International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Secure Cross Layer Architecture for IOT Devices in NGN

Anita Sethi, Sandip Vijay, Anurag Aeron

Abstract: ***Open platform, data filtration using deep analytics improved the driving experience, monitoring cost reduction and safety in heterogenous network. Main objective of this paper is analyzing the leverage of cloud platform with integration of end user devices with security and efficiency. Scalability with time duration are key factors of cross-layer architecture performance. Quick response to end-user and immediate service providing to the business applications makes it interactive to adapt. Reliable and secure commutation at different platforms makes it challenging to implement. It has been observed that turnaround time of receiving an alert is less than 250ms by the client. This paper deliberates the numerous security attacks and Quality of service parameters for improving the performance of network. Prime focus is on secure methodology, congestion and simulation work represents the enhancement of the performance of network. Receiver initiated acknowledgement with multi-hop and multicast communication methodology, cross-layer protocol improves the transmission rate and performance of network using link correlation heuristic. Observation shows that black hole attack can be easily occurs in the ad-hoc network as compared to grey-hole attack which degrades the performance of routing protocol in different scenarios. Impact of scalability on the performance of different routing protocols are observed.***

Index Terms: Mobility, NGN, Scalability, Security.

I. INTRODUCTION

5G technology provides fast and secure network functionality to Industrial control system, Self-directed vehicles and Internet of Things devices while carefully deployed. LTE or WiMAX both are used for 4G data networks where all carriers requires to agree that OFDM is one of the major indicators that a service can opt. Different narrowband channels with different frequencies are used in a single signal in OFDM digital modulation which is more efficient than TDMA and CDMA, uses time slots and multiple signals can be transmitted on the same channel respectively [1]. Throughout a geographical area, simultaneous connections with seamless handoff at multiple high-speed networks is provided by pervasive computing in 5G network. At numerous places like remote service areas and highly dense area coverage improvement technologies like picocell and femtocell fulfil the requirements of mobile users at home, offices and public buildings.

Revised Manuscript Received on 30 May 2019.
* Correspondence Author
Anita Sethi*, ICFAI University, Dehradun, Uttarakhand, India.
Sandip Vijay, Shivalik College of Engineering, Dehradun, Uttarakahnd
Anurag Aeron, ICFAI University, Dehradun, Uttarakhand, India.

Small antennas are deployed on utilities poles, cell towers, private and public structures and lampposts which provides data transfer speed up to 10 Gbps and beyond, fastest as compared to fiber-optic fixed networks [2]. Network slicing helps next generation network to create multiple logical partitions within resource allocations for specific use cases like mission-critical to IoT devices. Home appliances and smart meters, IoT devices requires low level of prioritization, moderated speed and latency of network, whereas remote surgery or manufacturing and autonomous vehicles requires high quality of services and very low latency. Intelligently resource utilization is supported in 5G leads to improved spectral utilization and monetization of deployed resources [3].

Distributed Denial of Service attack and Unauthorized access attempts are recognized by intrusion detection and prevention heuristics in IoT networks. Scanning techniques in the network plays an important role which changes the network path periodically to prevent the unauthorized access with high traffic maintenance. Suricata supports multithreaded processing for multicore CPU for improved performance and Fail2ban supports complex architecture for deployment in cloud environment on different servers and multiple apps with security supported by LLRP protocol [4].

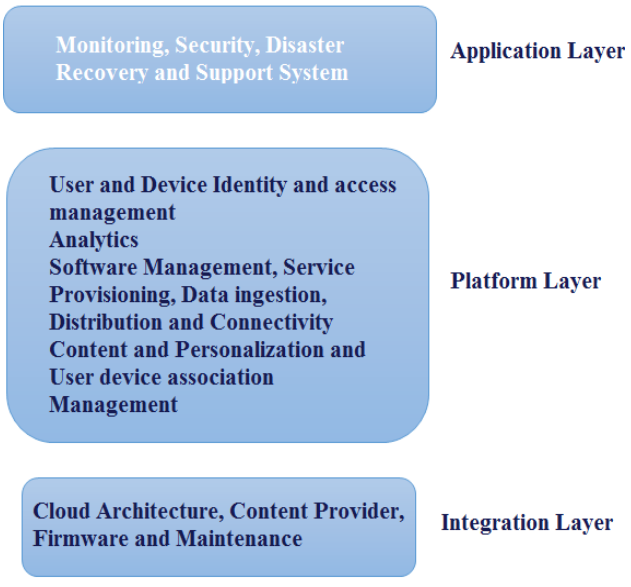


Fig. 1 Layered architecture for NGN systems

II. RELATED WORK

E2E delay, throughput, PSNR with maximum path gain and minimum path loss and other QoS parameters are improved by efficient buffering and channelization techniques, video distortion and reconstruction modelling.

Energy efficiency and channel utilization is improved by abolishing dedicated control packets with 5% enhancement in route optimality by using MAC overhearing with intelligent cross-layer route optimization algorithms. Moreover, energy delay reduction and high data accessibility is achieved with prefetching mechanism in cooperative caching in cross layer design by using clustering heuristic. Further, energy efficiency can be achieved with probability of target detection and delay before the first sensor detection act can extend the network lifetime in dynamic configuration of system parameters with several relevant network topology [4]. In worst traffic load conditions CO-FSR, will not forward data packets will result in better network performance and QoS with increased throughput and reduced average end to end delay in scalable scenario. MAC layer is responsible for selection of adaptive modulation methodology with TCP to improve PDR up to 99.5% and packet loss is reduced in lossy channel and frequent link failure and network partition degradation [5]. Maximum network utilization is achieved by Shannon capacity formula with distribution through messages for both power allocation and rate adaptation. Near optimal scheme which uses convergence rate that is faster than present methodology with some orders of magnitudes and noise measurements in power control devoid of message passing [6]. Cluster overlapping problem is resolved by using approximately equal size clusters selection in KOCH heuristic in scalable and load balanced scenario in constant time regardless of network size by Moustafa [7]. However, node connection change continuously due to mobility in wireless multimedia communication, so overlapping clustering problem can be resolved using grouping as in H-NAME. H-NAME efficiently handles the hidden node avoidance mechanism by using grouping strategy that splits each cluster into disjoint groups of non-hidden nodes which guarantees no interference between overlapping Clusters [8]. Cluster membership and Cluster overlap state using discrete time lumped Markov chain to prototypical the time variation of a system supports cluster stability which is maintained by probability distribution function [9]. AliChamam [10] different power consumption levels, full coverage and sensor connectivity to ClusterHeads with Tabu Search heuristic results in 100% optimal network lifetime values as compared to EESH and modified EESH with low computation time, suitable for large-sized sensor network. Navin Gautam [11] purposed distance aware ClusterHead selection method which outperform LEACH and LEACH-C by 63.28% and 36.27% in energy conservation in his DAIC protocol. Dilip Kumar [12] gives the ClusterHead selection method based on residual energy prolong the network lifetime 63% and 40% respectively and load balancing 12% and 42% respectively. Mehdi [13] repented a distance-based algorithm (SEECH) elects ClusterHead and relays based on nodes eligibilities show average of 45% and 75% performance is computed to LEACH and TCAC for different scenarios. Mirjeta [14] reviewed the clustering algorithm based on Motility, energy, degree and weight. Fifi Farouk [15] showed SEEC provides longer stability period, energy efficient and higher average throughput for homogeneous WSN by using multilevel architecture of clustering, result shows stability ratio is 15.44% better as compared with M-SEP, M-DEC and E-DEEC. Shiva D. [16] purposed two-level hierarchical clustering-based hybrid routing protocol for WSN which analytically evaluate the average query response time. Keisei [17] Okano purposed autonomous clustering based inter-domain routing protocol can adaptively charge in network gateways between different MANETs. Hiren Kumar [18] shows energy efficiency, throughput improved by 15% and prolonged lifetime of nodes is optimized by minimizing reclustering time using hieratical and cluster-based panel in EERR. Muhammad Kumran Naeem [19] suggested dynamic clustering scheme which increases network lifetime by 24.5% and 36% as compared to DDEEC and EDDEEC. Grid technology used in ad-hoc network saves energy up to 80% and 40% energy can be saved by placing nodes randomly at transmitter and receiver clusters. Degree of node reachability is used to calculate the group mobility degree, tested by r-test, results efficient capturing of change in network topology and represents the impact of node mobility of different mobility models. Each neighbor node encodes received packets with sensed packets using XOR network coding mechanism which results coding graph of 1.9 in network coding based probabilistic routing (NCPR) protocol as compared to simple probabilistic model. For detection and prevention of wider range of attacks collaborative security paradigms with a multi-party access control mechanism are used in cloud architecture for secure information sharing. During cyber-attack period it provides communication and collaboration by exchanging their security data.

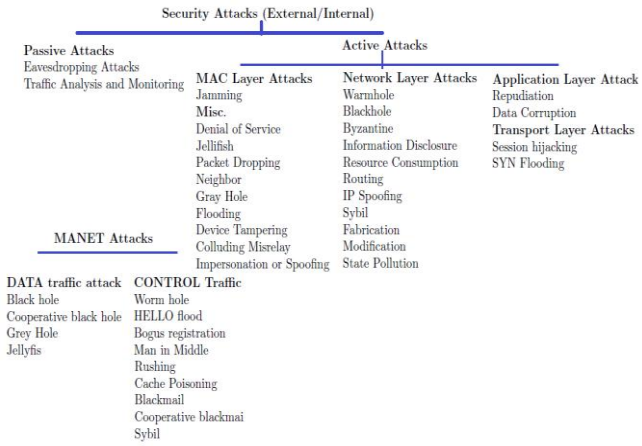


Fig. 2 Categorization of Security Attacks

III. CROSS LAYER ARCHITECTURE FOR HETEROGENEOUS AD-HOC NETWORK

Clusters are created to connect master node or client node using SSH and interfaces using API are used for task performance and queries submission. MQTT servers are used as messaging infrastructure with ultra-reliability and MQTT broker works as central distributor of messages. Real time data pipelines and streaming apps with scalability, fault tolerance and fast response are developed using kafka distributed platform.

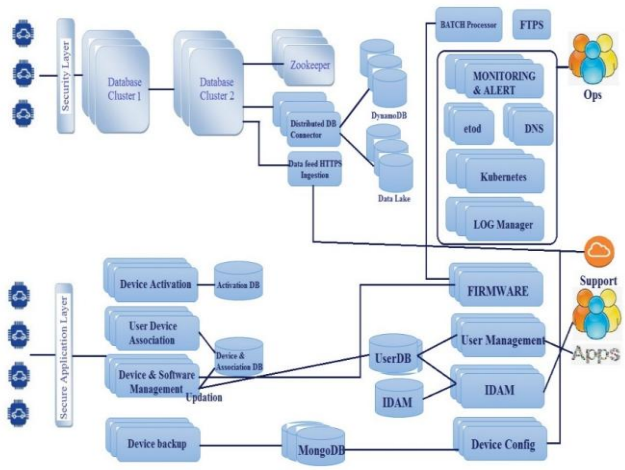


Fig.3 Framework for IoT devices and Cloud architecture

Authentication of the communication device is important phase and successful authentication provides access to the clould architecture. Data is transferred from the communicating device to cloud with high security. Vehicle health, convenience, security, safety and insights are the services provided to the end users in the on board device and saved in to device data. Application interface provides communication mechanisum of different apps in communication device. Vehicle health provide the information of fuel, notification, alerts, repair aggregation, maintenance and diagnostics by using different sensors in the vehicle timely.

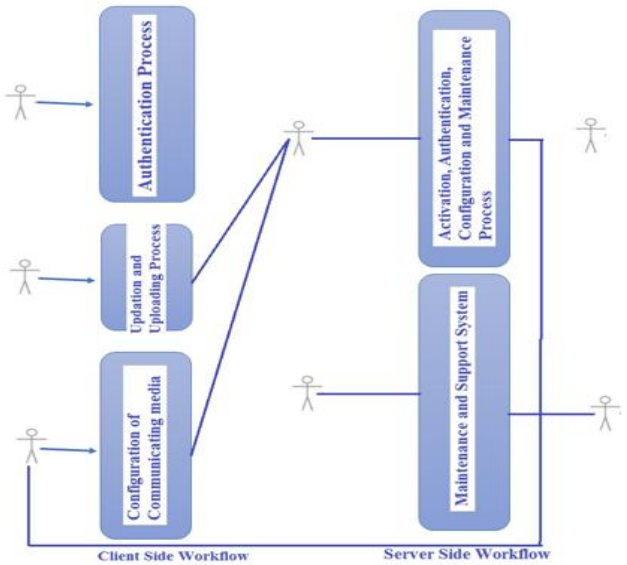


Fig. 4 Interaction between Client and Server side workflow

Vehicle location, geo-fancing, stolen vehicle tracking, speed limits are the services provided in security section. Fleet/Family tracking, crash detection, notification and assistance and on-demand roadside assistance are major safety apps are important for the end users. Trip details, business trips and driving behaviour is observed observed by the sensors and information is provided by different apps. On board service fetches the data from the vehicle and provide it to the requester by using queries. Wifi hotspot provsioning, configuration, enabling and disabling apps by using system specific calls after authentication communicate to the cloud architecture. TLS or SSH secure transport layer is used in cross-layer architecture when traffic from external source is entering in the cloud platform. Control packet contains the services information about interfaces of mobile/WEB and device, such as REST, MQTT, OTA, Firmware information, cloud information and kafka event streams. These services are essential for authentication at server via X.509 v3 TLS server certificates as well as client at application layer. Sensitive data is handled by Data at Rest Security with access control of authorization, authentication and encryption process. Symmetric keys are used for encryption of DAR. Server-side encryption is handled by cloud architecture while client-side encryption is transparent and make sure encrypted data should be transformed. In this framework at different places device authentication is necessary for security purpose. Token based authentication is used for primary IDs hypothetically different across the scenarios due to requirement IDs. Prior to device activation, occurrence of OTA is required which enables Anonymized Harman ID and secrets as part of the device activation scenario.

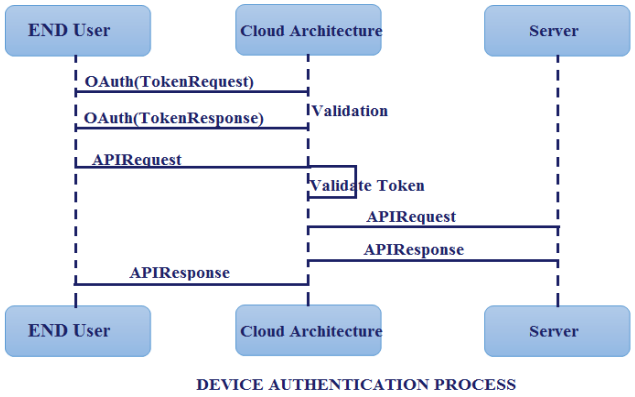


Fig. 5 Device Authentication Process

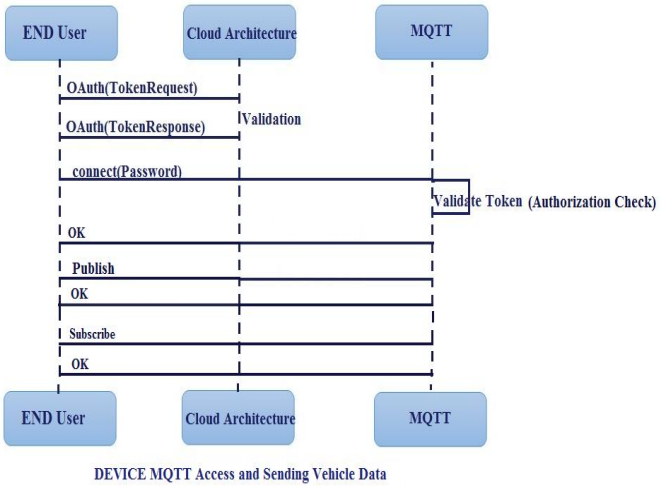
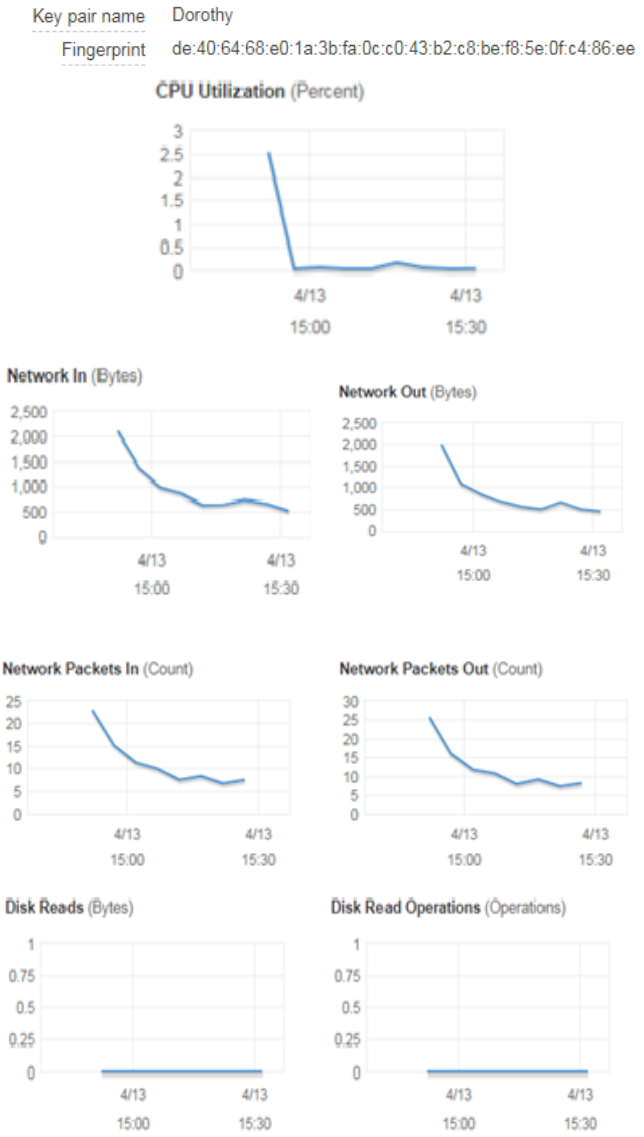
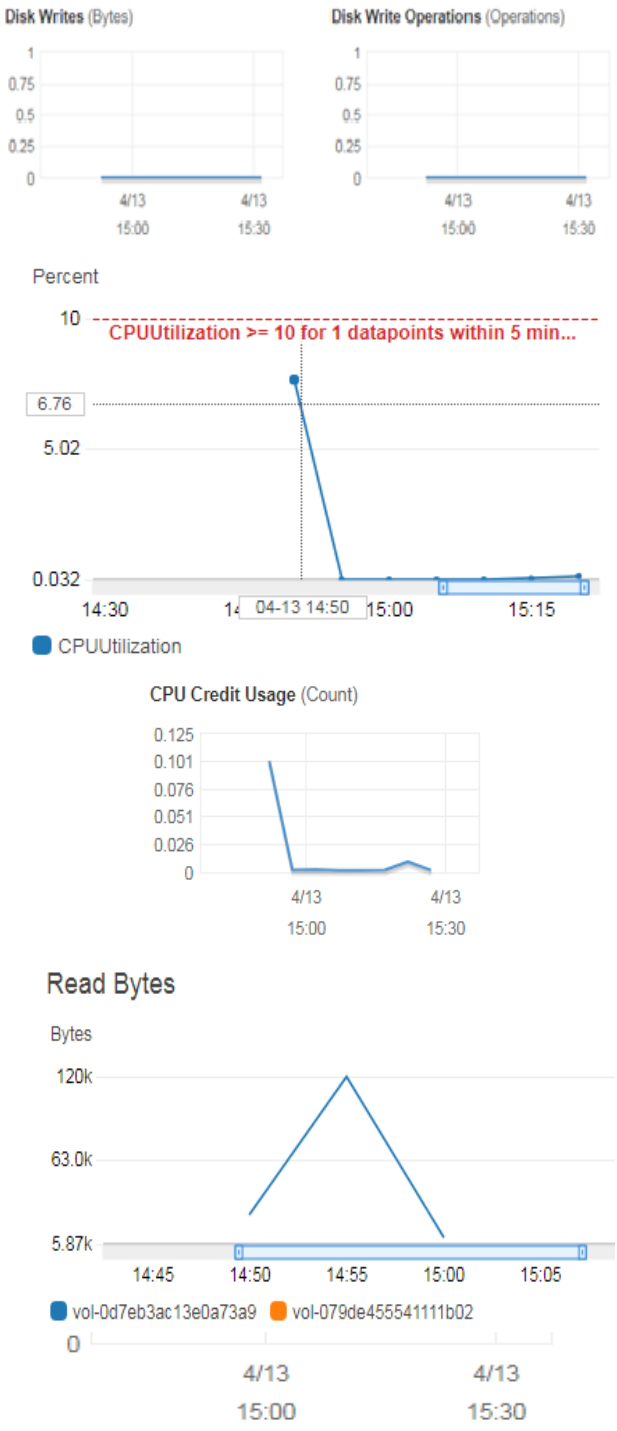


Fig. 6 Device MQTT Access and Sending Vehicle data

IV. RESULT ANALYSIS

Downtime due to link failure is adjustable while transmitting the data from client database to cloud architecture and in reverse from cloud to user application reliably. Data delivery time is less than 250ms in real time scenario when there is no link failure occurs. Prioritization to message forwarding is provided by schedular within minimum time duration and in case of failure messages would be persisted. Backup and failure recovery are important factors which are supported on board unit and responsible for checking the health of the object and in case of failure or crash occurs immediate restart is provided in the maintenance phase of the OBD unit. Update rate of the sensor framework which is adjustable is 60ms with +/- 8G magnitude default value. With Android platform updating time of sensor data is more than 60ms which is adjustable.





Attack/ Parameters	Greyhole attack Detection	Blackhole Detection
Total Sent Packet	50	50
Total Received Packet	50	50
Duration	6.60662Seconds	6.60662Seconds
Transmitted bits	401408bits	409600bits
Received bits	401408bits	409600bits
Throughput	0.244616 Mbps	0.246226 Mbps

Avereage End to End Delay	31.299ms	31.729ms
Average Packet Delivery Fraction	1	1
	After 20 sec Grey hole attack in wireless mesh network: Packet dropped!!!	After 50 sec Blackhole Attack in wireless mesh network! Packet dropped . . .

V. CONCLUSION

Whenever an instance of infrastructure or service is created in the cloud architecture, a secure connection is established using SSH. Secure Hash function is used for the security purpose. Numerous certificate generation heuristics are used for making network and user data secure. Different graphs represent the various resources utilization like CPU, hard disc and network interface in the cloud architecture. Observation shows that black hole attack can be easily occurs in the ad-hoc network as compared to grey-hole attack which degrades the performance of routing protocol in different scenarios. Impacts of scalability on the performance of different routing protocols are observed. Simulation is performed in NS3, which represents that after 20 sec of simulation grey hole attack is detected whereas black hole is detected after 50 sec.

REFERENCES

1. X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software defined networking for smart grid resilience: Opportunities and challenges," in Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, ser. CPSS '15, 2015
2. Prithviraj Patil, Akram Hakiri, Yogesh Barve and Aniruddha Gokhale "Enabling Software-Defined Networking for Wireless Mesh Networks in Smart Environments" IEEE proceedings 2016 pp. 112-119.
3. Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond C "A blockchain future for internet of things security" Digital Communications and Networks 4 2018 pp. 149–160
4. Mohamed S. Hefeida, Turkmen Canli and Ashfaq Khokhar "CL-MAC: A Cross-Layer MAC protocol for heterogenous Wireless Sensor Networks 2013 Ad Hoc Networks 11 pp. 213-225
5. Sang Hoon Lee and Lynn Choi "Cross-Layer Route Optimization using MAC Overhearing for Reactive Routing Protocols in MANETs" 2013 IEEE pp. 550-555.
6. BatoulSarvi, Hamid R. Rabiee, KiarashMizanian "An adaptive cross-layer error control protocol for wireless multimedia sensor networks" Ad Hoc Networks (2016) 1–13
7. Moustafa A. Youssef, Adel Youssef and Mohamed F. Younis "Overlapping Multihop Clustering for Wireless Sensor Networks" 2009 IEEE Transaction on Parallel and Distributed Systems Vol. 20, No. 12 pp. 1844-1855.
8. Anis Koubaa, Ricardo Severino, Mario Alves and Eduardo Tovar "Improving Quality-of-Service in Wireless Sensor Networks by Mitigating "Hidden-Node Collisions"" 2009 IEEE Transaction on Industrial Informations, Vol. 5 No. 3 pp. 299-312.
9. Khadige Abboud, Weihua Zhuang "Stochastic Modeling of Single-Hop Cluster Stability in Vehicular Ad Hoc Networks"2015 IEEE transactions on Vehicular Technology pp. 1-14.
10. Ali Chamam and Samuel Pierre "On the Planning of Wireless Sensor Networks: Energy-Efficient Clustering under the Joint Routing and Coverage Constraint" Aug. 2009 IEEE Transaction on Mobile Computing Vol. 8 No. 8 pp. 1077-1086.
11. Navin Gautam and Jae-Young Pyun "Distance Aware Intelligent Clustering Protocol for Wireless Sensor Networks" Apr. 2010 Journal of Communication and Networks Vol. 12 No. 2
12. Dilip Kumar "Performance analysis of energy efficient clustering protocols for maximizing lifetime of wireless sensor networks" 2014 IET Wireless Sensor Systems vol 4 Iss. 1 pp. 9-16
13. Mehdi Tarhani and Yousef Kavian "SEECH: Scalable Energy Efficient Clustering Hierarchy Protocol in Wireless Sensor Networks "2014, IEEE Sensors Journal 14(11) pp. 3944-3954 ·
14. MirjetaAlinci, EvjolaSpaho, Algenti Lala and VladiKolici "Clustering Algorithms in MANETs: A Review"2015 9th IEEE International Conference on Complex, Intelligent, and Software Intensive Systems pp. 330-335
15. Fifi Farouk, RawyaRizk and Fayez W. Zaki " Multi-level stable and energy-efficient clustering protocol in heterogeneous wireless sensor networks" Oct. 2014 IET Wireless Sensor Systems pp. 159-169.
16. Siva D. Muruganathan, Abu B. Sesay and Witold A. Krzymien "Analytical Query Response Time Evaluation for a Two-Level Clustering Hierarchy Based Wireless Sensor Network Routing Protocol" may 2010 IEEE Communications Letters Vol. 14 No. 5.
17. Keisei Okano, YutoAkoi, Tomoyuki Ohta and Yoshiaki KaKuda "An Autonomous Clustering-based Inter-domain Routing Protocol for Heterogeneous Mobile Ad Hoc Networks" 2014 10th International Conference on Mobile Ad-hoc and Sensor Networks pp. 144-150.
18. Hiren Kumar Deva Sarma, Rajib Mall and Avijit Kar "E2 R2: Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks" 2015 IEEE Systems Journals pp. 1-12
19. Muhammad Kamran Naeem, Mohammad Patwary and Mohamed Abdel-Maguid "Universal and Dynamic Clustering Scheme for energy Constrained Cooperative Wireless Sensor Networks" January 2017 IEEE ACCESS