}^q] \\
 t_i &= \left[\left(\frac{\sum_{j \in S_i} T_{ji} t_j}{\sum_{j \in S_i} t_j} \right) \cdot \left(\frac{\sum_{j \in S_i} t_j^2}{\sum_{j \in S_i} t_j} \right) \right] \\
 &= \left[\left(\frac{(\sum_{j \in S_i} t_j^2)^{\frac{q}{p}}}{(\sum_{j \in S_i} t_j)^{\left(1 + \frac{q}{p}\right)}} \right) \cdot \left(\sum_{j \in S_i} T_{ji} t_j \right) \right] \\
 &= \sum_{j \in S_i} \left(\frac{(e_i \cdot C \cdot \text{diag}(t), t)}{(e_i \cdot C \cdot t)^{(1+\infty)}} \right) \cdot (T_{ji}) \cdot (t_j)
 \end{aligned}$$

There remain N nodes within the NW, $i = 1, 2, \dots, N$, hence, those arrays of N expressions could be exhibited in the matrix format as,

$$t = (D \cdot T^t \cdot t)^{\left(\frac{1}{1+\infty}\right)}$$

3.7 ARA

As the output of matrix computation, the victim nodes (VNs) could be concluded. In a specific round i , the attacker's instant reward (IR) r_i remains the VNs in the round i when it has avoided identification by the close of the round i and zero when it has been identified in or prior to the round i .

The attacker's sum reward can be determined by,

$$\begin{aligned}
 J &= r_0 + \gamma r_1 + \gamma^2 r_1^2 + \gamma^3 r_1^3 + \dots \\
 &= \sum_{i=0}^{\infty} \gamma^i r_i
 \end{aligned}$$

in which γ depicts the discount factor, $\gamma < 1$ depicts that the attacker consistently joins low significance to an upcoming reward. The attacker's action will be depicted x as per the VNs' quantity per round. His sum discounted reward J remains a function of x .

$$J(x) = E(\text{total reward} | x \text{ victim nodes per round})$$

$$= \Pr(\text{false negative} | x \text{ victim nodes}) \cdot (x + \gamma J(x))$$

Providing

$$J(x) = \frac{x \cdot \Pr(\text{false negative} | x \text{ victim nodes})}{1 - \gamma \cdot \Pr(\text{false negative} | x \text{ victim nodes})}$$

The attacker's RF lessens to:

$$J(x) = \frac{(1-p)^x \cdot x}{1 - \gamma(1-p)^x}$$

3.8 UF assessment

It is indirectly presumed that the utilities, which describe the bargaining games (BGs), have been inferred out of independent's vNMUF.

$$Ud = - \left[b - (I \times C) - \left\{ \frac{\tau \times N}{1 - \tau} - 1 \right\} \times C^n \right]$$

The attacker requests services out of a service provider node (SPN). An SPN could select 'Serve' or 'Do not serve'.

3.9 DS

In this, it will be performed by employing BFPT by setting strategic communications betwixt the attacker and the defender.

- For the attacker/typical node: Provided the strategy of malignant identification, every kind θ of a node assesses the utility out of forwarding a message $a1$ as $\sum_{a2} (a2 | a1) u1(a1, a2, \theta)$ and $p(\theta)$ that lays weight upon $a1$ solely when it remains amidst the optimizing messages within the anticipated utility.
- For the malignant identification: This could advance in 2 phases. Initially, for each message $a1$, which has been forwarded with positive probability (PP) by some kind θ , the identification employs BFPT for calculating the posterior probability analysis, in which $a1$ occurs out of every kind θ .

4. Performance Analysis

This proffered model was performed in the NW simulator. This simulation's chief objective has been to enhance protection in the collaborating nodes' appearance. One hundred nodes have been randomly

structured in a 500 m x 500 m area of focus. The interaction array remained 20 m. Nodes followed the Random Waypoint paradigm, which discerns the attainability of correlation paths in MANET. The proffered MRep_CGM strategy assessed the malignant attacker’s conduct. This proffered strategy’s execution has been analyzed by assessing this with the associated SARSRG and GBFQL schemes concerning PD rate, mean utility, identification precision, energy utilization, and routing latency. The simulation outcomes have been computed by modifying the MNs’ percentage from ten to sixty, which might each cause the packet dropping.

Table – 2 exhibits the PDR correlation.

Table 2
PDR assessment

No. of MNs	SARSRG	GBFQL	MRCGM
10	96	52	20
20	156	102	25
30	248	186	59
40	356	248	82
50	425	345	106
60	548	423	124

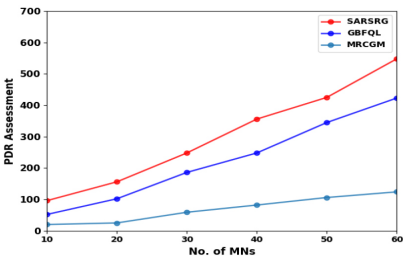


Figure 3
PDR Correlation

Figure 3 illustrates the PDR correlation betwixt the prevailing SARSRG and GBFQL methodologies and the proffered MRCGM methodology.

Table 3
EE assessment

No. of MNs	SARSRG	GBFQL	MRCGM
10	5.47	11.47	15.31
20	12.79	17.38	25.17
30	18.62	21.75	39.21
40	29.88	35.14	53.79
50	36.78	43.16	65.49
60	45.32	53.49	76.14

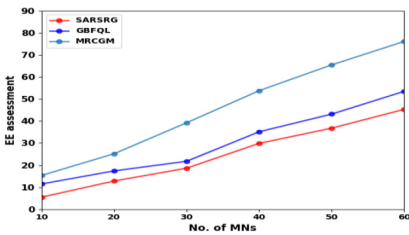


Figure 4
EE Correlation

Table – 3 exhibits the EE correlation and figure 4 illustrates the EE correlation betwixt the prevailing SARSRG and GBFQL methodologies and the proffered MRCGM methodology.

Table – 4 exhibits the DA correlation and figure 5 illustrates the DA correlation betwixt the prevailing SARSRG and GBFQL methodologies and the proffered MRCGM methodology.

Table 4
DA assessment

No. of MNs	SARSRG	GBFQL	MRCGM
10	80.15	85.33	97.48
20	78.14	86.96	95.18
30	79.13	87.23	96.48
40	80.49	86.45	95.47
50	81.25	85.17	97.56
60	79.16	86.14	96.15

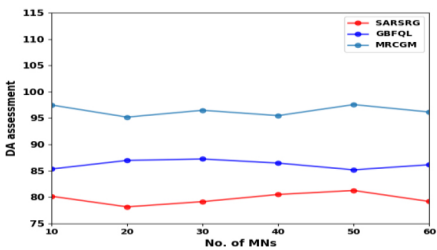


Figure 5
DA Correlation

Table 5 exhibits the EC correlation.

Figure 6 illustrates the EC correlation betwixt the prevailing SARSRG and GBFQL methodologies and the proffered MRCGM methodology.

Table 5
EC assessment

No. of MNs	SARSRG	GBFQL	MRCGM
10	8.25	5.13	3.76
20	13.76	11.88	5.22
30	21.13	18.72	8.32
40	29.25	25.46	12.74
50	41.47	32.28	19.86
60	54.89	46.16	25.45

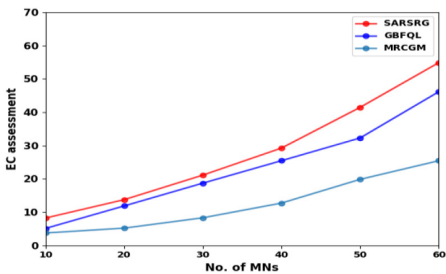


Figure 6
EC Correlation

Table 6 exhibits the RL correlation

Table 6
RL assessment

No. of MNs	SARSRG	GBFQL	MRCGM
10	88.28	52.75	25.16
20	112.72	86.27	33.77
30	139.75	102.75	56.19
40	182.47	156.47	71.68
50	235.17	213.48	86.17
60	289.17	265.18	102.45

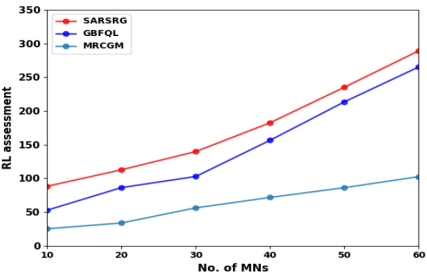


Figure 7
RL Correlation

Figure 7 illustrates the RL correlation betwixt the prevailing SARSRG and GBFQL methodologies and the proffered MRCGM methodology.

Table - 7 exhibits the overall comparative analysis betwixt the prevailing SARSRG and GBFQL methodologies and the proffered MRCGM methodology.

Table 7
Overall Analysis

Criteria	SARSRG	GBFQL	MRCGM
PDR	548 (packets)	423 (packets)	124 (packets)
EE	45.328 (%)	53.497 (%)	76.145 (%)
DA	79.16 (%)	86.14 (%)	96.15 (%)
EC	54.89 (%)	46.16 (%)	25.45 (%)
RL	289.17 (ms)	265.18 (ms)	102.45 (ms)

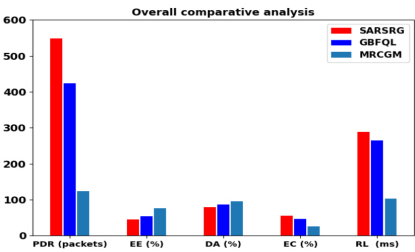


Figure 8
Overall Analysis

Figure 8 illustrates the Overall Comparative Analysis of the proposed and the existing methodology of the various techniques.

5. Conclusion

WS's area remains a much more significant study discipline. Because of the SNs' constrained abilities, giving protection to SNWs remains a competing job; nevertheless, there remain no famous WSNs implementations devoid of regarding WS. GT possesses the ability to evaluate an enormous quantity of feasible situations prior to executing the activity. The trajectory of implementing AT to WS remains potential. These strategies as well miss active updating of trust and correlating trust threshold and remain liable to denigrating or DoS attacks. This study proffers a DSS called MRCGM for handling aforesaid problems by defender have been given concerning charges collected upon obtaining and sustaining individualities. Consequently, this proffered MRCGM attains 124 kbps of Packet Drop Rate, 76.14% of energy efficiency, 96.1% of detection accuracy, 25.45% of energy consumption, and 102.45 ms of routing latency.

References

- [1] Kumar, M., Mukherjee, P., Verma, K., Verma, S., & Rawat, D. B. Improved deep convolutional neural network based malicious node detection and energy-efficient data transmission in wireless sensor networks. *IEEE Transactions on Network Science and Engineering* (2021).
- [2] Abdalzaher M, Seddik K, Elsabrouty M, Muta O, Furukawa H, Abdel-Rahman A. Game theory meets wireless sensor networks security requirements and threats mitigation: a survey. *Sensors* 16(7):1003 (2016) DOI 10.3390/s16071003.
- [3] Agarwal A, Sharma P, Alshehri M, Mohamed AA, Alfarraj O. Classification model for accuracy and intrusion detection using machine learning approach. *PeerJ Computer Science* 7(3): e437 (2021).
- [4] Kiennert C, Ismail Z, Debar H, Leneutre J. A survey on game-theoretic approaches for intrusion detection and response optimization. *ACM Computing Surveys* (2018).
- [5] Valli R., Dananjayan P. Utility enhancement by game theoretic approach using square grid topology in WSN. *Proceedings of 2011 International Conference on Process Automation, Control and Computing (PACC 2011); Coimbatore, India. 20–22 July 2011.*
- [6] Varsha Himthani, Vijaypal Singh Dhaka, Manjit Kaur & Prashant Hemrajani. V-Net architecture based advanced visually

- meaningful image encryption technique, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:7, 2183-2194 (2022), DOI: 10.1080/09720529.2022.2133255.
- [7] Sadkhan, S. B., & Ayad, M. Game Theory Role in Wireless Network Security–Status, Challenges and Future trends. In 2021 International Conference on Advance of Sustainable Engineering and its Application (ICASEA), pp. 230-235. IEEE (2021, October).
- [8] Ho, J. W. Game Theoretic Modeling for Mobile Malicious Node Detection Problem in Static Wireless Sensor Networks. *International Journal of Internet, Broadcasting and Communication*, 13(1), 238-242 (2021).
- [9] Anand, R., Sudarsanam, P., & Challa, M. Fault-Tolerant Cluster Head Selection Using Game Theory Approach in Wireless Sensor Network. In *Pervasive Computing and Social Networking*, pp. 399-416. Springer, Singapore (2022).
- [10] Medhavi Malik, Mohit Kumar, Vinay Kumar, Arun Kumar Gautam, Shikha Verma, Sarvesh Kumar & Dinesh Goyal. High level browser security in cloud computing services from cross site scripting attacks, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1073-1081 (2022). DOI: 10.1080/09720529.2022.2072434.
- [11] Singh R, Singh J, Singh R. Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks. *Wireless Communications and Mobile Computing*, (2):1–14 (2017).
- [12] Romero, E., Blesa, J., & Araujo, A. An adaptive energy aware strategy based on game theory to add privacy in the physical layer for cognitive WSNs. *Ad Hoc Networks*, 92, 101800 (2019).
- [13] Esposito, C., Tamburis, O., Su, X., & Choi, C. Robust decentralised trust management for the internet of things by using game theory. *Information Processing & Management*, 57(6), 102308 (2020).
- [14] Li, Y., & Wu, Y. Combine clustering with game to resist selective forwarding in wireless sensor networks. *IEEE Access*, 8, 138382-138395 (2020).
- [15] Clifford, D. C. Game Theoretic Model for Jamming Attack Mitigation in Wireless Sensor Networks. *Journal of Engineering and Applied Sciences*, 18(1), 317-328 (2021).

- [16] Wu, Y., Kang, B., & Wu, H. Strategies of attack–defense game for wireless sensor networks considering the effect of confidence level in fuzzy environment. *Engineering Applications of Artificial Intelligence*, 102, 104238 (2021).
- [17] Kantzavelou, I., Maglaras, L., Tzikopoulos, P. F., & Katsikas, S. A multiplayer game model to detect insiders in wireless sensor networks. *PeerJ Computer Science*, 8, e791 (2022).
- [18] Meryem Cherkaoui Semmouni, Abderrahmane Nitaj & Mostafa Belkasmi. Cryptanalysis of RSA with smooth prime sum, *Journal of Discrete Mathematical Sciences and Cryptography* (2022), DOI: 10.1080/09720529.2021.2000152.
- [19] Balaji, S., Julie, E. G., Robinson, Y. H., Kumar, R., & Thong, P. H. Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. *Computer Standards & Interfaces*, 66, 103358 (2019).
- [20] Kagade, R. B., & Jayagopalan, S. Optimization assisted deep learning based intrusion detection system in wireless sensor network with two-tier trust evaluation. *International Journal of Network Management*, e2196 (2022).
- [21] N. Baker, “ZigBee and Bluetooth strengths and weaknesses for industrial applications,” *IEEE Comput. Control Eng.*, vol. 16, no. 2, pp. 20–25 (2005), doi: 10.1049/cce:20050204.
- [22] S., Wei, C., Pan, L., & Yan, G. Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs. *Computer standards & interfaces*, 56, 107-115 (2018).
- [23] Almaiah, M. A. A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, pp. 217-234, (2021). Springer, Cham.
- [24] Ranaweera M, Seneviratne A, Rey D, Saberi M, Dixit VV. Anomalous data detection in vehicular networks using traffic flow theory. In: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). Piscataway: IEEE, 1–5 (2019).