Research Article

Framework with temporal attribute for secure data aggregation in sensor network

Mahantesh Mathapati[1] · T. Senthil Kumaran[2] · K. H. Shiva Prasad[3] · Kavita Patil[2]

Received: 9 July 2020 / Accepted: 27 October 2020 / Published online: 10 November 2020

Abstract
This study presents a cost-effective analytical model that is capable of resisting the majority of the lethal threats in WSN. The significant contribution of this paper is the inclusion of the temporal factors associated with the message transmission behavior of the sensors that act as a contributory player to retain maximum resource retention and maximum security. So the aim of the proposed system develops a cost-effective non-iterative framework that can offer robust, secure data aggregation in the presence of threats of unknown nature. The comparative analysis of the proposed system shows that it is capable of offering a higher degree of energy efficiency, reduced delay, and reduced computational time in contrast to existing models of secure data aggregation. The study outcome shows that proposed system is 45% faster with 56% of energy reduction capability than existing approaches.

Keywords Secure data aggregation · Wireless sensor network · Encryption · Data security

1 Introduction

Adoption of remote controlling the device as well as service has tremendously increased in the last decades over various commercial products. Such monitoring is carried out by the deployment of sensors using an exclusive structure of a network called Wireless Sensor Network (WSN) [1]. This formulates a sophisticated network model in a distributed manner equipped with different forms of sensor nodes that are dispersed in the area that demands to monitor various physical attributes [2]. After the deployments of the sensors are achieved, the next step is to collaborate with all the sensors in the form of a network, which leads to a sink node. This transmission of the data is carried out in two ways viz. data fusion and data aggregation. The data fusion is a mechanism where the cluster head node collects all the local data from the member node using TDMA and checks for their redundancy level [3]. The filtered and processed fused data is then forwarded directly to the sink node (in case of single-hop) or the next neighboring cluster head (in case of multiple hops). This process is called data aggregation [4]. Hence, data aggregation is a mechanism of aggregation of the data from the sensors in a collaborative manner and forwarding it finally to the sink node. However, in this process, there are multiple challenges. The first challenges are to carry out clustering so that better coverage is maintained for maximum nodes within a cluster that can sustain longer. Irrespective of various clustering mechanism in WSN, energy efficiency, traffic management as well as security is still an open-end problem. The second challenge, while performing data aggregation, is the consistent drainage of energy irrespective of any efforts. Hence, energy is a scarce resource that is sufficiently required to be carried out data aggregation. This problem aggravates when security is involved in it. At present, there are various secure routing approaches in WSN [5–7], where the encryption-based approach is considered as the core

✉ T. Senthil Kumaran, senthilvts@gmail.com; Mahantesh Mathapati, manteshkrishna@gmail.com; K. H. Shiva Prasad, shivaprasadgowda@gmail.com; Kavita Patil, kavita.patil3008@gmail.com | [1]RajaRajeswari College of Engineering, Visveswaraya Technological University, Belagavi, India. [2]ACS College of Engineering, Visveswaraya Technological University, Belagavi, India. [3]GITAM (Deemed To Be University), Bangalore, India.

security solution. It is to be known that irrespective of the availability of some of the strongest encryption techniques, they cannot be applied in resource-constrained sensor nodes. The availability of the energy as well as different other resources, e.g., memory, bandwidth, etc. is highly essential to run such complex algorithms while performing data aggregation. Therefore, there have been various research works being carried out in existing approaches towards exploring the mechanism for secure data aggregation [8, 9]. It has been observed that strategies are mainly using MAC protocols or use timestamp. It deploys authentication schemes towards resisting the denial-of-service attack, replay attack, and Sybil attack mostly. The existing secure data aggregation can be carried out considering a single aggregator as well as multiple aggregators. One of the most significant flaws of the single aggregation method is that they don't facilitate vital confidentiality and suffers from propagating stale routing data. The multiple aggregator methods offer data quality, but still, they are found not to provide resource conservation while performing data aggregation.

Therefore, there is still an extensive scope of evolving up with a new solution to this problem. The proposed paper identifies that the inclusion of the temporal parameter can significantly boost up the control mechanism of the malicious node as well as it can also control the energy depletion among the sensor nodes. This paper presents an analytical approach for secure data aggregation in the presence of uncertain adversaries in WSN and is meant for balancing the energy needs too.

The potential points as well as novel features of the proposed system are (i) inclusion of temporal parameters which is meant for direct control over the topology towards supporting encryption, (ii) inclusion of on-demand clustering unlike any existing approaches, (iii) performing light-weight encryption while routing. The advantages of results are (i) proposed system offers 56% of energy saving, (ii) 47% reduction in delay, and (iii) 45% faster processing time compared to existing security approaches. The organization of the paper is as follows: Sect. 2 discusses the existing research work towards secure data aggregation while Sect. 3 briefs of research problems. The highlight of the proposed methodology is briefed in Sect. 4, followed by a discussion of algorithm implementation in Sect. 5. Result discussion is carried out in Section VI while concluding remarks about the contribution are highlighted in conclusion Sect. 6.

2 Related work

This section discusses existing approaches and techniques, which are associated with the secure data transmission in the wireless sensor network. The work carried out by Guo et al. [10] has presented a security approach towards the physical layer over the wireless network, which is equally applicable to the sensory application. The authors have used beamforming mechanisms along with source decoding here; certain jammers are used to act as an impediment towards eavesdropper by forwarding artificial noise. The study claims a higher secrecy rate. A similar mechanism of stopping eavesdropping is also carried out by Wang et al. [11], where game theory logic has been used. The work carried out by Tian et al. [12] has used a cross-layer based scheme to construct a secrecy model for better data security using an optimization approach. The work carried out by Huang et al. [13] has used a conventional mechanism of intrusion detection system considering mobility factor over sensory application. The authors have developed a mobility pattern with the aid of an elastic collision model, which is mainly about capturing the essential information about the intruders. Deng et al. [14] have used a stochastic geometry to offer the security of the physical layers associated with sensory applications. According to the study, two different scenarios have been formulated where sensors of active form forward the message to the access point. In contrast, the access point further transmits it to the base station. The study outcome shows that if the access points are maximized, then the mean rate of secrecy minimizes.

The study carried out by Zhu et al. [15] has presented a unique security mode where the focus of security was in physical layers. This study carries out a discussion of the issues and challenges associated with the security factor of WSN as well as energy-related problems too. Another frequently used approach of data security in a wireless sensor network is trust. The study carried out by Liu et al. [16] has presented a trust-based solution to resist blackhole attack in the sensor network. According to the study, the system generates the identification information about the adversary based on the energy factor of the hotspots. The analysis was carried out using experimental and theoretical aspects. The work carried out by Kim and An [17] has presented the use of the public key encryption to offer data security while performing transmission. The author has presented a distributed scheme where the control message is subjected to various processing for resisting jamming attacks in the sensor network. Kong et al. [18] have a unique key generation technique to secure communication in a wireless sensor network. The security modeling was carried out over the physical layer using network coding. The presented concepts make use of the multipath channels to improve the secure data transmission where the secret key is yielded based on the impulse response of the communication channel.

The authors have presented a quantization approach with adaptive nature to enhance the secrecy. The work

carried out by Wang et al. [19] has constructed as a security mechanism for resisting threats against the physical layer, considering the case study of a smart city. The authors have implemented Wyner's model considering the mobility factor in the sensory application using probability theory. The authors have used Monte-Carlo simulation to assess its effectiveness. The work of Zhang et al. [20] has presented a trust-based security approach for modeling the intrusion detection system [34]. The authors have used a context of dynamic state to develop this trust model along with an assessment model for checking the legitimacy of the feedback obtained. The adoption of a group key has been considered in the work of Porambage et al. [21], where multicast protocols have been used for secure transmission. The work considering the case study of internet-of-things has developed a group key protocol for devices that has a shortage of resources with a target of improving the security and scalability factor in its data transmission performance. Similar approaches towards securing the physical layer are witnessed in the work of Moara-Nkwe et al. [22], where a unique key generation mechanism is presented, which uses the energy and error correction mechanism to offer security.

Study towards body area network and securing its sampling mechanism was discussed in the work of Dautov and Tsouri [23]. The authors have used an encryption approach of the compressed data, primarily focusing on the physical layer. The technique offers independence from using different encryption and also reduces resource dependencies much. The work of Biswas et al. [24] has used a Chaotic map to improve the encryption operation where public-key encryption is used for authenticating the communicating sensors. The study also harnesses the potential of evolutionary computing to enhance the operation of encryption associated with the sensor nodes. The work carried out by Zou and Wang [25] have presented a work towards the identification of an eavesdropping attack. According to this logic, the data transmission is permissible by the sensor node, which is chosen based on a higher secrecy rate. The work carried out by Lee et al. [26] have established a relationship between energy and security in wireless sensor network, which mainly emphasis on data integrity. The study evaluates that it can successfully control the energy efficiency. The work of Wu et al. [27] has developed a model which is claimed to offer resistance from complicated attacks. The idea of this work is mainly to check the feasibility of identifying uncommon and uncertain forms of attacks in the wireless sensor network. The adoption of the chaotic theory was considered in the work of Tayebi et al. [28], where direct sequence spread spectrum is used for offering privacy in communication over wireless networks. The work of Zhang et al. [29] have presented a logic of scheduling and associated them with the security scheme in a wireless sensor network. The study has showcased that the scheduling of sleep and awake states can significantly contribute towards the security scheme as well as energy efficiency together. The idea of this study was also to promote lesser use of encryption approaches using graph theory.

Therefore, the drawbacks of each technique are as follow: (1) Adoption of complicated concept like game theory can be used for mitigating adversaries with complex patterns; however, they still cannot be mapped for dynamic adversaries. (2) Layer-based approaches are too specific towards securing attacks. Although, cross-layer based scheme offers flexibility but still they are made specific to attack. (3) Majority of the other schemes are made to resist one kind of attacks only. (4) Adoption of probability modelling is a good attempt but they are not meant for resisting the adversaries when they dynamically change their attack strategy. (5) None of the work actually offers resistance to adversaries if they have newly joined the network.

Therefore, various research works are being carried out towards secure data aggregation in a wireless sensor network with different forms of approaches. However, these works have some evident advantages as well as an evident limitation, which is briefed in the next section.

3 Research problem

Irrespective of different forms of available approaches towards data aggregation in existing approaches, there are specific sets of open-end problems that are required to be addressed. Following are the identified research problems:

- *Biased Security on Layers*: Usually, an attacker intrudes or attempts to compromise the network using the routing protocol, which runs on the network layer, and its execution is carried out by the transport layer. The physical layer is the last option, where the attacker intruders. A closer look into the existing approaches of secure data aggregation shows that much work is carried out towards securing the physical layer and not the network or transport layer. Hence, existing approaches offers biased importance to the layers of operation when it comes to secure data aggregation in the wireless sensor network.
- *Improvement required in scheduling*: There are few scheduling approaches where it was proven helpful to offer security. However, they are more emphasized over data transmission, ignoring the dynamic environment and its challenging topology. An existing scheduling approach performs scheduling of data transmission. After the decision is taken, there is no second chance to look if the schedule path is compromised or about to

be compromised. Hence, stale information is included while performing a schedule.

- *Usage of complex encryption mechanism*: It is found that the existing system makes use of two forms of encryption approach. The first form of approach makes use of either a very complex encryption approach while making the system practically impossible to work in a real-time environment. The second form of approach makes use of a very simplified encryption method which can hardly withstand complex form of attack. No approach is tailored to sustain a complex and uncertain form of intrusion in the wireless sensor network.
- *Lack of Temporal approach inclusion*: The existing system has found lacking any adoption of time-based features, which is extremely important. When the existing solution of security is busy is safeguarding one node, the attack possibly takes place on other parts of the topology. The attack could happen to any node which has recently been authenticated. Hence, such authentication measures are not fruitful in case of dynamic attacks.
- *Iterative and Similar form of resource conservation plans*: Existing approaches claim to offer resource efficiency while performing security implementation, but while claiming its outcome fruitful, there is no evidence of how it reduces energy consumption. Apart from this, there is a need for a proper non-iterative method that can reduce energy consumption to a greater extent, which is also found missing in the existing literature.

Therefore, the problem statement of the proposed system will be "To develop a cost-effective non-iterative framework that can offer robust, secure data aggregation in the presence of threats of unknown nature." Developing such a solution is quite challenging as there is a need to balance resource utilization along with effective, secure data transmission concurrently. The next section discusses the proposed solution.

4 Research methodology

The prime aim of the proposed solution is to present a robust, secure data aggregation scheme for resisting any sort of lethal threat that significantly drains the energy of sensor nodes. The proposed implementation is carried out using a simplified analytical methodology where a framework is developed based on the reduced number of simulation parameters.

The prime logic of methodology is to use the enhanced scheduling mechanism integrated with the public key encryption system. The secure routing algorithm during data aggregation is designed considering adversarial node identification, clustering, distribution of key, and key updating. In this multi-tier scheme, agreement of session.

Key will be performed in Tier-1, while data transmission is carried out in Tier-2. From Fig. 1, it can be seen that the proposed system introduced various temporal parameters, which is meant for controlling the entire actions associated with data aggregation by the sensor nodes. This temporal factor also ensures uniformity in resource depletion so that it offers consistency in its performance as well as it can also have better control in secrecy. The temporal factor is the core backbone of the architecture as it is found not to be addressed in the existing system as a connection with the security breach. Therefore, the proposed modelling introduces temporal parameters like message forward allocation, which is responsible for allocating the aggregated data forwarding concerning a specific time. This parameter will offer more potential value in the analysis for investigating the effect of latency caused due to adversary. The proposed system will also formulate a new data packet that is meant for capturing temporal information concerning active and sleep time slots corresponding to the scheduling strategy. An extensive analysis is carried out considering various existing protocols in this stage of implementation. The prime focus of the implementation is basically to harness the temporal factors as the prime indicators of controls over malicious events and introduce a cost-effective encryption mechanism without much involvement of reengineering in it. The next section elaborates on the algorithm implemented.

5 Algorithm implementation

The prime intention of the proposed system is to carry out a secured transmission of the data in the wireless sensor network, considering different cases of vulnerabilities. The objective of this algorithm is to offer a higher degree of

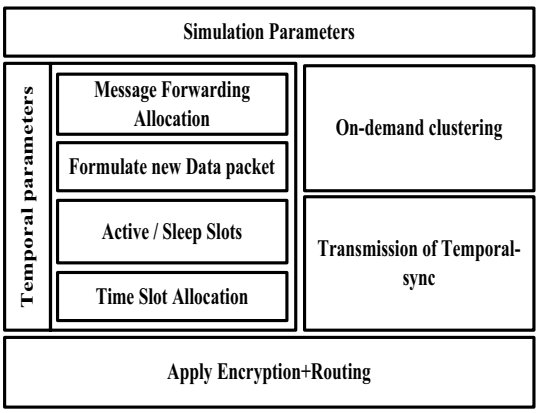

Fig. 1 Schematic architecture of the proposed system

secrecy as well as resistivity in communication. The complete operation of this algorithm is classified into two parts viz. (i) primary routing and (ii) secondary routing.

5.1 Primary routing operation

The primary routing algorithm is meant for performing data transmission in a highly accountable manner. The algorithm takes the input of n (nodes), Tr (transmission range), k (number of clusters), ts (time slots), which after execution, gives the outcome of smsg (forwarding of sync message). The steps of the operation are as follows:

Algorithm for Performing Primary Routing

Input: n, Tr, k, ts
Output: smsg
Start
1. For i=1: n
2. construct M=m ≤ Tr
3. [c p]→f1(M, h, i)
4. [sh mh]=f2(i)
5. For j=1: k
6. ID=f3(n, k)
7. ID=f4(GID = = k)
8. forward smsg
9. End
10. End
End

For all the n nodes (Line-1), the algorithm constructs an m matrix which has information about all the edges of the nodes connected (Line-2). The algorithm constructs another super-matrix M which retains all the edge information about the neighbouring nodes by shortlisting all the nodes residing closer to the transmission range Tr (Line-2). The next part of the algorithm is about applying a function f1(x), which takes the input arguments of the super matrix of adjacent nodes M and h hops from the base station to the target node (Line-3). This operation finally results in output arguments of cost c and path p (Line-3). The operation of f1(x) is about using graph theory for performing routing between the source and destination node with the shortest path based on cost. The term cost will mean all the effective resources, e.g., channel capacity, memory, energy, etc. required to carry out the target transmission. The next part of the implementation is about hops where the proposed system emphasizes on both single sh and multihop mh. The proposed system applies a function f2(x), which performs extraction of all the single hops for all the communicating nodes and constructs a multihop using the single hop information (Line-4). The proposed system also introduces a user-controlled clustering mechanism considering k number of clusters (Line-5). The algorithm then constructs a function f3(x), which is responsible for obtaining the identity ID of the clusters for the available nodes n and clusters k (Line-6). The next part of the algorithm is to construct another function f4(x) assess if the identity of group GID matches with the number of clusters k (Line-7). This operation leads to the generation of the updated identity of the nodes falling within specific clusters (Line-7). Finally, asynchronous message smsg is forwarded to all the respective nodes within a cluster. The contribution of this algorithm is (i) it generations a complete set of routing as an underlying network using graph which facilitates in data transmission, (ii) all the nodes and links are indexed, and the indexes are updating during every clustering operation. Hence, the network keeps its updated which is essential from a security viewpoint, (iii) the complete route establishment process is very simpler based on cost, and it is non-iterative at the same time which has a positive effect on the computational complexity control.

5.2 Secondary routing operation

This part of the algorithm is mainly meant for incorporating lightweight encryption towards the data transmission, considering certain temporal factor. The algorithm takes the input of n (nodes) and α (data transmission instance), which, after execution, leads to the generation of dfor (data forwarded). The steps of the algorithm are as follows:

Algorithm for Secondary Routing

Input: n, α
Output: dfor
Start
1. For i=1: n
2. α=rand (α)
3. msg→f5(msg, α)
4. For j=1: k
5. hu→find(f6(M))
6. b→b(M(hu))+msize
7. df or→forward to next-hop
8. End
End

The algorithm considers certain temporal factors α viz. (i) Data transmission duration T1, (ii) Time for forwarding synchronize message T2, (iii) Time for forwarding request and response message T3, (iv) Time to operate in sleep

mode T4, and (v) Time to forward acknowledgment T5. The complete operation of this algorithm is to associate the temporal factors with the active (T2, T3) and passive mode of operation (T4, T5). The computation of the active period is determined by multiplying the probability of successful data transmission with the size of the frame. The algorithm randomly initializes the temporal factors α (Line-2) with respect to timeslot ts. The next part of the algorithm is to construct a function f5(x), which is responsible for carrying out encryption over message msg with respect to the temporal factor α (Line-3). This operation leads to the generation of ciphered message msg. Considering all clusters k, the algorithm finds a prioritized message from M using a function f6(x), which leads to the exploration of the high urgency hu message (Line-5). The buffer b is then increased, considering the size of message size (Line-6), which leads to forward the data dfor to the next hop. Hence, the algorithm cost-effectively forwards the encrypted data with higher scalability towards addressing safer communication in a wireless sensor network in many resources and efficient manner. The next section discusses the results being obtained from the proposed study.

6 Result analysis

This section discusses the outcome obtained after implementing the proposed algorithm. Referring to the discussion carried out by Gaikwad and Dhage [30], it is stated that there are two forms of secure data aggregator model, i.e., single aggregator (E1) and multiple aggregators (E2). Hence, the proposed system (P1) is compared with existing aggregator model where the assessment is carried out considering a combination of three different frequently used security protocol, i.e., Rivest-Shamir Algorithm (S1) [31], Advanced Encryption Standard (S2) [32], Secured and Efficient Authentication (S3) [33]. The brief of justification are as follows:

(i) *Justification behind Adoption of S1, S2, and S3.*

Referring to IEEE Xplore, it is seen that there are 156 conference paper, 23 journals published discussing the adoption of S1 in sensory application. The significance of S1 is that it offers simplified sharing of public key and it uses factorized prime numbers that is quite challenging to crack. On the other hand, adoptions of S2 are found in 1167 conference and 179 journals as it supports security with hardware acceleration. Similarly, S3 algorithm is found to be cited by 143 researchers till date in last 5 years. This algorithm uses certificate based DTLS handshaking mechanism which is claimed to be better than conventional handshaking mechanism using public keys to support IoT application. All this usage statistics evidently shows that S1, S2, and S3 are frequently adopted encryption approaches owing to their simplified implementation of secure routing in WSN.

(ii) *Justification behind Adoption of E1 and E2.*

The discussion carried out in [31] evidently shows that single and multiple aggregators are the two existing approaches for secure data aggregations scheme. The paper has discussed cases of both the schemes which proved that majority of the existing secure data aggregation till date in current times fall in these categories. Therefore, proposed system is chosen to be compared with these existing approaches.

The analysis has been carried out considering 500–1000 sensor nodes with 10 J of energy and simulated over 1000 rounds of operation with 2000 bytes of data considered for transmission. The simulation area is considered to be $1000 \times 1000 m^2$.

The outcome in Figs. 2 and 3 shows that the proposed system (P1) performs well with the S3 security scheme and not much with S1 and S2. It is because the S3 scheme entails better supportability towards the distributed environment, which cannot be offered by S1 and S2; therefore, better energy savings are observed. However, S3 approach claims of 26% of overhead reduction by its inherent nature but S1 adoption offers higher energy depletion owing to maximized memory saturation within the node owing to larger key size. S2 algorithm is not recommended as similar encryption is applied on all the blocks. On the other hand, the E2 scheme performs better than the E1 scheme owing to the reduced size of the key for E2 compared to the E1 scheme. Hence, the proposed system offers reduced variable dependencies and faster operation, which also contributes to energy saving in comparison to the existing system of E1 and E2.

Figure 4 highlights the delay performance, which again shows similar trends of proposed system P1 when using the S1 security protocol. However, a closer look will show that the E2 scheme using the S3 security protocol doesn't offer a better solution toward controlling delay. It is because a proposed scheme uses a tree mechanism where the updating policy is taken care of by the shared memory system of the sensor, causing faster data transmission. The routing protocols developed in the proposed system make use of temporal factors which retains maximum consistency for almost all the routing operation involved in data aggregation. Therefore, the proposed system has better control of the time of operation, which is very important to control dynamic threats. Processing time performance can be seen in Fig. 5, which exhibits that the proposed system offers reduced computational complexity when working with an S3 security scheme. Apart from this, S2 approach

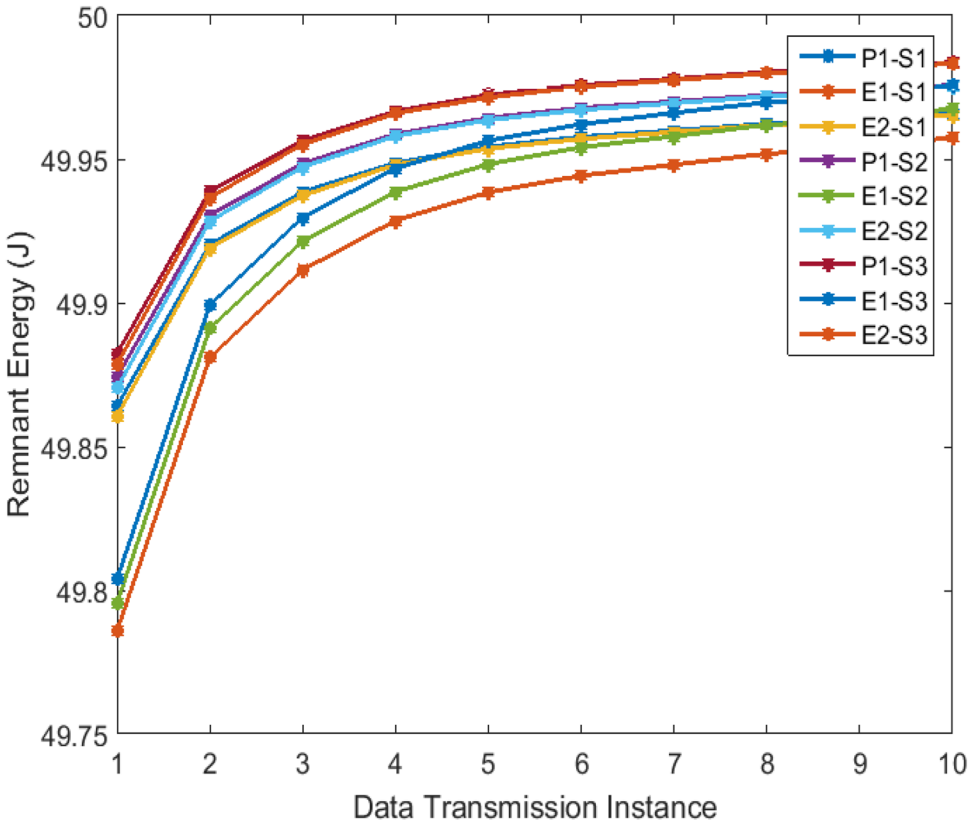

Fig. 2 Comparative analysis of remnant energy

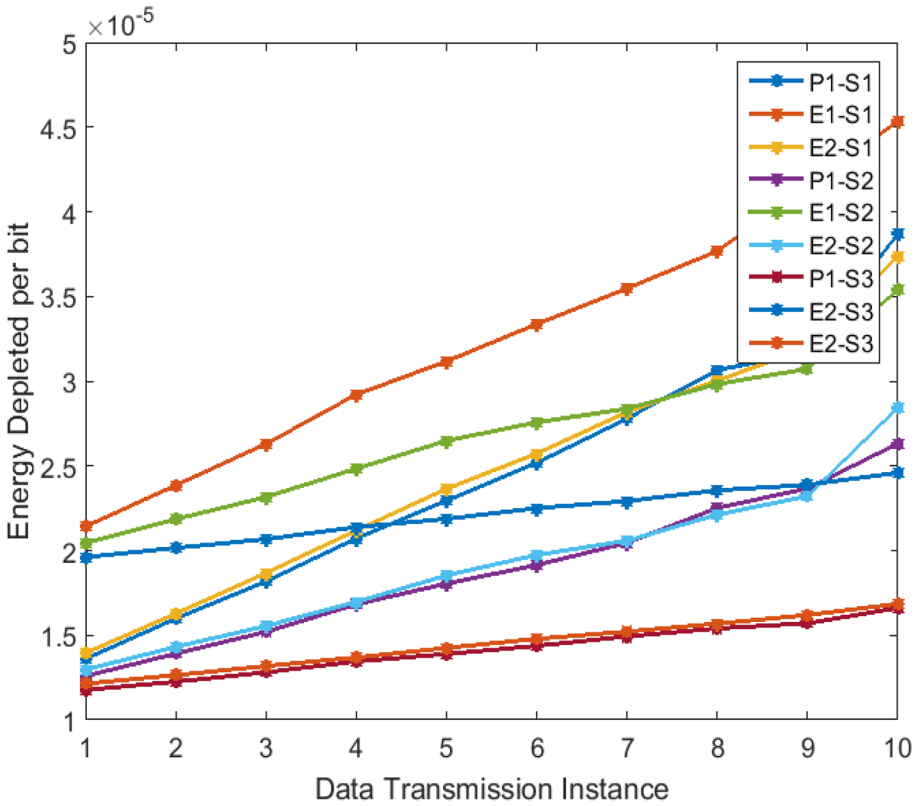

Fig. 3 Comparative analysis of energy depleted per bits

makes use of counter mode of operation during encryption which is reported to be too complicated and hence they will significantly degrade the security performance in WSN. Hence, existing approaches has different security effects.

Apart from this, the proposed system successfully performs data aggregation in the presence of uncertain attackers in the most secure way, unlike E1 and E2 scheme. It is, therefore, resistive against any key-based attack and jamming attack, mainly in the presence of a dense traffic environment. It also offers faster and effective verification with a reliable mechanism of authentication and data integrity.

Hence, without using many sophisticated entities, the proposed system provides a much better form of secure data aggregation scheme in contrast to the existing system. It is also computational cost-effective in its operation, and hence its scope in the application is more practical.

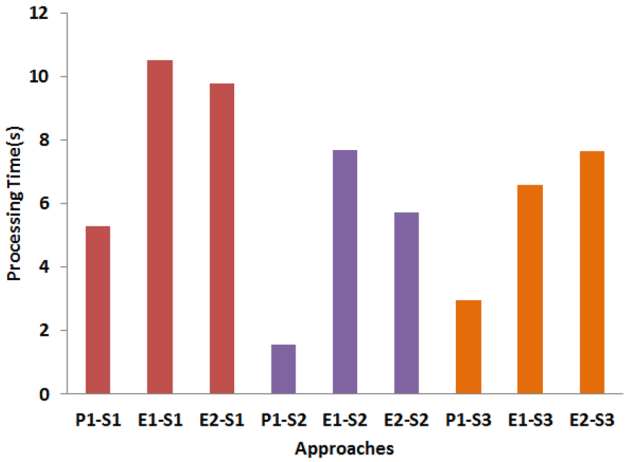

Fig. 5 Comparative analysis of processing time

7 Conclusion

Security has always been a more significant concern in a wireless sensor network. With the involvement of wireless sensor networks in upcoming technologies, i.e., Internet-of-Things, there is a need to emphasize secure data aggregation. This paper has presented a novel mechanism for resisting the threats and cost-effectively performing secure data aggregation.

The benefits of the proposed system are as follow: (i) the proposed system adopts light-weight encryption approach, (ii) a significant energy saving is offered in proposed system, (iii) it offers resistance towards jamming and resistance attack. Following are the scientific contribution of the proposed system: (i) the proposed system introduces the usage of 5 temporal factors unlike any existing approach to ensure round the clock security while the security operation is at progress, (ii) As all these temporal factors can be directly extracted from routing table, the proposed system is free of any computation towards this.

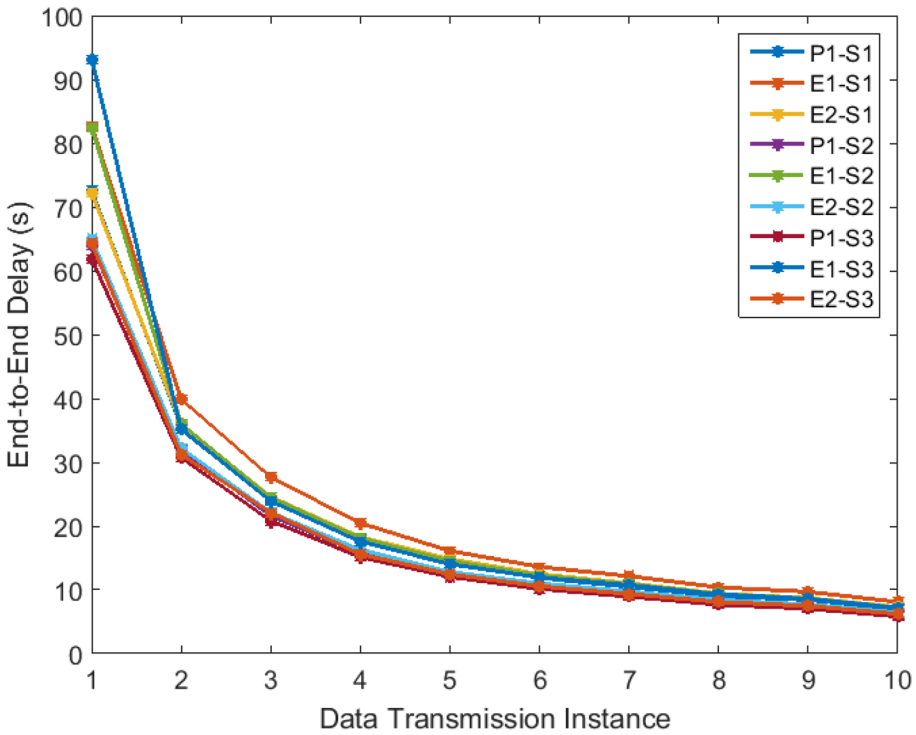

Fig. 4 Comparative analysis of end-to-end delay

Hence, no extra resources are consumed in this way, (iii) the proposed system offers a higher degree of flexibility towards getting itself integrated with multiple encryption schemes depending upon any futuristic application of sensory data, (iv) another essential contribution is that proposed system maintains a higher degree of consistency in the entire cycle of data aggregation which ensures maximum monitoring of pattern and its abnormality to identify an attack. Hence, attack identification becomes faster as well as easier in the proposed system, and deploying a cost-effective solution further makes it sustainable towards thwarting threats. The simulation results of the proposed system is that it offers 56% of saving of energy, 45% faster processing compared to existing secure data aggregation scheme, and proposed study also minimizes end-to-end delay by 47%. Our future work will be towards extending the current model for testifying its applicability over reconfigurable networks.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Rakavi A, Manikandan MSK, Hariharan K (2015) Grid based mobile sensor node deployment for improving area coverage in Wireless Sensor Networks. In: Proceeding of the 3rd international conference on signal processing, communication and networking (ICSCN), Chennai, 2015, pp 1–5
2. Zhan G, Shi W, Deng J (2009) SensorTrust: a resilient trust model for WSNs. In: Proceedings of the 7th ACM conference on embedded networked sensor systems, pp 411–412.
3. Li L, Li J (2011) Research of compressed sensing theory in WSN data fusion. Fourth international symposium on computational intelligence and design, Hangzhou 2011:125–128
4. Akila V, Sheela T (2017) Preserving data and key privacy in data aggregation for wireless sensor networks. In: Proceedings of the 2nd international conference on computing and communications technologies (ICCCT), Chennai, 2017, pp 282–287
5. Patil B, Kadam R (2018) A novel approach to secure routing protocols in WSN. In: Proceedings of the 2nd international conference on inventive systems and control (ICISC), Coimbatore, 2018, pp 1094–1097
6. Zin SM, Anuar NB, Kiah MLM, Pathan ASK (2014) Routing protocol design for secure WSN: review and open research issues. J Netw Comput Appl 41:517–530
7. Gulhane G, Mahajan NV (2014) Securing multipath routing protocol using authentication approach for wireless sensor network. In: Fourth international conference on communication systems and network technologies, Bhopal, pp 729–733.
8. Frej MBH, Elleithy K (2015) Secure data aggregation model (SDAM) in wireless sensor networks. In: IEEE 14th international conference on machine learning and applications (ICMLA), Miami, FL, 2015, pp 330–334.
9. Thompson SA, Samanthula BK (2017) Optimized secure data aggregation in wireless sensor networks. In: Proceedings of the 15th annual conference on privacy, security and trust (PST), Calgary, AB, pp 394–3942.
10. Guo H, Yang Z, Zhang L, Zhu J, Zou Y (2017) Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks. IEEE Access 5:19620–19630
11. Wang K, Yuan L, Miyazaki T, Zeng D, Guo S, Sun Y (2017) Strategic antieavesdropping game for physical layer security in wireless cooperative networks. IEEE Trans Veh Technol 66(10):9448–9457
12. Tian F et al (2018) Secrecy rate optimization in wireless multihop full duplex networks. IEEE Access 6:5695–5704
13. Huang H, Gong T, Zhang R, Yang L, Zhang J, Xiao F (2018) Intrusion detection based on k-coverage in mobile sensor networks with empowered intruders. IEEE Trans Veh Technol 67(12):12109–12123
14. Deng Y, Wang L, Elkashlan M, Nallanathan A, Mallik RK (2016) Physical layer security in three-tier wireless sensor networks: a stochastic geometry approach. IEEE Trans Inf Forensics Secur 11(6):1128–1138
15. Zhu J, Zou Y, Zheng B (2017) Physical-layer security and reliability challenges for industrial wireless sensor networks. IEEE Access 5:5313–5320
16. Liu Y, Dong M, Ota K, Liu A (2016) ActiveTrust: secure and trustable routing in wireless sensor networks. IEEE Trans Inf Forensics Secur 11(9):2013–2027
17. Kim D, An S (2016) PKC-based DoS attacks-resistant scheme in wireless sensor networks. IEEE Sens J 16(8):2217–2218
18. Kong Y, Lyu B, Chen F, Yang Z (2018) The security network coding system with physical layer key generation in two-way relay networks. IEEE Access 6:40673–40681
19. Wang H, Xu L, Lin W, Xiao P, Wen R (2019) Physical layer security performance of wireless mobile sensor networks in smart city. IEEE Access 7:15436–15443
20. Zhang Z, Zhu H, Luo S, Xin Y, Liu X (2017) Intrusion detection based on state context and hierarchical trust in wireless sensor networks. IEEE Access 5:12088–12102
21. Porambage P, Braeken A, Schmitt C, Gurtov A, Ylianttila M, Stiller B (2015) Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications. IEEE Access 3:1503–1511
22. Moara-Nkwe K, Shi Q, Lee GM, Eiza MH (2018) A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. IEEE Access 6:11374–11387
23. Dautov R, Tsouri GR (2016) Securing while sampling in wireless body area networks with application to electrocardiography. IEEE J Biomed Health Inf 20(1):135–142
24. Biswas K, Muthukkumarasamy V, Singh K (2015) An encryption scheme using chaotic map and genetic operations for wireless sensor networks. IEEE Sens J 15(5):2801–2809
25. Zou Y, Wang G (2016) Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. IEEE Trans Ind Inf 12(2):780–787
26. Lee J, Kim L, Kwon T (2016) FlexiCast: energy-efficient software integrity checks to build secure industrial wireless active sensor networks. IEEE Trans Ind Inf 12(1):6–14
27. Wu J, Ota K, Dong M, Li C (2016) A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. IEEE Access 4:416–424
28. Tayebi A, Berber S, Swain A (2018) Security enhancement of fix chaotic-DSSS in WSNs. IEEE Commun Lett 22(4):816–819
29. Zhang Z, Wu W, Yuan J, Du D (2018) Breach-free sleep-wakeup scheduling for barrier coverage with heterogeneous wireless sensors. IEEE/ACM Trans Netw 26(5):2404–2413
30. Gaikwad PB, Dhage MR (2015) Survey on secure data aggregation in wireless sensor networks. In: International conference

on computing communication control and automation, pp 242–246. IEEE.
31. Bahi JM, Guyeux C, Makhoul A (2010) Secure data aggregation in wireless sensor networks: homomorphism versus watermarking approach. International conference on ad hoc networks. Springer, Berlin, pp 344–358
32. Ozdemir S, Xiao Y (2009) Secure data aggregation in wireless sensor networks: a comprehensive overview. Comput Netw 53(12):2022–2037
33. Moosavi SR, Gia TN, Rahmani A-M, Nigussie E (2015) SEA: a secured and efficient authentication and authorization architecture for IoT-based healthcare using smart gateway. Elsevier-Proced Comput Sci 52:452–459
34. Anguraj DK, Smys S (2019) Trust-based intrusion detection and clustering approach for wireless body area networks. Wirel Pers Commun 104(1):1–20