Key Management and Cryptography in Wireless Sensor Networks

Afreen Rafiq, Varsha Boreda, Sai Eswari Dutta

Abstract: ***The use of Wireless Sensor Networks (WSN) in the field of military, battlefield, healthcare applications etc has seen a plethora of growth towards variety of sensory devices. Irrespective of different locations, the sensor nodes has to do its task. Hence, the dynamic wireless sensor networks should ensure better quality of sensor nodes that covers wider network area and additional services in relative to static WSNs systems. By doing so, it requires secure data communication among the sensor nodes in wireless environment. Key Management is the recent security concept enabled to provide secure communication between sender and receiver nodes. In this paper, we have proposed efficient key updates systems between the nodes. In any scenario, the nodes may join or leaves the network environment which facilitates to initiate a secret key between intended sender and intended receiver. A certificate less key secrecy system is designed for secure communication in wireless links. By designing so, we have addressed the issues like node authentication, data confidentiality and data integrity. Experimental analyses have shown the effectiveness of proposed system.***

Keywords: Wireless Sensor Networks, Dynamic networks, Sensor nodes, Sensory devices, Key management, Key updates and Node authentication.

I. INTRODUCTION

Nowadays, the exploration on wireless technologies has attracted many network users. Wireless networks is that the recent technology wherever tremendous volume of knowledge may be accessed from anyplace at any time. The outstanding options like fault resistance, self-adaptability, quantifiability, traceability etc have developed bigger impact among the wireless users [1]. Wireless networks comprise two sorts, namely, static wireless sensing element networks and dynamic wireless sensing element networks. In relative to the static WSNs, the dynamic WSNs make sure the correct node detection, relevant network coverage and facilitating best QoS. Henceforth, Dynamic Wireless sensing element Networks play a significant role in several components of the period of time systems. Most of the dynamic wireless sensing element networks square measure applied to find the criminal offences, aid systems, traffic flow and vehicle detection. Thus, security is one in every of the foremost vital ideas in dynamic WSN applications [2].Key management system is one in every of the solutions for effective security systems. within the read of security, authentication and

privacy make use of the key systems. Generally, key is the secret thing which is used for authenticating the users [3]. Similarly, key function is also used for encrypting and decrypting the information. Key is the fixed length streams of random bits which are only known for specific parties. It also makes use of mathematical functions to retrieve the original information using their keys. In order to effectively generate and manage the keys, the mathematical functions should be generated properly. Since, different features of WSN have impressed the users for different applications [4].

Key institution is any technique within the cryptography by that cryptographical key square measure changed between 2 parties, permitting the utilization of a cryptographical algorithmic rule. If the sender and also the receiver want to exchange encrypted messages, every ought to be equipped to code messages that square measure to be sent and rewrite messages received. The character of the militarization demand depends on the secret writing technique that's used. If they use a code, each shall need a duplicate of identical codebook [5]. If they use a cipher, they're going to want acceptable keys. If the cipher is of uneven key cipher, each shall want a duplicate of identical key. If AN uneven key cipher with the public/private key property, each shall want the other's public key.

The rest of the paper is organized as follows: Section II describes the connected work, Section III presents the planned work; Section IV presents the experimental analysis and results and concludes in Section V.

II. RELATED WORK

This section presents the fundamentals of security and prior works carried out by other researchers.

2.1 2.1 Security prerequisites for key administering schemes:

An effective key system is defined from generation and establishment of sensor networks. The following are the important points [6]:

- Nodes should be in admissible range for communication.
- Deployed nodes must ensure secure node-to –node communication.
- Additional nodes can also deploy which should ensure better communication systems.

Manuscript received on January 02, 2020.
Revised Manuscript received on January 15, 2020.
Manuscript published on January 30, 2020.
* Correspondence Author

Mrs. Afreen Rafiq*, Asst. Professor, Dept. of CSE, MRECW, Hyderabad, India. Email: afreenrafiq2@gmail.com

Ms. Varsha Boreda, Asst. Professor, Dept. of CSE, KMIT, Hyderabad, India. Email: varsha5592@gmail.com

Ms. Sai Eswari Dutta, Asst. Professor, Dept. of CSE, KMIT, Hyderabad, India. Email: saieswari3@gmail.com

- Any nodes can join or leave the networks.
- If the nodes are misbehaved, any alternate nodes should take care of further responsibilities. Similarly, the key management should satisfy the basic security requirements like confidentiality, authentication, integrity and non-repudiation [7].

Relied upon the application environment, the keys should be established properly. The evaluation metrics to be considered are security, efficiency and flexibility. In addition to, the metrics like node revocation, secrecy and collusion resistance [8].

a) Node revocation: If any nodes are compromised, then alternate nodes should be revoked or provoked.

b) Secrecy: Before outsourcing the data, it should be properly encrypted and then forward to the intended users.

c) Attacks resistance: In any scenario, the adversary may threaten the networks. A better key management system induces better resistance towards attacks.

d) Resilience: It depends on the execution of nodes from the memory of the sensor nodes [9].

2.2 Prior works:

This half portrays previous works processed by alternative researchers. The author in [10] mentioned concerning key administration method exploitation cluster based mostly WSNs. Their model was compared with the 2 stratified key management systems that proven that cluster based mostly model has generated economical keys in reduced time. They delineated a far better performance over cluster model. The author in [11] bestowed pairing based mostly key agreement protocols exploitation elliptic curves. This protocol acted as intermediate between users World Health Organization hold similar same keys. It reluctantly reduced key house and resolved the attacks like message larceny and reply attacks. The author in [12] presented key administration process over heterogeneous sensor networks. They have utilized on static sensor nodes which shown reduced communication overhead. The author in [13] presented key generation process for mutual authentication process in mobile sensor nodes. They supplied two keys, namely, pair wise and cluster keys. This key was supplied to elliptic curve digital signature algorithms. Relied upon the mobility of nodes, the pair wise and cluster keys are established. The author in [14] discussed about signcryption based heterogeneous systems. They introduced Elliptic Curve Cryptography (ECC) algorithm for lessened communication overhead and storage keys.

The author in [15] surveyed concerning potency metrics of dynamic key management systems that resource unnatural property of detector nodes that exhibited dynamic key established method. As indicated by the safe correspondence request in WSN, 2varieties of key organization area unit needed. One is combine shrewd key organization; the inverse is bunch key foundation. a handful plans has been anticipated that joins three stages usually [10]:(1) key setup before causation, (2) shared-key revelation once arrangement, associate degrees (3) manner key foundation if two detector hubs do not provide an on the spot key. The foremost modish combine perceptive key pre-conveyance answer is Random combine savvy Key topic [16] that addresses incidental capability disadvantage and offers some key strength. Its upheld Erodes and Reni's [17] work. Every police work part hub stores associate degree irregular arrangement of rear pair-wise keys to accomplish probability p that two hubs area unit associated. Neighboring hubs can tell on the off probability that they share a typical pair-wise key once they send and obtain "Key Discovering" Message within radio extent. Its imperfectness is that it penances key property to diminish the capability utilization.

Nearest (area based) combine-wise keys pre-conveyance subject [18] is another to Random pair savvy key arrange. It exploits the circumstance info to enhance the key convenience. Later on, Random key-chain primarily based usually key pre-appropriation answer is another impulsive key pre-circulation arrangement that started from the solution of basic probabilistic key distribution arranges [14]. It depends on upon probabilistic key sharing among the hubs of associate degree irregular diagram. There are unit various key support recommendations to fortify security of the designed up affiliation keys, and enhance flexibility [19]. Target is to solidly produce a completely unique affiliation or manner key by utilizing created keys, so the

Mystery's not com-secure once one or a substantial live of police work part hub is caught [20].

III. METHODOLOGY

Key maintenance and cryptography in a wireless sensor networks (WSN) can be decomposed into four phases. The first is the key distribution or pre-distribution phase where secret keys are distributed to sensor nodes for use with the security mechanisms (i.e., confidentiality, authentication and integrity). In a large scale WSN, it may be in feasible, or even impossible in uncontrolled environments, to visit large number of sensor nodes and change their security configuration. Thus, keys and keying materials may be pre-distributed to sensor nodes in a central location a priori to the deployment. This phase is also named as key setup. The second is the shared-key discovery phase, which starts after the sensor network deployment, each sensor node discovers its neighbors and a common key with each of them. The third is the key establishment phase where each pair of neigh-boring nodes, which do not have common keys, establish one or more keys. Key establishment between two nodes can be achieved by using pre-distributed keying materials and by exchanging messages directly over their insecure wireless link or over one or more secure paths on which each link is secured with a secret key. Sensor nodes have a limited life time, and they are subject to variety of attacks including node capture. New sensor nodes may be deployed and security materials on existing ones may need to be updated. Thus, the fourth is the key update phase where the secret keys which are used to secure the links between neighbor-ing nodes are updated. We classify and evaluate key maintenance solutions by considering following properties:

1. Underlying network architecture. In distributed WSN, there is no resource rich member and sensor node has equivalent capabilities in hierarchical WSN, there are one or more resource rich central stations, and there is a hierarchy among the sensor nodes based on their capabilities.

2. Communication style. A secure unicast communication between a pair of neighboring nodes requires a pair-wise key shared between them. Are usable pair-wise key is used to secure the unicast communication between more than one pairs of neighboring nodes. Disadvantage is that more than one links are compromised when a reusable pair-wise key is compromised. For improved security, a dedicated pair-wise key may be assigned to each pair of neighboring nodes.

A secure multicast communication within a group of sensor nodes requires a group-wise key, and a secure broadcast communication within a WSN requires a network-wise key.

3. Key pre-distribution method. Keys and keying materials are distributed to sensor nodes based on a probabilistic, deterministic or hybrid algorithm.

4. Key discovery and establishment method. A set of solutions pre-distribute a list of keys, called a key-chain, to each sensor node, and a pair or a group of sensor nodes can secure their communication if they have a key in common. Other solutions pre-distribute keying materials (i.e., one-way hash functions, pseudo-random number generators, partial key matrices and polynomial shares). A pair or a group of sensor nodes can use these materials to securely generate a common key. So after overall observations we can be used Non-Credentials Key Governance Process (NC-KGP) algorithm for key management and cryptography in wireless sensor networks.

IV.PROPOSED WORK

4.1 Motivation:

The advancements made in the wireless technologies have attracted several wireless users with its unique features. We have analyzed different mechanisms which drives the event of key management systems. Most of the key management system's performance restricted by its node constraint and mobility constraints. Environment variables are responsible for achieving better key establishment systems. In order to gather the information about its nearest nodes, the secret key should be efficiently and effectively generated with uncompromised mathematical operators. Inspired by this fact, we have designed non-certificate key establishment process in Dynamic Wireless Sensor Networks (DWSNs). Though, different sorts of key governance process have been researching, the issues like restricted energy and processing capability are not yet resolved.

4.2 Proposed Non-Credentials Key Governance Process(NC-KGP):

A. Prerequisites keys for NC-KGP:

- Non-credentials public and private key: The base station creates a pair of public and private keys from Key Generation Center (KGC). This process is done before the deployments of nodes.
- Independent keys: This key is created for every node.
- Creation of pair wise keys: It is created between the nodes for mutual authentication process.
- Cluster keys: This key is distributed to its node in groups. Cluster head will be chosen by its nodes in networks.

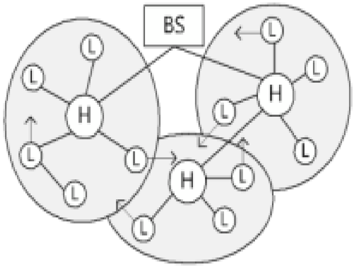


Fig.1. System Architecture

B. Steps in NC-KGP:

System Set-up: This process initiates the number of sensor nodes with the help of Base Station (BS). Each node registers itself with its parameters before the deployment process.

founding of pair wise key: Initially, a node sends "Hello message and public key" to its neighboring nodes and collect its details like energy rate, transmission rate, packet length etc. a try of Master keys and cryptography keys area unit generated. Try of master keys is established for secure message transmission. try of cryptography keys is generated for triple-crown validation of HMAC systems.

Establishment of clusters: After the deployment of nodes by H sensor, the L sensor is generated for content transformation and security validation process. This process creates cluster keys for every node in its groups.

Key tidings: Key tiding is the process of validating the keys for every stipulated time to eliminate the activities processed by adversaries.

Motility of nodes: This step gets succeed only when cluster key is efficiently administered by H sensors. Every change in the node is monitored progressively that updates the cluster keys.

Revocation of keys: Intrusion Detection Systems (IDS) is introduced by the Base station (BS) to study and monitors the malicious events. With the advent of node's status, the information gets updated and processed to the Base Station.

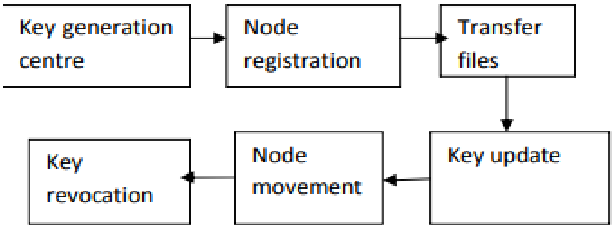
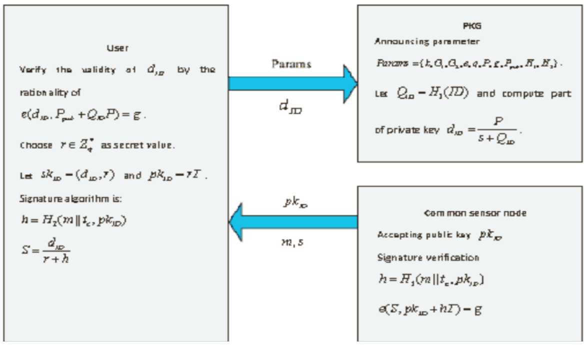


Fig.2. Proposed workflow



Verify the validity of d_{ID} by the rationality of

$e(d_{ID}, P_{pub} + Q_{ID}P) = g$.

Choose $r \in Z_q^*$ as secret value.

Let $sk_{ID} = (d_{ID}, r)$ and $pk_{ID} = rT$.

Signature algorithm is:

$h = H_2(m \| t_c, pk_{ID})$

$S = \frac{d_{ID}}{r+h}$

Announcing parameter

$Params = \{k, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$.

Let $Q_{ID} = H_1(ID)$ and compute part of private key $d_{ID} = \frac{P}{s+Q_{ID}}$.

Accepting public key pk_{ID}

Signature verification

$h = H_2(m \| t_c, pk_{ID})$

$e(S, pk_{ID} + hT) = g$

Fig.3. Execution process of NC-KGP scheme

V. EXPERIMENTAL STUDY

This section presents the experimental analysis of our planned NC-KGP theme with static no. of nodes below restricted assets. The target of the study is to effectively utilize the energy of the nodes with reduced knowledge loss and while not compromising the accuracy of authentication. The subsequent square measure the analysis metrics analyzed:

A. Efficiency of keys:

While doing the protocol analysis, the process value taken by hash operation square measure eliminated. Since the validation formula involves scalar multiplication and additive pairing method, the planned NG-KGP theme effectively analyzes the message operate with sure limitations. The length of public key and pair wise keys generation square measure done by purpose compression of cluster G1 that shows that the planned theme incurs less bits for key generation than the present schemes.

B. Processing cost:

Generally, the processing cost is studied by the interchanging parameters of the sensor nodes. Since bilinear pairing is used for generating master keys and pair wise keys. Below the fig.4 represents the processing cost taken by analyzing the neighboring nodes. It is inferred that our proposed scheme includes lesser processing cost as the no. of neighboring nodes.

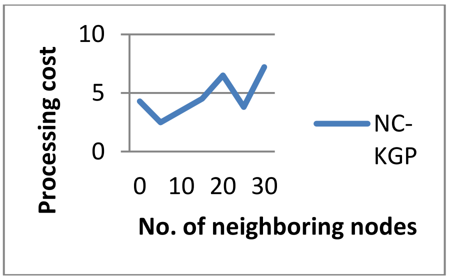


Fig.4. Processing cost analysis of NC-KGP scheme

C. Energy Consumption study:

Since the nodes ar dynamic in nature, the secure communication depends on the energy consumed by the nodes exploitation the updated neighboring nodes from the bottom Station. Supported the storage of public keys, the energy analysis is finished. From the fig.5, it's inferred that the information measure and energy of our planned theme is comparatively tiny and appropriate for WSN.

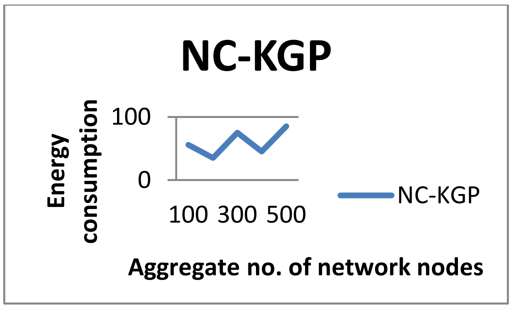


Fig.5. Energy consumption analysis

VI.RESULTS

The algorithm is Non-Credentials based Key Governance Process (NC-KGP) can be used gather the information regarding its nearest nodes processing cost, the secret key should be efficiently and effectively generated with uncompromised mathematical operators. So the following Table-I depicts the NC-KGP status and their processing node costs for number of neighboring nodes based on which approach has been used for the key maintenance and cryptography in wireless sensor networks as well as Table-II also depicts the results of key maintenance for aggregate no. of network nodes in WSN. These two tables are given below

Table-I: Process of key maintenance solutions in WSN.

NC-KGP status	Processing cost	No. of neighboring nodes	Problem	Approach	Mechanism
active	0	0	Dedicated Pair-wise	Probabilistic	Key Generation
active	5	10	Dedicated Pair-wise	Probabilistic	Key Generation
active	10	20	Dedicated Pair-wise	Probabilistic	Key Generation
active	15	30	Dedicated Pair-wise	Probabilistic	Key Generation

Table-II: Results of key maintenance for network nodes in WSN.

NC-KGP status	Energy Consumption	Aggregate No. of network nodes	Problem	Approach	Mechanism
active	0	0	Group wise	Deterministic	Key Generation
active	50	100	Group wise	Deterministic	Key Generation
active	100	200	Group wise	Deterministic	Key Generation
active	150	300	Group wise	Deterministic	Key Generation

VII. CONCLUSION

Developments made in Dynamic Wireless Sensor Networks have made us to delve into the study of security schemes and its adoption in real-time practices. This paper is the study of enhancing the security mechanism without compromising the energy consumption and data loss. To resolve this issue, we have proposed Non-Credentials based Key Governance Process (NC-KGP) scheme which mutually authenticates the wireless users without revealing their original identities. Most of the key management system's performance restricted by its node constraint and mobility constraints.

Environment variables are responsible for achieving better key establishment systems. In order to gather the information about its nearest nodes, the secret key should be efficiently and effectively generated with uncompromised mathematical operators. Simulation analysis has been carried out in terms of keys efficiency, processing cost and energy consumption analysis. The results have shown that our proposed scheme works better than the other baseline algorithms.

REFERENCES

1. Seung-Hyun Seo et al, “Effective Key Management in Dynamic Wireless sensing element Networks”, IEEE transactions on info forensics and security, 10 (2), 2015.
2. Andrea Tassi, Francesco Chiti, Romano Fantacci, and Fabio Schoen " Associate in Nursing Energy-Efficient Resource Allocation theme for RLNC-Based Heterogeneous Multicast Communications” IEEE Communications Letters, Vol. 18, No. 8, August 2014.
3. Andrea Tassi, Francesco Chiti, Romano Fantacci, And Fabio Schoen “An Energy-Efficient Resource Allocation theme For RLNC-Based Heterogeneous Multicast Communications”. IEEE Communications Letters, Vol. 18, No. 8, August 2014.
4. Bo Zhu, Member, IEEE, Sanjeev Setia, Sushil Jajodia, Senior Member, IEEE, Sankardas Roy, Member, IEEE, and Lingyu Wang, Member, IEEE. “Localized Multicast: economical and Distributed duplicate Detection in Large-Scale sensing element Networks” IEEE Transactions On Mobile Computing, Vol. 9, No. 7, July 2010.
5. Taekyoung Kwon, Member, IEEE, JongHyup Lee, Student Member, IEEE, and JooSeok Song, Member, IEEE . “Location-Based Pairwise Key Predistribution for wireless sensing element Networks” IEEE Transactions On Wireless Communications, Vol. 8, No. 11, Nov 2009.
6. Wei-Shou Li, Student Member, IEEE, Tung-Shih Su, Student Member, IEEE, and Wen-Shyong Hsieh. “Multi-Neighbor Random Key Pre-Distribution: A Probabilistic Analysis”. IEEE Communications Letters, Vol. 13, No. 5, May 2009
7. Azzam I. Moustapha, Member, IEEE, and Rastko R. Selmic, Member, IEEE. “Wireless sensing element Network Modeling victimization changed repeated Neural Networks : Application to Fault Detection”. IEEE Transactions On Instrumentation And activity, Vol. 57, No. 5, May 2008.
8. Wenliang Du, Member, IEEE, Jing Deng, Member, IEEE, Yunghsiang S. Han, Member, IEEE, and Pramod K. Varshney, Fellow, IEEE.“A Key Predistribution theme for sensing element Networks victimization readying Knowledge”. IEEE Transactions On Dependable And Secure Computing, Vol. 3, No. 1, January-March 2006
9. X.-J. Lin and L. Sun, “Cryptanalysis and improvement of a dynamic and secure key management model for graded heterogeneous sensing element networks,” in Proc. IACR Cryptol. ePrint Archive, 2013, pp. 698–698.
10. D. Du, H. Xiong, and H. Wang, “An economical key management theme for wireless sensing element networks,” Int. J. Distrib. sensing element Netw., vol. 2012, Sep. 2012, Art. ID 406254.
11. X. He, M. Niedermeier, and H. de Meer, “Dynamic key management in wireless sensing element networks: A survey,” J. Netw. Comput. Appl., vol. 36, no. 2, pp. 611–622, 2013.
12. M. Rahman and K. El-Khatib, “Private key agreement and secure communication for heterogeneous sensing element networks,” J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 858–870, 2010.
13. M. R. Alagheband and M. R. Aref, “Dynamic and secure key manage-ment model for graded heterogeneous sensing element networks,” IET Inf. Secur., vol. 6, no. 4, pp. 271–280, Dec. 2012
14. M. Eltoweissy, M. Moharrum and R. Mukkamala, “Dynamic Key Management in sensing element Networks,” Communications Magazine, IEEE, vol 44, pp 122- one hundred thirty, April 2006.
15. P Krishna Kishore, “An Authentication of Significant security for accessing Password through Network System” volume.12, pages.3130-3133, publisher: http://www.ripublication.com, International Journal of Applied Engineering Research, 2017.
16. P Krishna Kishore, “An efficient probability of detection model for wireless sensor networks” pages. 585-593, book. Proceedings of the First International Conference on omputational ntelligence and Informatics, publication date:2017, publisher: Springer, Singapore.
17. P Krishna Kishore, “DITFEC: Drift Identification in Traffic-Flow Streams for DDoS Attack Defense Through Ensemble Classifier” book: Computing and Network Sustainability, pages. 299-307, publisher: Springer, Singapore, 2019.
18. P Krishna Kishore, “Detection, Defensive and Mitigation of DDoS Attacks through Machine learning Techniques: A Literature” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, pages. 2719-2725, November 2019.
19. Arvinderpal S. Wander, Nils Gura, Hans Eberle,Vipul Gupta, and Sheueling Yangtze Kiang Shantz.(2005) EnergyAnalysis of Public Key Cryptography for Wireless sensing element Networks. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, pages 324– 328.
20. He Daojing, Chen Chun, Chan Sammy, Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless sensing element Networks, IEEE Transactions on Industrial physical science sixty, 5348-5354 (2013).
21. Li Chun-Ta, Weng Chi-Yao, Lee Cheng-Chi, a complicated Temporal Credential-Based Security theme with Mutual Authentication and Key Agreement for Wireless sensing element Networks, Sensors 13, 9589-9603 (2013).
22. Yu Yong, metallic element Jianbing, Sun Ying, Security Analysis of a Distributed Reprogramming Protocol for Wireless sensing element Networks, IEICE Transactions o info And Systems E96D, 1875-1877 (2013).
23. Sun Da-Zhi, Li Jian-Xin, Feng Zhi-Yong, the safety and improvement of a two-factor user authentication theme in wireless sensing element networks, Personal and omnipresent Computing seventeen, 895-905 (2013).
24. Kifayat Kashif, Merabti Madjid, Shi Qi, Component-based security system &#40;COMSEC&#41; with QoS for wireless sensing element networks, Security and Communication Networks half dozen, 461-472 (2013).

AUTHORS PROFILE

Mrs. Afreen Rafiq, received bachelor's degree in IT from Osmania University, in 2013. She has completed mtech in Software Engineering from CSE, Osmania University in 2015 with major in location and qos based web service recommender system.

Ms. Varsha Boreda Assistant Professor in the department of Computer Science and Engineering at Keshav Memorial Institute of Technology(KMIT).She has received bachelor's degree in CSE from JNTUH, in 2013. She has completed MBA in Finance and Marketing, Osmania University in 2017. She is interested in cryptography, Data communication. Her current research include Networking.

Ms. Sai Eswari Dutta has received bachelor's degree in CSE from JNTUH, in 2013. She has completed MTech in CSE from JNTUH in 2015. In 2016 she started her professional career as Assistant Professor in department of CSE, JNTUH. Her current field placement is with Keshav Memorial Institute of Technology(KMIT).She has also published national and international papers in reputed journals. Her current research include Computer Networks, Security.