Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE BROADCAST COMMUNICATION IN SENSOR NETWORKS: FORTIFYING THE KD AUTHENTICATION PROTOCOL

GURUPRAKASH B[1],RAJALAKSHMI J [2], ANGEL HEPZIBAH R [3], NAZRIN SALMA S [4], MARIAPPAN E[5], RAMNATH M[6]

[1]Associate Professor, Department of Computer Science and Engineering (AI&ML), Sethu Institute of Technology, Kariapatti, Tamil Nadu, India
[2]Associate Professor, Department of Electronics and Communication Engineering Sethu Institute of Technology, Virudhunagar, Tamil Nadu, India
[3]Assistant Professor, Department of Artificial Intelligence and Data Science, Ramco Institute of Technology, Rajapalayam, Tamil Nadu, India
[4]Assistant Professor, Department of Science and Humanities (General Engineering), R.M.K. College of Engineering and Technology, Thiruvallur, Tamil Nadu, India
[5]Associate Professor, Department of Artificial Intelligence and Data Science, Ramco Institute of Technology, Rajapalayam, Tamil Nadu, India
[6]Assistant Professor , Department of Artificial Intelligence and Data Science, Ramco Institute of Technology, Rajapalayam, Tamil Nadu, India
E-mail: [1]guru_netprakash@yahoo.co.in, [2]lakshmijeyapal@gmail.com, [3]rangelhepzibah@gmail.com, [4]nazrinsalmaphd@gmail.com,[5]mapcse.e81@gmail.com, [6]ramnath25@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) are self-organizing networks composed of sensor nodes deployed in potentially hostile environments, making them highly susceptible to various security threats. Among these, Broadcast Service Attacks pose significant risks by injecting invalid packets through compromised nodes, leading to excessive power consumption, memory overload, bandwidth variation, and disruption of reliable data aggregation. Ensuring secure broadcast authentication in WSNs is a critical and complex challenge.
This research focuses on mitigating Broadcast Service Attacks using the Kurosawa-Desmedt (KD) authentication scheme. The proposed approach is evaluated and compared against the Feige-Fiat-Shamir (FFS) security algorithm using the NS-2 simulator. Simulation results demonstrate that the KD algorithm outperforms the FFS approach in terms of Packet Delivery Ratio, End-to-End Delay, Detection Accuracy, and Average Energy Consumption. The practical applicability and benefits of the proposed method are also briefly discussed. Furthermore, the application of this work has been discussed briefly in this paper.
Keywords: *Broadcast Service Attack, Predictive Hash Based Broadcast Protocol, Fiege Fiat Shamir Security Algorithm, Kurosawa-Desmedt Algorithm, Health Care Monitoring.*

1. INTRODUCTION

Wireless Sensor Network consisting of many self-configured sensors connected together to transmit and receive information with proper security. In this broadcast attack, the malicious nodes and unauthenticated packets may intrude the wireless sensor nodes that causes poor delivery of messages at the terminus. Therefore, security is a major concern, which traverse any information to the destination in Wireless Sensor Network [1], [2], [3].

A Wireless Sensor Network comprises hundreds of sensor nodes, each of which is sensing, processing, and sharing information capabilities to supervise the real world around us. Wireless Sensor Network has many applications and play a vital role in structured health monitoring, military surveillance like military target tracking, enemy movement on the battlefield, tracking tanks on the battlefield, battlefield awareness, tracking the passage of troops, location of personnel in the building, environmental monitoring such as environmental pollutants, environmental contaminant detection, ecological habitat monitoring, biological chemical attacks, forest fire monitoring and other applications like controlling /measuring traffic flows on roads, vehicular movement, Industrial process control, building security monitoring, , context-aware computing etc., [4], [5], [6].

The remaining sections of the article are structured as follows: In section 2, Broadcast Service Attack is described in detail. In section 3, the existing

methods of detection are explained clearly. In section 4, the proposed mechanism is elaborated. In section 5, simulation results are discussed in detail for the existing system. Finally, a conclusion is elucidated in section 6.

2. RELATED WORKS

While broadcasting a message from one end to another end, if it is not properly filtered out, unauthorized (invalid) packets may be received by the destination known as Broadcast Service Attacks. Researchers in general have used many techniques in order to mitigate the Broadcast Service Attack and thereby sending the authenticated message to the destination with optimum efficiency by analyzing various kinds of parameters. The various techniques used by the researchers are discussed briefly in the review (3). This inadequacy in WSN performance made me to undergo this research by using the Predictive Hashing Based Broadcast Protocol (PHBBP) technique along with Kurosawa-Desmedt (K-D) algorithm [7], to augment the resistance in the Broadcast Service Attack.

In Predictive Hashing Based Broadcast protocol with Kurosawa-Desmedt (K-D) algorithm, the information in the packet can be divided into two halves, one is the message portion (MAC details) and another one is the key portion. The message portion has been delivered without delay is named as Predictive Hash, which are authenticated and leftover messages are considered as unauthenticated and are buffered. This is how, we can mitigate the Broadcast Service Attack and traversing authenticated packets alone to the recipient.

Many researchers have initiated various techniques and approaches to enhance the performance (Broadcast Service Attack) in WSN. Those different kinds of techniques and approaches have elucidated issues like attacks and security in WSN, is being discussed briefly in this review.

In a Digital Signature Algorithm, a signatory has two keys. One is the private key and the other is the public key. The private key is used by the signatory to generate a digital signature on messages but the public key is used by anyone to verify signatures on messages. Thus, the digital signature resists the broadcast attack (unauthenticated messages) and allows the authenticated message to the verifier [8].

In Batch-based authentication, the broadcasted packets are sent in batches. Each batch is associated with a key. All the batches are sent in batch period. At the end of the batch period (BP), the source node starts the delay period (DP). The batch key is kept secret by the source node during the batch period and delay period. The source node displays the corresponding batch key in the key disclose period (KP) when delay period expires. The messages received by the recipient within the batch period are authenticated andothers are not authenticated [9].

An Elliptic Curve Digital Signature Algorithm (ECDSA) is used as an effective multi-user authentication protocol in WSN. This algorithm removes modular inversion operation of the signature to simplify the verification process. Public key uses bloom filters to save the storage space of sensor nodes. Based on one-way hash key, a messaging-filtering scheme is proposed against broadcast attack. This scheme generates pre-authentication hash key chains only for the sink and users. Utilizing the pre-authentication hash key, one can authenticate the messageto the destination [10].

The weak pre-authenticator approach provides pre-inexpensive authentication. This pre-authentication requires a hash function to ensure the authenticity of a weak pre-authenticator. Furthermore, an adaptive window in this methodology indicates the sensor nodes to decide whether the message can be forwarded before authentication or vice versa. Here, a weak pre-authenticator is used to authenticate the message in the network transmission [11].

According to efficient broadcast authentication methodology, an efficient OR-based Bloom filter is used to minimize the authentication delay and computational overhead. OR-based Bloom filter plays a major role in authenticating the message [12][15].

In the multilevel μ-TESLA approach, they utilize a variable weak authenticator along with broadcast authentication that performs the signature verification and packet forwarding. A sender broadcast messages with a message authentication code (MAC) with a secret key. The receiver authenticates and buffered the message only when they receive the corresponding key. During authentication, μ-TESLA divides the broadcasting period into several time intervals and assigning separate keys to separate time intervals. Thus, the

Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MAC assisted key is helpful to authenticate the message within the stipulated time [13][14].

Though various approaches have been imposed in WSN in order to mitigate the Broadcast Service Attack, the yielded results efficiency is not up to the desired level. This inconsistency asserts me to execute this research by using a kind of new approach called Predictive Hash-Based Broadcast Protocol that uses FiegeFiatShamir security algorithm and Kurosawa-Desmedt algorithm, to supplement the parameter efficiency in WSN.

III. METHODOLGY

Predictive Hash Based Broadcast Protocol technique along with Kurosawa-Desmedt algorithms proposed in this research in order to resist Broadcast Service Attack in a wireless sensor network. In this method, the broadcast packet consists of a message portion and a key portion. While transmitting the message portion (MAC details) that is delivered without delay, named as Predictive Hash (PH) and does not have to be buffered. The other messages received after the delay are invalid packets and are buffered. This is schematically shown in figure 1.

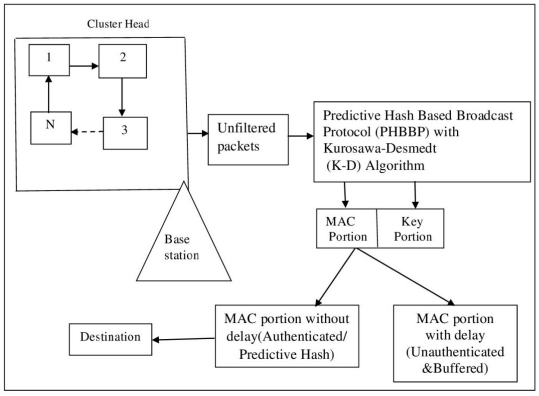

Figure 1. Broadcast Service Attack

The overall scheme behind this communication is explained briefly as follows. This Predictive Hash-Based Broadcast protocol (PHBBP) is comprised of Predictive Hash (PH) technique and Size Selective Forwarding (SSF) technique, which uses One-way Key Chain (OKC) in the network, provided the last key is pre-installed to all sensor nodes. If One-way Key Chain keys are once exhausted, another One-way Key Chain can be received from Broadcast Source. Here, the packets are divided into full-length packets and shortened packets. Full-length packets consist of Message portion (M), Key portion (K), and Predictive Hash portion (PH). A shortened packet consists of a time interval index and a Predictive Hash portion (PH). Here, One-way Key Chain and packet types are used to limit the forwarding level at each node.

Furthermore, the PH Based Broadcast Protocol is also used along with K-D Algorithm to segregate malicious nodes. The flowchart in the figure. (ii) shows clearly, the significant process carried out in this algorithm. Here we select the cluster head as base station and apply PHBBP.In this cluster head, the normal nodes communicate with Kurosawa-Desmedt Algorithm and the base station monitors the status of the nodes. The nodes, which violate the algorithm, are malicious nodes and others are normal nodes. Thus, the malicious nodes are separated from normal nodes for further communication. This is how, we can mitigate the Broadcast Service Attack and traversing authenticated packets alone to the recipient.

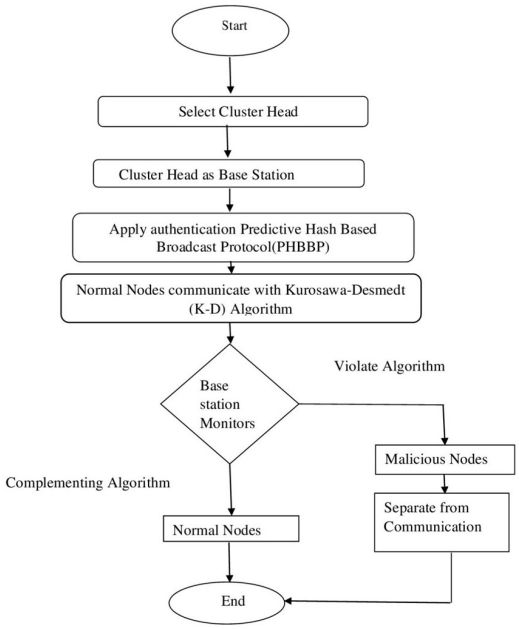

Figure 2. Flow chart for K-D Algorithm

Kurosawa-Desmedt Algorithm

Sharing algorithm between nodes

Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

C=[c=Ar],π,Ek,(m)
K=[(k0+τk1)TAr], τ=H(c)
Generate authenticated packets
J 0
Repeat
C Є Span(A) VcЄ Span(A0)
Where Span (A)={Ar | r Є Zk P}
Hashing
Pr[h(x)=h(x')] | h
If malicious nodes
(Pk,Sk) R Gen(1γ)
b R{ 0,1 }
Return
If | m0 | = | m1 |
Return m forward Security
Ps =(k,G,[A],[A0],h0h1) Digital

The purpose of Kurosawa-Desmedtalgorithm is to identify malicious nodes that can be achieved on sharing Kurosawa-Desmedt algorithm between nodes. The implementation of Kurosawa-Desmedtalgorithm is reducing the number of public keys which in turn minimize the computational complexity is briefly elucidates below.

In Kurosawa-Desmedt algorithm, on adding an additional element to the cipher text during encryption, reduces the size of the public key, (for example public keys of 100 group elements to 6 group elements).ThisKurosawa-DesmedtAlgorithm use the Decisional Diffie-Hellman (DDH) assumption to modify the setup of cipher text'C' to a random vector in the span of 'A' (Public Parameters). This change randomizes the value of 'K' (Public Keys) from challenge cipher text.This causes tight security protection and reduces the computational complication.

Scenario

Predictive Hash Based Broadcast Protocol technique along with Kurosawa-Desmedt algorithm is proposed in this paper and is schematically represented as shown in figure (iii).

In this section, the performance of the proposed scheme is evaluated using a network simulator (NS2). Here the network includes 100 nodes deployed randomly in a 1000 X 1000 m2 field. The nodes are mobile nodes. The transmission protocol used is UDP and the size of the protocol is 512 bytes.

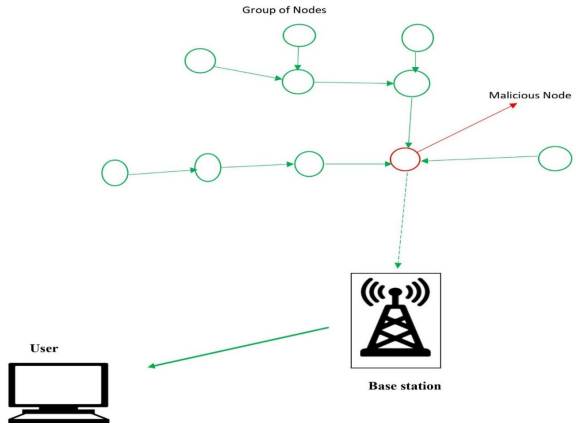

Figure 3. Broadcast Schematic Diagram

Table 1. represents the comparative environmental simulation settings for K-D algorithm and FFS algorithm.

Sl. No.	Description	Simulation Parameter details for K-D Algorithm	Simulation Parameter details for FFS Algorithm
1	Area	1000 X 1000 m^2	1000 X 1000 m^2
2	Nodes	100	100
3	Transmission Protocol	UDP	UDP
4	Packet Size	512 bytes	512 bytes
5	Antenna	Omni directional Antenna	Omni directional Antenna
6	Simulation Time	100 Sec	100 Sec
7	Application Traffic	CBR	CBR
8	Initial Energy	0.3J	0.3J
9	Transmitting power	0.15mw	0.15mw
10	Receiving power	0.15mw	0.15mw
11	Routing Protocol	AODV	AODV
12	Que Type	Drop tail	Drop tail
13	Type of Attack	Broadcast Service Attack	Broadcast Service Attack
14	Algorithm	K-Dalgorithm	FFS Algorithm
15	Propagation	Two Ray Ground	Two Ray Ground

Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. RESULTS AND DISCUSSION:

In this section, the performance of sensor nodes in hostile environment is simulated using Network Simulator (NS2), which is an object-oriented discrete event driven network simulator targeted at networking research. It provides support to Transmission Control Protocol (TCP) routing and multicast protocol simulation on all wireless networks.The nodes are mobile nodes. In this investigation, totally 100 sensor nodes are deployed in an area of 1000m*1000m size, where User Datagram Protocol UDP is used as a communication protocol and the size of the packet is 512 bytes.

The parameters such as Packet Delivery Ratio, Energy Consumption, Detection of Accuracy and End-to-End delay have been discussed below in detail.

Packet Delivery Ratio is defined as the ratio of number of packets delivered to the total number of packets sent from base station to destination.

Figure 4 represents the practical representation of number of nodes against the Packet Delivery Ratio. It is found that the Packet Delivery Ratio is very less before implementing the algorithm. Packet Delivery Ratio has been increased invariably in K-D Algorithm, when compared with FFS Algorithm. On seeing the graph, the Packet Delivery Ratio is improved well in K-D Algorithm.

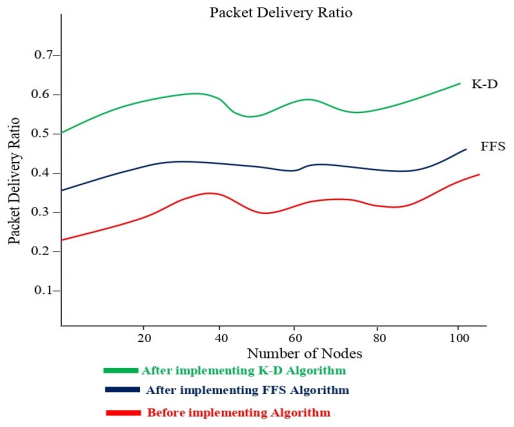

Figure 4. Packet Delivery Ratio

In figure 5 the Percentage of Faults is drawn against Packet Delivery Ratio. It is noticed that Packet Delivery Ratio against percentage of faults is considerably increased after implementation of K-D Algorithm when compared with FFS Algorithm.

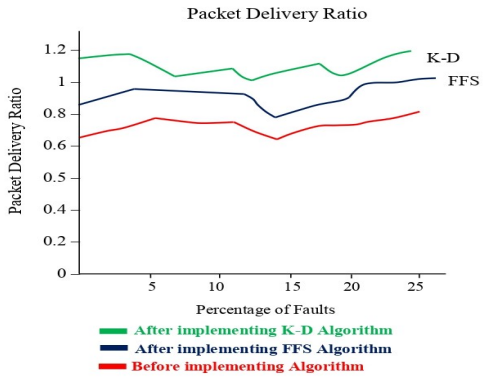

Figure 5. Packet Delivery Ratio against errors

Energy consumption is nothing but the total energy for transferring one bit of data successfully without error between two sensor nodes. The energy consumption rate for sensors in a wireless sensor network varies greatly based on the protocols used by the sensors used for communication.

Figure 4 focuses on reduction of energy consumption on introducing all the schemes, in which the energy in Joule is drawn against the number of nodes.

On analyzing the graph, it is seen that energy consumption is reduced considerably more in KD algorithm when compared with the other two schemes.

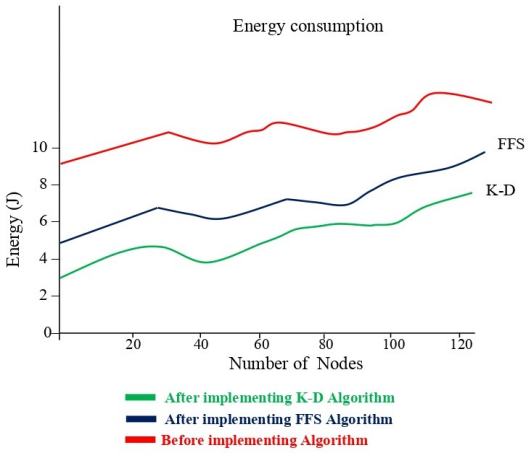

Figure 6. Energy Consumption of nodes

In figure 7, the graph is illustrated between Number of nodes and Delivery ratio. The graph indicates the accuracy level is more in K-D Algorithm when compared with FFS Algorithm and other algorithm.

Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

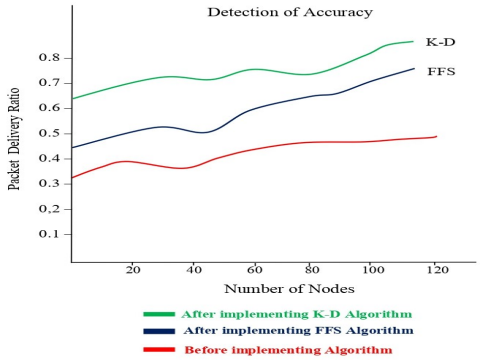

Figure 7. Detection of Accuracy

End to End delay refers to the total time taken for group of packets to be transmitted across a network from the base station to destination.

The End-to-End delay has been simulated using NS2, K-D algorithm and FFS algorithm. Figure. (viii) reveals that End-to-End Delay has been significantly reduced. Furthermore, End to End delay is reduced in K-D algorithm compared with FFS Algorithm.

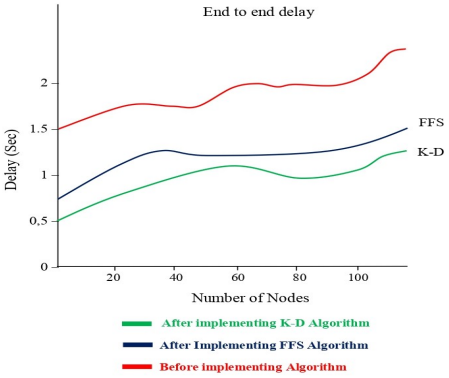

Figure 8. End to end delay

5. APPLICATION IN HEALTH CARE MONITORING

One of the applications of Predictive Hash Based Broadcast Authentication Protocol along with Kurosawa-Desmedt algorithm is health care monitoring and is shown in figure 9.

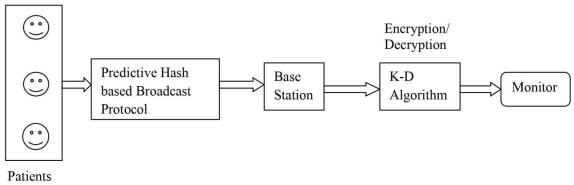

Figure 9. Application in Health Care Monitoring using K-D Algorithm

During the implementation of this system in the medical monitoring application, the hospital physician can diagnose the patient's disease without seeing and physically touching the patient. In the schematic diagram, the stored patient`s data have been segregated using Predictive Hash Based Broadcast Authentication Protocol. This predictive hash protocol authenticates the abnormal patient with the disease and this authenticated data transfers to the base station. (The purpose of the FiegeFiatShamir (FFS) security algorithm and Kurosawa-Desmedt algorithm is merely to enhance security protection. The FiegeFiatShamir (FFS) security algorithm and) The purpose of the extraordinary performance of Kurosawa-Desmedt algorithm is merely to enhance security protection. The Kurosawa-Desmedt algorithm only makes it possible for physicians in the hospital alone to monitor patients in the hospital. Intruders cannot reach the monitor to find out the details of the patient because we exclusively use the Kurosawa-Desmedt algorithm. This data has been checked with the help of a monitor by a doctor in the hospital, in particular for the emergency patient who is not physically available in the hospital premises. Thus, data received from the base station provides immediate care to the patient who requires urgent treatment.

6. CONCLUSION

In Wireless Sensor Networks, overall network performance can significantly degrade due to various security attacks. This research focused on mitigating the Broadcast Service Attack, which is known to severely impact power efficiency, data integrity, and resource utilization. By implementing the Kurosawa-Desmedt (K-D) authentication algorithm, the broadcast attack was effectively reduced, leading to noticeable improvements in network performance.Through simulation using the NS2 tool, key performance metrics—including Packet Delivery Ratio, End-to-End Delay, Detection Accuracy, and Average Energy Consumption—were analyzed both before and after the implementation of the K-D and Feige-Fiat-Shamir (FFS) algorithms. The results demonstrate that the K-D algorithm consistently outperforms the FFS approach across all measured parameters. Specifically, the K-D algorithm showed a marked increase in Packet Delivery Ratio and a reduction in both End-to-End Delay and Energy Consumption.

These findings confirm that enhancing broadcast authentication using the K-D algorithm significantly strengthens the network's resilience and operational

efficiency, thereby improving the overall performance of Wireless Sensor Networks.

8. DECLARATIONS

Competing interests:

The authors declare that they have no competing interests.

Availability of data and materials:

The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

Funding:

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgements:

The authors would like to acknowledge the anonymous reviewers for their thoughtful comments.

REFERENCES

[1] Zehua Zhou, Xiaojing Xiang, Xin Wang, Jianping Pan: "A holistic sensor network design for energy conservation and efficient data dissemination", Computer Networks 55 (2011) 131–146.

[2] AsmaMesmoudi, Mohammed Feham, Nabila Labraoui: "Wireless sensor networks localization algorithms: a comprehensive survey", International Journal of Computer Networks &Communications (IJCNC) Vol.5, No.6, November 2013.

[3]Kyung-Ah Shim: "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks", IEEE Communication Surveys & Tutorials, Vol. 18, No. 1, First Quarter 2016

[4] Yong Wang, GarhanAttebury, and Byrav Ramamurthy: "A Survey of security issues in Wireless Sensor Networks", IEEE Communications 2nd QUARTER 2006, Volume 8, No. 2.

[5] Al-Sakib Khan Pathan, Hyung-Woo Lee, ChoongSeon Hong: "Security in Wireless Sensor Networks: Issues and Challenges", Feb. 20-22, 2006 ICACT2006.

[6]Harish Radhappa, Lei Pan, James Xi Zheng and Sheng Wen:" Practical overview of security issues in wireless sensor network applications", International Journal of Computers and Applications, 2017.

[7] Romain Gay, Dennis Hofheinz, and Lisa Kohl," Kurosawa-Desmedt Meets Tight Security", International Association for Cryptologic Research 2017, J. Katz and H. Shacham (Eds.): CRYPTO 2017, Part III, LNCS 10403, pp. 133–160, 2017.

[8] Kui Ren, Shucheng Yu, Wenjing Lou, and Yanchao Zhang:" Multi-User Broadcast Authentication in Wireless Sensor Networks", IEEE transactions on vehicular technology, Vol. 58, No. 8, October 2009.

[9] Yun Zhou, andYuguang Fang: BABRA:" Batch-based Broadcast Authentication in Wireless Sensor Networks",. IEEE GLOBECOM 2006 proceedings, San Francisco, CA, USA, 27 Nov.-1 Dec. 2006

[10] Jie Xu, andLanjun Dang: "Multi-User Broadcast Authentication Protocol in Wireless Sensor Networks against DoS Attack", The Open Cybernetics &Systemics Journal, 2014, 8, 944-950.

[11] I. ALMomani , O. Karajeh, L. Abdullah: "Reducing the vulnerability of broadcast authentication against denial of service attacks in wireless sensor networks", The Mediterranean Journal of Computers and Networks, Vol. 7, No. 2, 2011.

[12]BacemMbarek, Are f Meddeb, Wafa Ben Jaballah and Mohamed Mosbah:" An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks ", Procedia Computer Science 109C (2017) 553–559.

[13]Peng Ning, An Liu and Wenliang Du:" Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks" ACM Journal Name, Vol. , No.4 , 20, Pages 1–35[25] Nabarun Nandy, Debanjan Banerjee, Chittaranjan Pradhan "Color Image Encryption Using Dna Based Cryptography", 2017, Https://Doi.Org/10.1007/S41870-018-0100-9.

[14] M Kaliappan, E Mariappan, MV Prakash, B Paramasivan, Load Balanced Clustering Technique in MANET using Genetic Algorithms.. Defence Science Journal 66 (3), 251-258.

[15] M Sivaram, M Kaliappan, SJ Shobana, MV Prakash, V Porkodi Secure storage allocation scheme using fuzzy based heuristic algorithm for cloud, Journal of Ambient Intelligence and Humanized Computing, pp.1-9