International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 3, June 2023, pp. 3131∼3139
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i3.pp3131-3139

Survey on data aggregation based security attacks in wireless sensor network

Nikhath Tabassum [1], Geetha D. Devanagavi[2], Rajashekhar C. Biradar[1], Chaya Ravindra[1]
[1]School of Electronics and Communication Engineering, REVA University, Bengaluru, India
[2]School of Computing and Information Technology, REVA University, Bengaluru, India

Article Info

Article history:

Received Aug 10, 2022
Revised Oct 16, 2022
Accepted Dec 2, 2022

Keywords:

Attacks in wireless sensor network
Black hole attack
Decryption
Encryption
Symmetric key

ABSTRACT

Wireless sensor network (WSN) has applications in military, health care, environmental monitoring, infrastructure, industrial and commercial applications. The WSN is expected to maintain data integrity in all its network operations. However, due to the nature of wireless connectivity, WSN is prone to various attacks that alter or steal the data exchanged between the nodes. These attacks can disrupt the network processes and also the accuracy of its results. In this survey paper, we have reviewed various attacks available in the literature till date. We have also listed existing methods that focus on data aggregation based security mechanisms in WSN to counter the attacks. We have classified and compared these methods owing to their encryption techniques. This paper intends to support researchers to understand the basic attacks prevalent in WSN and schemes to counter such attacks.

Corresponding Author:

Nikhath Tabassum
School of Electronics and Communication Engineering, REVA University
Bengaluru, India
Email: nikhath.tabassum@reva.edu.in

1. INTRODUCTION

Wireless sensor network (WSN) is a collection of sensor nodes that collect the data from surroundings and communicate with each other. Such networks have applications in augmented reality under AI-5G [1], thermoelectric powered smart building monitoring [2], marine environmental exploration and under water military operations [3], civilian applications [4] and Internet of things [5]. Since the sensor nodes communicate among themselves wirelessly and the sensor nodes are present in larger numbers and distributed over larger area, they are prone to various attacks. Though the data is encrypted before transmission and decrypted after reception, there are various attacks that can be launched on these sensor nodes to either corrupt the data that is being transmitted or to capture/compromise the sensor node [6]. The corruption of data can be through addition of fake packets, deletion of valid packets or by copying the information that is transmitted or hacking into the encrypted message to alter the information contained in the packet. The nodes that are compromised include those nodes whose identity has been stolen by malicious nodes [7]. Thus, the malicious nodes try to be a part of the network with this stolen identity and disrupt the functions in the network [8]. The malicious nodes also overwhelm the normal sensor nodes with fake packets so that the node's memory is full and the valid packets also gets dropped. Receiving the overwhelming amount of fake packets will also drain the battery of the normal nodes. The malicious nodes mislead the normal sensor nodes by pretending to be the closest neighbors or convincing the nodes to choose malicious nodes in the pretext of having shortest route.

All these attacks by the malicious nodes have to be prevented by strengthening the encryption and

decryption techniques, by identifying valid nodes and detecting compromised nodes by measuring packet drops and battery depletion rate [9]. Electing trusted cluster head [10] who is aware of the position of its cluster members [11] and secure routing path between cluster head and its members [12]. Also selecting secure transmission path is important [13], [14].

In this survey paper, we have listed various security requirements in WSN, different types of attacks and various methods/schemes that counter these attacks. We have classified these methods into different categories and compared them on the basis of encryption techniques and security requirements. The rest of the paper is organized as follows: section 2 describes the attacks and schemes to counter the attacks, and section 3 concludes the review article.

2. ATTACKS AND SCHEMES TO COUNTER THE ATTACKS

In order for the WSN to work efficiently and correctly, the data collected and shared by the sensor nodes must be protected. If a malicious node attacks a sensor node and corrupts the data, the results of the operation for which the sensor nodes are deployed will be compromised. In this section, we discuss various security requirements, data attacks and also some of the methods that counter these attacks.

2.1. Important security requirements in wireless sensor network (WSN)

Data gathered by sensor nodes is shared with the sink node or base station for further processing [15]. This process of data integration should be secure. It must not reveal the information of the sender or receiver or the message content to unauthorised nodes. For WSN to be secure, it must satisfy the following security requirements.

- Data confidentiality: The WSN must have data confidentiality. The unauthorized sensor node should not be able to access the data shared between the authorized nodes [16].
- Availability: The data and services offered by the network should always be available to all the nodes [17].
- Data integrity: The data is expected to reach base station from sensor node in its original form without any changes. Data integrity is crucial for decision making at the base station which receives the data from the sensor nodes [18].
- Data privacy: There must be data privacy in wireless sensor network. The data of one sensor node must not be disclosed to another neighboring node of the same network [19].
- Non repudiation: The sensor nodes must provide non repudiation as they cannot deny their participation in the communication process [20].
- Data freshness: The WSN should maintain data freshness and discard the old and duplicate packets from the network [21].
- Authenticity: The access control to the sensor nodes must be authenticated to avoid any malicious nodes accessing the data [22]. The sensor nodes must be authenticated before the transmission or reception of data [23].

2.2. Different types of attacks in wireless sensor network (WSN)

The sensor nodes are deployed in large numbers for environmental monitoring, data aggregation and target tracking in public places and in hostile environments. This makes them vulnerable to attacks. The sensor nodes have low processing power and small memory, due to which complex mechanism to prevent the data attacks is not feasible. The most common attacks are listed below.

- Black hole attack: It consumes all the packets sent by the sensor nodes and removes them in pretext of having best routes [24].
- Sinkhole attack: It is similar to black hole attack. In this type, the malicious node knows the exact position of sink node. It tries to deviate the sensor node packets to itself in the pretext of reaching the sink node with shortest path [25].
- Wormhole attack: Two malicious nodes create a wormhole channel between them. They claim that this channel between is the best route and trick the other sensor nodes too to take this path. Once, the sensor nodes take this path, the malicious nodes are able to read the data bytes transferred on this channel and can change the traffic flow [26].

- Selective forwarding attack: In this attack, particular types of packets are eliminated or packets addressed to particular destination are removed. Instead of these missing packets, some other packets are sent to the destination [27].
- Sybil attack: This attack seizes many of the valid identifiers in the network. If a node finds a sybil neighbor node then the sensor node thinks that it is its nearest neighbors and chooses the sybil node as the next hop neighbor. This attack induces fake packets in the network and disrupts the functioning of the network [28].
- Flooding attack: In this attack the malicious node tries to flood the memory of the target node by sending connection request messages. So, the valid node cannot take up genuine request as its memory is full [29].
- Eavesdropping attack: The attacker tries to eavesdrop on the secure data being transmitted to a sensor node. It then tries to use this data to isolate the node from the network. So, if the data is not properly encrypted it can easily fall prey to this attack [30].
- Traffic analysis attack: In this type of attack, the attacker collects all the information of a sensor node with respect to the message type, message length, and message pattern [31], [32].
- Node replication attack: It is similar to sybil attack, but in the attack the attacker tries to copy the memory of a sensor node. It then infuses fake packets and disrupts the network functionality by deleting, modifying the packets [33].
- Packet injection attack: The attacker forges valid data packets and injects into the network. These forged data packets are hard to distinguish from the original data packets if the original data packets have weak encryption [34].
- Packet duplication attack: In this attack a valid packet is duplicated and sent to a node repeatedly to drain all its resources, thereby disrupting the network [35].

The various types of attacks are classified as active or passive, external or internal as in Table 1. The active attacks are the ones that try to change the nature of the data by altering or modifying it. But the passive attacks do not change the content, it only tries to copy the data. The external attacks are launched by sensor nodes that are external to the network i.e not a part of the network. The internal attacks are launched by malicious nodes that capture sensor nodes that are part of the network. The Figure 1 shows lists the data aggregation schemes that employ various strategies to overcome the attacks. These have been classified based on the topology of the network and the type of encryption used. In the next section we discuss the measures taken by these methods to overcome the attacks.

2.3. Counter measures against various attacks

The attacks faced by the sensor nodes have to be prevented for secure transmission of the data among the nodes. There are various schemes that effectively overcome various threats and attacks by malicious nodes in the network. We have listed the counter measures carried by different schemes for different attacks in this section.

2.3.1. Eavesdropping

To prevent eavesdropping, multi-functional secure data aggregation (MFSDA) [36] method utilizes a homomorphic encryption method. As the attacker cannot have all the keys to encrypt the messages exchanged between sensors, it can prevent the attacks caused by eavesdropping. Fog-assisted secure healthcare data aggregation (FASHDA) [37] makes use of symmetric encryption techniques to maintain the confidentiality of the message even if the attackers are eavesdropping. light-weight structure based data aggregation routing (LSDAR) [38] have symmetric encryption and it is passed from one neighbor to another or utilize random pairwise key based symmetric encryption method as in cluster-based private data aggregations (CSDAs) [39]. There are methods such as data aggregation scheme for heterogenous wireless sensor network (DAHWSN) [40] where the encryption is done before the sensor nodes are included in the network. The base station stores the key derivation function (KDF) in the sensor nodes. So, the keys are known to base station and sensor nodes only. Instead of having encryption for the entire data, energy-efficient adaptive slice-based secure data aggregation (EASBSDA) [41] has sensor nodes split their data into slices. These slices are encrypted using symmetric key cryptography separately and transmit to the target nodes. In this way even if the attacker get eavesdrop message, it gets only a slice of the information which cannot be constructed to get a complete message. A random key management method as in energy-efficient and privacy-preserving data aggregation algorithm (EEPDA) [42] is utilised or an elliptic curve based method for encryption in queries privacy-preserving mechanism for data

aggregation (QPDA) [43] can also be utilized to overcome eavesdropping attack.

2.3.2. Sybil

In FASHDA [37] the sensor nodes insert hash value in the message packets so that the aggregators can differentiate between valid and fake packets. In a cluster based topology as in DAHWSN [40] when a data packet is sent to cluster head, the sensor node utilizes the time stamp and its identifier to indicate fresh and valid packets. The cluster head verifies the data packets with respect to the signature of the sensor node. This signature is calculated by sensor node based on the timestamp and secret key. In another cluster based scheme in secure authentication with protected data aggregation scheme (SAPDAS) [44], each cluster member calculates an hybrid medium access code (HMAC) value and includes this in the packet before transmitting it to the cluster head. The cluster head in turn transmits these packets to the base station. The base station then checks this HMAC value to validate the packets which can neutralize the attack. In reliable and secure end-to-end data aggregation (RSDA) [45] data slicing and digital signature is used. It is very effective locally but not effective for centralized process for authentication. Drawback is that since it is a centralized method, locally the nodes cannot detect fake packets. So, in SCBFDA [46] a secondary message authentication code (SECMAC) (message authentication code) value is calculated at each sensor node. On reception, the receiving node also calculates the SECMAC value and verifies it. So it is easy to detect fake packets.

Table 1. Classification of different attacks

Number	Method	Active	Passive	External	Internal
1	Black hole attack	✓	×	✓	×
2	Sinkhole attack	✓	×	✓	×
3	Wormhole attack	✓	×	✓	×
4	Selective forwarding attack	✓	×	✓	×
5	Sybil attack	✓	×	✓	×
6	Flooding attack	✓	×	✓	×
7	Eavesdropping attack	×	✓	✓	×
8	Traffic Analysis attack	×	✓	✓	×
9	Node replication attack	✓	×	×	✓
10	Packet injection attack	✓	×	✓	×
11	Packet duplication attack	✓	×	✓	×

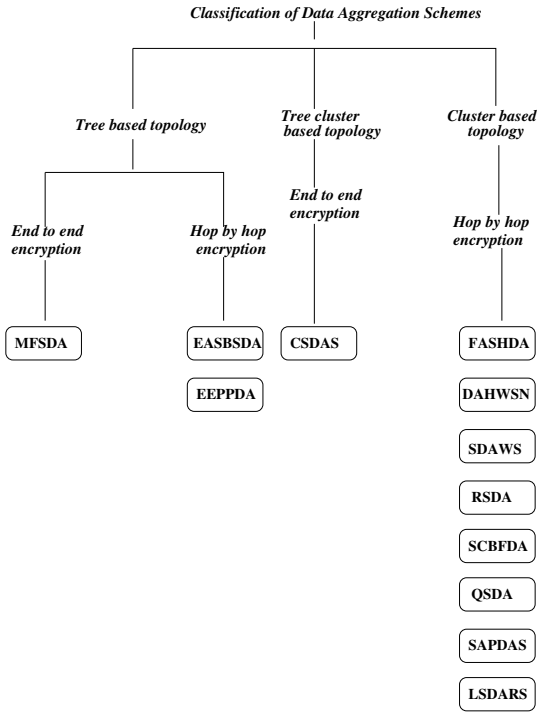

Figure 1. Classification of data aggregation schemes with respect to topology and encryption

2.3.3. Node replication

In FASHDA [37] technique, the attackers can only access the secret key of the affected node and not other nodes keys. So, it has a localized effect on network. But if it attacks the aggregator node, then it may effect the functioning of the other nodes connected to the aggregator node and disrupt the network at a larger scale. Therefore, the compromised node should be isolated which is not done effectively by FASHDA [37]. But if the aggregator node is a cluster head and it is attacked as in DAHWSN [40], the cluster head cannot send fake packets to the base station because cluster member keys are not known to the cluster head but this attack can very well delete all the packets that are received at cluster head therefore compromising the availability of the packets. In recoverable concealed data aggregation scheme (RCDAS) [47] the attack is nullified as it is uses digital signatures for authentication that identifies and blocks the fake malicious nodes.

2.3.4. Traffic analysis

In MFSD [36] the sinknode has the decryption keys, so it cannot access information such as message length and pattern. In FASHDA [37], the encryption key is with the server and the attacker however can know the aggregator node and server node identity and its location. But it can use this information to launch sinkhole and sybil attacks. Each valid node calculates the signature based ID and inserts into the data packets as in DAHWSN [40]. It utilizes homomorphic end to end encryption technique that will not allow the attacker to know the content and hence the traffic in the network. In EASBSDA [41] and SAPDA [44] even if the attacker almost accesses pairwise keys, it cannot have all the secret keys shared between the sensor nodes and hence cannot detect traffic. Each node knows only its keys. Another way is to slice the data and encrypt it separately as in CSDAS [39] and SAPDAS [44] have random pairwise keys shared between the neighboring nodes. Due to data slicing and random key for ciphering, the traffic analysis becomes difficult. But, if there are cluster heads changing constantly, so getting to know the cluster head and attacking will take long time and difficult to analyze traffic.

2.3.5. Black hole attack

In this attack either the malicious node deletes all the packets directed towards it or it makes the nodes believe that it is part of the best route and introduces fake packets in bulk such that the valid router drops the packets as it will be overwhelming for it to handle. In, DAHWSN [40], the network topology has clusters. The cluster head verifies the identity of its cluster members by signature verification. So the malicious nodes will not be able to send fake packets. The clsuter head when it sends the packets to the base station, the base station verifies the identity of the cluster head by batch verification signature. So, the malicious nodes can be detected if it sends fake packets. In RSDA [45] the data is segregated into 4 slices, each slice is encrypted separately. The transmitting node sends 2 encrypted packets each to two aggregators with digital signatures. So, if a malicious node persuades the aggregator to share the data, the data received at the base station by the second aggregator will be incomplete without the first aggregator data. So the base station knows if the data is fake. For authentication, in FASHDA [37] each node has a valid hash value inserted in the packets, so that the aggregator nodes can detect the authentic packets and discard fake packets. In SAPDA [44] it generates a hybrid medium access code (HMAC) value depending on the original data and time stamp and in SDAWS [48] this scheme utilizes water marking scheme to validate the nodes. In a cluster head based topology as in SAPDAS [44] the cluster heads communicate with the other trusted cluster head only. The gateway node authenticates the cluster heads. The base station receives the data only from authenticated cluster heads. The base station generates KDF as in DAHWSN [40] and embeds in each sensor nodes memory. The base station also generates private key and secret key along with new identifier for each sensor node. This is known only to the sensor node and base station. A sensor node when it transmits a packet to the cluster head, it calculates a signature based on secret key time stamp and its ID, which is again verified by cluster head to confirm the validity of the sensor node.

2.3.6. Flooding attack

In the flooding attack, duplicate packets are generated in bulk to drain the sensor node of its battery and memory. To avod this, in FASHDA [37] and SAPDAS [44] when a aggregator node receives data from sensor node, it checks for the time stamp to confirm whether it is a fresh packet or a duplicate packet. If it is a duplicate packet, it is discarded and if the packet happens to be a fresh packet, then it is stored.

2.3.7. Packet alteration, packet injection and packet duplication

In FASHDA [37] fake packets are detected by the sensor node. If the attacker resends old packets, it is identified through time stamp checking and in DAHWSN [40], it will check for cluster head in the valid sensor list which is maintained by the base station and can overcome packet alteration sent by malicious nodes. The Table 2 compares various algorithms based on the different security requirements. Almost all the methods preserve the data confidentiality and privacy of data. The various schemes have been classified depending on the type of the encryption utilized as in Table 3. Symmetric encryption has the same key for encryption and decryption [49], [50]. The key must be transmitted securely between the sensor nodes. In asymmetric encryption [51] there are two keys namely the public key and secret key. If the public key is used for encryption, then the secret key will be used for decryption.

Table 2. Comparison of different schemes with respect to security requirements

Number	Method	Availability	Non repudiation	Privacy	Data freshness	Authentication	Access control	Data integrity	Data Confidentiality
1	MFSDA	×	×	✓	×	×	×	×	✓
2	FASHDA	×	×	✓	✓	×	×	✓	✓
3	DAHWSN	✓	✓	✓	✓	✓	✓	✓	✓
4	SDAWS	×	×	✓	×	×	×	✓	✓
5	RSDA	✓	✓	✓	×	✓	✓	✓	✓
6	EASBSDA	×	×	✓	×	×	×	×	✓
7	SCBFDA	×	×	✓	×	✓	✓	✓	✓
8	SAPDAS	✓	✓	✓	✓	✓	✓	✓	✓
9	EEPPDA	×	×	✓	×	×	×	×	✓
10	QPDA	×	×	✓	×	×	×	×	✓
11	LSDAR	×	×	✓	×	×	×	×	✓
12	CSDAS	×	×	✓	×	×	×	×	✓

Table 3. Comparison of cryptography techniques for different schemes

Number	Method	Symmetric key encryption	Asymmetric key encryption
1	MFSDA	×	✓
2	FASHDA	✓	×
3	DAHWSN	✓	×
4	SDAWS	×	✓
5	RSDA	×	✓
6	EASBSDA	✓	×
7	SCBFDA	×	✓
8	SAPDAS	✓	×
9	EEPPDA	✓	×
10	QPDA	×	✓
11	LSDAR	✓	×
12	CSDAS	✓	×

2.3.8. Discussions

The symmetric key cryptographic technique is simpler and has less computation overhead. But the security provided is less compared to asymmetric key cryptographic technique. The asymmetric key cryptography has high computation overhead, complex and consumes more energy. To conserve the battery power, the topology of the network is also a contributor. The tree topology is structured and has a fixed hierarchy, but has higher packet loss and drains the battery power of the sensor nodes as the paths are fixed. In case of cluster based topology all the cluster members communicate with cluster head only. The cluster head should have high energy and must be able to handle greater computational overhead. So, a hybrid tree-cluster based topology will be more desirable to overcome the disadvantages of tree based and cluster based topologies.

3. CONCLUSION

The security in wireless sensor networks often gets compromised due to the constraints like limited battery power, smaller memory and lesser computational capacity to carry out complex, encryption and decryption techniques. With these limitations, there are schemes that efficiently overcome the various attacks that

sensor nodes encounter. We have discussed various attacks in WSN. We have also discussed and classified the aggregation schemes based on their topology and encryption techniques.

REFERENCES

[1] M. Khan, "Advances in wireless sensor networks under AI-5G for augmented reality," *Virtual Reality and Intelligent Hardware*, vol. 4, no. 3, pp. 2–4, Jun. 2022, doi: 10.1016/j.vrih.2022.06.003.

[2] Q. Lin, Y.-C. Chen, F. Chen, T. DeGanyar, and H. Yin, "Design and experiments of a thermoelectric-powered wireless sensor network platform for smart building envelope," *Applied Energy*, vol. 305, Jan. 2022, doi: 10.1016/j.apenergy.2021.117791.

[3] H. Li *et al.*, "An extended-range wave-powered autonomous underwater vehicle applied to underwater wireless sensor networks," *iScience*, vol. 25, no. 8, Aug. 2022, doi: 10.1016/j.isci.2022.104738.

[4] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," *Applied System Innovation*, vol. 3, no. 1, pp. 1–24, 2020, doi: 10.3390/asi3010014.

[5] S. Rani, R. Maheswar, G. R. Kanagachidambaresan, and P. Jayarajan, *Integration of WSN and IoT for smart cities*. Cham: Springer International Publishing, 2020.

[6] Y. Choi, "Cryptanalysis on privacy-aware two-factor authentication protocol for wireless sensor networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 1, pp. 605–610, Feb. 2018, doi: 10.11591/ijece.v8i1.pp605-610.

[7] R. Kowsalya and B. Roseline Jeetha, "Cluster based data-aggregation using lightweight cryptographic algortihm for wireless sensor networks," in *Materials Today: Proceedings*, Feb. 2021, doi: 10.1016/j.matpr.2021.01.163.

[8] B. J. Chelliah, M. S. A. Vigil, and M. S. B. Praba, "Node clone detection using a stable overlay network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 316–322, Feb. 2020, doi: 10.11591/ijece.v10i1.pp316-322.

[9] B. Hasan, S. Alani, and M. A. Saad, "Secured node detection technique based on artificial neural network for wireless sensor network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 1, pp. 536–544, 2021, doi: 10.11591/ijece.v11i1.pp536-544.

[10] N. Tabassum, G. D. Devanagavi, and R. C. Biradar, "Clock synchronization in wireless sensor networks using least common multiple," *International Journal of Electronics and Communications*, vol. 82, pp. 446–457, Dec. 2017, doi: 10.1016/j.aeue.2017.10.014.

[11] N. Tabassum, D. D. Geetha, and R. C. Biradar, "Joint position estimation and synchronization of clocks in WSN," in *Lecture Notes in Networks and Systems*, vol. 235, 2022, pp. 409–418.

[12] M. Al-Sadoon and A. Jedidi, "A secure trust-based protocol for hierarchical routing in wireless sensor network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 3838–3849, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3838-3849.

[13] M. C. Belavagi and B. Muniyal, "Multiple intrusion detection in RPL based networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 467–476, 2020, doi: 10.11591/ijece.v10i1.pp467-476.

[14] N. Tabassum, G. D. Devanagavi, R. C. Biradar, and M. T. Lazarescu, "Comparative node selection-based localization technique for wireless sensor networks: a bilateration approach," *International Journal of Communication Systems*, vol. 33, no. 15, Aug. 2020, doi: 10.1002/dac.4559.

[15] B. Bhushan and G. Sahoo, "Requirements, protocols, and security challenges in wireless sensor networks: an industrial perspective," *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, pp. 683–713, 2019, doi: 10.1007/978-3-030-22277-2_27.

[16] V. Shankar, "Contemporary secured target locality in wireless sensor networks," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 194–198, Nov. 2021, doi: 10.1016/j.gltp.2021.08.023.

[17] Y. Zhang, L. Liu, M. Wang, J. Wu, and H. Huang, "An improved routing protocol for raw data collection in multihop wireless sensor networks," *Computer Communications*, vol. 188, pp. 66–80, Apr. 2022, doi: 10.1016/j.comcom.2022.02.016.

[18] K. Hameed, A. Khan, M. Ahmed, A. Goutham Reddy, and M. M. Rathore, "Towards a formally verified zero watermarking scheme for data integrity in the internet of things based-wireless sensor networks," *Future Generation Computer Systems*, vol. 82, no. 1, pp. 274–289, May 2018, doi: 10.1016/j.future.2017.12.009.

[19] X. Qi, X. Liu, J. Yu, and Q. Zhang, "A privacy data aggregation scheme for wireless sensor networks," *Procedia Computer Science*, vol. 174, pp. 578–583, 2020, doi: 10.1016/j.procs.2020.06.127.

[20] H. U. Yildiz, K. Bicakci, B. Tavli, H. Gultekin, and D. Incebacak, "Maximizing wireless sensor network lifetime by communication/computation energy optimization of non-repudiation security service: node level versus network level strategies," *Ad Hoc Networks*, vol. 37, pp. 301–323, Feb. 2016, doi: 10.1016/j.adhoc.2015.08.026.

[21] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: active and passive attacks - vulnerabilities and countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362–367, 2021, doi: 10.1016/j.gltp.2021.08.045.

[22] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *Journal of Information Security and Applications*, vol. 52, Jun. 2020, doi: 10.1016/j.jisa.2020.102502.
[23] B. Hu, W. Tang, and Q. Xie, "A two-factor security authentication scheme for wireless sensor networks in IoT environments," *Neurocomputing*, vol. 500, pp. 741–749, 2022, doi: 10.1016/j.neucom.2022.05.099.
[24] I. Kaushik and N. Sharma, "Black hole attack and its security measure in wireless sensors networks," *Advances in Intelligent Systems and Computing*, vol. 1132, pp. 401–416, 2020, doi: 10.1007/978-3-030-40305-8_20.
[25] A. ur Rehman, S. U. Rehman, and H. Raheem, "Sinkhole attacks in wireless sensor networks: a survey," *Wireless Personal Communications*, vol. 106, no. 4, pp. 2291–2313, 2019, doi: 10.1007/s11277-018-6040-7.
[26] N. Dutta and M. M. Singh, "Wormhole attack in wireless sensor networks: a critical review," in *Advances in Intelligent Systems and Computing*, vol. 702, 2019, pp. 147–161.
[27] H. Fu, Y. Liu, Z. Dong, and Y. Wu, "A data clustering algorithm for detecting selective forwarding attack in cluster-based wireless sensor networks," *Sensors*, vol. 20, no. 1, Dec. 2019, doi: 10.3390/s20010023.
[28] A. Angappan, T. P. Saravanabava, P. Sakthivel, and K. S. Vishvaksenan, "Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6567–6578, Jun. 2021, doi: 10.1007/s12652-020-02276-5.
[29] R. U. Rasool, H. Wang, U. Ashraf, K. Ahmed, Z. Anwar, and W. Rafique, "A survey of link flooding attacks in software defined network ecosystems," *Journal of Network and Computer Applications*, vol. 172, Dec. 2020, doi: 10.1016/j.jnca.2020.102803.
[30] Q. Wang, "Defending wireless communication against eavesdropping attacks using secret spreading codes and artificial interference," *Computers and Security*, vol. 103, Apr. 2021, doi: 10.1016/j.cose.2020.102175.
[31] J. R. Ward and M. Younis, "A cross-layer traffic analysis countermeasure against adaptive attackers of wireless sensor networks," *2016 IEEE Military Communications Conference*, 2016, pp. 271-276, doi: 10.1109/MILCOM.2016.7795338.
[32] H. Ghamgin, M. S. Akhgar, and M. T. Jafari, "Attacks in wireless sensor network," *Australian Journal of Basic and Applied Sciences*, vol. 5, no. 7, pp. 954–960, 2011.
[33] M. Numan *et al.*, "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020, doi: 10.1109/ACCESS.2020.2983091.
[34] V. P. Illiano and E. C. Lupu, "Detecting malicious data injections in wireless sensor networks," *ACM Computing Surveys*, vol. 48, no. 2, pp. 1–33, Nov. 2015, doi: 10.1145/2818184.
[35] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity issues in wireless sensor networks: current challenges and solutions," *Wireless Personal Communications*, vol. 117, no. 1, pp. 177–213, Mar. 2021, doi: 10.1007/s11277-020-07213-5.
[36] P. Zhang, J. Wang, K. Guo, F. Wu, and G. Min, "Multi-functional secure data aggregation schemes for WSNs," *Ad Hoc Networks*, vol. 69, no. 1, pp. 86–99, Feb. 2018, doi: 10.1016/j.adhoc.2017.11.004.
[37] A. Ullah, G. Said, M. Sher, and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer-to-Peer Networking and Applications*, vol. 13, no. 1, pp. 163–174, Jan. 2020, doi: 10.1007/s12083-019-00745-z.
[38] K. Haseeb, N. Islam, T. Saba, A. Rehman, and Z. Mehmood, "LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks," *Sustainable Cities and Society*, vol. 54, Mar. 2020, doi: 10.1016/j.scs.2019.101995.
[39] W. Fang, X. Wen, J. Xu, and J. Zhu, "CSDA: a novel cluster-based secure data aggregation scheme for WSNs," *Cluster Computing*, vol. 22, no. S3, pp. 5233–5244, May 2019, doi: 10.1007/s10586-017-1195-7.
[40] H. Zhong, L. Shao, J. Cui, and Y. Xu, "An efficient and secure recoverable data aggregation scheme for heterogeneous wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 111, pp. 1–12, 2018, doi: 10.1016/j.jpdc.2017.06.019.
[41] P. Hua, X. Liu, J. Yu, N. Dang, and X. Zhang, "Energy-efficient adaptive slice-based secure data aggregation scheme in WSN," *Procedia Computer Science*, vol. 129, pp. 188–193, 2018, doi: 10.1016/j.procs.2018.03.033.
[42] L. Zhou, C. Ge, S. Hu, and C. Su, "Energy-efficient and privacy-preserving data aggregation algorithm for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3948–3957, May 2020, doi: 10.1109/JIOT.2019.2959094.
[43] X. Liu, X. Zhang, J. Yu, and C. Fu, "Query privacy preserving for data aggregation in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2020, 2020, doi: 10.1155/2020/9754973.
[44] N. Goyal, M. Dave, and A. K. Verma, "SAPDA: secure authentication with protected data aggregation scheme for improving QoS in scalable and survivable UWSNs," *Wireless Personal Communications*, vol. 113, no. 1, pp. 1–15, 2020, doi: 10.1007/s11277-020-07175-8.
[45] W. Y. Alghamdi, H. Wu, and S. S. Kanhere, "Reliable and secure end-to-end data aggregation using secret sharing in WSNs," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, Mar. 2017, pp. 1–6, doi: 10.1109/WCNC.2017.7925558.

[46] M. Shobana, R. Sabitha, and S. Karthik, "An enhanced soft computing-based formulation for secure data aggregation and efficient data processing in large-scale wireless sensor network," *Soft Computing*, vol. 24, no. 16, pp. 12541–12552, 2020, doi: 10.1007/s00500-020-04694-1.
[47] C. M. Chen, Y. H. Lin, Y. C. Lin, and H. M. Sun, "RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 4, pp. 727–734, 2012, doi: 10.1109/TPDS.2011.219.
[48] D. E. Boubiche, S. Boubiche, H. Toral-Cruz, A.-S. K. Pathan, A. Bilami, and S. Athmani, "SDAW: secure data aggregation watermarking-based scheme in homogeneous WSNs," *Telecommunication Systems*, vol. 62, no. 2, pp. 277–288, Jun. 2016, doi: 10.1007/s11235-015-0047-0.
[49] W. Zhou, P. Li, Q. Wang, and N. Nabipour, "Research on data transmission of wireless sensor networks based on symmetric key algorithm," *Measurement*, vol. 153, Mar. 2020, doi: 10.1016/j.measurement.2019.107454.
[50] J. R. and N. G. Cholli, "An efficient approach for secured communication in wireless sensor networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1641–1647, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1641-1647.
[51] K. Havashemi rezaeipour and H. Barati, "A hierarchical key management method for wireless sensor networks," *Microprocessors and Microsystems*, vol. 90, Apr. 2022, doi: 10.1016/j.micpro.2022.104489.

BIOGRAPHIES OF AUTHORS

Nikhath Tabassum received her Ph.D. in 2021. She is currently working as Assistant Professor in REVA University. She has published papers in reputed international journals and conferences. Her research interest include wireless sensor networks, ad-hoc networks and network security. She can be contacted at email: nikhath.tabassum@reva.edu.

Geetha D. Devanagavi received her Ph.D in 2014. She is currently a Professor at REVA university. She has 26 years of teaching experience. Her research interest include wireless sensor networks, network security, and computer networks. She has good number of publications in reputed international journals. She has guided 4 Ph.D. scholars. She can be contacted at email: dgeetha@reva.edu.in.

Rajashekhar C. Biradar is currently working as Pro Vice Chancellor at REVA university, India. He has 32 years of teaching experience. His research interest include Ad-hoc networks, sensor networks, mesh networks, network security, and wireless sensor networks. He has good number of publications in reputed international journals. He has published 65 papers in peer reviewed national and international journals, 73 papers in reputed national and international conferences and 4 book chapters. He has guided 7 Ph.D. scholars. He received "Best Ph.D. Thesis Supervisor Award, 2021" by BITES, Govt. of Karnataka, India. He has been listed in Marquis' Who's Who in the World (2012 Edition), USA and Top 100 Engineers by IBC, UK. As per Google Scholar, he has more than 1,900 citations with h-index of 23. He can be contacted at email: provc@reva.edu.in.

Chaya Ravindra is assistant professor in REVA University. She has completed Ph.D. in the year 2021. She has published 15 international journals and 4 international conference papers. Her research interest are in optical communication and wireless sensor network. She is a member of UACEE and IETE. She can be contacted at email: chaya@reva.edu.in.