International Journal of Research in Circuits, Devices and Systems

E-ISSN: 2708-454X
P-ISSN: 2708-4531
IJRCDS 2023; 4(1): 22-28

www.circuitsjournal.com
Received: 12-10-2022
Accepted: 13-11-2022

Narasambattu Sri Sishvik
School of Computer Science Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Corresponding Author:
Narasambattu Sri Sishvik
School of Computer Science Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Next generation infotainment system for automobiles with vehicular ADHOC network

Narasambattu Sri Sishvik

Abstract
The automobile industry has been innovating and stuffing a lot of technological features ever since the ECU became the brain of the vehicle. But we will be seeing more on how the infotainment system is going to become advanced and an important part of a vehicle in the near future, not just to make it more luxurious and affordable than ever but also improving the safety part. Like changing the ride quality, traction control, ABS, EBD, etc, right to the specifics of each component. With advantages, we might be also able to find the limitations of it. The Mobile Ad-Hoc Network (MANET) incorporates a collaborative networking scenario, where dynamic host movement results in frequent topology changes. In MANET, nodes cooperate during route establishment, and the data packet must travel from source to destination through multi-hop intermediate links. The nodes in a MANET can be localized in a restricted zone, where manual intervention to set-up fixed infrastructural support is practically infeasible. However, cooperative packet forwarding and data transmission is quite a common scenario in the context of MANET. Still, due to dynamic topological changes, weak, intermittent links appear within one-hop communication. This leads to a higher possibility of packet drop events and also increases the retransmission scenario, which affects the energy performance of the network. Addressing this issue, the study models a novel and intelligent packet forwarding approach based on the game theory, where trust evaluation in terms of node reputation factor also plays a very vital role. The approach also enforces an incentive modelling to stimulate the cooperation between mobile nodes during the MANET routing scenario. Here's how the limitations might affect, when the legacy system of Vehicular Adhoc network might be overburdened/ overused with channel capacity, high latency, poor optimisation and hetero-network processing. Thus, this paper offers a comprehensive and detailed research of what and how the current state of the art infotainment systems can be improvised to be efficient, safer and advanced to meet the expectation of an automobile manufacturer and the users of the automobile as well.

Keywords: Infotainment system, vehicular ADHOC network, cloud environment, latency

1. Introduction
Mobile Adhoc Networks (MANETs) relate to a special type of wireless ad-hoc network, where bumps are mobile and move singly in any direction with tone- organizing capabilities [1, 2]. The crucial-features of MANET include its own dynamic characteristics due to knot mobility and also decentralized networking scripts where the network forms for a temporary interval of time to negotiate a specific task. The term decentralized means that the network conformation during the communication script doesn't dodge reliance on pre-existing communication infrastructural chines [3, 4, 5]. MANET includes a wide range of use-cases, like military dispatches, disaster operation in confined mortal areas, etc. The trend of the emphasized exploration in MANET is substantially concerned about the timely prosecution of the task with dependable data transmission and event indeed if unreliable radio- link is present during the communication script [6].
A collaborative event of packetforwarding is a ultramodern approach to insure the time-dependent high- outturn wind in MANETs. Still, encouraging the other bumps in the MANET terrain for packet forwarding for an individual knot's tone- interest is a veritably gruelingtask. However, also the possibility of intermittent link-breakage between one- hop neighbours increases, If intermediate bumps aren't meetly chosen during the route- set up and packet forwarding between source to the destination knot. Further, the unreliable communication link also increases the probability of packet drops and retransmission events. This means the mileage factor of different packet forwarding strategies will go down and also will affect the energy and outturn performance in MANET ultimately [7, 8]. From the security standpoint also, the collaborative packet forwarding strategies should be robust and

flexible enough to deal with every possible route change and also cleave to the communication protocol directions without compromising the QoS and energy parameters. Still, the traditional packet forwarding approaches are shrouded with a set of design limitations and fail to stimulate selfish bumps to cooperate in communication [9]. The high reasons can be that in MANET, utmost of the mobile bumps generally operate with limited energy and memory capacity. This makes a knot to come tone- centered, and that way, it only participates in communication when it brings the knot more benefits for its interest than cost [10, 11]. This way, the possibility of the presence of tone- centered bumps set amid the other pivotal networking factors leads to dislocation of the overall communication and network performance from both energy and security view- point [12]. Thus, by addressing the design loopholes in the traditional data encouraging approaches, the proposed study realizes that it's essential to design a medium that can effectively encourage a knot in packet forwarding indeed if the transmission happens through unreliable links. This way, a high outturn success rate is envisaged with maximum packet- delivery rate. The medium concertedly incorporates the game fine model along with a trust- grounded character evaluation strategy to increase the mileage factor of packet forwarding schema. During the packet forwarding cases, responsibility of each knot is validated and it also enforces collaborative prices. The attack-resistant security modeling frame is formulated and estimated with respect to birth approaches, and the performance metric for confirmation includes energy, outturn, network burden, and also the rate of successful packet forwarding.

2. Literature review

This section explores the most significant and affiliated literature, which is studied for the investigational analysis purpose. In [55-70], it outlines the exploration problem that corresponds to the design limitations of the being system. A. Evolutionary Game Theoretical Concept The experimental analysis shows that the evolutionary game theoretical approach is most popular since through mathematics, it can dissect the strategic relations among the MANET decentralized bumps, which act as decision- making agents. The authors in [13] introduced anon-cooperative game modelling to defend different attack scripts in MANETs. The system model incorporated a new intrusion discovery medium where conduct between a brace of the bushwhacker and regular bumps are considered as anon-cooperative andnon-zero game. Authors in [14] also proposed an analogous approach to defend against maximum possible murderous security pitfalls in MANET. The study of authors in [15] also directed their exploration towardscross-layer optimization. For this purpose, it has incorporated a game proposition- grounded approach to ameliorate the communication script in vehicular networks.

Also, authors in [16, 17, 18] also extemporized a collaborative game theoretical approach to easing the communication performance of MANETs by relating the froward bumps. B. Incitement- Grounded Abstract Medium For numerous times, there have been colorful exploration approaches to strengthen the collaborative packet-forwarding programs in MANET where incitement- grounded mechanisms encouraged tone- centered bumps to bear like a normal knot and share in cooperative forwarding schema. In MANET, it's substantially observed that a regular knot on tone-generated data packets as well as of other bumps anyhow of its resource application factor. On the other hand, a tone-centered knot or vicious knot will tend to drop the data packets to reserve as important coffers as possible to negotiate its intended task. Thisnon-cooperative intention, in the long run, affects the communication performance from trustability and effectiveness points of view. This incurs a situation where the network becomes susceptible to colorful forms of murderous attacks. The incitement- grounded strategies are classified into three major orders, which can be shown in [61]. Virtual currency results include tamper-evidence tackle, trusted thirty party, etc.

Character value- grounded approaches can either be global character- grounded systems or original character grounded systems. Game proposition- grounded results find categorization into onestage game or repeated game. The authors in [19] introduced a credit- grounded approach which is simply meant for the detention tolerant networks. The medium is designed grounded on a service- position precedence. The outgrowth of the study shows that it's quite a useful schema. Still, the credit- grounded approaches are substantially plant helpless against conspiracy attacks and also don't insure a advanced discovery rate when tone-centered knot identification is concerned. It also lacks energy effectiveness, but the outturn performance is plant entirely satisfactory. The authors in [20, 21, 22] also directed their exploration in a analogous direction. The credit-grounded incitement medium refers to a policy where the knot gets stimulant to route the data packets at a specific cost trait. In the environment of trust and character-grounded medium, each knot assesses its conterminous neighbour's character factor which is estimated grounded on the knot conditioning and depending upon the probabilistic factor, each knot chooses its conterminous neighbour during the packet forwarding paradigm. There live different collaborative strategies which are explored by the authors in the studies [23-28], where game-theoretical approaches are applied to enhance the network performance concerning acceptable QoS and energy factors. The near conclusion of the studies exhibits how different types of collaborative strategic styles similar as repeated games,non-cooperative games, evolutionary game approaches, etc. insure an advanced degree of packet forwarding among bumps with the objectification of tone- literacy capabilities. This makes these approaches suitable and more applicable to the futuristic MANET intelligent operations.

From a security standpoint also, it can be stated that these approaches insure better packet delivery rate and energy performance to some extent. Also, the ferocious medium with an evolving game approach can fluently identify the tonecentred knot conditioning and the network intrusion it causes for its benefits. Another analogous collaborative packet forwarding approach by the authors in [29] is designed grounded on the principle of dynamic incitement medium. In this approach, each knot selects a specific strategy to identify a tone-centred knot within its vicinity and passively encourages it to cooperate in communication. After assaying colorful exploration approaches, it's observed that collaborative packet forwarding grounded on the evolving game model can insure a better outturn wind indeed if a noisy one- hop untrustworthy link is established between two bumps. Colorful approaches claim that the evolutionary game, if intelligently modelled and enhanced, can insure not only better outgrowth in terms of energy but also an

effective network performance. The approach, in numerous cases, has been plant to effectively identify the possibility of the tone-centred knot conditioning in terms of intrusion and successfully engage them in collaborative packet forwarding. Therefore, it's considered as one of the most suitable approaches to insure better outturn and energy performance in dynamic MANET operations. Farther check on colorful recent approaches related to vicious knot discovery and termination in MANET leads to a study by authors in [30] that introduced a distinct approach of calculation termination of cluster head election medium and also employ a security medium grounded on Finite State Machines (FSM) to identify and mitigates pitfalls in MANET. Another approach by the author in [31] also mechanized a security approach which can help in securing the information during distributed routing of MANET. The outgrowth of the study is observed relatively promising but still the design lacks compass of extemporization as it's validated through only simulation study to secure information which travels across MANET. Another study by authors in [32] also worked in the analogous line of exploration and envisaged for a better compass of optimization of AODV routing protocol by strengthening its conventional security features. Still, the limitation of this approach is it's only robust against Black- hole attacks. Another study by the authors in [33] estimated the performance of security aspects of DSR protocol in MANET routing terrain. An original positioning approach to identify meddler knot in MANET is plant in the study of [34]. A new authentication and security approach is mechanized in the study of authors in [35] to secure the communication and routing script in MANET. The outgrowth of the study shows that the approach takes vastly lower time to validate the bumps who wants to join the network. The farther section outlines the exploration gap grounded on the theoretical analysis, which assists in formulating the proposed design methodology by taking the nascence's as a reference model.

3. Problem finding and gaps

The expansive check and analysis of the being studies reveal that utmost of the traditional approaches have design loopholes and can be described as follows • The collaborative data forwarding mechanisms and their strength factors are substantially overlooked during the design and development of security protocols and intrusion discovery systems. Also, veritably many studies are plant to dissect the problem of packet-forwarding between bumps with an effective and evolving game approach. Studies have claimed that the game modelling approach can encourage collaborative data forwarding and can also increase the outturn performance in MANET routing [13, 14, 36].

- Despite having colorful advantages, limited studies have cited game- grounded decision modelling to assess individual knot conduct in MANET dynamic routing [28, 29, 37]. Also, in numerous cases, the one- hop data transmission model to pretend the tonecentred knot in packet forwarding is ignored.
- Utmost of the credit and character- grounded mechanisms are plant suitable only when small and medium scale operations are concerned, but utmost of the time, not ideal with the large scale MANETs [20, 21, 22, 29].
- The being ways of incitement- grounded mechanisms encourage a tone-centred knot in collaborative packet forwarding and more likely to enhance the outturn performance. Still, due to the iterative process of retransmission, the energy consumption rate and network burden may increase [9, 19, 38].
- Utmost of the ways don't involve a penalty medium if tone-centred bumps are detected. But with a penalty, the tone-centred knot will either help in packet forwarding or flee to another cluster of the network to save its limited coffers. This way, the networking coffers can be effectively employed, and the possibility of packet drops will be minimized [39].
- Both credit and character- grounded mechanisms don't insure energy-effective performance and advanced resiliency against conspiracy attacks. On the other hand, the character- grounded approach also collectively doesn't guarantee advanced discovery delicacy of tone-centred bumps in MANET [6, 7, 19, 22].
- The game proposition- grounded approach lacks effectiveness when it comes to outturn and energy performance and has not been studied much in the history [16, 17, 18].
- The analysis of the being literature also shows that veritably many approaches concertedly address the energy and network performance issues. This is because their intelligent game Page 2 of 5 models might have handed confluence towards better outturn result but don't insure effective energy and detention performance in the real- time environment from the operation demand standpoint [23-40].

Hence, there are algorithms for relating the tone-centred bumps during the packet forwarding conditioning but veritably lower studies concerned about designing the algorithms with minimum computational conditions similar as memory, processing time, etc. [21, 22, 39]. From the time complexity view- point, if the packet forwarding algorithm follows the notion of distributed computing approach, also it should be a light- weight computational model that can be fluently stationed for sustainable service delivery prosecution; besides having a positive influence on controlling the detention constraints in critical operations of MANET [40-50]. The current study thereby attempts to develop a robust jointapproach of game and character which can encourage and stimulate anon-cooperative knot in maximum packet-forwarding and insure an advanced degree of outturn with minimum communication outflow and transmission burden in MANET [50-70].

4. Conclusion

In the MANET routing and communication script, it's essential to maximize the possibility of packet forwarding indeed in the presence of unreliable radio links. Still, as MANET operates with resource- constrained tone-configuring mobile bumps which generally move in any direction and the topology stoutly changes every time, in the absence of a centralized authority, it's challenging to ensure minimal energy consumption satisfying the QoS constraints with advanced outturn outgrowth. The study introduces an intelligent packet forwarding approach grounded on an evolutionary one- hop packet forwarding game model that assesses the communication script in the presence of unreliable links. Targeting the real- time use cases, the study modelled the system considering strong hypotheticals and

designed the packet forwarding schema with a cut-off value corresponding to the upper bound ofre-transmission count. Then, the upper limit of retransmission count is modelled as $1 \leq p \leq ts$ for a brace of bumps that can be I, J.

The rate of confluence is also stabilized by assessing the proposed game- grounded packet forwarding strategies. The condition of confluence to stable countries is anatomized with respect to the high three factors, which are upper bound of re-transmission factor, collaborative price factor, and the probability of successful packet forwarding with cooperative strategy, independently. The entire system model is estimated in a numerical computing terrain, and the outgrowth attained is further anatomized, considering different parameters. The experimental result shows how these three high factors appreciatively impact the rate of confluence and also insure advanced outturn and lower possibilities of packet drops. The quantified outgrowth also indicates that the energy performance enhancement in the proposed system environment is roughly 50 as compared to the conventional birth results, and also the system outperforms other models in terms of outturn and communication burden. The outturn performance enhancement is attained roughly 30, which is quite an effective outgrowth as the proposed system ensures a advanced probability of successful data transmission with upper boundedre-transmission number. With a robust academic base, the study forms a theoretical base to give an advanced degree of packet forwarding in unstable radio links of dynamic MANET surroundings. It's also observed that the system significantly identifies the tone-centred knot intrusion and diverts them to cooperate in packet forwarding with lower network outflow.

Theoretical modelling is intended to break the below-pronounced exploration issue to a significant extent. The design of the frame takes birth logical approach as a reference model by assessing the affiliated studies of the history. Still, the outgrowth shows that the rate of packet drop is reduced to a lesser extent in the proposed approach but still it has a better compass to be extemporized for different IoT network objects. Another significant point to be stressed is the system evaluation only considers maximum 900 mobile bumps but it's observed that till 700 the network burden remains minimal for the system but it increases when the number of bumps are set to 900 due to increase in the size of data business. Still, the system performance has not been estimated taking IoT objects into consideration and also the computational complexity can be optimized to a lesser extent. This work can be acclimated for a unborn line of exploration which can include minimizing the complexity of network outflow and energy issue in IoT routing dynamics when gauged up with colorful networking realities and objects. The operating conditions also differ from the traditional approaches of routing and communication convention protocols. It also envisaged a less complicated and robust approach to manage the routing performance with further dependable operations in dynamic IoT.

References

1. Khan BUI, Olanrewaju RF, Anwar F, Najeeb AR, Yaacob M. A survey on MANETs: Architecture evolution applications security issues and solutions, Indonesian J. Electr. Eng. Comput. Sci., vol. 2018;12:832-842.
2. Olanrewaju RF, Khan BUI, Anwar F, Pampori BR, Mir RN. MANET security appraisal: Challenges essentials attacks countermeasures & future directions, Int. J Recent Technol. Eng. (IJRTE). 2020;8(6):3013-3024,
3. Raghunandan GH, Chaithanya GH, Hajare R. Independent robust mesh for mobile adhoc networks, Proc. 4th Int. Conf. Electron. Commun. Syst. (ICECS), 2017, 125-128.
4. Kumar S, Saini ML, Kumar S. A survey: Swarm based routing algorithm toward improved quality of service in MANET, Int. J. Manage. Technol. Eng. 2018;8(5):311-322.
5. Jamal T, Butt SA. Malicious node analysis in MANETS, Int. J. Inf. Technol. 2019 Dec;11(4):859-867.
6. Almazyad S. Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks, Neural Comput. Appl. 2018 May;29(9):597-607.
7. Rama Abirami K, Sumithra MG. Preventing the impact of selfish behavior under MANET using neighbor credit value based AODV routing algorithm, Indian Acad. Sci. 2018 Apr;43(4):1-7.
8. Bisen D, Sharma S. Fuzzy based detection of malicious activity for security assessment of MANET, Nat. Acad. Sci. Lett. 2018 Feb;41(1):23-28.
9. Seregina T, Brun O, El-Azouzi R, Prabhu BJ. On the design of a reward-based incentive mechanism for delay tolerant networks, IEEE Trans. Mobile Comput. 2017 Feb;16(2):453-465.
10. Lau G, Al-Sabah M, Jaseemuddin M, Razavi H, Bhuiyan M. Context-aware RAON middleware for opportunistic network, Pervas. Mobile Comput. 2017 Oct;41:28-45.
11. Khan BUI, Olanrewaju RF, Anwar F, Shah A. Manifestation and mitigation of node misbehaviour in adhoc networks, Wulfenia J. 2014;21(3):462-470.
12. Rajesh M. A review on excellence analysis of relationship spur advance in wireless ad hoc networks", Int. J. Pure Appl. Math. 2018;118(9):407-412.
13. Poongothai T, Jayarajan K. A noncooperative game approach for intrusion detection in mobile adhoc networks, Proc. Int. Conf. Comput. Commun. Netw. 2008 Dec, p. 1-4.
14. Paramasiva B, Pitchai KM. Modeling intrusion detection in mobile ad hoc networks as a non cooperative game", Proc. Int. Conf. Pattern Recognit. Informat. Mobile Eng. 2013 Feb, 300-306.
15. Wang J, Lang P, Zhu J, Deng W, Xu S. Application-value-awareness cross-layer MAC cooperative game for vehicular networks, Veh. Commun. 2018 Jul;13:27-37.
16. Vijayakumaran C, Macriga TA. An integrated game theoretical approach to detect misbehaving nodes in MANETs, Proc. 2nd Int. Conf. Comput. Commun. Technol. (ICCCT), 2017 Feb, p. 173-180.
17. Tembine H, Altman E, El-Azouzi R. Delayed evolutionary game dynamics applied to medium access control, Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst., 2007 Oct, p. 1-6.
18. Baras JS, Jiang T. Cooperative games phase transitions on graphs and distributed trust in MANET, Proc. 43rd IEEE Conf. Decis. Control (CDC), 2004 Dec, p. 93-98.

19. Xie Y, Zhang Y. A secure service priority-based incentive scheme for delay tolerant networks", *Secur. Commun. Netw.*, vol. 9, no. 1, pp. 5-18, Jan. 2016.
20. L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks, Mobile Netw. Appl. 2003;8(5):579-592.
21. Tyagi, Amit Kumar. Building a Smart and Sustainable Environment using Internet of Things (February 22, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, 2019 February 26-28.
22. Nobahary S, Babaie S. A credit-based method to selfish node detection in mobile ad-hoc network, Appl. Comput. Syst. 2018 Dec;23(2):118-127.
23. Zheng J, Wu Y, Zhang N, Zhou H, Cai Y, Shen X. Optimal power control in ultra-dense small cell networks: A game-theoretic approach, IEEE Trans. Wireless Commun. 2017 Jul;16(7):4139-4150.
24. Zheng J, Cai Y, Wu Y, Shen X. Dynamic computation offloading for mobile cloud computing: A stochastic game-theoretic approach, IEEE Trans. Mobile Comput. 2019 Apr;18(4):771-786.
25. Akkarajitsakul K, Hossain E, Niyato D. Cooperative packet delivery in hybrid wireless mobile networks: A coalitional game approach, IEEE Trans. Mobile Comput. 2013 May;12(5):840-854.
26. Li Y, Xu X, Cao Q, Li Z, Shen S. Evolutionary game-based trust strategy adjustment among nodes in wireless sensor networks, Int. J. Distrib. Sensor Netw. 2015;11(2):1-12.
27. Shen S, Huang L, Fan E, Hu K, Liu J, Cao Q. Trust dynamics in WSNs: An evolutionary game-theoretic approach, J. Sensors. 2016 Apr, 1-10.
28. Al-Jaoufi MAA, Liu Y, Zhang ZJ, Uden L. Study on selfish node incentive mechanism with a forward game node in wireless sensor networks, Int. J Antennas Propag. 2017 Oct, 1-13.
29. Chen Z, Qiu Y, Liu J, Xu L. Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game, Comput. Math. Appl. 2011 Nov;62(9):3378-3388.
30. Sonekar SV, Pal M, Tote M, Sawwashere S, Zunke S. Computation termination and malicious node detection using finite state machine in mobile adhoc networks, Proc. 7th Int. Conf. Comput. Sustain. Global Develop. (INDIACom). 2020 Mar, 156-161.
31. Mir RN. Secure distributed routing in mobile ad hoc networks using proactive secret sharing, Proc. 10th Int. Conf. Cloud Comput. Data Sci. Eng. (Confluence), 2020 Jan, 459-463.
32. Fu Y, Li G, Mohammed A, Yan Z, Cao J, Li H. A study and enhancement to the security of MANET AODV protocol against black hole attacks", Proc. IEEE Smart World Ubiquitous Intell. Comput. Adv. Trusted Comput. Scalable Comput. Commun. Cloud Big Data Comput. Internet People Smart City Innov. (Smart World/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2019 Aug, p. 1431-1436.
33. Menaka R, Mathana JM, Dhanagopal R, Sundarambal B. Performance evaluation of DSR protocol in MANET untrustworthy environment, Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), 2020 Mar, p. 1049-1052.
34. Monakhov YM, Monakhov MY, Telny AV. Method for local positioning of the node violating information security in mobile networks intrusion detection systems, Proc. Dyn. Syst. Mech. Mach. (Dynamics), 2019 Nov, p. 1-7,
35. Amin U, Shah MA. A novel authentication and security protocol for wireless adhoc networks", Proc. 24th Int. Conf. Autom. Comput. (ICAC), 2018 Sep, p. 1-5.
36. Sahnoun A Habbani, El Abbadi J. A coalition-formation game model for energy-efficient routing in mobile ad-hoc network, Int. J Electr. Comput. Eng. 2018;8(1):26-33.
37. Qin X, Wang X, Wang L, Lin Y, Wang X. An efficient probabilistic routing scheme based on game theory in opportunistic networks, Comput. Netw. 2019 Feb;149:144-153.
38. Samian N, Zukarnain ZA, Seah WKG, Abdullah A, Hanapi MZ. Cooperation stimulation mechanisms for wireless multihop networks: A survey, J Netw. Comput. Appl. 2015 Aug;54:88-106.
39. Al Sharah A, Alhaj M, Hassan M. Selfish dynamic punishment scheme: Misbehavior detection in MANETs using cooperative repeated game, IJCSNS, 2020;20(3):168-173.
40. Joshi SS, Biradar SR. Communication framework for jointly addressing issues of routing overhead and energy drainage in MANET, Procedia Comput. Sci. 2016 Jan;89:57-63.
41. Khushboo Tripathi, Manjusha Pandey, Shekhar Verma. Comparison of reactive and proactive routing protocols for different mobility conditions in WSN. In Proceedings of the 2011 International Conference on Communication, Computing & Security (ICCCS '11). Association for Computing Machinery, New York, NY, USA, 2011, 156–161. https://doi.org/10.1145/1947940.1947974
42. Patel NJ, Tripathi K. Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method. International journal of scientific research in science, engineering and technology. 2018;4:281-287.
43. Tripathi K, Agarwal T, Dixit SD. Performance of DSDV Protocol over Sensor Networks, International Journal of Next-Generation Networks (IJNGN). 2010;2:53-59.
44. Jain A, Tripathi K. Malicious detection using secure mutual trust-based routing on an intrusion detection system in WSN. International Journal of Recent Technology and Engineering. 2019;8(3):3144-3150.
45. Jain K Tripathi. Biometric Signature Authentication Scheme with RNN (BIOSIG_RNN) Machine Learning Approach," 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I), 2018, p. 298-305. Doi:10.1109/IC3I44769.2018.9007284.
46. Tripathi K, Dixit SD. Effect of Channel Fading on the Performance of Wireless Ad Hoc Network Routing Protocols, Applied Mechanics and Materials. 2012;197:643-648,.
47. Jajula SK, Tripathi K, Bajaj SB. Review of Detection of Packets Inspection and Attacks in Network Security. In: Dutta, P., Chakrabarti, S., Bhattacharya, A., Dutta, S., Piuri, V. (eds) Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks

and Systems. Springer, Singapore, 2023, 491. https://doi.org/10.1007/978-981-19-4193-1_58
48. Ranchhodbhai PN, Tripathi K. Identifying and Improving the Malicious Behavior of Rushing and Blackhole Attacks using Proposed IDSAODV Protocol", International Journal of Recent Technology and Engineering. 2019;8(3):6554-6562.
49. Midha S, Triptahi K. Extended TLS security and Defensive Algorithm in OpenFlow SDN, 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2019, p. 141-146. Doi:10.1109/CONFLUENCE.2019.8776607.
50. Midha S, Tripathi K. Extended Security in Heterogeneous Distributed SDN Architecture. In: Hura, G., Singh, A., Siong Hoe, L. (eds) Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering, 2021, 668. Springer, Singapore. https://doi.org/10.1007/978-981-15-5341-7_75
51. Somisetti K, Tripathi K, Verma JK. Design, Implementation, and Controlling of a Humanoid Robot," 2020 International Conference on Computational Performance Evaluation (ComPE). 2020, p. 831-836, doi: 10.1109/ComPE49325.2020.9200020.
52. Nair MM, Tyagi AK, Sreenath N. The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges, 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, p. 1-7. Doi: 10.1109/ICCCI50826.2021.9402498.
53. Tyagi AK, Fernandez TF, Mishra S, Kumari S. Intelligent Automation Systems at the Core of Industry 4.0. In: Abraham A., Piuri V., Gandhi N., Siarry P., Kaklauskas A., Madureira A. (eds) Intelligent Systems Design and Applications. ISDA 2020. Advances in Intelligent Systems and Computing, 2021, 1351. Springer, Cham. https://doi.org/10.1007/978-3-030-71187-0_1
54. Goyal, Deepti, Tyagi, Amit. A Look at Top 35 Problems in the Computer Science Field for the Next Decade, 2020. 10.1201/9781003052098-40.
55. Madhav AVS, Tyagi AK. The World with Future Technologies (Post-COVID-19): Open Issues, Challenges, and the Road Ahead. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. 2022. https://doi.org/10.1007/978-981-16-6542-4_22
56. Mishra S, Tyagi AK. The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. In: Pal S., De D., Buyya R. (eds) Artificial Intelligence-based Internet of Things Systems. Internet of Things (Technology, Communications and Computing). Springer, 2022. Cham. https://doi.org/10.1007/978-3-030-87059-1_4
57. George T, Tyagi AK. Reliable Edge Computing Architectures for Crowdsensing Applications," 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, p. 1-6. Doi:10.1109/ICCCI54379.2022.9740791.
58. Rekha G, Tyagi AK, Anuradha N. Integration of Fog Computing and Internet of Things: An Useful Overview. In: Singh P., Kar A., Singh Y., Kolekar M., Tanwar S. (eds) Proceedings of ICRIC 2019. Lecture Notes in Electrical Engineering, 2020, 597. Springer, Cham. https://doi.org/10.1007/978-3-030-29407-6_8
59. Sheth HSK, Tyagi AK. Mobile Cloud Computing: Issues, Applications and Scope in COVID-19. In: Abraham, A., Gandhi, N., Hanne, T., Hong, TP., Nogueira Rios, T., Ding, W. (eds) Intelligent Systems Design and Applications. ISDA 2021. Lecture Notes in Networks and Systems, Springer, Cham, 2022, 418. https://doi.org/10.1007/978-3-030-96308-8_55
60. Tyagi, Amit Kumar, Shamila M. Spy in the Crowd: How User's Privacy Is Getting Affected with the Integration of Internet of Thing's Devices (March 20, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, 2019 February 26-28.
61. Tyagi AK, Sreenath N. Intelligent Transportation System: Past, Present, and Future. In: Intelligent Transportation Systems: Theory and Practice. Disruptive Technologies and Digital Transformations for Society 5.0. Springer, 2023. Singapore. https://doi.org/10.1007/978-981-19-7622-3_2
62. Tyagi AK, Sreenath N. Fog and Edge Computing in Navigation of Intelligent Transportation System. In: Intelligent Transportation Systems: Theory and Practice. Disruptive Technologies and Digital Transformations for Society 5.0. Springer, Singapore. 2023. https://doi.org/10.1007/978-981-19-7622-3_7
63. Tyagi AK, Sreenath N. Security, Privacy, and Trust Issues in Intelligent Transportation System. In: Intelligent Transportation Systems: Theory and Practice. Disruptive Technologies and Digital Transformations for Society 5.0. Springer, Singapore. 2023. https://doi.org/10.1007/978-981-19-7622-3_8
64. Tyagi AK, Sreenath N. Artificial Intelligence—Internet of Things-Based Intelligent Transportation System. In: Intelligent Transportation Systems: Theory and Practice. Disruptive Technologies and Digital Transformations for Society 5.0. Springer, Singapore. 2023. https://doi.org/10.1007/978-981-19-7622-3_10
65. Tyagi AK, Sreenath N. Future Intelligent Vehicles: Open Issues, Critical Challenges, and Research Opportunities. In: Intelligent Transportation Systems: Theory and Practice. Disruptive Technologies and Digital Transformations for Society 5.0. Springer, Singapore. 2023. https://doi.org/10.1007/978-981-19-7622-3_15
66. Madhav AVS, Tyagi AK. Explainable Artificial Intelligence (XAI): Connecting Artificial Decision-Making and Human Trust in Autonomous Vehicles. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems. Springer, Singapore, 2023, 421. https://doi.org/10.1007/978-981-19-1142-2_10
67. Nair MM, Tyagi AK. Preserving Privacy Using Blockchain Technology in Autonomous Vehicles. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2021. Lecture Notes in Networks and Systems, 2022, 481. Springer, Singapore. https://doi.org/10.1007/978-981-

19-3182-6_19
68. Tyagi A, Niladhuri S, Priya R. Never Trust Anyone: Trust-Privacy Trade-offs in Vehicular Ad-Hoc Networks. Journal of Advances in Mathematics and Computer Science. 2016;19(6):1-23. https://doi.org/10.9734/BJMCS/2016/27737
69. Tyagi AK, Kumari S, Fernandez TF, Aravindan C. P3 Block: Privacy Preserved, Trusted Smart Parking Allotment for Future Vehicles of Tomorrow. In: Gervasi O. *et al*. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science. Springer, 2020, 12254. Cham. https://doi.org/10.1007/978-3-030-58817-5_56
70. Varsha R, *et al*. Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles'. International Journal of Hybrid Intelligent System, 2020 Jan1;16(4):223-236.