ISSN: 2584-0495 Vol. 2, Issue 9, pp. 1170-1175

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

Evaluating TCP and Alternative Protocols for Enhanced Efficiency and Reliability in Wireless Sensor Network for Congestion Avoidance

K. Ramkumar, Shrikant Upadhyay, Binod Kumar, Anindita Chakraborty, Siddharth Prakash and Jaina Sumith Gupta

Cite as: Ramkumar, K., Upadhyay, S., Kumar, B., Chakraborty, A., Prakash, S., & Gupta, J. S. (2024). Evaluating TCP and Alternative Protocols for Enhanced Efficiency and Reliability in Wireless Sensor Network for Congestion Avoidance. International Journal of Microsystems and IoT, 2(9), 1170-1175. https://doi.org/10.5281/zenodo.14068374

Published online: 23 Sept 2024

DOI: https://doi.org/10.5281/zenodo.14068374

International Journal of Microsystems and IoT
Vol. 2, Issue 9, pp.1170-1175; DOI: https://doi.org/10.5281/zenodo.14068374

Evaluating TCP and Alternative Protocols for Enhanced Efficiency and Reliability in Wireless Sensor Network for Congestion Avoidance

K. Ramkumar[1], Shrikant Upadhyay[2], Binod Kumar[3], Anindita Chakraborty[4], Siddharth Prakash[5] and Jaina Sumith Gupta[2]

[1]Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Tamilnadu, Chennai, India
[2]Department of Electronics and Communication Engineering, MLR Institute of Technology, Hyderabad, India
[3]Department of CSE & IT, Jharkhand Rai University, Ranchi, Jharkhand, India
[4]Department of Computer Science and Engineering-AIML, Brainware University, Kolkata, India
[5]Swarnrekha Group of Institutions (Director), Ranchi, Jharkhand, India

ABSTRACT
TCP is a protocol which is connection oriented that build a bridge between receiver and sender nodes before the initial packet transmission fire. If executed for WSN, where exact facts might be in order of small bytes, then a three-way complete activity will be become a difficult for a low volume of facts or data. Furthermore, in previous earlier attempt, a WSN is visualizing as framework of multi-hop where every intermediate hop connection is identified by its wasted and inaccurate vulnerable radio medium. As, TCP is protocol with end-to-end feature, schedule to structure TCP connectivity among two nodes end, that are notable number of hops separating each other which may be very large. Thus, for sensor nodes it is quite difficult for those nodes that are long way from sink to set sufficient round to help WSN applications that needed transmission of data continuously. In addition, the end-to-end technique become responsible for longer response in scenario of traffic or congestion and the result would give a larger number of portion drops. These portion drops mean there is unnecessarily power utilization or consumption. So, to ensure reliability, TCP follow end-to-end acknowledgment strategy, which low down the network throughput and increase the transmission time. In this paper, we have considered two protocols for the analysis of different parameters under different scenario, and this will help to measure the level of congestion and may help in increasing trustability for WSN. Delivery ratio of AODV is 83% and 78% of DSR is achieved with 25% load fraction of AODV and 23% for DSR.

KEYWORDS
Transport layer, WSN, congestion, avoidance mechanism

1. INTRODUCTION

Thus, for sensor nodes it is quite difficult for those nodes that are long way from sink to get sufficient round to help WSN applications that needed transmission of data continuously. In addition, the end-to-end technique becomes responsible for longer response in scenario of traffic or congestion and the result would give a larger number of portion drops. These portion drops mean there is unnecessary power utilization or consumption. TCP follows TCP follows end-to-end acknowledgment strategy, which low down the network throughput and increase the transmission time [1-2].

The critical characteristics of UDP construct it inappropriate for WSN, despite the unconnected paradigm it provides. Congestion control and flow control mechanism is not offered by UDP as in case of traffic it simply drops the packet and there is no scope of retrieving the packets lost. Also, in UDP there is no such process of acknowledgment and thus depend on the minor layer of MAC algorithms or in some higher layer like application layer to obtain the packet loss [3].

Covering the unique features of WSN the crucial requirement of WSN transport layer is:

The flow of data in model should be reasonable and logical for the application like hybrid and/or real-time, event-driven, steady etc. [4]. Must have end-to-end reliable Ness with congestion control mechanism. Provide trustability for downstream and upstream.

The critical characteristics of UDP construct it inappropriate for WSN, despite unconnected paradigm it provides. Congestion control and flow control mechanism is not offered by UDP as in case of traffic it simply drops the packet and there is no scope of retrieving the packets lost [5-6]. Also, in UDP there is no such process of acknowledgment and thus depend on the minor layer of MAC algorithms or in some higher layer like application layer to obtain the packet loss.

2. EVENT TO SINK RELIABLE TRANSPORT

If the present evaluated trustability at BS (Base Station) drops under the essential trustability with no traffic then ESRT extend the reporting frequency ‘f’ suddenly. If found no traffic and the level of trustability is high, then ESRT lower down ‘f’ consciously. In some cases, traffic is identified, and trustability drops, ESRT lower down the value of ‘f’ exponentially. For structure where traffic is identified although high trustability degree, ESRT decays describing frequency to free from traffic without arrangement of trustability [7]. Although, ESTR attempt to utilize on the best position where some action is accurately described to BS (Base Station) without creating traffic to network. This transport protocol assumes that BS has large radio power and attains all sensor nodes in individual scattered message. The BS spreads the updated evaluated value of ‘f’ to entire network [8]. Consequently, on getting the occasion outline frequency, every sensor node evaluates its

describing event time span and verify at intermediary level at final stage of every describing interval to find any feasible traffic. If sensor nodes find traffic, it fixes a traffic entitle bit of the case announce packet whenever these packages reached at BS, the BS gets total view of traffic level of network. This protocol protects power by measuring the value of 'f' and its evaluation was done by analytical designing and simulation [9-10].

3. TC/ IP (TINY PROTOCOL)

In [14,18] author proposed a protocol known as tiny TCP/IP which inclined to adjust the TCP/IP protocol escort to build it workable for wireless sensor network and supply trustability for E2E (end to end) & hop by hop. Such protocol considered that every sensor node identifies its structural locality a theoretical and decay into its prearranged sub array. Every sensor node acquires the initial twice octets rely on dimensional locality inside the sub array [11]. It suggests four different conversions of the surviving protocol of TCP/IP i.e. dispersed TCP concealment (DTC), spitted factors headers compacting, dimensional IP location allotment and application covered routing. Similar IP array of sensor nodes does not require to send a complete IP header so, that IP header can be suppressed and splitted between sensor nodes of similar sub array. UDP datagram of locally IP transmission are used to generate an application covering layer network on peak of physical trigger network [12]. At the end, DTC generates the packet reliability using spitted technique. A novel idea generated by tiny TCP/IP in form of TCP packages hiding inside the network to lower down the burden of end-to-end retransfer of particles where the packet loss arises.

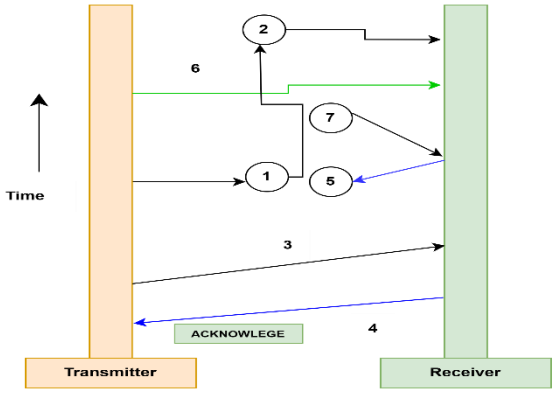

Fig. 1. Distributed TCP

Fig. 1 depicts the recovery of packet loss where middle nodes 5 & 7 store packages 1 & 2 individually so, on such case this pair of lost their packets where node 5 provides package 1 and node 7 redeliver packet 2 for the R_x (Receiver). In a poor scenario R_x get the lost package from the T_x if the lost package not tracked by any middle nodes and it has been calculated using both simulation and real time wireless sensor network [13].

The reliability of the protocol relies on the capacity of tracking the last observed packets and this will be unsuitable for various applications which depend upon mobility. This protocol doesn't specify any traffic plan control method and doesn't highlight the method for downstream or upstream trustability [14-15].

4. RELIABLE ASSYMETRIC TRANSPORT LAYER PROTOCOL

Dependable and unbalanced transport protocol supplies crucial end to end occasion trustability, sequential end to end inquiry trustability and crucial traffic control [16]. It also chooses a subgroup of trigger nodes known as crucial nodes (C-nodes) that will protect the entire region to be noticed in term of power in well plan way. This protocol generates a sub array which contains C-nodes and only C-nodes are eligible to participate in definite data moving to downstream & upstream nodes and vanish particle recovery [17]. This protocol provides from different features:

1. A very low quantity of nodes participates in lost information retrieval and follows splitted power known traffic control.
2. An unnecessary node doesn't point end to end connections overhead.
3. Traffic mechanisms to control can be distributed to adjust the congestion flow effectively.
4. As this protocol provides trustability in upstream & downstream and used acknowledge (ACK) and no acknowledge (NACK) mechanisms.

Fig. 2 depicts the inquiry and occasion trustability mechanisms. Traffic command is managed by C-node and the existence of traffic is considered if downtime arises without accepting any acknowledge from BS. In such a case, C-node convinces its adjacent unnecessary nodes to prevent from dispatching any information till the traffic is unblocked [18]. The execution of reliable asymmetric protocol is assessed using simulation. Nevertheless, the aspect of identifying traffic by hidden acknowledge which is not a suitable solution as acknowledge is hidden due to various reasons along with link drop [19].

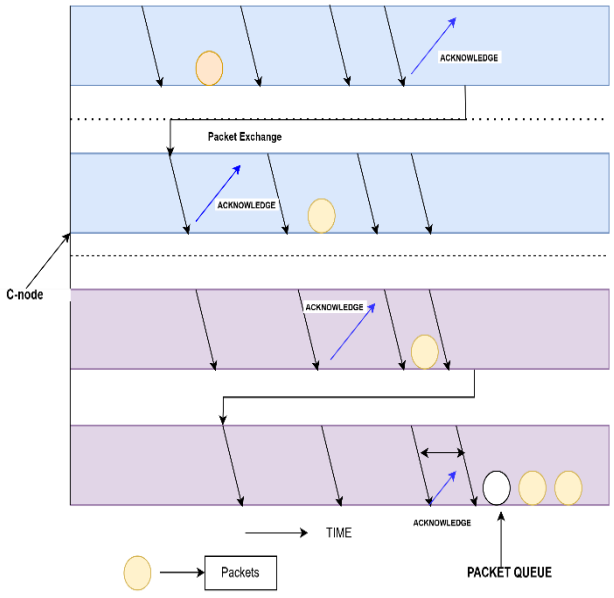

Fig. 2. Trustability mechanism: First block represents connection less no acknowledge, second block is acknowledge based for loss identification and third block denotes event loss identification

Packet rows per child i.e. every trigger node continues individual indexed row for every child along with its rows and sub-tree length per child [20]. It also includes command information inside the packages data, therefore rejecting the doses to the sequential trigger nodes.
When trigger nodes find traffic, it acknowledges the sequential nodes to minimize their transmission data rate as depicted in Fig. 3.

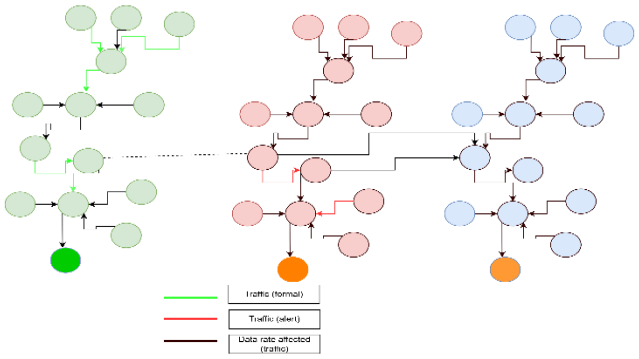

Fig. 3. Fair traffic mechanism: 1- node for regular congestion and acknowledge the lower data to control data flow, 2- limit data flow under traffic and 3- traffic is removed and all lower nodes are now ready for data flow

Since fair traffic control tries to implement the traffic command finding in transport layer, which is independent of fundamental MAC layers and network. Traffic control is evaluated using simulation with a real time WSN environment.

5. RESOURCE MANAGEMENT IN TRANSPORT LAYER PROTOCOL

Cloud agent in form of sensor that process and collects information using different sensor networks. It activates fact sharing on huge amount and cooperates for different applications ob cloud between users. It combines various network with a quantity of recognizing applications with cloud evaluated platform by granting requests to be collaborative they may stretch over many firm [21]. Cloud with sensor activates users to comfortably process, gather, access, share, store, analyze, visualize and discover for a huge quantity of sensor data for various kind of implementations and using storage assts and computational IT of the cloud [22].
Infrastructure based on sensor cloud provides facility automatically to last users when requested, so that their virtual sensors act as a part of IT assets like memory, CPU, disk storage etc. related proper sensor data with their service instances can be used by last agent via interface using web dallier.
In the past few years, cloud assess play an important role as a chief model for the utilization of resources [23]. It supplies these assets on the vend as facility that can be absorbed in a transparent and flexible fashion. Cloud provider and users are the two major actors in such a scenario. The aim of the user is to get assets allotment associated with the model that we used. The scale factor is the main aim of cloud provider that generates a huge set of assets [24].
Assets allotment system may assume all procedure construction to guarantee that applications demand considered correctly by the source's infrastructure. Resource allocation technique also provides the present status of each asset in cloud domain to put suitable algorithm to allocate the local/physical resources for different applications. Cloud agents can only see the restricted assets so, assets allotment system is very important and acts as an intelligent agent.
Trigger modelling language can be utilized to denote any real trigger's metadata with their real location, type, precision etc. It also follows XML encrypting method for description and measurement process of real sensors. This encoding process for real sensor implemented across different hardware, applications, platforms (OS) etc. with less intervention of human. To resolve the control arises from their relevant sensor, a mapping was agreed between the virtual and physical sensor [25-27].
Since real sensor nodes have limited resources in terms of battery power, memory storage, BW etc. Storage of data for long duration and processing of huge data by the sensor will be a challenging one. Here, cloud agent plays a very crucial role where large quantity of data from various trigger networks arises and stored [28]. Agreement of data is very tedious at cloud server with sensor and the selection of resource allocator should be done in such way that it will finish its task inside the time and allotment should be inaccurate and cost improved [29].
Agent dependent platform will help in allotment of sensory resources within sensor cloud server and accessible for whole users. Thus, agents have a very important role in setting down the proper resource in proper database. The programming of agent was done in such a way that if data is arriving from the trigger network, then agent will put assets management approach onto it and it will be saved in definite platform/server for easy availability to last users with controllers [30-33].

6. SIMULATION RESULTS

Similar to network simulator-2, NS-3 is considered as distinct occasion simulator, and the main reason of its growth is to amplify research in network technology. It is also an open-source toll launched in year 2008 with its latest version 3.21 [34-35]. It is an updated simulator, and it is not an extension of NS-2 neither it supports any API's associated with NS-2. NS-2 program first coded in OTcl (object tool command language) and results would be visualized utilizing Xgraph are NAM (network animator) but coding which is purely based on C++ is quite different. NS-3 simulator consists of all programs which are purely written in C++ with python essential. Graphical tool which is not available in NS-3 but graphical analysis can be described using NetAnim which is also a open source tool. The basic architecture of NS-3 used for the simulation is depicted in Fig. 4 below.

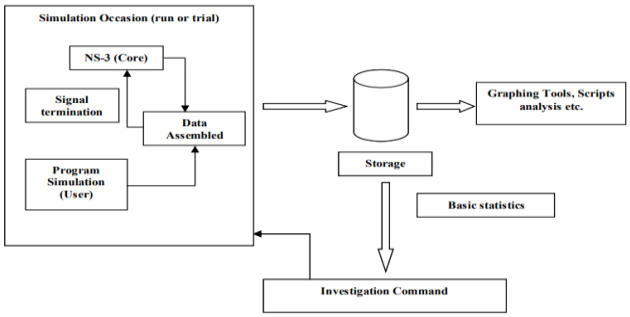

Fig. 4. Simulation procedure using NS-3

TABLE I
PARAMETERS FOR IMPLEMENTATION

Parameters	**Value**
Routing Protocol	**DSR, AODV**
Number of nodes	Variable
Simulation Time	10 sec, 50 sec & 100 sec
Pause Time	5 ms
Environment Size	800 x 800
Transmission_Range	200-250m
Traffic_Size	CBR (Constant Bit Rate)
Packet_Size	512
Packet_Rate	5 packets/s
Maximum Speed	20m/s
Queue Length	50
Simulator	NS-3
Mobility Model	Random Waypoint
Antenna Type	Omnidirectional

Using above parameter as shown in Table I some networks are created which will help to analyze the network in term of their packet drop, packet delivery, throughput etc. The scenario depicted in Fig. 5 consist of six node with source node (0) and destination node (5)

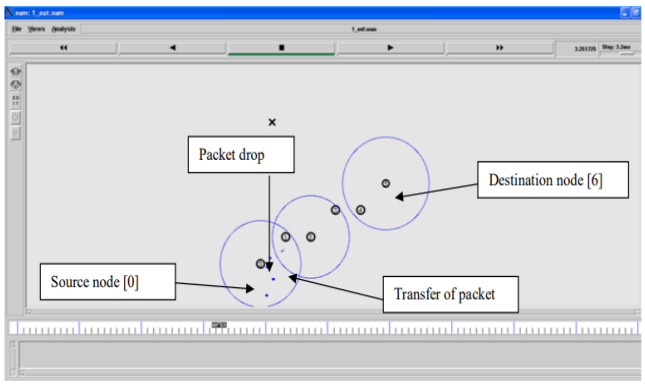

Fig. 5. Network Animator for 6 nodes with source node [0] and destination node [5]

The second scenario depicted in Fig. 6 consists of sixteen nodes with source node (0) and destination node (15).

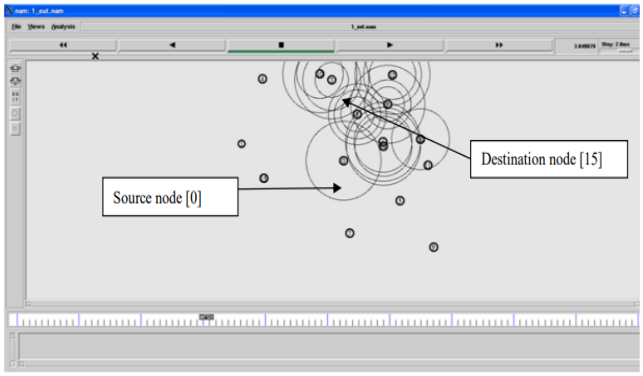

Fig. 6. Network with 16 nodes with source node [0] and destination node [15]

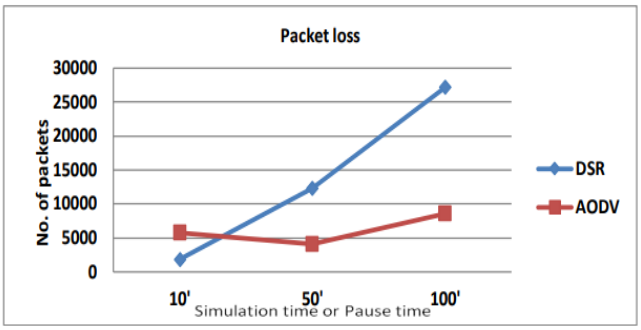

Fig. 7. Loss of packet

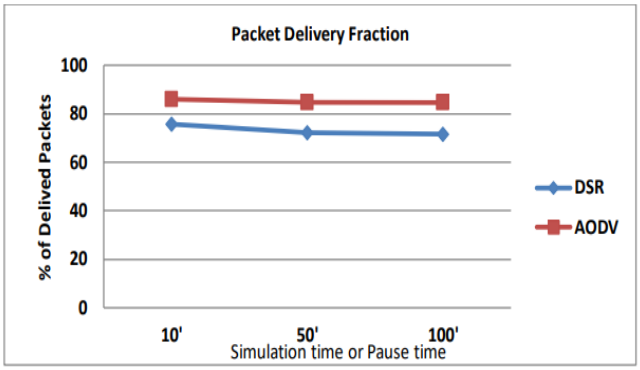

Fig. 8. Ratio of packet delivery

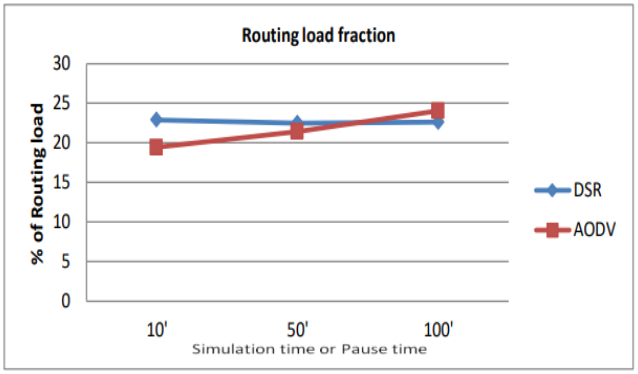

Fig. 9. Load fraction

From figure 7, a packet loss increases more for DSR routing protocol with increase in simulation time in comparison to AODV routing protocol. From figure 8, packet delivery fraction is very good for AODV routing protocol comparison to DSR routing protocol. So, under such a scenario AODV perform much better than DSR routing protocol. From figure 9 routing load fraction is low for DSR routing protocol comparison to AODV routing protocol under such scenario.

7. CONCLUSION

Transport layer protocol play a vital role to control the congestion by maintain overflow of queue and maintain end to end reliability of network. A crucial transport layer protocols with its practical limitations are discussed deeply to identify its limitations and proper applications. Also, role of intelligent agent in collecting facts between the user and cloud are also discussed to ensure the best usage of assets. Tool used for the simulation i.e. NS-3 is demonstrated to build the network as per requirement for verification. The result obtained for DSR and AODV reflect the outcome in term of load fraction, packet loss and data delivery in which the performance of AODV protocol is quite efficient i.e., 83-84% with low loss of 9995 packets compared to DSR.

REFERENCES

[1] Stann F, Heidemann J (2003). RMST: reliable data transport in sensor net-works. In: First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, 102–112

[2] Park, S -J, Vedantham R, Sivakumar R, Akyildiz I F (2004). A scalable approach for reliable downstream data delivery in wireless sensor networks. In: Proc. International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Tokyo, Japan, 78–89.

[3] Wan C -Y, Campbell A T, Krishnamurthy L (2002). PSFQ: A reliable transport protocol for wireless sensor networks. In: Proc. ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA, 1–11.

[4] Sankarasubramaniam Y, Akan O B, Akyildiz I F (2003). ESRT: event-to-sink reliable transport in wireless sensor networks. In: Proc. 4th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '03), New York, NY, USA, 177–188.

[5] Sundaresan K, Anantharaman V, Hsieh H -Y, Sivakumar A (2005). ATP: a reliable transport protocol for ad hoc networks. IEEE Transactions on Mobile Computing, 4(6):588–603.

[6] Wang C, Sohraby K, Li B (2005). SenTCP: A hop-by-hop congestion control protocol for wireless sensor networks. In: Proc. IEEE INFOCOM, Miami, USA.

[7] Iyer Y G, Gandham S, Venkatesan S (2005). STCP: A generic transport layer protocol for wireless sensor networks. In: Proc. IEEE ICCCN, San Diego, CA, USA.

[8] Lu C, Blum B, Abdelzaher T, Stankovic J, He T (2002). RAP: A Real-Time Communication Architecture for Large-Scale Wireless Sensor Networks. In: Proc. IEEE RTAS.

[9] Ee C -T, Bajcsy R (2004). Congestion control and fairness for many-to-one routing in Sensor networks. In: Proc. ACM Sensys 04, Baltimore, MD, USA, 148–161.

[10] K. T. Lan (2010). What's Next? Sensor+Cloud?. in Proceeding of the 7th International Workshop on Data Management for Sensor Networks, 978–971, ACM Digital Library.

[11] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan (2000). Energy-efficient communication protocol for wireless microsensor networks. in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2.

[12] Wang C, Sohraby K, Lawrence V, Li B, Hu Y. (2006). Priority-based congestion control in wireless sensor networks. In: Proc. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 22–31.

[13] Sundaresan K, Anantharaman V, Hsieh H -Y, Sivakumar A (2005). ATP: a reliable transport protocol for ad hoc networks. IEEE Transactions on Mobile Computing, 4(6):588–603.

[14] Wan C -Y, Campbell A T, Krishnamurthy L (2002). PSFQ: A reliable transport protocol for wireless sensor networks. In: Proc. ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA, 1–11.

[15] Park, S -J, Vedantham R, Sivakumar R, Akyildiz I F (2004). A scalable approach for reliable downstream data delivery in wireless sensor networks. In: Proc. International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Tokyo, Japan, 78–89.

[16] S. Mueller, R. P. Tsang, and D. Ghosal (2005). An Efficient N-to-1 Multipath Routing Protocol in Wireless Sensor Networks. In IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 672 – 679.

[17] Fang W-w., Chen J-m., Shu L., Chu T-s. & Qian D-p (2010). Congestion avoidance, detection and alleviation in wireless sensor networks. J Zhejiang Univ Sci, 11(1), 63 – 73.

[18] Monowar M., Rahman O., Pathan A. & Hong C (2012). Prioritized Heterogeneous Traffic-Oriented Congestion Control Protocol for WSNs. International Arab Journal of information technology. 9(1),39 – 48.

[19] Ghaffari A. (2015). Congestion Control mechanisms in wireless sensor networks: A survey. Journal of network and computer applications,52(1), 101 – 115.

[20] Konak, D. W. Coit, and A. E. Smith (2006). Multi-objective optimization using genetic algorithms: A tutorial. Reliability Engineering and System Safety, 91(9), 992-1007.

[21] Y. He, Y. Ji, Y. Zhang and X. Shen (2006). A new energy efficient approach by separating data collection and data report in WSNs. in WCMC'06, 1165-1170.

[22] Haritha, V., Latha, J., Swetha Reddy, A., Upadhyay, S., Venkatesh, R. (2023). Energy Efficient Data Management in Health Care. Proceedings of the 3rd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2023, 682–688.

[23] Alqahtani EJ, Zagrouba R, Almuhaideb A. (2019). A Survey on Android Malware Detection Techniques Using Machine Learning Algorithms. *Sixth International Conference on Software Defined Systems* (SDS-2019), . Epub ahead of print 2019. DOI: 10.1109/sds.2019.8768729.

[24] Glodek W, Harang R. (2013). Rapid Permissions-Based Detection and Analysis of Mobile Malware Using Random Decision Forests. MILCOM 2013, *IEEE Military Communications Conference*,. DOI: 10.1109/milcom.2013.170.

[25] Galeano-Brajones, J. Carmona-Murillo, J. Valenzuela-Valdés, J.F. Luna-Valero, F. (2020). Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. *Sensors*, 20, 816-825.

[26] MC Saxena, F Banu, A Shrivastava, M Thyagaraj et. Al (2022). Comprehensive Analysis of Energy Efficient Secure Routing Protocol for Sensor Network", Material Today, 62(7), 5003-5007.

[27] Mousavi, S.M., St-Hilaire, M. (2015). Early detection of DDoS attacks against SDN controllers. In Proceedings of International Conference on Computing, Networking and Communications (ICNC), Anaheim, CA, USA, 77–81. doi:10.1109/ICCNC.2015.7069319.

[28] S. Upadhyay, Tarun Kumar, Pooja V et. al. (2024). Machine Learning Based Beamforming Algorithm for Massive MIMO System in 5G Communication. Journal of Electrical System, 20 (3), 971-971.

[29] Munirathinam, T., Upadhyay, S., Babitha Lincy, R., .Beaulah Jeyavathana, R. (2022). Big Data Analytics with Deep Learning based Intracranial Haemorrhage Diagnosis and Classification Model" Proceedings - International Conference on Augmented Intelligence and Sustainable Systems, ICAISS 2022, 877–883.

[30] Kumar, M., Kumar, D., Akhtar, M.A.K (2018). Mathematical Model for Sink Mobility (MMSM) in Wireless Sensor Networks to Improve Network Lifetime. In: Verma, S., Tomar, R., Chaurasia, B., Singh, V., Abawajy, J. (eds) Communication, Networks and Computing. CNC 2018. Communications in Computer and Information Science, 839. Springer, Singapore. https://doi.org/10.1007/978-981-13-2372-0_12

[31] M. Kumar, S. Mittal and Amir K. Akhtar (2021). Energy Efficient Clustering and Routing Algorithm for WSN. 14(1), 282 – 290.

[32] M. Kumar , P. Mukherjee , S. Verma , Kavita et. al. (2023). A Novel SDN-Based Security Framework for Wireless Sensor Networks Using TDCNN and PGF-ECC. Human-centric Computing and Information Sciences, 13, 1-16.

[33] S. Upadhyay, M. Kumar, A. Upadhyay (2023). Digital Image Identification and Verification using Maximum and Preliminary Score

Approach with Watermarking for Security Enhancement and Validation. Journal of Electronics, 12 (7),1-15.

[34] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan (2002). An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 1(4), 660-670.

[35] M. Saleem, G. A. D. Caro, and M. Farooq (2011). Swarm intelligence-based routing protocol for wireless sensor networks: Survey and future directions. Information Sciences, 181(20), 4597-4624.

AUTHORS

K. Ramkumar having more than 23+ years of rich experience in Teaching in Engineering Colleges including IT Experience. Presently working as Professor (CSE) in SRM Institute of Science and Technology, Vadapalani Campus, Chennai. Prior to joining SRM Chennai I was Professor (CSE) and Associate Dean (E & T) in SRM University, Sonepat, Delhi-NCR, Haryana. Previously served as HOD of IT Department in Kings Engineering College, Chennai. His broad research area is Artificial Intelligence and Biomedical Data Analytics.

E-mail: ramkumar1975@gmail.com

Shrikant Upadhyay received his BTech degree from Dehradun Institute of Technology, Dehradun, India and MTech degree in Digital communication from DIT, Dehradun, India in 2011. He completed his Ph.D in year 2018 from JNU, Jaipur. Currently, he is working as an Associate Professor, Department of Electronics and Communication Engineering, MLR Institute of Technology, Hyderabad, India. His research area includes IoT for healthcare, WSN, AI and Machine Learning.

E-mail: shrikant.upadhay@mlrit.ac.in

Binod Kumar received Master of Technology from BIT, Mesra, Ranchi and Ph. D from Kalinga University, Raipur. He is presently working as an Associate Professor in the Department of CSE & IT at Jharkhand Rai University, Ranchi. His research area includes AI, ML, Image processing, IoT.

E-mail: bit.binod15@gmail.com

Anindita Chakraborty received her B.Tech degree in Computer Science and Engineering from W.B.U.T, West Bengal, India in 2013 and M.Tech degree from IEM, Kolkata, West Bengal in 2017. Her area of interest area artificial intelligence, machine learning, internet of things, computational intelligence, cryptography and network security.

E-mail: ani.9012@gmail.com

Siddharth Prakash Director of Swarnrekha Group of Institutions (SGi), having over ten years of experience in leading and managing educational institutions. He is also a trustee in Swarnrekha Educational Trust which has a thirty-year legacy of providing quality education in India. He received his Ph.D degree in Civil Engineering from Kaling University. SGi is running many schools and colleges across India. He is also serving as Director in Sri Sai Laxmi Aluminum Die Casting Public Limited (SSLDC), Based in Tirupati, India.

E-mail: siddharthprakash101@gmail.com

Jaina Sumith Gupta pursuing BTech Department of Electronics and Communication Engineering, MLR Institute of Technology, Hyderabad, India His research area includes IoT, WSN, Routing Algorithms.

E-mail: sumithgupta3@gmail.com