International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 7; Issue 2(L); February 2018; Page No. 10408-10412
DOI: http://dx.doi.org/10.24327/ijcar.2018.10412.1762

Research Article

# REGION BASED CLUSTER HEAD SELECTION AND KEY DISTRIBUTION FOR WIRELESS SENSOR NETWORK

**Niraj Nirmal., Manish K. Ahirwar and AnjnaDeen**

University Institute of Technology RGPV, Bhopal, India

## A R T I C L E I N F O

*Article History:*

Received 16th November, 2017
Received in revised form 4th December, 2017
Accepted 25th January, 2018
Published online 28th February, 2018

*Key words:*

Wireless Sensor Network, Key Management, Clustering, MGKM

## A B S T R A C T

Sensors play an important role in the era of technology these days. Sensors are used everywhere to capture information owing to the environment in which they are used. The group of sensors communicating via a wireless medium to facilitate process of communication for knowledge transfer is termed as wireless sensor networks. In some of the cases the information captured by these sensors may be very critical and needed to be secured. So security in the field of wireless sensor networks is a hot topic of research. The other main reason is because of wireless medium of communication and limited network lifetime because of limited battery life of sensors. Wireless sensor networks consist of large number of sensor nodes. Some of the sensor is stationary and some may be mobile. So, various algorithms have been proposed for security of these networks. To efficiently manage security nodes are grouped together to form clusters. Several clustering algorithms have been proposed. But the main problem is key distribution for the nodes in cluster and key redistribution. Whenever any node leaves or joins the network keys need to be redistributed. So this key management and redistribution overhead is a major issue. So in this paper region based clustering and key management algorithm is proposed for wireless sensor networks.



## INTRODUCTION

Wireless Sensor Network (WSN) [1] is the self-organized [13] and infrastructure less network that consist of many small devices that called sensors. In literature, sometimes it is treated as a special type of the wireless networks [2]. These networks are useful in our life; they are widely used in many applications [22]. WSN is used in mainly military surveillance but also in commercial and ecological areas. Due to sensitive data are communicated through it these networks must be secure [26]. Due to nature of WSN, Security is very important issue, just because of many security threats. It is noticed that at this point by studying the communication links in these networks, which is the radio links that is subject to many faulty information and malicious attacks [18]. Sensor devices in general have a limitation in its resources; these limitations can control the nature for WSNs, also affect the security level for this type of networks. WSNs also present several particular challenges in terms of design and implementation [22]. WSNs have limited capabilities such as battery power, transmission range, processing hardware and memory of the sensor nodes combined with the special location-based conditions met and makes the energy efficiency and the scalability factors even more crucial.

**Corresponding author:* **Niraj Nirmal**
University Institute of Technology RGPV, Bhopal, India

Moreover, the challenge of prolonging network lifetime under the above restrictions is difficult to be met by using only traditional techniques [7]. Consequently, it becomes unavoidable to follow clustering techniques [26] leading to more efficient protocols. Beyond the typical challenges related to limited energy, limited capabilities, and network lifetime, there are the following additional important considerations in the design process of clustering algorithms [29] for the WSNs.

***Cluster formation:*** The CH selection and cluster formation proceduresshould generate the best possible clusters. However they should also preserve the number of exchanged messages low and the total time complexity should remain constant and independent of the growth of the network. This yields a very challenging trade-off [29].

***Application Dependency:*** When designing clustering and routingprotocols for WSNs, application robustness must be of high priority and the designed protocols should be able to adapt to a variety of application requirements [29].

***Secure communication:*** As in traditional networks, the security of datais naturally of equal importance in WSNs. The ability of a WSN clustering scheme to preserve secure communication is ever more important when considering these networks for military applications.

***Synchronization:*** Slotted transmission schemes such as TDMA allownodes to regularly schedule sleep intervals to minimize energy used. Such schemes require corresponding synchronization mechanisms and the effectiveness of these mechanisms must be considered.

***Data aggregation***: Because this process makes energy optimization possible it remains a fundamental design challenge in many sensor network schemes nowadays. However its effective implementation in many applications is not a straightforward procedure and has to be further optimized according to specific application requirements [26].

### *Applications of WSN*

The characteristics of nodes in WSNs make it suitable for use in wide variety of applications [5]. The nodes can be deployed in the area to be monitored without visiting the area physically. The nodes can self-organize themselves, creating the infrastructure on the y. Although there are some limitations with these nodes, still, it has been widely adopted for various applications. WSNs can be used in applications like military target tracking and surveillance, natural disaster relief, biomedical health monitoring, hazardous environment exploration and seismic sensing [3].

### *Military Applications*

In military scenarios, it is advantageous to transmit the sensor network's collected data to the ultimate end-users via an Unmanned Aerial Vehicle (UAV) that acts as an airborne relay. Fixed infrastructure is infeasible in hostile environment or in inhospitable terrains deployed for group of soldiers in enemy territories. Sensor networks provide the required communication mechanism quickly for such applications. Other applications include cooperative target identification and tracking [30].

### *Monitoring Applications*

Sensors currently under deployment sense temperature, humidity, visual and infrared light, acoustic, vibration, pressure, chemicals, mechanical stress, magnetic e ect etc. to name a few. Wireless sensor nodes are often deployed for monitoring ofvehicles, animals, machines, medical purposes, environment studies, structural health etc [30].

### *Emergency Operations*

WSNs prove useful in situations of emergency like search or rescue operations during natural disasters. Few such disasters are earth quake, forest re, flood etc. For example, to produce a temperature map of the area or to determine the perimeter of areas with high temperature from outside, sensor nodes can be deployed from an airplane over a wild re in a forest. Major factors favoring WSNs for these tasks are self-configuration of the system with minimal overhead, independent of xed or centralized infrastructure, nature of the terrain of such applications, freedom and exibility of mobility, and the unavailability of conventional communication infrastructure (Akyildiz and Vuran) [30].

### *Health Care*

Applications of WSNs in health-care are controversial and vary from post-operative and intensive care to long term surveillance of elder patients. In the rest case, sensors are directly attached to patients, thereby, eliminating the need for cables. In the latter case, automatic drug administration is achieved by embedding sensors into drug packaging. If the drug is administered to incorrect person, an alarm may be triggered.

## LITERATURE REVIEW

D. S. Sanchez *et al*. [4] discussed key management is very important for mobile sensor network (MSN) security. According to the characteristics of MSNs, key management has necessary to enable direct (without intermediaries) key establishment between two arbitrary nodes. They apply combinatorial design theory to pre-distribute Blundo's polynomials to MSN nodes. In This approach combination of Liu and Ning polynomial evaluation optimization which increase the scalability of polynomials. It also solves the combinational design existence problem of Çamtepe and Yener key pre-distribution scheme (KPS) [1] without a decrease in network scalability or resiliency. The analysis of paper shows that this scheme has great properties, including direct pairwise key establishment, which conducts authentication, increased scalability, tolerance to node captures and very low computational and communication overhead [14].

I.-H.Chuang *et al*. [5] discussed methods for security-sensitive applications in wirelesssensor networks (WSN), A resource-efficient key management protocol [11] is essential and the dynamic pair-wise key and group key management protocols are also important for far situated and mobile WSN. In this paper, a two-layered dynamic key management (TDKM) approach for cluster-based WSN (CWSN) is proposed. Both pair-wise key and group key are distributed in three rounds for key material exchange without encryption/decryption [9] and exponentiation operations in TDKM. In theoretical analysis, TDKM is compared with other key management protocols to show its efficiency [8]. Finally, the relationships between the number of groups and the system performance including key generation overhead, network security, and secured data transmission overhead in CWSN are analyzed.

S. Agrawal *et al*. [6] in this paper, authors propose a key update protocol which securely updates the session key between a pair of nodes with the help of random inputs in mobile sensor networks. Initially, a unique master key is obtained using symmetricbi-variate polynomial shares. This key is further used in authenticating and establishing the pair-wise key between a pair of nodes. Random inputs from both the participating nodes are used to update the pair-wise key in the mobile WSN setup. The security analysis shows that the proposed protocol resists known-key, impersonation, replay, worm and sink hole attacks [17][19]. The proposed protocol also provides forward secrecy, key freshness, and mutual key control [10].

S. U. Khan *et al*. [7] described Wireless Sensor Network (WSN) technology is being increasingly adopted in a wide variety of applications ranging from home/building and industrial automation to more safety critical applications including e-health or infrastructure monitoring. Considering mobility in the above application scenarios actually introduces additional technological challenges, especially with respect to security. The resource constrained devices should be robust to diverse security attacks and communicate securely while they are moving in the considered environment. To this aim, proper authentication and key management schemes [12] supporting node mobility should be used. This paper presents an effective mutual authentication and key establishment scheme for heterogeneous sensor networks [14] consisting of numerous mobile sensor nodes and only a few more powerful fixed sensor nodes. Moreover, OMNET++ simulations are used to provide a comprehensive performance evaluation of the proposed scheme. The obtained results show that the proposed solution assures better network connectivity, consumes less memory, has low communication overhead during the authentication and key establishment phase and has better network resilience against mobile nodes attacks compared with existing approaches for authentication and key establishment [14].

### *Proposed Approach*

In the proposed approach we have to use first of all region based clustering. For this approach we consider all the nodes of Wireless Sensor Network in XY-plane. In proposed approach wireless sensor network is divided into regions such that region size in x direction is less than the range of wireless nodes so that all the regions can communicate with each other. Consider the network shown below having 4 regions and a cluster head in each region.

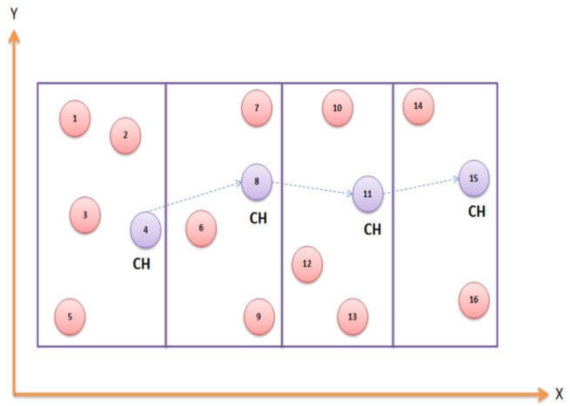



**Fig 1** Region based Cluster head selection

### *Cluster Head selection*

Cluster head is selected according to the algorithm shown below:

Algorithm ClusterHeadSelection

1. Select a node from $i^{th}$ region such that it covers maximum coverage area and maximum X distance so that it is closest to next $(i+1)^{th}$ region.
2. Cluster head of $(i+1)^{th}$ region will be selected as the node in range of cluster head of $i^{th}$ region and having maximum Y and X distance.

The above process will continue until all regions cluster head selection will be completed.

### *Key generation and distribution*

The key generation and distribution will be done through Multi group key management [27] algorithm through which keys for all the nodes in a region will be derived from the master key of cluster head.

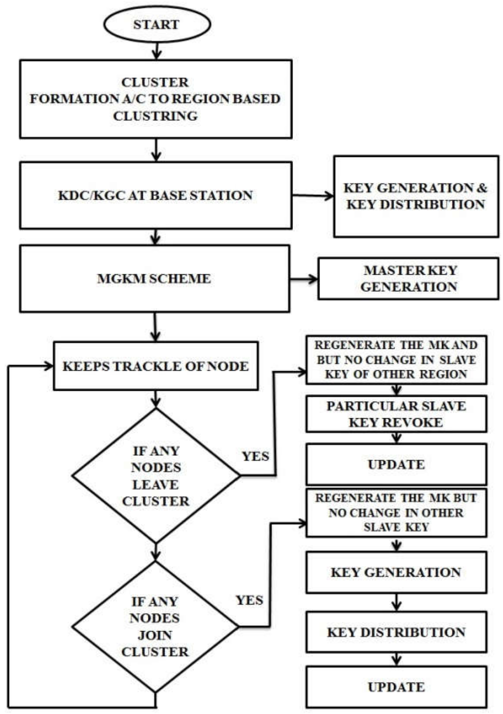



**Fig 2** Flow diagram of Proposed work

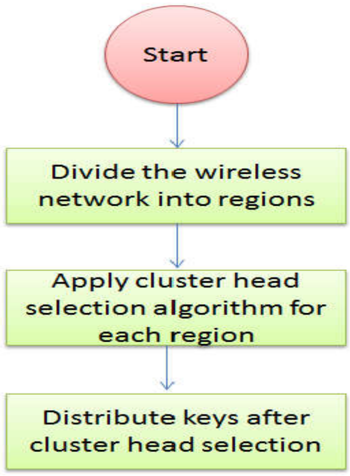



**Fig 3** Flow diagram of Existing System

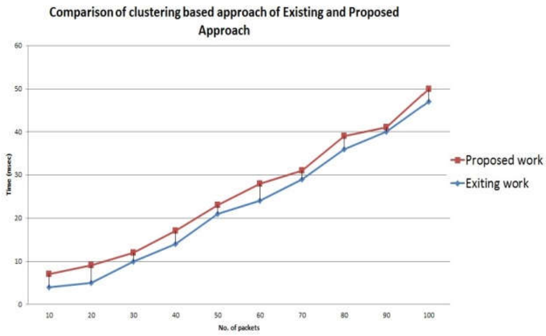
Multi Group Key Management Scheme [27]

1. Determine $p_1, \cdots, p_r, q_1, \cdots, q_r$ from safe prime numbers.
2. For $i = 1$ to $r$
3. $\phi_i = (p_i - 1) \times (q_i - 1);$
4. $x_i = (p_i - 1)/2;$
5. $y_i = (q_i - 1)/2;$
6. $e_i = 4 \times Random + 1;$
7. $d_i = {e_i}^{2(x_i-1)(y_i-1)-1} \mod 4x_iy_i;$
8. End For
9. $n = 1;$
10. For $i = 1$ to $r$
11. $n = n \times (x_iy_i);$
12. End For
13. For $i = 1$ to $r$
14. $M[i] = n/(x_iy_i);$
15. $N[i] = M[i]^{(x_i-1)(y_i-1)-1} \mod (x_iy_i);$
16. End For
17. $e_M = 0;$
18. For $i = 1$ to $r$
19. $e_M = (e_M + (e_i \times M[i] \times N[i])) \mod n;$
20. End For
21. While($e_M \mod 4 != 1$) $e_M = e_M + n;$
22. sleep;
23. Interrupt(when $j^{th}$ key pair should be updated)
24. $e_j = 4 \times Random + 1;$
25. $d_i = {e_i}^{2(x_i-1)(y_i-1)-1} \mod 4x_iy_i;$
26. goto 17;

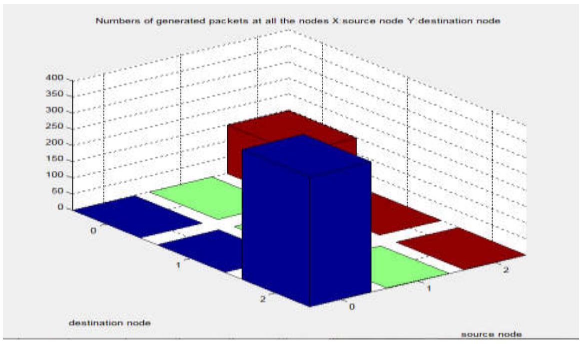
## EXPERIMENTAL SETUP & RESULTS

### *Simulation parameters*

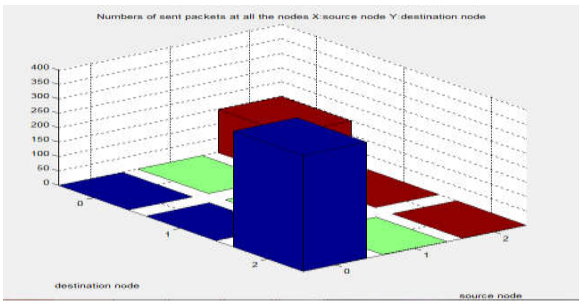
| Parameter Name | Value |
|---|---|
| Channel | Wireless Channel |
| Propagation | Two Round Ground |
| Queue | Priority Queue |
| Antenna | Omni Antenna |
| Queue Length | 50 |
| Routing protocol | DSDV |
| Total Simulation Time | 1000 |



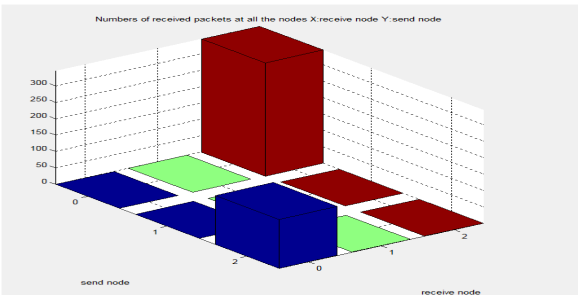

**Graph 1** Comparison of Clustering Based Key management of Existing and Proposed Approach



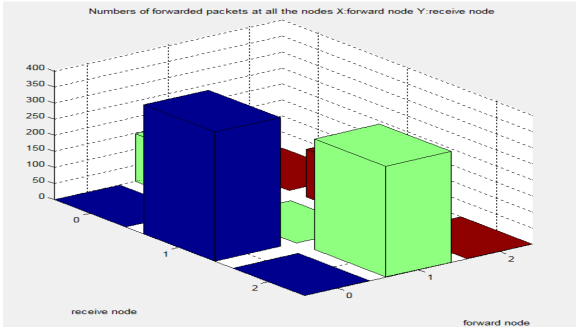

**Graph 2** Graph showing packets generated using MGKM by two nodes in different regions



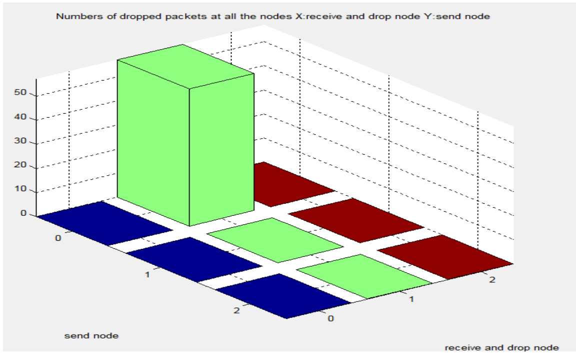

**Graph 3** Graph showing that all packets generated by source nodes are processed and forwarded to destinations




**Graph 4** Graph Showing That All Packets Sent by Source Nodes are Received by Destinations




**Graph 5** Graph showing there are two intermediate nodes (CHs) who forwarded all the packets




**Graph 6** Graph showing that all packets are dropped at node which is not registered to cluster head (CH)

## CONCLUSION AND FUTURE WORK

In this paper a Clustering based key management approach is illustrated using NS2. The proposed scheme is analysed on the basis of throughput of network including number of generated packets, number of actual packet sent and number of received packets. Graphs clearly illustrates that the entire packet forwarding for inter region communication is done by cluster heads for secure and safe approach. In Future this work can be extended by considering more performance parameter. These are Increase Network lifetime, Calculate Packet drop ratio, other key management methods and other Routing protocols for better routing.

## References

1. W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inform. Sys. Sec., vol. 8, no. 2, pp. 228-258, 2005.
2. M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," *J. Parallel Distrib. Comput*., vol. 70, no. 8, pp. 858–870, 2010.
3. M. R. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," IET Inf.Secur., vol. 6, no. 4, pp. 271-280, Dec. 2012.
4. D. S. Sanchez and H. Baldus, "A deterministic pairwise key predistribution scheme for mobile sensor networks," in Proc. 1st Int. Conf. SecureComm, Sep. 2005, pp. 277-288.
5. I.-H. Chuang, W.-T.Su, C.-Y.Wu, J.-P.Hsu, and Y.-H. Kuo, "Two layered dynamic key management in mobile and long-lived cluster based wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007,pp. 4145-4150.

6. S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, "A novel key update protocol in mobile sensor networks," in Proc. 8th Int. Conf.ICISS, vol. 7671. 2012, pp. 194-207.
7. S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, "An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks," in Proc. 6th Int. Conf. CRiSIS, Sep. 2011, pp. 1-8.
8. X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," *EURASIP J. Wireless Commun*. Netw., vol. 2011, pp. 1-11, Jan. 2011.
9. N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in Proc. 6th Int. Workshop Cryptograph. Hardw.Embedded Syst., 2004, pp. 119-132.
10. S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Proc. 9th Int. Conf. ASIACRYPT, vol. 2894. 2013, pp. 452-473.
11. S. Seo and E. Bertino, "Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing," CERIAS, West Lafayette, IN, USA, Tech. Rep. CERIAS TR 2013-10, 2013.[Online]. Available:https://www.cerias.purdue.edu/apps/reports_and_papers/.Seung-Hyun
12. S. H. Seo, J. Won, and E. Bertino, "POSTER: A pairing-free certificateless hybrid sign-cryption scheme for advanced metering infrastructures," in Proc. 4th ACM CODASPY, 2014, pp. 143-146.
13. Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in Proc. 2nd ACM Int. Conf. WSNA, 2003, pp. 141-150.
14. X.-J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks," in Proc. IACR Cryptol.ePrint Archive, 2013, pp. 698-698.
15. P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," in Proc. 5th Eur. Conf. WSN, vol. 4913. 2008, pp. 305-320.
16. K. Chatterjee, A. De, and D. Gupta, "An improved ID-based key management scheme in wireless sensor network," in Proc. 3rd Int. Conf. ICSI, vol. 7332. 2012, pp. 351-359.
17. W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in mobile sensor networks: Theory and approaches," *Secur. Commun. Netw*., vol. 5, no. 5, pp. 496-507, 2012.
18. M. A. Rassam, M. A. Maarof, and A. Zainal, "A survey of intrusion detection schemes in wireless sensor networks," *Amer. J. Appl. Sci*., vol. 9, no. 10, pp. 1636-1652, 2012.
19. Bhavana Butani, Piyush Kumar Shukla, Sanjay Silakari "Optimized and Executive Survey of Physical Node Capture Attack in Wireless Sensor Network" in IJCNIS Vol. 6, No. 11, October 2014.
20. DeshrajAhirwar, Manish K. Ahirwar, Piyush K. Shukla and PankajRichharia "An analytical survey on Network Security Enhancement Services" in (IJCSIS) *International Journal of Computer Science and Information Security*, Vol. 9, No. 3, March 2011.
21. AnkurKhare, Piyush Kumar Shukla, Murtaza Abbas Rizvi and Shalini Stalin "An Intelligent and Fast Chaotic Encryption Using Digital Logic Circuits for Ad-Hoc and Ubiquitous Computing" in Entropy 2016, 18, 201; doi:10.3390/e18050201.
22. Piyush Kumar Shukla, Kirti Raj Bhatele, Lokesh Sharma, Poonam Sharma and Prashant Shukla "Design, Architecture, and Security Issues in Wireless Sensor Networks" in A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series.
23. Parvez Khan, Anjana Jayant Deen, Manish Ahirwar "Enhance wireless Capacity through Multi-hop Scheduling" in *International Journal of Scientific & Engineering Research*, Volume 5, Issue 10, October-2014.
24. Piyush Kumar Shukla, SachinGoyal, Rajesh Wadhvani, M. A. Rizvi, Poonam Sharma and NeerajTantubay "Finding Robust Assailant Using Optimization Functions (FiRAO-PG) in Wireless Sensor Network" Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2015, Article ID 594345, 2015.
25. S. Chattopadhyay and A. K. Turuk, "A scheme for key revocation in wireless sensor networks," *International Journal on Advanced Computer Engineering and Communication Technology,* vol. 1, 2012.
26. A.S. Poornima, B.B. Amberker," Secure data collection using mobile data collector in clustered wireless sensor networks", *IET Wirel. Sens. Syst.,* Vol. 1, Iss. 2, pp. 85-95, 2011.
27. Min-Ho Park, Young-HoonPark, Han-You Jeong, and Seung-Woo Seo,"Key Management for Multiple Multicast Groups in Wireless Networks", IEEE Transactions on Mobile Computing, VOL. 12, NO. 9, SEPTEMBER 2013.
28. Lee, S., and Kim K.," Sensor authentication scheme for clustering routing protocols in wireless sensor networks", 2010 IEEE Sensors Conf., Kona, HI, USA, pp. 1819-1822, November 2010.
29. Rabia Noor Enam, Rehan Qureshi, and Syed Misbahuddin,"A Uniform Clustering Mechanism for Wireless Sensor Networks", *International Journal of Distributed Sensor Networks*, Volume 2014, Article ID 924012, 14 pages, 2014.
30. Sana H. Jokhio, Imran Ali Jokhio, Andrew H. Kemp,"Light-weight framework for security-sensitive wireless sensor networks applications", *IET Wirel. Sens. Syst*., Vol. 3, Iss. 4, pp. 298-306, 2013.


*******