IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Location Dependent Key Management Method for WSN With Reduced Path Length And Considering Cell Head

Nidhi Tawra[1*], Prerna[2], Bhawna Gupta [3]

[1*]Computer Science and Engineering, Meerut Institute of Engineering and Technology, AKTU, Meerut, India
[2] Computer Science and Engineering, Meerut Institute of Engineering and Technology, AKTU, Meerut, India
[3] Computer Science and Engineering, Meerut Institute of Engineering and Technology, AKTU, Meerut, India

e-mail: nidhi.tawra@miet.ac.in, prerna.chaudhary@miet.ac.in, bhawna.gupta@miet.ac.in

[*]*Corresponding Author: nidhi.tawra@miet.ac.in*

Available online at: www.ijcseonline.org

Accepted: 15/Jun/2018, Published: 30/Jun/2018

***Abstract*—** Wireless Sensor Networks (WSNs) consists of sensor nodes (SNs) which are deployed in hostile areas to monitor the environmental* or physical conditions such as temperature, sound, pressure etc. WSNs are used in military operations, civilian operations, forest fire detection and healthcare monitoring etc. These SNs forwards their sensor data via multi-hop wireless paths to the Base Station (BS) and are assembled with limited energy, resource, and memory and communication range. We consider base station to be highly secure, unlike sensor nodes which are threat prone. We assume that the attacker can extract security credentials from the compromised nodes. As these sensor nodes are resource constraint, so the number of hops required sending data from event region to base station needs to be reduced. Moreover, as the sensor nodes have limited memory so the number of keys to be stored on these sensor nodes needs to be reduced. This paper basically focuses on reducing the path length of an event region to the base station as well as reducing the number of keys. We also calculate the number of suspicious nodes and cells in the network.

***Keywords*—**Sensor nodes, security, key management, data gathering, wireless sensor networks.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of spatially distributed sensor nodes (SNs) to monitor the environmental*or physical conditions such as temperature, sound, pressure etc. These SNs forwards their sensor data via multi-hop wireless paths to the Base Station (BS). These SNs are assembled with limited energy resource, limited memory, and limited communication range. WSNs are deployed in large and remote terrains having limited resources. WSNs are used in military operations, civilian operations, forest fire detection and healthcare monitoring etc. [1].

Since WSNs are used in hostile areas, they are more vulnerable to attacks. So, providing security is very essential for these networks. The security attacks on the network can be external or internal. In external attacks, the attacker does not enter into the deployment region. These attacks basically focus on communication within their network and the attacker tries to violate cryptographic primitives such as Confidentiality, Integrity, and Authentication (CIA). Some of the external attack area MIMA (man in the middle attack) and eavesdropping. However, in internal attacks, the attacker enters into the deployment region and tries to disrupt the routing process. Some of the internal attacks are Sybil attack, wormhole attack, sinkhole attack etc. This paper focuses on the mitigation of external security attacks by reducing the path length of an event region to the base station as well as reducing the number of keys. To ensure main security requirements, cryptographic techniques are used. The important aspect of cryptography is Key Management (KM). It involves key pre-distribution, shared key discovery and path key establishment [2]. There are two types of Key Management Schemes (KMS) in cryptography, symmetric key cryptography, and asymmetric key cryptography. In symmetric key cryptography same key used for encryption and decryption. Some of the symmetric key algorithms are DES (Data Encryption Standard), 3DES (Triple DES), AES etc. In asymmetric key cryptography there are two different keys for encryption and decryption, these keys are referred to as public key and private key. The major techniques used in asymmetric key cryptography are RSA, Diffie-Hellman, ECC (Elliptic Curve Cryptography) etc.[3]

In Key Management, there is a requirement of key revocation in the cases when the nodes are compromised by an adversary. If multiple nodes are compromised by an attacker, he can get the keys and can control the communication of entire network. Moreover, the attacker can insert the bogus data into the network through these compromised nodes. If the number of compromised nodes grows in the network, it may lead to the formation of a fraudulent report. So, revocation scheme is required to prevent the compromising of rest of the network.

There are many methods presented in [4] to [5] which focuses on a hop by hop security of data. In these methods majority of communication takes place one SN to other but there are applications like healthcare, fire detection and healthcare monitoring where the majority of communication takes place between the sensor nodes present the area where an event occurred and the base station so the hop by hop security can be hampered [6]. As a result, there is a requirement for the end to end security. This paper focuses to provide end to end security.

Contributions

The objective of the proposed method is:

1) Find out the suspicious nodes and the cells.
2) Reducing the path length in reaching the sensed data from event region to the base station.
3) Reducing the number of keys used.
4) Providing the end to end security.
5) Secure data delivery to the base station.

II. RELATED WORK

E-G [7] presents a dynamic, flexible and scalable technique to suit a large distributed sensor networks. This method provides the same level of security as provided by conventional pair-wise key distribution scheme with less no of keys. The main advantage of this method is that nodes can be revoked from security threats even when some nodes are being compromised by an adversary. This method basically provides hop by hop security for WSNs.

When an event occurs in a monitored region, a cluster of n nodes surrounding the event can detect it and subsequently an event report is generated. For validating the generated report, the concept of collaborative signature which is created by "e" a threshold number where "e" lies between 1 and n. Any report which does not include a valid endorsement is blocked by the intermediate cells and sinks. In the literature, some methods based on this approach are present. One such approach is based on the hop by hop authentication [8] which takes place in an interleaved manner. This method can verify the reports deterministically. Another method, known as the statistical en-route filtering [9] extracts fake reports by making use of a probabilistic approach. The common disadvantage of both these methods is that there is no protection guaranteed by compromising n nodes. In order to solve this problem, LBRS (Location based resilient secrecy)[10] makes use of two approaches: key generation by location binding and key selection in a location-guided manner. As a consequence, the endorsement keys can only be used in the region of the occurrence of the event. This leads to prevention of attacks that use the security requirements of compromised nodes on a global scale. Since it is possible for an attacker to create false events in an area by compromising n nodes in it, so, LBRS method cannot satisfy the requirement of authenticity for data.

In addition to the methods described above location dependent end to end data security (LEDS)[11] method has also been described in the literature where a virtual grid is used to fragment the terrain regulated by a WSN. Inside each cell, each node individually derives a node key and a cell key. This derivation is dependent on the location of the keys and the cells. The reports generated by this method are subjected to a filtering process which results in only relevant reports being extracted. Each of these reports has an endorsement which is derived by a threshold on the number of nodes.

Apparently, the LEDS method has remarkable advantages like the availability of data is guaranteed, minimal effects of node compromising attacks and node to node security. Techniques like node localization are not feasible because they are dependent upon artificial agents like intelligent software or a robot.

The Multi-BS-key management protocol (MKMP) [12] is a recent extension of LEDS. This method displays increased coverage, security of data, power consumption and cost incurred in storage. Also, this method has a key revocation scheme of distributed nature to deal with the problem of compromising nodes. Even with this extension, the MKMP method suffers from the same kind of disadvantages as that of LEDS as far as the outcomes of node compromising are considered. Also, it is very easy for an attacker to make a false report in a cell which would eventually be taken by the sink without suffering any rejection at the intermediate nodes. Both these methods suffer from a huge overhead of bidirectional hop by hop communication between a cell and a base station and also from huge computational cost which can be credited to the generation of authentication keys and setting up the root.

LKMP-RSCR (Location dependent key management protocol for a WSN with a randomly selected cell reporter)[13]. The LKMP-RSCR protocol is assumed to be employed over a wide area of a smart city of a predetermined size and shape monitored using large-scale sensor nodes. This method has two new contributions: the cell reporters of this method increase the security of data by making it more difficult for an attacker to generate a fake report and reducing the effect of node compromising on the sensor network. The second contribution comes from an assumption that hybrid communication scheme is included in the sensor network. Due to this data transmitted to a node from the base station takes place by a single hop alone. On the contrary, data sent by the back to the base station takes place through multiple hops. This ensures much less communication overhead as the

packets transmitted by the base station reach a node without unnecessarily flooding the packets in the entire sensor networks. Also, the computational cost involved is reduced as some of the security credentials are created at the base station and then distributed to each of the nodes in the network. All the computations pertaining to routing are performed at the base station instead of at the nodes.

According to [14] the data sensed by the sensors in a sensor network has to be interpreted for some action to take place. This interpretation consists of computation like maximum, minimum, average etc. These computations can be done at either the node or the base station in a hierarchical fashion. For reducing the amount of data received at the sink it is better than this analysis is performed on the network. The sensed data should be aggregated while it is headed towards its destination for saving the energy. The aggregators are some specially designated sensor nodes which collectively receive the data from all the other nodes. The aggregator then condenses this data received before forwarding it. If this aggregation process does not involve a lot of CPU processing it is definitely beneficial. It is advantageous if the aggregator nodes are more powerful than the other sensor nodes.

Another prime concern while setting up a sensor network is that of data security. Sensor networks are mostly deployed in remote and hostile areas due to which plenty of security issues like management of the keys, maintaining privacy, authorizing access and preventing unauthorized access.

For the above-mentioned reasons, an aggregating data in a secure manner is necessary. After the aggregator node has gathered data it is its responsibility to secure the individual messages and then integrate them. Therefore the techniques of encryption and authentication without decryption are performed at the aggregator nodes. Decryption should be performed only at the sink.so that the entire process is energy efficient.

Several methods for secure data aggregation have been proposed in the literature one method [15] proposes a protocol which answers queries meant for the information gathered by the sensors. It involves data authentication to guarantee privacy but the data is sent unencrypted which is a treat to privacy. Another method [16] of secure data aggregation focuses on energy efficiency by identifying and stopping the redundant data transmitted. Only those sensors which have different data to transmit to the aggregator are allowed to do so by sending a secure pattern. The disadvantage here is that the power saving is not significant because each sensor has to transmit a data packet corresponding to a pattern at least once.

The keys that a sensor node uses for encryption is fixed which is a cause of serious security issues. In [17], secure data aggregation is achieved by removing redundancy in sensor readings without encrypting them while still maintaining data privacy, although, the privacy guarantee is not very high. However, this method is energy efficient. In [14], secure data aggregation is achieved by following a hybrid approach. This approach guarantees the privacy of the sensed data through the use of a homomorphic cipher system. This method allows many operations to be performed on the cipher texts. This encryption technique permits numerous operations over cipher texts that avert decoding at the intermediate nodes that are the aggregators and reduces energy efficiency. Also, the secure data aggregation level which is homomorphic in nature is extended to a double layer hierarchical aggregation protocol by using a watermarking technique of authentication. On comparing it to the existing cipher systems, it is observed that computation and communication costs were greatly reduced. The ease of implementation of this method is an added advantage. So, this paper also uses [14] for secure data aggregation.

The approaches in [18] & [19], authentication schemes based on symmetric keys and hash mechanisms are proposed for wireless sensor networks. These schemes are based on key sharing mechanisms where each authentication key is shared between groups of nodes. However, this scheme is not free from problems arising from node compromising attacks. As an attacker can always alter the key by extracting keys from a sensor node. Other types of symmetric keys mechanisms need the nodes to be synchronized among themselves. Examples of these schemes are TESLA [21] and its other versions. These schemes are not suitable for a large-scale wireless sensor network because it requires time synchronization initially.

In another message authentication scheme [22], a secret polynomial is used for message authentication. The idea of this scheme has been derived from threshold secret sharing, where the degree of the polynomial is used to determine the threshold. If the number of message transmissions falls below the threshold the aggregator node begins verifying the authenticity of the incoming message by polynomial evaluation. If the number of message transmissions is above the threshold the entire system is broken. So that it becomes difficult for the attacker to regenerate the secret polynomial and to raise the threshold level, a perturbation factor also refer to as random noise, serves the role of preventing the attacker to find out the coefficient corresponding to the polynomial in [23]. However, this random noise can be eliminated using error correcting codes.

In public key approaches, the sender's private key is used to generate digital signature corresponding to the message and then the message along with the signature is transmitted. This message is authenticated at every node including the intermediate and the final receivers using the public key of the sender. Recent developments in ECC (Elliptic curve Cryptography) indicate that using public key mechanisms has many advantages as far as usage of node memory, The complexity of the message and security of the message is concerned owing to the key management method of this approach that is relatively very simple.

The communication protocols being used today are derived from mixnet [24] DC-net[25]. These protocols are anonymous in nature. Through a mixnet anonymity is

guaranteed by rearranging packets using a group of mix servers, one of which is trusted. The message forwarded by the sender is encrypted along with the identification of the recipient using the public key of the mixnet. In this way, a set of encrypted messages is gathered in the mixnet. These messages are decrypted, reordered and then sent to the respective recipients. The nature of the background traffic affects such protocols and hence the anonymity provided by these protocols cannot be proved.

In DC net[25], a few participant pairs exchange their respective private keys. This protocol provides guaranteed anonymity of the sender without the need of having servers that can be trusted but in this protocol, at a particular time only one user is permitted to send data. Thus, this protocol requires extra bandwidth to deal with contention and collision.

A ring signature-based approach [26] for providing anonymity of the sender has been recently developed. Through this approach and anonymous signature for the message sent by the sender with authenticated content is generated at the sender. Then, an autonomous system is randomly selected by a member of the ring in order to generate a ring signature. The ring is connected together by the track door information of this ring member. However, this approach lacks flexibility and is very complex.

III. PROPOSED METHOD: A LOCATION DEPENDENT KEY MANAGEMENT METHOD FOR WSN WITH REDUCED PATH LENGTH AND CONSIDERING CELL HEAD(LKMP-RPL)

A. System Assumptions

Our method assumes that sensor nodes are deployed in a large area of which size and shape are predetermined. This area is under surveillance of WSN having n sensor modes and a base station (BS) with unlimited resources. The BS collects the event report and verifies it. The BS can directly send data to the base station, however, data from the node of the event region reached to the base station node by node. The chosen area is divided into a grid of n' cells and each cell has fixed t number of nodes. Each node finds out their location with the help of secure localization scheme [27]-[29]. Fig 1 shows the placement of nodes.

Following are some assumptions:

1) **Channel confidentiality may compromise:** The attacker may eavesdrop the traffic, monitor any messages placed into the channel, and can copy the messages for replay. This can be done using compromised nodes or custom equipment to monitor and place the fake messages into the channel.
2) **Channel may not available:** The attacker can jam the channel, due to which data may not be received by the base station or may be delayed. Small jammers can result into the huge amount of loss of functionality of the network.
3) **Lack of integrity on the channel:** The message can be changed in transit and the sender may not know about it. This can be achieved by an attacker with the help of directional antennae so that the message can be jammed at a single recipient and then fraud message is transmitted.
4) **Trusted base station:** Base station is assumed to be secured but the sensor nodes area is vulnerable to capture. The attackers can mount an attack on the nodes using Joint Test Action Group (JTAG) which allows reprogramming of nodes so the behavior of nodes can be altered.
5) **Compromise of node key information:** This means that key information is removed from the node from the network.

We also assume that system is safe at the time bootstrapping which is a short time period after nodes are being deployed, at that time the attacker can select some nodes and get their keying information. Moreover, the base station cannot be compromised because it has more security. The attacker has no access to uncompromised nodes.

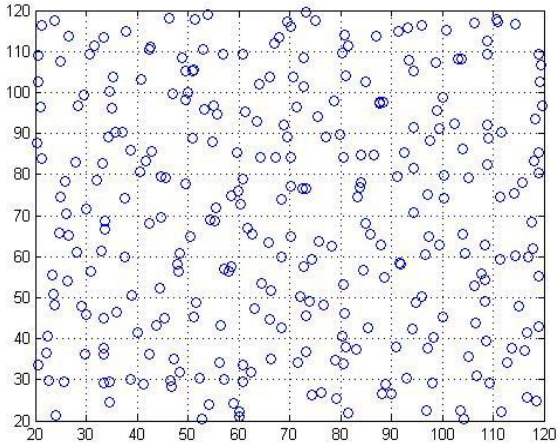

Fig. 1. Placement of nodes where n=120, p=10, and t =3

B. Proposed Method

Wireless Sensor Networks consists of sensor nodes which are deployed in hostile areas. We consider base station to be highly secure, unlike sensor nodes which are threat prone. We assume that the attacker can extract security credentials from the compromised nodes. Our security method consists of following steps:

1) We consider a terrain of n*n m^2.
2) There are n' square cells of p*p m^2.
3) Each cell has t nodes which are deployed randomly using rand () function.
4) Each cell has a cell head which is chosen randomly among the nodes of the cell.

5) Each node has an initial master key K, location of the base station is considered as (x_0, y_0), each node has its id.
6) We calculate the center location of each cell using formula floor(xa-x_0)/delta and floor(ya-y_0) / delta where xa, ya is the location of node and x_0, y_0 is the location of the base station and p is the length of the cell. We consider only one base station.
7) Each node has a key which is shared between base station and node which is calculated using concatenation of initial master key K, id of node and location of the base station (x_0, y_0) and then applying SHA-1 hash function. Similarly, cell key is calculated using concatenation of K, time slot and center location of the cell (xc, yc) and then applying the SHA-1 algorithm.
8) Each node then creates a list consists of the list of its cellmates, central location of its cell and cell key. This list is encrypted using cell key and symmetric key encryption.
9) This list is sent to the base station by each node via cell head to cell head in a range of 15 m where base station verifies the list and calculates the number of suspicious nodes and cells.
10) If an event is generated in a region, event report contains location and cell id. This report is encrypted using cell key.
11) Each node in the cell calculates its share Ci using its unique shared key with base station mod q, where q is the prime number and sends it to the cell head.
12) The cell head concatenates the share from each node and sends the encrypted event report as well as that concatenated share Cnew to the nearest cell head.
13) That nearest cell head creates a Mac of Cnew using the key which is calculated by applying a hash function on the concatenation of center location of event region, a central location of the cell in which cell head is present, a location of the cell head and location of the base station.

C. Simulation Setup

We considered an insecure WSN in which BS is located at (0, 0). Each node in this network has a fixed communication range. BS station can directly communicate with nodes while data sensed by the nodes reach the base station node by node. The communication between the nodes is considered symmetric. We considered an area of 120 x 120 where side length of each cell is considered as 10m and each cell has 3 nodes. The initial master key is considered as 12345.
We used MATLAB as a simulation tool.

IV. RESULTS AND DISCUSSION

The simulation is carried out using MATLAB. We did the simulations on the nodes and calculated the path and number of keys using cell head(LKMP-RPL)and without using cell head(LKMP-RSCR)[13]. We also calculated the number of suspicious nodes and cells and finally revoked them.

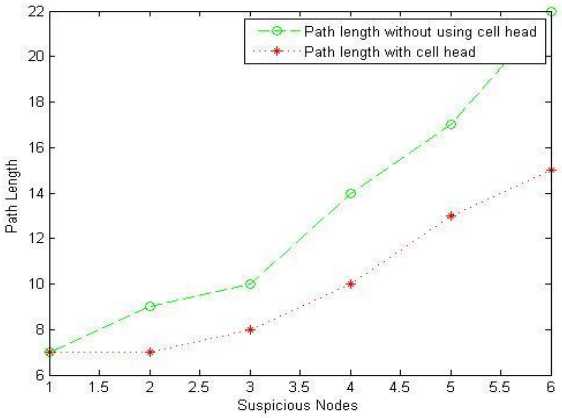

Fig. 2. Path Length with using cell head (LKMP-RPL)and without using cell head. (LKMP-RSCR)

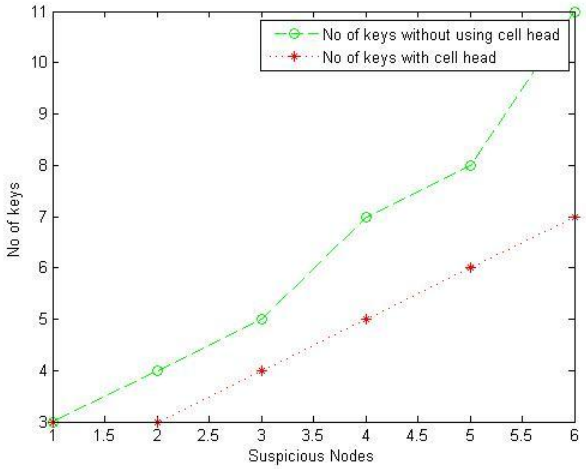

Fig. 3. No of keys with using cell head(LKMP-RPL) and without using cell head(LKMP-RSCR)

The results show that with considering cell head path length, the number of hops required to reach base station from the event region is decreased with the increase in the number of suspicious nodes. Moreover, the numbers of keys which are required for establishing path also decreases.

V. CONCLUSION and Future Scope

WSNs are resource constraint devices and SNs are more vulnerable to physical capture because they are deployed in remote and hostile environments. So, security is needed in these resource-constrained devices. To achieve it, symmetric key cryptography is used. The data reaches the base station from the event region should take minimum hops to save energy of these resource constraint devices. With the use of cell head, the path length is decreased and the number of

keys required to provide cell to cell authentication also decreased.

Symmetric key cryptography has following limitations:

1) Symmetric key cryptography creates more damage to WSNs than public key cryptography if captured by an adversary.
2) Distributing a shared key at the time of bootstrapping is a problem in symmetric key cryptography. For that purpose, random pair-wise key distribution can be used but that may create high communication and memory overhead.
3) There is a problem of authenticity, as both sender and receiver are using the same key. It is hard to know that whether the message is coming from the authentic user or not.
4) Hence, there is a need for lightweight cryptography to mitigate the aforementioned limitations.

In the future work, we can attempt to study and implement ECC(asymmetric key cryptography) for providing location-based security in WSN.

REFERENCES

[1]. Redondo-López, L., Prayati, A., López-Navarro, J. M., Martínez-Ortega, J. F., & García-Hernando,"*Problem Solving for Wireless Sensor Networks":, Computer Communications and Networks. ISBN 978-1-84800-203-6. Springer-Verlag London, 2008.*

[2]. Chan, H., Perrig, A., & Song, D. "Random key predistribution schemes for sensor networks,". In proceedings of IEEE *Security and Privacy, Symposium*, May 2003, pp 197-213.

[3]. Sahoo, S. K., & Sahoo, M. N. "An elliptic-curve-based hierarchical cluster key management in wireless sensor network," In Proceedings of Springer In *Intelligent Computing, Networking, and Informatics*, 2014,pp. 397-408.

[4]. X. He, M. Niedermeier, and H. de Meer, "Dynamic key management in wireless sensor networks: A survey," J. Netw. Comput. Appl., vol. 36, no. 2, pp. 611–622, 2013.

[5]. S. H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol. 10, no. 2, pp. 371–383, Feb. 2015.

[6]. K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 7, no. 5, pp. 585–598, May 2008.

[7]. Eschenauer, L., & Gligor, V. D. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, November 2012, pp. 41-47.

[8]. S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in Proc. IEEE Symp. Secur. Privacy, May 2004, pp. 259–271.

[9]. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE J. Sel. Areas Commun., vol. 23, no. 4, pp. 839–850, Apr. 2005.

[10]. H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc), 2005, pp. 34–45.

[11]. K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 7, no. 5, pp. 585–598, May 2008.

[12]. H.-W. Ferng, J. Nurhakim, and S.-J. Horng, "Key management protocol with end-to-end data security and key revocation for a multi-bs wireless sensor network," Wireless Netw., vol. 20, no. 4, pp. 625–637, 2014.

[13]. Fakhrey, H., Tiwari, R., Johnston, M., & Al-Mathehaji, Y. A,"The Optimum Design of Location-Dependent Key Management Protocol for a WSN With a Random Selected Cell Reporter",*IEEE Sensors Journal*, *16*(19),2016,pp.7217-7226

[14]. Bahi, Jacques M., Christophe Guyeux, and Abdallah Makhoul, "Two security layers for hierarchical data aggregation in sensor networks, "*International Journal of Autonomous and Adaptive Communications Systems"pp.* 239-270,2014.

[15]. B. Przydatek, D. Song, and A. Perrig. Sia: Se-cure information aggregation in sensor networks,"In Proceedings of ACM SenSys conference", pages 255–265, 2003.

[16]. H. Cam, S. Ozdemir, P. Nair, D. Muthuavinashinap-pan, and H. O. Sanli, "Espda: Energy-efficient secure pattern based data aggregation for wireless sensor networks", Computer Communication journal (29), pages 446–455, 2006.

[17]. S. Sharma, D. Kumar, K. Kishore, "Wireless Sensor Networks-A Review on Topologies and Node Architecture", International Journal of Computer Engineering, Vol-1(2), pp(19-25) Oct-2013.

[18]. F. Ye, H. Lou, S. Lu, L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks", *Proc. IEEE INFOCOM*, 2004-Mar.

[19]. S. Zhu, S. Setia, S. Jajodia, P. Ning, "An Interleaved Hop-By-Hop Authentication Scheme for Filtering False Data in Sensor Networks", *Proc. IEEE Symp. Security and Privacy*, 2004

[20]. A. Perrig, R. Canetti, J. Tygar, D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels", *Proc. IEEE Symp. Security and Privacy*, 2000-May.

[21]. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U.Vaccaro, M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences", *Proc. Advances in Cryptology (Crypto '92)*, pp. 471-486, 1992-Apr.

[22]. W. Zhang, N. Subramanian, G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks", April 2008 *Proc. IEEE INFOCOM*, 2008-Apr.

[23]. D. Chaum, "Untraceable Electronic Mail Return Addresses and Digital Pseudonyms", *Comm. ACM*, vol. 24, no. 2, pp. 84-88, Feb. 1981.

[24]. D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability", *J. Cryptology*, vol. 1, no. 1, pp. 65-75, 1988.

[25]. R. Rivest, A. Shamir, Y. Tauman, "How to Leak a Secret", *Proc. Advances in Cryptology (ASIACRYPT)*, 2001.

[26]. M. Wei, R. Aragues, C. Sagues, and G. C. Calafiore, "Noisy range network localization based on distributed multidimensional scaling," IEEE Sensors J., vol. 15, no. 3, pp. 1872–1883, Mar. 2015.

[27]. S. Tomic, M. Beko, and R. Dinis, "RSS-based localization in wireless sensor networks using convex relaxation: Noncooperative and cooperative schemes," IEEE Trans. Veh. Technol., vol. 64, no. 5, pp. 2037–2050, May 2015.

[28]. O. Gungor, F. Chen, and C. E. Koksal, "Secret key generation via localization and mobility," IEEE Trans. Veh. Technol., vol. 64, no. 6, pp. 2214–2230, Jun. 2015.

[29]. V. Prasad, V.S. Sunsan, "Multi path dynamic routing for data integrity and delay Minimization differentiated services in wireless sensor network", International Journal of Scientific Research inResearch Paper" Vol.4, Issue.4, pp.20-23, August 2016.

Authors Profile

Nidhi Tawra pursued M.Tech in Computer Science and Engineering from JAYPEE Institute of Information Technology, Noida.in 2017 and B.Tech in Computer Science and Engineering from Krishna Engineering College, Ghaziabad in 2014. Currently, she is working as an Assistant Professor in Meerut Institute of Engineering and Technology, Meerut.

Prerna pursued M.Tech in Computer Science and Engineering from Uttarakhand Technical University, Dehradun in 2014 and B.Tech from Uttarakhand Technical University, Dehradun in 2012. Currently, she is working as an Assistant Professor in Meerut Institute of Engineering and Technology, Meerut.

Bhawna Gupta pursued M.Tech in Computer Science and Engineering from JAYPEE Institute of Information Technology, Noida.in 2017 and B.Tech in Information Technology from Meerut Institute of Technology, Meerut in 2013.Currently, she is working as an Assistant Professor in Meerut Institute of Engineering and Technology, Meerut.

