International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Efficient Temporal-key Based Encryption Mechanism for WSN-ETEM

Premakumar MN, Ramesh S

Abstract: ***Wireless sensor networks (WSNs) are a promising technology for several industrial real-time and quotidian applications. Due to inherent limitations in WSN, security is a crucial issue. Cryptographic primitives are the fundamental components for designing security protocols to achieve security and privacy in WSN. Based on the review, it has been analyzed that the majority of security protocols for WSN are based on encryption and key distribution. The main open issue for these approaches concerns the establishment of security with an involvement of complex procedure, which presents considerable memory overheads, in contrast with the limited resources of sensor nodes. Therefore, the proposed work presents the modeling of an analytical approach for efficient encryption using temporal key management for robust security services to resists potential attacks and enables secure communication. The utilization of temporal-key mechanism in encryption operation offers additional support to routing operation in the network for secure data transmission with negligible computational overhead, thus preserving a higher level of energy savings in packet transmission operation. The validation of the proposed system performance is carried out a simulation study, which shows the effectiveness of the proposed system in terms of node remaining energy and processing time.***

Keywords: WSN, Security, Authentication, Encryption, Key distribution, routing, sensors

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are a collection of inexpensive micro sensor devices that are typically deployed in surveillance areas. These micro sensor devices have the inherent features of an ad hoc function that communicates over a radio channel, designed to sense events, collect information, and pass collected information to the user via a local repository center called the base station-(BS) [1-2]. As an emerging technology, WSN has practical value and has become a backbone for various applications and has gained global attention in many organizations. The sensor devices or nodes in the distribution area can get a lot of detailed and reliable information for various applications such as military, automobile industry, agriculture, urban management, security surveillance, biomedical, environmental monitoring, disaster relief, smart home, smart healthcare, and so on[3]. However, WSN is mainly organized in harsh surroundings where human intervention is quite difficult. There is a real challenging factor associated with the sensor nodes as it belongs to resource constraints nature such as energy, bandwidth, computing potential, and storage volume are limited, making WSN vulnerable [4]. The security of WSN has caused widespread social concern. Especially in critical applications like military target detection, healthcare for which information is very sensitive, and once WSN is attacked, and then it can lead to catastrophic consequences. Therefore, a robust, efficient security protocol is required in WSN to attain confidentiality protection and authentication functions to enable a fairly safe environment for node communication and data transmission against malicious activity [5-6]. Therefore, the challenges associated with WSN security have become a key issue in the research field. Over the past few years, a lot of research has been done on security aspects of WSN to provide reliable communication and data sharing operations. Unfortunately, many traditional security techniques are not feasible and are not suitable to be implemented in WSNs with resource deficient nodes as they are associated with high computational complexity [7-8]. Therefore, the major challenge in WSN security is the trade-off between energy use reduction and security enhancement [9]. As WSN is nowadays adopted in various realtime and delay-sensitive applications, it is necessary to promote security features about hybrid approaches with high energy efficiency as different types of information exchange processes occur in WSNs and have different security needs [10]. Therefore a single security mechanism cannot meet these requirements. Therefore, the proposed research work offers a novel security approach formulated using an encryption mechanism and temporal key management scheme. Thereby the proposed schemes enable less-complexity based robust security implementation mechanism that can restrict the adverse impact of security threats and various types of attacks and meets the higher energy-efficiency requirements by supporting user demand clustering operation during routing process for the data transmission. Finally, the performance validation of the proposed methodology is analyzed regarding the remaining energy and processing time. The remainders of this paper are ordered as follows: Section-II is carried review of existing literature. Section-III illustrates research problem based on the review study. Section IV discusses proposed design. Section-V presents algorithm as operational strategy for implementing proposed methodology. Section VI presents result and discussion. Finally the conclusion is presented in Section VII.

Revised Manuscript Received on March 30, 2020.
***** Correspondence Author
Premakumar MN*, Research Scholar, Department Electronics & Communication, Dr. AIT, Bengaluru, Karnataka, India. Email: premakumar1976feb@gmail.com
Dr. Ramesh S**, Professor and Head, Department of Electronics & Communication Engineering, Dr. AIT, Bengaluru, Karnataka, India

II. LITERATURE SURVEY

Enormous security approaches based on Key distribution and encryption techniques in WSNs have been presented in the existing research literatures. This section provides a brief review of various existing schemes to analyses its effectiveness and drawbacks to support further researches in the field of WSN security. A security approach based on key negotiation routine is introduced by the work of Gandino et al. [11] to address the weakness of existing transitory master-key management, which is vulnerable to node compromise attacks during its initialization phase. The presented approach uses a key calculation mechanism which minimizes the time needed for the initialization phase by splitting it into hierarchical subphases with an additional level of security. The work done by Choi et al. [12] offered a location-oriented key management scheme where the authors have established a key update and revocation operation, incorporating grid information to resist insider attackers effectively. Another similar study considering location-oriented key management mechanism is conducted in the study of Fakhrey et al. [13] and [14], where an event-related report is associated with multi-layer security. Also, the authors have constructed a key revocation mechanism for both compromised nodes to overcome the possibility of an attack. Research work in the direction of addressing huge computational complexity introduced by random pre-deployment secret keys is carried out in the study of Gandino et al. [15]. In this, the q-composite scheme is applied to explore the effective features of random key predeployment to improve it with lower complexity demand. Ding et al. [16] considered all essential attributes and characteristics of the network as a graph and introduced a graph-based approach for designing key pre-deployment strategies to bring better security and connectivity among constraint devices in the network. Qi et al. [17] offered an adaptive power control mechanism using a rule-based strategy to extend the node service duration for a solar-powered WSN node. The energy control strategies designed considering battery deprivation, where Poisson distribution is used to simulate the energy utilization variation by each sensor node. The work in the direction of securing sensitive data exchange and overhead caused by an excessive rekeying factor in resource constraint sensor network is presented by Mughal et al. [18]. In this, a group communication environment is considered where communication establishes in the form of logical trees for every group. Therefore, the authors have presented a logical tree-based robust mobility control strategy. The work of Nkwe et al. [19] discussed the challenges associated with physical layer security management using a key generation based approach. After which the study has introduced different key generation methods based on power and error-correcting codes, which enables a mechanism for generating keys by reading received signal strength-(RSS) value. Xu et al. [20] presented a search based lightweight approach for establishing a public-key encryption technique for cloud-integrated WSN. The outcome demonstrates that the presented approach provides a time-efficient mechanism for generation chipper text to provide energy efficiency and a secure communication environment.

Chu et al. [21] presented a memory-efficient authentication mechanism for WSN. Rather than using a traditional approach using the hash function, the presented approach with an interesting aspect data protection uses Arithmetical operation with a less computational cost, which is integrated with hardware architecture based on Altera DE2 board and FPGA. Yi et al. [22] offered a block encryption security mechanism to ensure the basic security requirements for sensor networks. Here, the presented security approach utilizes the concept of a chaotic substitution box with limited computation to ensure energy efficiency. Shim et al. [23] carried a survey work on public-key cryptographic primitives based security mechanisms for WSN. The authors here discussed the valuable function of cryptographic primitives and highlighted some existing research issues regarding time, power utilization, and resource occupation on constrained sensor devices. The presented survey study offers valuable insights into aspects of WSN security and energy efficiency. Oliveira et al. [24] suggested an admission control mechanism with the AES symmetric algorithm in WSN that prevents true nodes communication from malicious nodes. This approach uses a filtering mechanism for eliminating malicious node and RPL protocol that reduces additional control messages. Alghamdi et al. [25] suggested a secure and energy-efficient scheme using Dij-Huff Method based optimization is an approach for WSN. Gope et al. [26] studied the existing techniques in WSN for enabling anonymous user authentication. The study provides an efficient authentication mechanism for user anonymity, untraceability, and reliable communication. Chen et al. [27] introduced a hybrid approach using comprehensive sensing technique and watermarking based reconstruction engine IoT gateway nodes. Independent of key synchronization, this approach can resist only ciphertext attacks and plaintext attacks.

III. RESEARCH PROBLEM

- Many existing schemes are not suitable to deal with different types of attack. Hence, if one node is compromised then whole networking system may suffer.
- The existing techniques designed on complex mechanism to provide advance security mechanism most of the time introduces computational complexity which is not suitable for constrained environment.
- Dynamic parameters used to build security methods have not received widespread attention in existing literatures
- The selection of simulation tools for performance assessment is also a significant concern that should be considered by researchers. The performance validation of proposed system with another existing system which is implemented in different computing tool and technique can never give accurate results.

IV. PROPOSED SYSTEM

The proposed research work presents a scheme based on an efficient encryption mechanism using temporal key management that brings robust security services to resists potential attacks and enables a secure environment for performing data transmission and communication in WSN. The design of the proposed scheme is formulated using an analytical approach considering network dynamicity and resource constraints of WSN nodes. The overall design of the proposed system is carried out in a sequential phase implementation module.

The architecture of the proposed system is illustrated in fig.1

The proposed security design consists of two core modules i.e., communication module and security module. The communication module contains the process of network deployment and energy-aware clustering operation in the deployment network. The second core module of the proposed system is responsible for establishing a security mechanism based on robust encryption using temporal key management operation. The utilization of temporal-key mechanism in encryption operation offers additional support to routing operation in the network for secure data transmission, and that can deal with different forms of security threats and potential attacks.

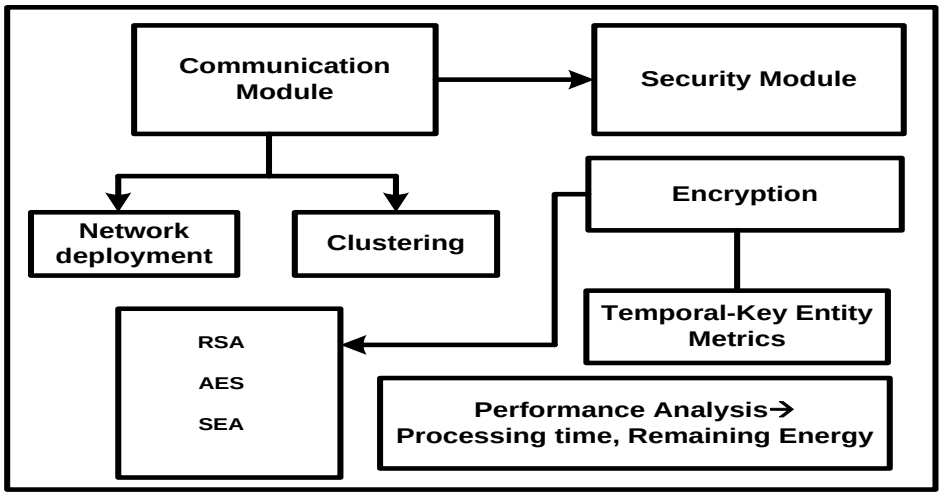

Fig.1 Proposed System Architecture

The communication module is the initial phase of the proposed system, where network deployment is established under the uniform random placement of sensor nodes. Further, the proposed system considers the localization of Base Station-(BS) anywhere in or around the deployment region. The initial procedure of the proposed system is carried out in a sequential manner that it accomplishes the opening level of security necessities, which are needed for the next implementation phase of energy-aware clustering and encryption-based security operation. Therefore, the proposed initial network deployment mechanism retains the accountability of the sensor and its positional information through the network in order to execute a higher strength of security and efficient routing operation. Therefore, the system applies the algorithm in a manner in which each node learns other sensors related information by maintaining an updated hop table and helps the sensor node to establish an optimal path concerning the source node and the target node in the routing decision process. The proposed system considers the necessity of data aggregation in WSN and designs an efficient and energy-saving clustering mechanism, which retains a significant level of security concerns. The proposed system introduces the formation of on-demand clusters, which means that the development of clusters in the network relies on the needs of users/applications, and the clusters have the lowest level, so that they can be short-listed before making a routing and provides higher coverage structure from source to destination. Therefore, as the system develops a limited cluster as required, it also limits the access of the attacker. The design of a security model is established in a multi-layer encryption policy to deal with different types of security vulnerabilities and attacking scenarios in large-scale WSN during path establishment and node communication process. In this module, temporal key-management, including multiple attributes are considered, such as active session node-(ASN), passive session node-(PSN), Sync-time-(SYT), and packet priority level-(PPL). All of these attributes are dynamic because they change over time. Finally, after all of these entities have been processed, the algorithm will generate the final encrypted information. Therefore, the operational design of the encryption mechanism is performed in a manner that is less dependent on the temporary key factor. Therefore, it is robust as well as flexible for any form of encryption strategy. Also, the encryption policy-(RSA, AES, and SEA) is defined based on the msg priority, so each packet is encrypted, and the system ensures its confidentiality and integrity. Another benefit is its robustness to different forms of attacks that often occur in large-scale WSNs. This also brings negligible computational overhead, thus preserving a higher level of energy savings in communication and packet transmission operation. The next section presents algorithm description of introduced security implementations where the contribution of the proposed system can be effectively visualized as it offers both energy efficiency and secure environment to perform data transmission and communication operation without affecting overall network performances.

V. ALGORITHM DESCRIPTION

This section presents an algorithm description of the proposed system for network deployment and temporal key-enabled encryption mechanisms. The significant steps involved in algorithm design as follows:

Algorithm-1: Node Placement and Cluster Formation

This part of algorithm is responsible for establishing preliminary part of the security implementation where the system considers input variable as N-(Number of Nodes), A_d-(deployment area), B_S (Base station) and Radius-(R).

Input: N, A_d, B_S, R
Output: Link establishment-(L_E) and cluster Id-($C_{R\text{-}Id}$)
Start
Step-1: $N \rightarrow f_{rand}(x_i. y_i) < A_d$
Step-2: $B_S \rightarrow (x_i. y_i) > A_d$
Step-3: Compute: $d \rightarrow N_a, N_b$
Step-4: for $i = 1: N$
Step-5: Estimate Cov $\rightarrow N_N$
Step-6: Compute $L \rightarrow \sum^N_R$ *such that* $|\vec{d}| \leq R$
Step-7: $L_E \rightarrow [L]$
Step-8: Init C_R (number of clusters required)
Step-9: for i → 1: N
Step10: Compute $H_{info} \rightarrow N_N$
Step 11: Construct → $H2_M$, If $H_M \neq N+1$
Step 12: end
Step 13: $C_{R\text{-}Id} \rightarrow f_{rand}$ (1-1*(N/ C_R))+1, (i*(N/ C_R))
End

The above-presented algorithm initially takes input for executing the initial process of network deployment, where it considers a set of sensors nodes-(N), a base station (BS), and area (Ad). The first step of the algorithm is subjected to the placement of the node with respect to coordinate metric in a random manner using f_{rand} under-considered simulation area-(step-1). Further, the system performs its next step of localizing BS just outside the simulation area of network-(step-2). The next step of the algorithm computes the distance between the nearby nodes where the system initially stores the spatial coordinates of each node in the networks (NN) in a matrix-(S). This process assists the algorithm to estimate distance among the nodes (N)-(Step-3). The next step associated with the computation of coverage-(*Cov*) of every node in the network-(NN) - (step-5) to further compute the possible links (l) related to single node-(N) using condition stated in step 6. In addition, a functional routing operation is merged between the links established to enable the optimal path among all nodes in the network-(N_N) and the BS-(step7). The system here also maintains a matrix with respect to path formation considering location information of each node and BS. The next step of the proposed algorithm is subjected to an estimate specific number of cluster formation. The algorithm initializes variables for a number of clusters required-(CR) to perform secure data transmission (Step-8). The qualified cluster and its associated sensor nodes will be listed, which provides a valid path for the routing, ultimately optimizing data aggregation performance. The formation of clusters entirely a matrix-based operation in which information of route structure, hop, and node-id (id) is considered. Using this information, the algorithm can implement any encryption policy considered in the proposed system depending upon the complexity of the route formation. In order to estimate a possible number of clusters, the algorithm initially takes information-(Hinfo) about single-hop-(H1), which is maintained in all sensor nodes and stored into a matrix HM-(step10). If the size of the HM is found greater than the algorithm presents the computation of another matrix with multi-hop entity-(H2m) in step-11. Further, the next process of algorithm is executed to produce id of the cluster-(CR-Id) using random function frand with various levels of computation-(step13). Thus, the algorithm generates clusters for energy-efficient and secure routing operation, which aids an additional security mechanism in support of security based on the encryption technique. The next algorithm description is presented for implementing a security module using a temporal key-based encryption scheme. The significant steps involved in the algorithm are as follows:

Algorithm-2 Encryption using temporal-key

The proposed system adopts a simplified algorithm implementation, so that the resource constraint nodes of WSN cannot suffer with high computational complexity. The algorithm takes input in the form of Time instance for active session node-(ASN_I), passive session node-(PSN_I), time instance of information arrival-(I_{T1}), Sync-time-(SYT), RREQ/RREP pkt exchange-(Pexc) time instance for route acknowledgement-(RTack) and packet priority level-(PPL).
Input: ASN, PSN, SYT, PPL, Pexc, $Rack_I$, PPL
Output: E_{info}
Start
Step1: Init → ASN, PSN, PPL, PPL, I_{T1}
Step2: Compute: → *[*SYT, Pexc, $Rack_I$]
Step3: if card: imp(pkct) → **(**I_{T1}*PPL)/100
Step4: Get $I_{T1specifc}$ → P_i Flag (I_{T1}, PPL-pckt)
Step5: E_{info} ← Encyp(Pckt, PPL)
Step6: update:→ msg(E_{info})
End

The above mention algorithm is accountable for ensuring communication security between two different sensor nodes based on different temporal key oriented attributes. Algorithm execution mainly considers all types of information associated with both active modes and passive modes of communication (step-1, step-2). In this phase, the random pattern of data generation indicates the situation of different types of packets arrival, and when a time instance is involved, a particular form of packet nonlinearity can also be seen. Based on the time-oriented analysis, the proposed system introduces temporal factors with the rapid dissemination of information across all nodes reduces the likelihood of packet-information being compromised by a malicious user. For this, the cardinality of high-priority messages is computed in relation to the time instance information arrival-(IT1) (step-3). The next step also calculates the specific time instance of the data arrival with the flag value (step-4). Further, the encryption operation prioritizes data packets with precedence and time instances for packets waiting in the queue using three different types of encryption strategies and merges their operational aspects with the proposed conceptual security model (step-5, step6). Finally, performance analysis is carried out to ensure the efficiency and stability of the proposed algorithm. The next section presents the numerical performance analysis to validate the scope and effectiveness of the proposed system. The assessment of proposed system performance is carried out with different performance metrics such as remaining energy and processing time.

VI. RESULTS AND DISCUSSION

This section explores the effectiveness of the proposed system in terms of scalability under different encryption strategies. The proposed study also performs comparative analysis with existing system-(SecLEACH [28]) and LS-LEACH [29]) to justify its scope in terms of energy efficiency and robustness.

The design implementation of the entire model is performed on the numerical computing tool installed on windows 10. The simulation parameters for the experimental task are demonstrated in table1.

Table.1Simulation Parameters

Parameters	Values
Nodes	200
Area	10x10
BS	1
ASN	0.2
F_{Size}-(FrameSize)	1
ASN_I	(F_{Size} * ASN)
PSN_I	(1- ASN)* F_{Size}
SYT	20%-35 %
Pexc	80%-90%
$Rack_I$	20%-35%

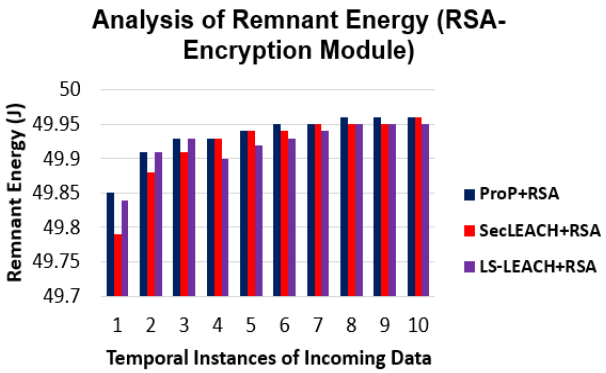

Fig.2 Analysis of Remnant energy with proposed RSA encryption policy

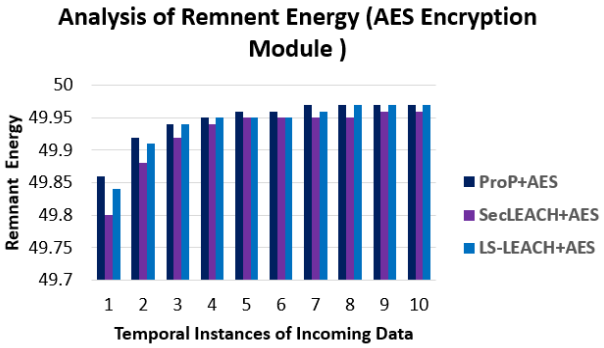

Fig.3 Analysis of Remnant energy with proposed AES encryption policy

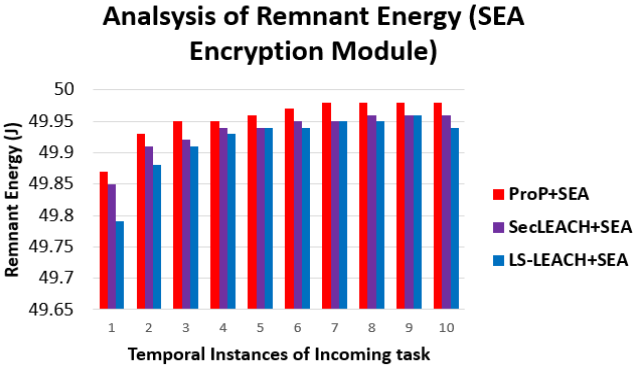

Fig.4 Analysis of Remnant energy with proposed SEA encryption policy

The comparative analysis from fig.2, fig.3, and fig.4 shows the effective outcome of energy efficiency when three different encryption policies i.e., RSA, AES, and SEA are applied over three different security protocols. It clearly shows that the amount of remaining energy in the case of the proposed system achieves better performance compared to the existing system.

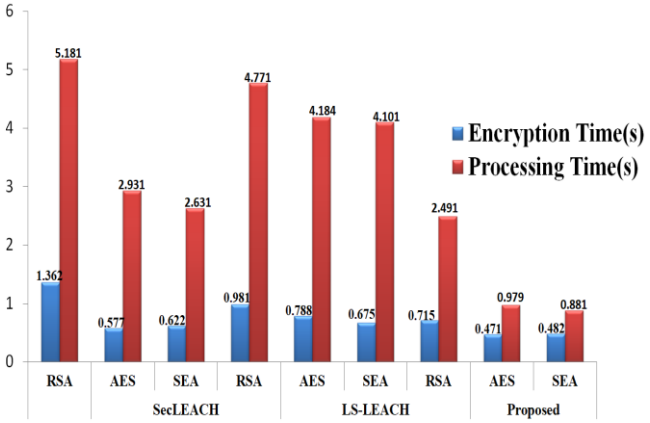

Fig.5 Comparative Analysis in terms of time (sec)

Fig.5 demonstrates the effectiveness of the proposed system in terms of processing time when compared to existing techniques with a combination of three different encryption strategies. The prime factor behind this is that the introduced system is not based on an iterative process to execute routing operation, and considering the temporal key management, it involves less computational complexity.

VII. CONCLUSION

This paper proposed modeling of novel energy-aware secure communication strategy for large-scale WSN by considering a novel temporal-key management with an encryption mechanism. The design is fully analytical and introduces three different modes of the encryption operation. Finally, extensive analysis with performance assessment is carried on a numerical tool that exhibits the effectiveness of the proposed system regarding better energy-saving and efficient services compared to existing systems.

REFERENCES

1. Carlos-Mancilla, Miriam, Ernesto López-Mellado, and Mario Siller. "Wireless sensor networks formation: approaches and techniques." Journal of Sensors 2016 (2016).
2. Fraternali, Francesco. "Towards Large-Scale Autonomous Wireless Sensor Networks." arXiv preprint arXiv:1906.12001 (2019).
3. Ali, Ahmad, Yu Ming, Sagnik Chakraborty, and Saima Iram. "A comprehensive survey on real-time applications of WSN." Future internet 9, no. 4 (2017): 77.
4. Yarbrough, Brian, and Neal Wagner. "Assessing security risk for wireless sensor networks under cyber attack." In Proceedings of the Annual Simulation Symposium, p. 1. Society for Computer Simulation International, 2018.
5. Dener, Murat. (2014). Security Analysis in Wireless Sensor Networks. International Journal of Distributed Sensor Networks. 2014. 10.1155/2014/303501.
6. Grover, Jitender & Sharma, Shikha. (2016). Security issues in Wireless Sensor Network — A review. 397-404. 10.1109/ICRITO.2016.7784988.
7. Sharma, Gaurav, Suman Bala, and Anil K. Verma. "Security frameworks for wireless sensor networks-review." Procedia Technology 6 (2012): 978-987.

8. Alotaibi, Majid. "Security to wireless sensor networks against malicious attacks using Hamming residue method." EURASIP Journal on Wireless Communications and Networking 2019, no. 1 (2019): 8.
9. Modares, Hero, Rosli Salleh, and Amirhossein Moravejosharieh. "Overview of security issues in wireless sensor networks." In 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, pp. 308-311. IEEE, 2011.
10. Kifayat, Kashif & Merabti, Madjid & Shi, Qi & Llewellyn-Jones, David. (2010). Security in Wireless Sensor Networks. 10.1007/978-3-642-04117-4_26.
11. F. Gandino, R. Ferrero, B. Montrucchio and M. Rebaudengo, "Fast Hierarchical Key Management Scheme With Transitory Master Key for Wireless Sensor Networks," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1334-1345, Dec. 2016.
12. J. Choi, J. Bang, L. Kim, M. Ahn and T. Kwon, "Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks," in *IEEE Systems Journal*, vol. 11, no. 2, pp. 494-502, June 2017.
13. H. Fakhrey, M. Johnston, F. Angelini and R. Tiwari, "The Optimum Design of Location-Dependent Key Management Protocol for a Multiple Sink WSN Using a Random Selected Cell Reporter," in *IEEE Sensors Journal*, vol. 18, no. 24, pp. 10163-10173, 15 Dec.15, 2018.
14. H. Fakhrey, R. Tiwari, M. Johnston and Y. A. Al-Mathehaji, "The Optimum Design of Location-Dependent Key Management Protocol for a WSN With a Random Selected Cell Reporter," in *IEEE Sensors Journal*, vol. 16, no. 19, pp. 7217-7226, Oct.1, 2016.
15. F. Gandino, R. Ferrero and M. Rebaudengo, "A Key Distribution Scheme for Mobile Wireless Sensor Networks: q - s -Composite," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 34-47, Jan. 2017.
16. J. Ding, A. Bouabdallah and V. Tarokh, "Key Pre-Distributions From Graph-Based Block Designs," in *IEEE Sensors Journal*, vol. 16, no. 6, pp. 1842-1850, March15, 2016.
17. N. Qi, K. Dai, F. Yi, X. Wang, Z. You and J. Zhao, "An Adaptive Energy Management Strategy to Extend Battery Lifetime of Solar Powered Wireless Sensor Nodes," in *IEEE Access*, vol. 7, pp. 88289-88300, 2019.
18. M. A. Mughal, P. Shi, A. Ullah, K. Mahmood, M. Abid and X. Luo, "Logical Tree Based Secure Rekeying Management for Smart Devices Groups in IoT Enabled WSN," in *IEEE Access*, vol. 7, pp. 76699-76711, 2019.
19. K. Moara-Nkwe, Q. Shi, G. M. Lee and M. H. Eiza, "A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks," in *IEEE Access*, vol. 6, pp. 11374-11387, 2018.
20. P. Xu, S. He, W. Wang, W. Susilo and H. Jin, "Lightweight Searchable Public-Key Encryption for Cloud-Assisted Wireless Sensor Networks," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3712-3723, Aug. 2018.
21. S. Chu, Y. Huang and W. Lin, "Authentication Protocol Design and Low-Cost Key Encryption Function Implementation for Wireless Sensor Networks," in *IEEE Systems Journal*, vol. 11, no. 4, pp. 2718-2725, Dec. 2017.
22. L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu and J. Liu, "A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network," in *IEEE Access*, vol. 7, pp. 53079-53090, 2019.
23. K. Shim, "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577-601, Firstquarter 2016.
24. L. M. L. Oliveira, J. J. P. C. Rodrigues, A. F. de Sousa and V. M. Denisov, "Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms," in *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2186-2195, Dec. 2016.
25. T. A. Alghamdi, "Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method," in *IEEE Access*, vol. 6, pp. 53576-53582, 2018
26. P. Gope and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks," in *IEEE Transactions on Industrial Electronics*, vol. 63, no. 11, pp. 7124-7132, Nov. 2016.
27. T. Chen, K. Hou, W. Beh and A. Wu, "Low-Complexity Compressed-Sensing-Based Watermark Cryptosystem and Circuits Implementation for Wireless Sensor Networks," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 11, pp. 2485-2497, Nov. 2019
28. L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab and A. A. F. Loureiro, "SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks," Fifth IEEE International Symposium on Network Computing and Applications (NCA'06), Cambridge, MA, 2006, pp. 145-154.
29. M. Alshowkan, K. Elleithy and H. Alhassan, "LS-LEACH: A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications, Delft, 2013, pp. 215-220.

AUTHORS PROFILE

Premakumar MN, Completed B.E in Electronics & Communication Engineering in 2000, M.Tech from Digital Communication Engineering in 2004 and MBA in Marketing & HR Management in 2007. He is pursuing my PhD in the Department Electronics & Communication. Currently He is working in Harman Connected Services as a Program Manager.

Professor Ramesh S, received the B.E degree in Electronics & Communication Engineering from Gulbarga University, Karnataka, India in 1990, and M.Tech Degree in Industrial Electronics from Visvesvaraya Technological University, Belgaum, India in 2001 and Ph.D. Degree from Dr. MGR Educational & Research Institute, Chennai, India in 2013. He is working as Professor in the Department of Electronics & Communication Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India. His research areas include Digital Communication, Cryptography and Network Security and VLSI Design. He has authored more than 30 papers in National/international Conferences and Journals.