International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Blockchain Based Packet Delivery Mechanism for WSN

S. Raj Anan, Rama Chaithanya Tanguturi, Soundara Rajan D S

Abstract: -The latest trend in the research filed implies the importance of data security in wireless sensor networks. There are various approaches identified for securing the data by using trust wide security such as cryptographic systems and routing protocols. However, these approaches are very critical to identify the optimal path in the network and attacks by unauthorized node cannot be prevented. In this paper, a new algorithm for combining the AODV (Ad Hoc On-Demand Distance Vector) routing protocol and particle swarm optimization (PSO) is implemented to produce trustable routing in every location through block chain. The possible routing procedure will enhance the routing nodes to acquire routing information among all the nodes but will never allow the node to capture the information. The routing protocol on the blockchain is used to utilize the path efficiently without deviation caused by other anchor nodes. It also identifies the congestion in the entire path of the particular network and avoids tampering of information between the nodes. The blockchain enabled with PSO algorithm and AODV routing protocol provides the simulation results about the efficient packet delivery system. The Security has been performed in every node used to identify the best route for producing the efficient throughput and quality of services.

Index Terms: Wireless sensor networks (WSN), PSO, AODV, Blockchain.

I. INTRODUCTION

A wireless sensor network (WSN) with autonomous sensors monitors the physical or environmental conditions, such as temperature, sound, pressure, etc. and also cooperatively pass their data through the network to the prime location [1]. The extensive deployment of sensor networks is quite practical these days. A network of this numerous sensors allows an efficient solution to various challenging tasks: traffic monitoring, monitoring of building with respect to the structure, fire, and security, military sensing and tracking, distributed measurement of seismic activity, real-time pollution monitoring, wildlife monitoring and wildfire tracking [2]. The existing key pre-distribution schemes such as basic probabilistic and q composite schemes used in the sensor networks forms a pair wise key for the establishment and authentication between sensor nodes and mobile sinks. An attacker places a replicated mobile sink preloaded with some compromised keys to obtain a large number of keys by capturing a small fraction of nodes to gain control of the network [3].

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Dr. S. Raj Anand*, CSE, PACE Institute of Technology & Sciences, Ongole, Andrapradesh, India.
Dr. Rama Chaithanya Tanguturi, CSE, PACE Institute of Technology &Sciences, Ongole, Andrapradesh, India.
Soundarrajan D S, IT, PACE Institute of Technology &Sciences, Ongole, Andrapradesh, India.

To overcome this, a three-tier security scheme was further proposed that makes use of the polynomial pool based scheme [4] and pairwise authentication schemes, which further reduces these attacks to some extent but the energy level in this scheme is not high. Mobile ad hoc network (MANETs) is a
wireless network that has a routable networking environment on top of a link layer in ad hoc network. MANET is a peer-to-peer self-forming and self-healing network which has a central controller to determine, optimize, and distribute the routing table which is not present in mesh network. The device of the MANET has the power to move independently in any direction with many anonymous MANET routing protocols like AODV or DSR [6-9]. The different cryptosystems are used to implement the same function to measure the performance of routing changes. It is an added advantage for ANODR to overcome the inefficient anonymous routing of MANET. An improved AODV routing protocol which is based on minimal route, is used to simulate the throughput and reduce the end-to-end delay and other parameters for evaluating the performance of the wireless sensor network by OPNET[11]. The destination sequence distance vector (DSDV) and ad hoc on demand distance vector (AODV) routing protocols are popularly used in mobile ad hoc networks. Among the two protocols, AODV is more reliable with the affordable burden compared to DSDV [12]. The performance evaluation of different network parameters on different topologies based on varying the pause time with respect to constant speed (node speed) in different terrain areas as small (1000 m. x 1000 m.), large (2000 m. x 1000 m.) and very large (2000 m. x 2000 m.) using AODV routing protocol and monitoring of critical conditions with the help of important parameters like packet delivery fraction, average end- to- end delay, average throughput, NRL and packet Loss [13]. Energy Aware Routing Protocol (ETARP) is used to discover and select routes based on the maximum utility to incur additional cost in overhead compare to the common AODV routing protocol [14]. The flip ambiguity problem has been solved by distributed two-phase PSO algorithm to improve the efficiency and precision of the entire network. Moreover, the unknown nodes with minimum two or three near-collinear references are made to be localized in our research [15]. A multi-objective particle swarm optimization algorithm was used to find the optimal solution. The global optimum is obtained according to the proportion of selection [16]. The proof of work (PoW) in original bitcoins is to carry the pulling out and to store new data blocks by blockchain technology. It also adopts the reliable data possession to replace.[18]. A novel blockchain-based contractual routing (BCR) protocol is used for a network of untrusted IoT devices.

In view of the traditional secure routing protocols in which a central authority (CA) is required to formulate the identification and authentication of each device. It produced the routing overhead of the BCR protocol in 5 times lower compared to AODV at the cost of a slightly lower packet delivery ratio. BCR is fairly resistant to both Blackhole and Greyhole attacks. The results show that the BCR protocol enables distributed routing in different IoT networks.[19]. Reinforcing the trust in distributed environments without the need of authorities is a technological advance which will change the industry's perspective. The IoT which is one among the disruptive technologies such as big data and cloud computing. To overcome its limitations since its conception, blockchain will be one of the next replacements [20]. The feasible routing information is given by routing scheme obtaining the routing nodes on the blockchain which will make the routing information traceable and impossible to tamper with [21].

II. ARCHITECTURAL MODEL OF AODV AND PSO

Figure 1 shows the architecture model of congestion avoiding flow system of the routing protocol. The AODV protocol has been used to send the packet from source to destination. If either source or destination has been attacked by a malicious node for affecting of all the packets, the PSO algorithm used to gather the authorized node by using the method of blockchain. After the arrival of all the packets in every node, overall performance has been analyzed with statistical measurement of poison distributed scheme. This scheme used to measure the performance of the authorized node for obtaining the smooth flow control of the packets in every route. Figure 1 shows N_1, N_2.N_n are a number of nodes. Each node is sending the pre-request (PREQ) as a packet to the destination. The receiver has observed each path and finding the packets without a malicious node. The receiver then sends the reply as an acknowledgment to the source. In this case, the packet delay time has been identified and sending the packet without any caution of delay.

III. METHODOLOGY OF WORKING PRINCIPLES OF AODV AND PSO

The AODV has used to implement in various networks to adopt the route efficiently with same energy level by using PSO on blockchain technology. The reason behind avoiding congestion is used:

- To increase the efficient throughput of the system.
- To increase the lifetime of the network.
- To maintain the quality of services.

Figure 2 indicates the sequence numbers for making node communication within the time stamps. The nodes can compare themselves about the priority of their information among nodes. The sequence number increases with respect to the type of message send by each node. This sequence number of each node is shared to rest of the nodes.

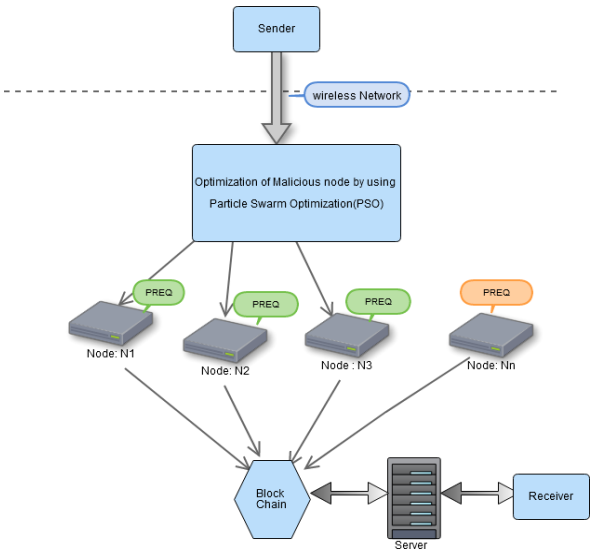

Figure 1: packet Delay time of source and destination using AODV and PSO

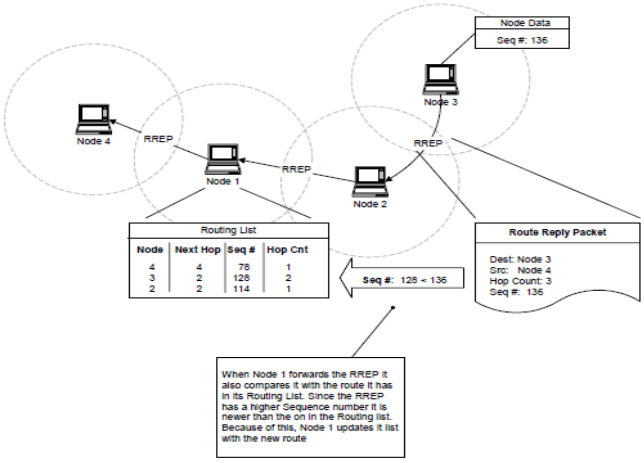

Figure 2: Packet Delivery of node in the number of Hop count using AODV protocol

Particle Swarm Optimization (PSO) is a heuristic designed algorithm which creates no assumptions about the problem being optimized. PSO can be used in candidate solutions on optimization problems that are partially irregular, noisy, change over time, etc[17].

IV. WHY BLOCKCHAIN REQUIRED ON AODV AND PSO?

The blockchain is an imperishable digital ledger of economic transactions that can record all financial transactions with its virtual values. The blockchain network has decentralized authority to communicate the information between the nodes. Also, it is a shared and absolute ledger, where the information is open for all nodes. When any intrusion takes place by a node within the network, the other nodes get the prompt information about this malfunction.

Therefore, the overall actions that is built on the blockchain is transparent and everyone involved is accountable for their actions [22]. In this connection, the blockchain technology has been implemented in every node. If the nodes are used to capture the route to its destination, every node blocks the shortest route to reach its recipient point. These situations arise that every node can be visibly digesting every other node information, but cannot be theft and modify the information about another node. The PSO algorithm is used only for measuring the route which is not affected by malicious users. In this case of blockchain technology, the route can be blocked by every node which in turn only authorized node can be blocked as a chain and information might be shared only authorized node. The malicious node cannot be interfered in any situation to control every data. In order to obtain the blockchain technology in AODV, produced the efficient energy level and improve the throughput for producing the Quality of Service.

V. PACKET DELIVERY RATIO CALCULATED USING POISON DISTRIBUTION

A discrete random variable X with assumed values X = 0, 1, 2, 3,..∞ is said to follow Poisson distribution if its probability mass function is

$$P(X=x) = \begin{cases} \frac{e^{-\lambda}\lambda^{x}}{x}, x = 0,1,2,..\infty : o, otherwise \end{cases} \quad (1)$$

Here λ is the parameter of the Poisson distribution.

Let X denotes the number of nodes x_1, x_2...x_i in every direction of network during packet transmission. The nodes establish the communication through their anchor nodes in the form of x_1->x_2, x_2->x_3, x_3->x_i. The AODV protocol is used to measure every path for obtaining the request from the source and it is used to connect to destination through every hop. The packets are transferred irrespective of the number of hops already connected. When node fails due to the network disruption it gets retransmitted from the source. These cases analyze through PSO technique to optimize the congestion path where it is exactly occurred. Sometimes the malicious nodes try to interrupt communication through accumulating the paths between the nodes. Hence the nodes are decentralized to communicate each other and control by blockchain. The properties like time and information of the nodes are shared amount the authorized nodes alone. The probability of infinite number of events is measured using the Poison distribution. This calculation gives the number of nodes successfully linked to reach its destination path without any congestion in stipulated time. Equation 2 shows the estimated process time of packet delivery irrespective of a number of nodes.

$$DelayTime = \frac{ProcessTime}{EstimationTime} X \cdot No \cdot of \cdot Nodes \quad (2)$$

VI. ALGORITHM:

INTEGRATION OF AODV AND PSO

Step1: Initialize number of nodes n_1, n_2, n_3, n_4..... n_i

Step2: Calculate a number of Hops Let h=hopCount.

Step3: Initialize the router=i where i=1,2,3…k

Step4: Identifying the position of every path with respect to a number of nodes n_1,n_2,..n_i.

Step5: if (i>1)

if((n_1+i)+(n_2+i) < Previous estimate router

i)Calculate Transmission rate(T_r)

where T_r=Time of Node n_1 → Time of Node n_2 Link//Transmission time measured between node n_1 and n_2

Let N_1=n_1+i →Starting node of the route

Let N_2=n_2+i → Neighbor node of the route

Similarly calculate N_3,N_4..N_i //Link the nodes N_1,N_2…Nn

Calculate Distance= $\sqrt{(N_1 - N_2)^2 + (N_3 - N_4)^2}$

//Find the Distance between nodes to identify
// shortest distance

Calculate Process Time= $\frac{Distatnce}{T_r}$

$$DelayTime = \frac{ProcessTime}{EstimationTime} X \cdot No \cdot of \cdot Nodes$$

//Where (i)Process Time-> Starting time of the
// node
// (ii) Estimation time->Ending time of the
// node

Link to router i with neighbor node to set short distance based on Delay Time.

Increase the hop count h_{++} and node is connected to neighbor node i.e n_{++}.

else

Remove the Unused link from the router.
the router is not Initialized.

Step6: To find the malicious node by using blockchain

For h in 0 to n
Let block=0; target=n.
if(distance<target)
The current block is moved to the next block for the authorized link.
else

Step7: End the process of an Algorithm

VII. RESULT AND SIMULATION

The simulation result of this research work has been shown how the AODV and PSO algorithm can be executed using the probabilistic approach of Poison distribution. Equation 1 shows the poison distribution value of n=10 and the estimated time has been measured in terms of AODV. The average time delay is measured in the point of view is 0.17. Each node has to travel around the other node with time delay. In this scenario 0.17 is the ratio has been done by AODV protocol. Figure 3 shows the average time delay has happened from node 1 to 10.

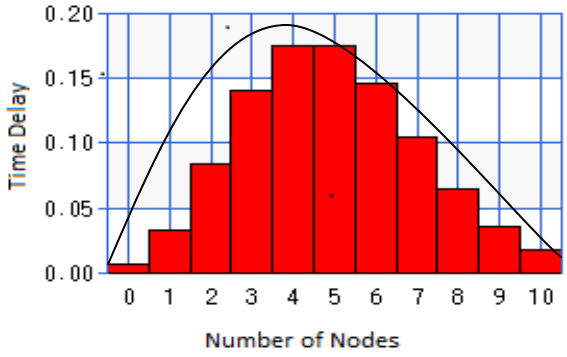

Figure 3: Probabilistic value of time delay using poison distribution

Table 1 shows the delay time calculation for packet delivery with process time in seconds and estimated time. This calculation is based on equation 2 for observing the utilization of the communication path. Figure 4 shows the delay time of packet delivery between source and destination based on the calculation of estimated time in packet delivery. The average delay time of packet transmission with n=5(no of nodes) and Estimated time of 5 nodes is 0.999. In every hop, the processing time and the estimated time has been measured. The processing time has awaited the communication of node 0.03 in seconds for 5 nodes. That is every hop of the distance is varying the certain level and finally reaches to the destination with 0.03 in seconds.

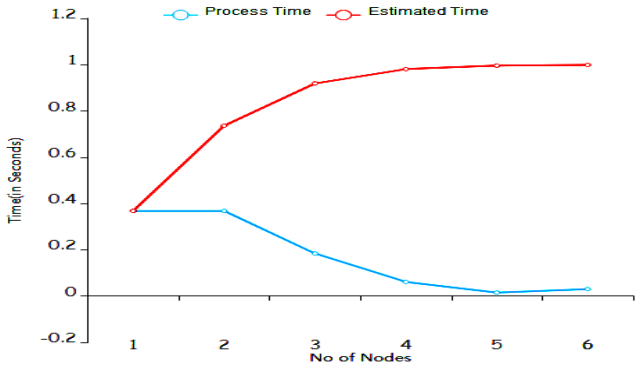

Figure 4: Measurement of Delay time between Estimated and process time

Table 1: Calculation of Process Time and Estimated Time

No of Nodes	Process Time (in seconds)	Estimated Time (in seconds)
0	0.368	0.368
1	0.368	0.736
2	0.184	0.919
3	0.061	0.981
4	0.015	0.996
5	0.03	0.999

When the packet is to send from source to destination, the distance and time have been measured. If average time is exceeded the estimated time, then the PSO algorithm used to identify the congestion and where exactly the path has to be connected. Table 2 shows the Pre-request (PREQ) of packet delivery from source to destination. The number of packets has delivered with data 0,1,..10 and the delay time is measured in every path. The final measurement was taken as 99.16 for 50 seconds is the approximate time for more data with quality of service. Figure 5 shows how the data had been flowing from source to destination that represents in the graphical picture. The flow of data and time delay in every path are represented in figure 5. Once the packet delivery ration has identified by using AODV and PSO, then the security measures should be implemented by using blockchain. The data has been authorized in terms of security. The information is distributed in the intermediate nodes, but an only authorized node can communicate and established the communication.

Table2: Experimental Results of RREQ for measuring packet delivery in AODV

No of Nodes	Pause Time(m/s)	Packet Delivery Ratio
1	0	99.5
2	10	99
3	20	99.4
4	30	99.5
5	40	98.76
6	50	99.16

Figure 6 shows how the packet delivery ratios are measured in every node and how it can be transferred from source to destination by

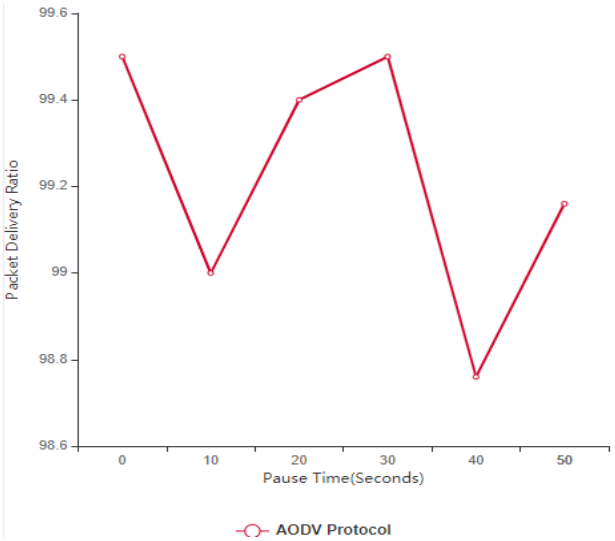

Figure 5: RREQ for measuring packet delivery in AODV

authorized communication. In figure 6, 50 packets are sent from node 1 to node 8 for finding the packet Delivery ratio and measured in every node. The security is adopted in every node for identifying the malicious node. In this case, figure 6 shows the average efficiency of security measures is taken 99 percent.

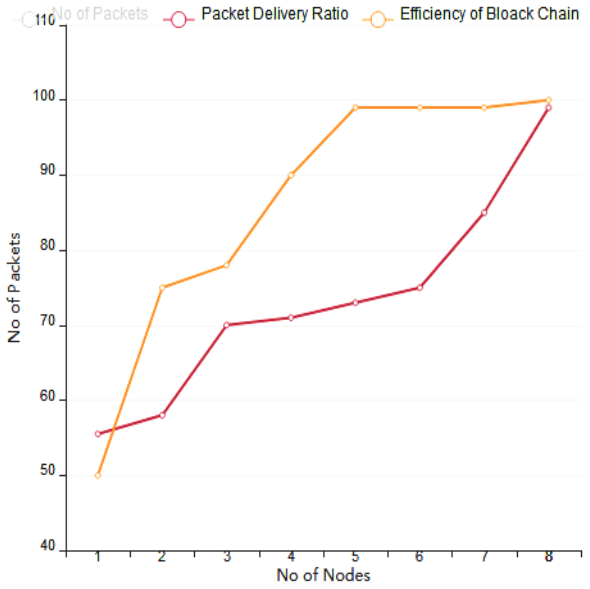

Figure 6: Packet Delivery Ratio with the efficiency of Block Chain

VIII. CONCLUSION

In this paper, we have identified how AODV has integrated with the PSO algorithm for finding the exact delay. The congestion has occurred anywhere of the path, but both algorithms have used to find the exact path for avoiding the congestion. The probabilistic approach of poison distribution has implemented for measuring the delay time when the number nodes are communicated with each other. The efficiency of the AODV protocol has to be identified when the nodes are interconnected by blockchain with the PSO algorithm, The Quality of Service (QoS) has defined in this paper based on packet delivered ratio from source to destination without any congestion. In this scenario packet delivery ratio has implemented with 99.16 for 100 packets which is accumulated in 50 m/s. Finally, the variation of the packet delivery has been achieved within the estimated time. The future enhancement of the work will be extracted for how the data will be secured using consensus mechanism of blockchain in the various levels of networks using n number of nodes.

REFERENCES

1. Amar Adnan Rasheed, “A Dissertation Security schemes for wireless sensor network with moble sinks”, Texas A&M University, May 2010,.pp.153-157.
2. Sung-Jin Choi, Kyung Tae Kim, and Hee Yong Youn, “An energy-efficient key pre-distribution scheme for wireless sensor networks using eigenvector”, College of Information and Communication Engineering, Sungkyunkwan University, Vol 1, 2013, pp. 440-746.
3. D. David Neels Pon Kumar, K.Arun Kumar, M.S.Arthy Professor, Assistant Professor, Student, “ An overview of mobile sink and static access node replication attacks in WSN”, International Journal of Engineering Science and Innovative Technology (IJESIT) Vol 1, 2012, pp.313-320.
4. S. Saranya Devi, N.Suganthi. “An efficient key pre-distribution scheme for Wireless Sensor Network”. International Journal of Communications and Engineering Vol 06, 2012, pp.402-407.
5. Wenliang du., Jig Deng, Yunghsiang. “A PairwiseKey Pre distribution Scheme for Wireless Sensor Networks”, ACM, Vol 1, 2003, pp.1-5.
6. Yang Qin, dijiang Huang, “STARS: A statistical traffic pattern discovery system for MANETs”, Senior Member IEEE, Vol 1, 2014, pp.1-2.
7. J.Kong and X.Hong, “ANODR: Anonymous on-demand routing with untraceable routes for mobile ad-hoc networks”, in ACM MobiHoc’03. Annapolis, MD, Vol 1, 2003, pp 1-2.
8. B. Zhu, Z. Wan, M. S. Kankanhalli. F, Bao, and R. H. Deng, “Anonymous secure routing in mobile ad-hoc networks,” in LCN’04, Vol 1, 2004, pp 102-103.
9. Kenneth W. K. Lui, Jun Zheng, and H. C.,”Particle Swarm Optimization for Time- Difference of Arrival Based Localization, EURASIP, Department of Electronic Engineering, Vol 1, 2007, pp. 414-417,.
10. A.Boukerche, K. EL-Khatib. L. Xu. And L. Korba, “SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks,” in IEEE LCN’04, Vol 1, 2004, pp.618-619.
11. R.Song, L. Korba, and G. Yee, “AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks,” in SASN’05, Vol 1, 2005, pp.1-5.
12. Yan Yu "Improved AODV routing protocol for wireless sensor networks and implementation using OPNET", Intelligent Control and Information Processing (ICICIP), VOL.10, 2012, pp.70-713.
13. Sabin Bhandari and Sangman Moh "Feasibility Study of DSDV and AODV Routing Protocols in Mobile Sensor Networks", Contemporary Engineering Sciences, Vol.7, 2014, pp.1641-1647.
14. Siddharth Singh, Naveen Hemrajani "Performance Evaluation of AODV Routing Protocol in Wireless Sensor Networks with the Constraints of varying terrain areas by varying pause time", International Journal of Emerging Trends & Technology in Computer Science, Vol 2, 2013, pp.75-79.
15. Pu Gong, Thomas M. Chen, and Quan Xu, ETARP: An Energy-Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks, Journal of Sensors, Vol 2015, pp.1-5.
16. Dan Li and Xian bin Wen, "An Improved PSO Algorithm for Distributed Localization in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Vol 2015, pp.1-8.
17. Ziwen Sun, Li Tao, Xinyu Wang, and Zhiping Zhou, "Localization Algorithm in Wireless Sensor Networks Based on Multiobjective Particle Swarm Optimization", Vol.2015, pp.1-9.
18. Keisuke Kameyama,” Particle Swarm optimization-A survey” IEICET trans. Inf. & Syst.Vol.7, 2009, pp.1354-1361.

19. Yongjun Ren et al., “Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks”, Mobile Information Systems, Vol.2018, pp.1-11.
20. Gholamreza Ramezan et al., “A Blockchain-Based Contractual Routing Protocol for the Internet of Things Using Smart Contracts”, Wireless Communications and Mobile Computing, Vol.2018, pp.1-15.
21. Ana Reyna et al., “On Blockchain and its Integration with IoT. Challenges and Opportunities”, Future Generation Computer Systems, Vol.88, 2018, pp.173-180.
22. Jidian Yang et al., “A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks”, Sensors, Vol.19, 2019, pp.1-19.
23. https://blockgeeks.com/guides/what-is-blockchain-technology.

AUTHORS PROFILE

Dr.S.RajAnand received M.E, Computer Science and Engineering from Jaya Engineering college, under affiliated toAnna University, Chennai and Ph.D.,in Computer Science and Engineering fromVel Tech Dr. Rangarajan and Dr. Sagunthala R & D Institute of Science and Technology, Chennai He is currently working as Associate Professor in Department of Computer Science &Engineering at PACE Institute of Technology & Sciences. His research interest includes, Networking, Wireless Sensor Networks andNetwork Security. He has published 18 papers in National and International Journals.

Dr. Rama Chaithanya Tanguturi completed his Doctor of philosophy in Anna University. Areas of interest include AI, ML & Cyber Security. Currently working as Professor & Head, Department of CSE, PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India.

Soundarrajan D S received his M.Tech degree in Computer Science and Engineering from Joggiah College of Technology andSciences, Kalagampudi,West Godavari District. At present he is engaged in Topology Control in Mobile Ad Hoc Networks WITH COOPERATIVE COMMUNICATIONS. He is currently working as Associate Professor in Department of Information Technology at PACE Institute of Technology & Sciences.