Indian Journal of Science and Technology, *Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/99397, October 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Security over the Wireless Sensor Network and Node Authentication using ECCDSA

B. R. Tapas Bapu[1*] and L. C. Siddanna Gowd[2]

[1]Department of Electronics and Communication Engineering, St.Peters University, Chennai - 600054, Tamil Nadu, India; tapasbr@yahoo.com

[2]AMS College, Namakkal - 637013, Tamil Nadu, India; gowda.lcs@gmail.com

Abstract

Objectives: The networks using wireless sensor are becoming the preferred considerations for the critical mission applications. These applications normally remain unattended for years and have to perform reliably for lifetime. However the performance of these systems is subject to significant degradation over time because of realities in sensing and failure, communication in real world, node faults and clock drift. Hence it becomes essential to continuously monitor the natural deteriorations and have provisions for self-healing as necessary. Methods/Statistical Analysis: The self-healing, error correction and node authentication are proposed by this paper. The network having wireless sensors has nodes that are dynamically forming into clusters. Every cluster group will be having a cluster head for verifying the whole node. Findings: The cluster head would authenticate any incoming node of this network through generating and verifying signatures on any message using the Elliptic Curve Cryptography based Digital Signature Algorithm (ECCDSA). The registration of new node and authentication of the node constitutes the successful process of the authentication and cluster head would store the information about authentication in server. Application/ Improvement: The presence of malicious nodes if any will be identified using the distribution process of the self-healing key and the malicious nodes will be thrown out of the cluster by cluster head so as to guarantee the network as secured. After identifying and removing this malicious node in the cluster, the properties of that malicious node would be stored in the server for future reference. During error correction process, any node having the property same as this malicious one will be identified and informed to the cluster head by any neighbor node. Then using the technique of Forward Error Correction (FEC), the Cluster Head (CH) will block that node having the same malicious property after comparing with the one stored in the server.

Keywords: Cluster Head, Greedy Algorithm, MAODV, PEACH, Self- Healing Routing

1. Introduction

The Wireless Sensor Networks (WSN) have a node which is rich in resources called Base Station (BS) and a huge number of other sensor nodes that are constrained in the resources distributed spatially in hostile environment around the BS[1]. The primary task of the sensor node will be sensing the physical phenomena happening in its immediate environment and then processing and transmitting these sensed data to base stations or other nodes. The application of WSN is found useful in sensitive systems requiring tracking, controlling and monitoring of environmental parameters. But any sensor node is constrained because of power, communication, storage and computation. The method of communication preferred in a WSN will be large multi hop method[2], because of the presence of huge number of nodes. The security in this WSN becomes critical, since manually monitoring and maintaining the nodes is difficult after deployment. In this scenario monitoring and maintaining these sensor nodes and their communication networks has become one of the major issues in WSN. With the rapid development of electronics and communication technology the particular demand on secured communication is felt in any type of the available communication networks. The signature and the key exchange are the important components to provide secured communication in any

*Author for correspondence

of the public-key-algorithms like DSA, Elliptic Curve Cryptography (ECC) and RSA[3,4]. Victor Miller and Neal Koblitz independently proposed in year 1985 the application of Elliptic-curve system to cryptography. THE problem of discrete logarithm applied to group of public curves is found more difficult to apply than corresponding problems in any finite underlying field[5,6]. The Public-key cryptography has become very effective solution in providing secured mobile communications[7]. One of the highly efficient public-key encryption systems is ECC and is basically based on elliptic-curve concepts having ability for creating efficient, smaller and faster cryptographic key. The ECC could be used along with other methods of public-key-encryption like Diffie-Hellman key-exchange and RSA for communication privacy obtained through authentication of the sender, encryption and the digital signature for ensuring message integrity[8]. The ECC could help in establishing an equivalent security having lower power of computing and lesser usage of battery resource. The algorithms of Public-key Cryptography could provide a way in achieving the requirements for security viz; authentication and confidentiality[9]. In the current scenario of Internet, the detection of the attack on network has become a highly challenging task to the operator of any network. It is challenging in the sense that targets in the network attack will be dynamic and not steady. A new type of attack may be launched by the attacker on every time. The detection system should be capable of detecting different attacks of various ranges having wide variety of the characteristics[10]. The anomaly-based detection and signature-based detection are the types of approaches available in commercial-detection systems for detecting[11] network attacks. The detection using signature is useful for identifying patterns in the unauthorized behavior, whereas anomaly detection is useful for identifying abnormal pattern in behavior. In the FEC the retransmission is made outdated through correcting any errors in the data packet by these receiver nodes based on error-correcting-code encoded in the data by the source node. A coding gain is provided by error-control-coding and this reduces the power required for transmitting for any specific Frame-Error-Rate (FER) or Bit Error Rate (BER)[12]. This paper has proposed a framework for self-healing, which can enable flexibility in the choice of constituent components for masking and detection of the faults along with network reconfiguration.

A number of different approaches have been developed by the researchers for providing secured sensor networks, with each method having advantages and also limitations. The Key-distribution and Node-authentication are the critical operations in secured-sensor networks and different schemes in these are discussed[13]. A scalable and efficient protocol for re-authentication over the wireless-sensor network along with security[14] and analysis of performance about the protocol has been provided by these authors. Also to re-authenticate the mobile node, an efficient way of the membership verification has been suggested along with performance analysis about our membership-verification. Another efficient scheme of key-distribution having threshold self-healing with sponsorization of wireless networks with no infrastructure is proposed in[15] and it is claimed that this scheme is satisfying forward security that disables any revoked internal user from generating the key for a new session. This paper has developed a method of attacking the forward security and also the backward security of proposed key-distribution scheme and thus proved the original key-distribution scheme having threshold self-healing will be insecure[16.] An efficient and novel, key exchanges and node authentication protocol, supporting the Irregular distribution. The computational and communication overhead of this protocol is reduced to one third of the requirements of previous protocols. This improvement proposed has enabled efficient key-exchange and node re-authentication even in the presence of irregularly distributed sensors in the WPAN and smart home to support the different convergence services. A survey of mobility approach in topology healing for wireless-sensor networks have been surveyed by[17]. Deployment of the additional-mobile robots[18,19] and mobility of the sensor nodes are two of the major mobility strategies that could be listed. Dutta et al. have proposed many computationally efficient and secure solutions which are capable of reducing the resource costs and also provide backward and forward security but yet the session keys are left being exposed by the proposed schemes[20]. The Forward-Error Correction (FEC) will allow recovery from the error by incorporation of redundant data in controlled manner. The Unequal Error Protection (UEP) based on FEC used in transporting image could achieve efficiency in the combat against wireless-link errors[21]. The Elliptic Curve Cryptography has been proposed for application of elliptic curves in Public-Key-Cryptography consisting of digital signature, encryption and key-exchange for reducing the cost of computation in Discrete Logarithm Problem (DLP). The ECC has many advantages as compared to

other techniques of public-key-cryptography like RSA – it is the best algorithm known in providing solution to elliptic curve discrete logarithm problem (ECDLP), it is lacking sub-exponential attack on the ECC whereas any mathematical problem will be taking exponential time in ECC[22]. The Diffie-Hellman (DH) and RSA are considered as the first generation noteworthy public-key algorithms in use. The security in RSA depends on difficulty in factoring product of the two large value primes. DH will be related to the problem commonly known to be problem of the discrete logarithm in finite groups. The elementary theory of numbers is the bases for both the DH & RSA. Thus the security concept of these two schemes is found to be closely related even though they are formulated differently.

2. Wireless Sensor Network

The nodes are dynamic in the wireless sensor network. So dynamically the nodes in the network will be formed as cluster. In each cluster group based on the energy the cluster head will be select. The cluster head will validate the incoming node *along with* the entire node in the network. Using Elliptic Curve Cryptography based Digital Signature Algorithm (ECCDSA) the nodes in the network will authenticate successfully. Then the cluster head will store the authentication information in server. if any malicious node present in the network the cluster head will identified through self healing key distribution process and throw out the node from the cluster and store the malicious node property in the server. In error correction, if any another node with same property of malicious is entering *in*to the cluster the neighbor node will inform to the cluster head and CH will verify about the node property with the server then it block*s* the node which has same property of malicious with the help of Forward error correction (FEC) technique.

2.1 Node Deployment

The algorithm suggested is found related to restricted energy in sensor network. The introduction of cluster head in the wireless-sensor-network has become the efficient and accepted method because of its better capability for aggregation and data scalability in large Wireless Sensor Networks. The clustering process could also conserve the limited energy resources of sensor nodes.

2,2 Cluster Head Formation

A cluster head is selected by every node depending on its energy and distance. The sub-nodes are chosen by a cluster heads depending on the coverage area. Cluster head of source nodes forms groups depending on similarity. The data could be sent to the server through the cluster heads after the creation of the group.

2.3 Energy Efficiency

The Energy and the security are interrelated to one another - Higher the security requirements, Higher will be the energy requirement. Hence providing better security will tend to consume more energy and rapidly reduces the energy levels of the nodes. The operations of cryptography required for the procedure of authentication consumes more energy for its performance. But the operations of cryptography are performed by almost all entities within any network. Optimizing the use of the available energy is the essential issue in any WSN as it resources are constrained with limited energy. It is proposed that cluster head is performing many of these cryptograph operations requiring high energy consumption. Cluster head is generating private-keys used in cryptography operation of nodes and will be distributing those keys to nodes for future uses. The node will be doing a process of verifying signature and signing on message. Hence it could be stated that energy efficiency could be achievable through implementing this type of protocol.

The following Figure 1 wireless sensor network security describes the security over the network by Node authentication, self healing and Error correction process.

2.4 Elliptic Curve Digital Signature

The ECDSA is one variant of the DSA, which utilizes ECC. The application of ECDSA will allow entities of WSN authentication for resolving the weaknesses of the ECDH while authenticating the broad casted packets present especially in the WSN broadcast as primitive fundamental communication. The broadcast authentication is providing implicitly two extra cryptographic services namely non-repudiation of any signed message and data integrity. The data integrity service prevents alteration of data through use of Secure Hash Algorithm (SHA). The Non-repudiation of any sensor data could be achieved through generating ECDSA over sensor devices so as to ensure denial of transaction is not possible. In comparison to the algorithm of asymmetric-key, the algorithms

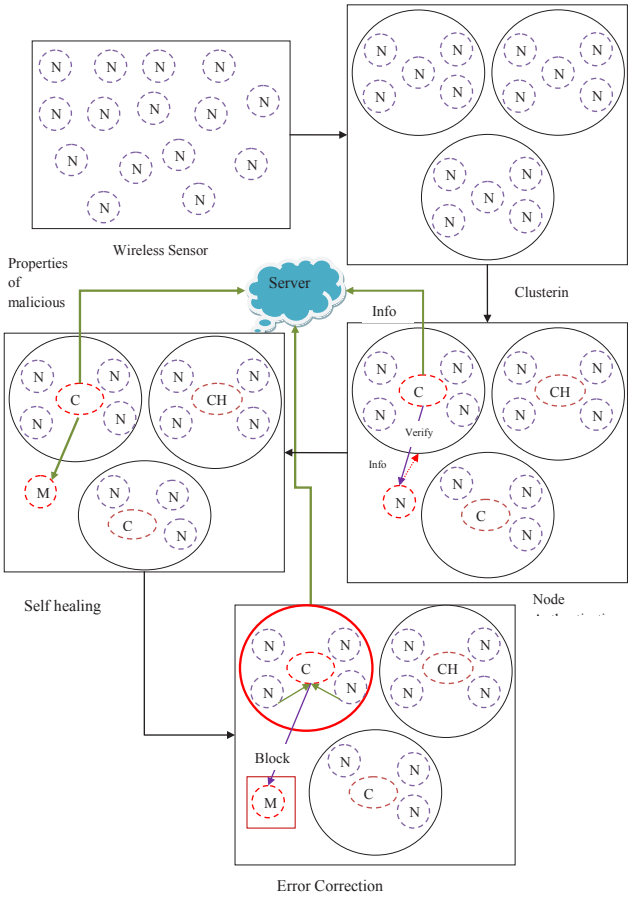

Figure 1. Wireless Sensor Network Security.

of symmetric-key μ Tesla has been designed as primitive light weight cryptography to efficiently authenticate the messages broad casted in WSN. It is not supporting the non-repudiation of these sensor data. The need for delayed authentication and time synchronization has made the solutions based on symmetric key to be vulnerable due to more variety of the possible attacks and also another concern is the scalability.

2.5 Self-Healing

Self-healing will be a phrase applicable to this process of the recovery from trauma, psychological disturbances, etc., which is directed and motivated by patient who is often guided only through instinct. Such processes will be encountered by mixed fortunes because of the amateur nature, even though the major asset being self-motivation. Self-healing react, diagnose and discover the network disruptions. The components of self-healing could detect failures or malfunctions of the system and initiate corrective actions depending on the defined policies in recovering the node or network. The recovering in automatic manner from the damages helps in improving the availability of the services. In the event that a node is failing, the system might enter into inconsistent state wherein the middle ware organization and the agents will not be able to work as per their specifications. To consider this type of the failures, deployment of Self-Healing Subsystem (SHS) as additional feature in each node is done. These SHS will interact with organization middle ware and local-agent middle ware relying on functionalities that will be provided by middle ware agent for interacting with the SHS on the other nodes. Alive signals are exchanged periodically by SHS with a communication service (receive and send) of agent middle ware. Monitoring of live signals is used for the detection of node failures. When a failure is detected by SHS, it tends to adapt the structure of this local organization wherein the agents of failing node have been involved and through possible interaction with SHS of other nodes involved in bringing back system to the consistent state which enables continuation of the function though in the degraded modes.

2.6 Algorithm

1: Init: specified network G(V, E), Initialize every vertex through random number ID among [0,1] elected uniformly at random.
2: while true do
3: If vertex V is deleted, do
4: Nodes in UN (V, G) [N(V, Gh) are reconnected into entire binary tree. To join the tree, go top down, left to right, mapping the nodes to entire binary tree in escalating order value.
5: MINID is least ID of the any node in UN (V, G)[N(V, Gh). Disseminate MINID toward all nodes in the UN(v, G) N (v, Gh) in Gh tree. All these nodes now set their ID to MINID.
6: end while

2.7 Self-Healing Key Distribution with Revocation Capability

Self healing mechanism is an efficient method to dispense personal key allocate to choose cluster nodes. Instinctively, the cluster header arbitrarily split every group session key $K\ m$ into twice t-degree polynomials, $q\ m\ (x)$ and $pm\ (x)$, like that $K\ m = p\ m\ (x) + q\ m\ (x)$. The cluster head distributes share $p\ m\ (l)$ and $q\ m\ (l)$ to every decided group member Ul. This permits cluster header has both $p\ m\ (l)$

and $q\,j\,(l)$ to improve $K\,m$ by calculate $K\,m = pm\,(l) + qm\,(l)$. Thus, pretentious there are m sessions, we can build (j+1) broadcast polynomials in session j to distribute the shares of $\{\,p1\,(x)\,,\ldots,\,pm\,(x);\,q\,m\,(x),\ldots\ldots,\,q\,j\,(x)\,\}$ to all select cluster headers. If any $U\,l$ receives transmit message, it can improve all $\{\{\,p\,1(l)\,,\ldots,\,p\,m\,(l);\,q\,m\,(l)\,,\ldots\ldots,\,q\,j\,(l)\,\}$ and calculate session key $K\,m = p\,m\,(l) + q\,m\,(l)$. But revoke cluster header obtain nothing from this transmit message. Additionally, if selected cluster nodes Ul receives key allocation messages in m2and m1, where $m1<m\,2$, but not key allocation significance for session m, where $m1<m<m2$, it can l recuperate lost key $K\,m$ by initial improving $qm\,(l)$ and $p\,m\,(l)$ from transmit message in sessions $m2$ and $m1$, correspondingly and compute $K\,m = pm\,(l) + qm\,(l)$.

2.8 Forward Error Correction

Forward error correction (FEC) is digital signal processing method utilized to improve data reliability. FEC enhance the reliability by establishing redundant data, so it is called error correcting code, earlier to data storage or transmission. Without retransmission Forward error correction allows error correction and it requires redundancy transmission. It has high latency, high bandwidth, as is the trend.

1) Assign Memory Registers with zeros on reset
   mr1=0, mr2=0, mr3=0, mr4=0
2) Store incoming bit in the memory register mr_in.
   mr_in = data_in
3) After arrival of input bit and data in is valid the operation starts and the output is calculated as
   x1 = mr_in + mr2 + mr4;
   x2 = mr_in + mr1 + mr3 + mr4;
   x3 = mr_in + mr1 +mr2 +mr3+mr4 ;
4) Carry out shifting operation
   mr4=mr3;
   mr3=mr2;
   mr2=mr1;
   mr1=mr_in;

2.9 Node Addition/Block

The nodes that would be behaving in accordance with authentication protocol applied are to be included in the network. It will be responsibility of this authentication protocol in allowing any node for starting communication in secured manner with another member node. This technique should be capable of blocking useless or malfunctioning nodes.

3. Performance Analysis

A description of models and the simulation environment are given in detail: Routing protocols: MAODV, AODV, Number of the nodes: 50, 40, 30, 20, 10, Simulator: NS2, The Simulation Time: 150secs, The Area: 300m*1500m, The Transmission range: 250m

3.1 Process Performance

In [Figure 2] shows process performance. The node authentication, self healing and error correction process are shown.

3.2 Self Healing

The healed nodes in the network are represents in this graph.

In [Figure 3] shows healed nodes. When the malicious node entering to the clustering the cluster head will block the malicious node. This graph represents blocked (healed) nodes.

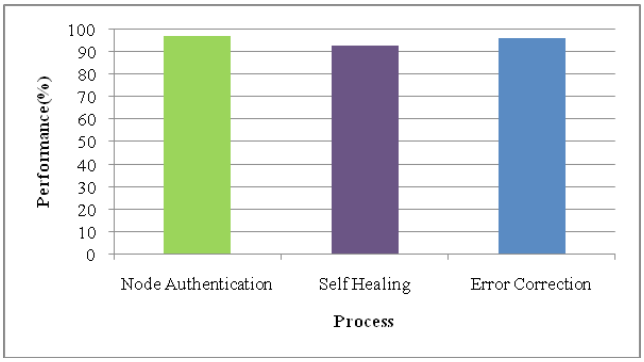

Figure 2. Process performance.

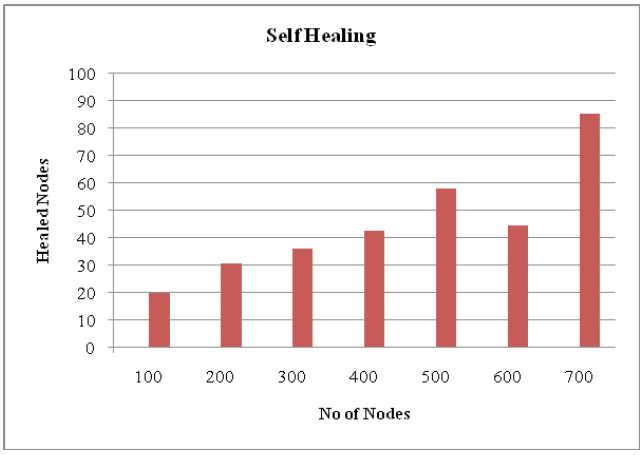

Figure 3. Self healing.

3.3 Node Deployment

The node deploy in the wireless sensor network. After deployment nodes are formed as a cluster.

In [Figure 4] shows Node Deployment. Based on the energy the cluster head will be select.

3.4 Malicious Node Identification

To find malicious node the cluster head make request to cluster nodes. Once request receives from cluster head the cluster nodes make reply to the cluster head.

The Figure 5 shows Malicious Node Identification. If cluster nodes not reply to cluster head that node be consider as malicious. Then the malicious node will be thrown out from the cluster. The cluster nodes information will be store in the server with the help of cluster head.

3.5 Cluster Formation

The node from cluster moves to another cluster. In order to form the cluster, the node request to another cluster node. The cluster head will send the information about cluster nodes to server.

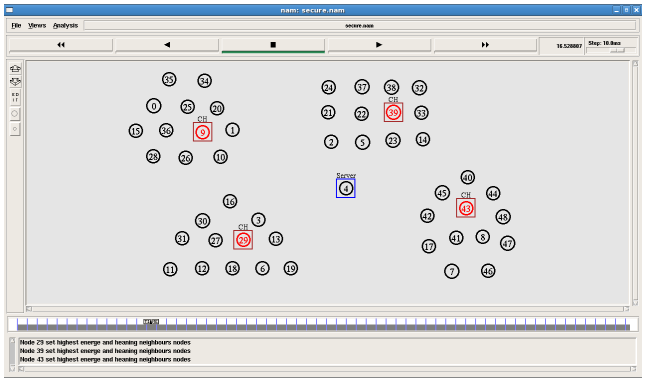

Figure 4. Node Deployment.

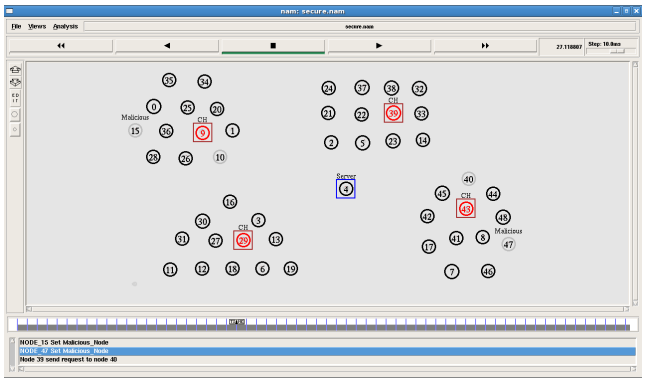

Figure 5. Malicious Node Identification.

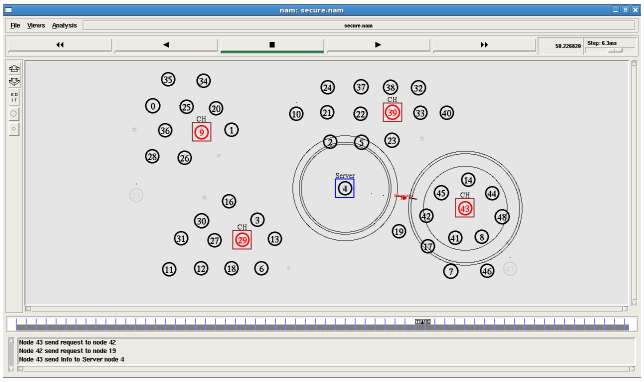

Figure 6. Cluster Formation.

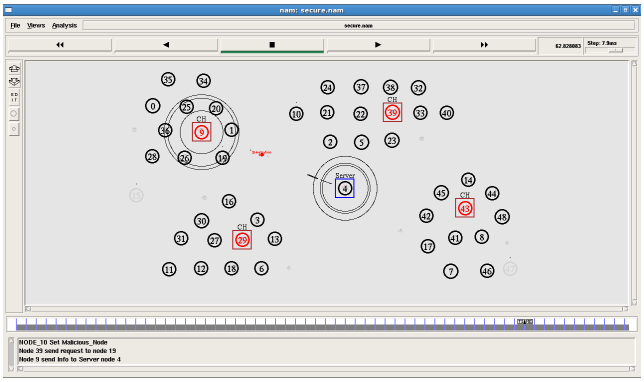

Figure 7. Node Block.

The [Figure 6] shows cluster formation. If the node is active then it forms the cluster. If it is malicious then it moves to another cluster.

3.6 Node Block

If the malicious node activity differs in another cluster then that node is formed as a cluster.

The [Figure 7] shows Node Block. If the malicious node activity same in another cluster then cluster head will inform to server about malicious activity. Then cluster head will block the malicious node.

4. Conclusion

The WSN is finding applications in various domains and therefore the gathered information will be sensitive and must be kept confidential. The authentication of the node is becoming necessary for achieving this confidentiality. Various schemes have been proposed for authentication and this paper discusses on some significant ones. Many of the schemes for authentication are focusing only on security

whereas the other critical challenges that are compelling the authentication process are providing computation overhead, proper scalability and reduced communication.

5. References

1. Chelli K. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures, Proceedings of the World Congress on Engineering WCE London, U.K. 2015; 1:1–6.
2. Agrawal S, Raw RS, Tyagi N, Misra AK. Fuzzy Logic based Greedy Routing (FLGR) in multi-hop vehicular AD HOC networks. Indian Journal of Science and Technology. 2015 Nov; 8(30):1–14.
3. Verma SK, Ojha DB. A discussion on elliptic curve cryptography and its applications. IJCSI International Journal of Computer Science Issues. 2012; 9(1):1–4.
4. Kaushal J, Patel P, Nirav M, Raja R. Secure end to end data aggregation using public key encryption in wireless sensor network. International Journal of Computer Applications. 2015.
5. Stallings W. Cryptography and network security principles and practice fifth edition, person. 2011; 122(6):1–22.
6. Mukund R, Joshi J, Karkade RA. Network security with cryptography. IJCSMC. 2015; 4(1):201–04.
7. Bakir SHA, kiah MLM, Zaidan AA, Zaidan BB, Alam GM. Securing Peer to peer mobile communications using public key cryptography: new Security strategy. International Journal of the Physical Sciences. 2011; 6(4):930–38
8. Nimbhorkar S, Malik LG. Prospective utilization of elliptic curve cryptography for security enhancement. International Journal of Application or Innovation in Engineering and Management (IJAIEM). 2013; 2(1):1–6.
9. Mohammad A, Alia A, Tamimi AA, Omaima NA, AL-Allaf A. Cryptography based Authentication Methods. Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA. 2014; 1:1–6.
10. Raam KVJ, Rajkumar K. A novel approach using parallel ant colony optimization algorithm for detecting routing path based on cluster head in wireless sensor network. Indian Journal of Science and Technology. 2015 Jul; 8(16):1–7.
11. Eriksson O. Error Control in Wireless Sensor Networks a Process Control Perspective. 2011; 1–50.
12. Hariharan R, Mahesh C, Prasenna P, Kumar RV. Enhancing privacy preservation in data mining using cluster based greedy method in hierarchical approach. Indian Journal of Science and Technology. 2016 Jan; 9(3):1–8.
13. Wang H, Zhang Y. Cryptanalysis of an Efficient Threshold Self-Healing Key Distribution Scheme. IEEE Transactions on Wireless Communications. 2011; 10(1):1–4.
14. Goel S, Behniwal M, Sharma AK. Authentication and Key Distribution Schemes for Wireless Sensors Network. IJARCSSE. 2013; 3(7):41–7.
15. Chaudhary N, Gupta S. A survey on coverage problem in wireless sensor network. IJECS. 2015; 4(5):11952–5.
16. Theofanis P, Lambrou **L.** Optimized Cooperative Dynamic Coverage in Mixed Sensor Networks. ACM Transactions on Sensor Networks, USA. 2015; 11(3):46.
17. Kumar AVN, Ajith A. Hole and border detection methods and coverage enhancement in WSN: A survey. IJARCSSE. 2015; 5(6):1267–77.
18. kowsalya SSNK, Sathyaseelan S. Sensor deployment algorithm for hole detection and healing with the presence of obstacle Ncr access. 2015; 4(4):1–8.
19. Chen Z, Xu M, Yin L, Lu J. Unequal error protected JPEG 2000 broadcast scheme with progressive fountain codes, Tsinghua. 2011.
20. Abitha KS, Anjalipandey A, Kaliyamurthie DKP. Secured data transmission using elliptic curve cryptography. IJIRCCE. 2015; 3(3):1–7.
21. Kim CSMSH. A study on the integrated security system based real-time network packet deep inspection. International Journal of Security and its Applications. 2014; 8(1):113–22.
22. Kim J, Baek J, Shon T. An efficient and scalable re-authentication protocol over wireless sensor network. IEEE Transactions on Consumer Electronics. 2011; 57(2):5–6.