INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Improving Wireless Sensor Network Security: Multifaceted 5G Protections Enhanced by Restoring Algorithm

Anagandula Nirisha[1], Aenugu Rasagnya[2]*, Sahiti Uriti[3], Himanshu Jain[4]

1 MLR Institute of Technology, Hyderabad, 500043, Telangana, India
2 Malla Reddy Engineering College, Hyderabad, 500015, Telangana, India
3 Gayatri Vidya Parishad College for Degree and PG Courses (A), Visakhapatnam, 530045, Andhra Pradesh, India
4 Duke University, North Carolina, USA

OPEN ACCESS

Received: 22-06-2024

Accepted: 26-06-2024

Published: 31-07-2024

Citation: Nirisha A, Rasagnya A, Uriti S, Jain H (2024) Improving Wireless Sensor Network Security: Multifaceted 5G Protections Enhanced by Restoring Algorithm. Indian Journal of Science and Technology 17(30): 3054-3061. https://doi.org/10.17485/IJST/v17i30.2041

* **Corresponding author**.

nishithareddyaenugu.ajr@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: To develop the security Algorithm for 5G Wireless Sensor Networks (WSNs) to enhance security using the Restoring algorithm. **Methods:** Initially a security code is generated from the restoring algorithm and is used to construct an initial level of security. Here we make use of simple mathematical logic to obtain various security codewords for different security levels. The proposed approach improves the security of 5G WSNs against several security threats. For testing the presented approach, we consider Packet Delivery Ratio (PDR) and Delay as parameters for result comparison, moreover, Network Simulator is used to validate the technique of the proposed. **Findings :** The proposed method can be employed in 5G WSNs to minimize the current weaknesses and reinforce the security against possible security threats (i.e. Black hole attacks, session hijacking, DoS attacks, etc.). Besides, the presented approach can be used to protect against cyber threats. **Novelty:** The proposed method combines the necessary security features generated from the restoring algorithm and simple logical mathematics with 5G WSNs to develop the basic layer of security. With the application of logical mathematics, more security codes have been employed to provide different levels of security and as a result, it improves the 5G WSN security by efficiently optimizing the security threats.

Keywords: Restoring Algorithm; Digital codes; 5G WSNs; Network simulator; Security

1 Introduction

WSN plays an essential role in the 5th Generation (5G) technology; as such networks are employed in various fields in day-to-day life. Such as agriculture, weather prediction, and defense as part and all of them make use of the Internet of Things (IoT) to implement in real-time applications. To accomplish such goals multi-hop communication is employed between end nodes, so experience various security issues. Several lemmas, algorithms, and methodologies have been used to provide security

to such systems, which includes the spreading of keys (i.e. public and private keys), software-defined networks (SDNs), and energy of the node are used to mitigate security issues in 5G WSNs. These methods are not operative for 5G WSN communications due to various causes, such as the mathematical complexity of designed key distribution security algorithms being too much to implement in 5G WSNs, and the presence of weaknesses in the software-defined network applications layer. Also, the existing methodologies used simple digital code to provide network security, however, these methods are also prone to security threats at every hop. The development of 5G is particularly generated for higher data rates, improved end connections between nodes, and less delay while sustaining Quality of Service (QoS), however, familiarized with various security threats across Open System Interface layers[(1)]. These tasks prove the necessity of better security procedures to avoid security threats that negotiate data authentication, integrity, and confidentiality, as well as handling security apprehensions over private data.

Although the art of work in 5G security reported these concerns[(2)], also limited algorithms used the zero-knowledge technique to mitigate the security concerns without negotiating sensitive evidence. Current approaches such as key-based distribution and energy-based monitoring may not resolve the cause in active WSN situations due to difficulty and possible imprecision. No doubt Software Networks in 5G advance communication bandwidths but prompt security threats such as spoofing attacks and Denial of Service (DoS) over network virtualization[(3,4)]. Furthermore, the algorithms based on machine learning are unprotected from data variations which require security protocols accomplished to address several threats through network layers. Therefore, an efficient protocol to secure 5G WSNs is needed to safeguard authentication, confidentiality between end node communications

In this approach, a novel technique using a logical mechanism is employed to generate a basic code that increases belief and privacy in multi-hop environments. Furthermore, we enlarge the codeword by making use of different measures, using various logical approaches to get various levels of security (i.e. here we called these level 1 and level 2) to provide complete security to protect 5G WSNs. Also, we afford another security level called the third level of protection to confirm node authentication. The proposed scheme decreases communication latency between end nodes by reducing the number of requisite bits to defend and implement the procedure in a modern fashion. A network simulator is employed to authenticate the usefulness of the presented approach.

Wireless Sensor Networks (WSNs) are demanding modules of the Internet of Things (IoT), associative uses such as smart healthcare, smart grids[(5,6)], VANETs[(7,8)], and smart shipping[(9–11)], particularly in the context of 5G technology. These systems are necessary for accumulating and communicating data across different locations. However, their combination with 5G presents substantial security contests, including problems with password execution and susceptibilities in periodic key security, as presented in earlier studies[(12,13)]. The addition of Wireless Sensor Networks (WSNs) with 5G devices and sensors accelerates unified data collection through public nets within the Internet of Things (IoT) structure[(14)]. This interaction connects the mutual experiences of WSNs and 5G to competently and securely gather the communicated data, thus assisting numerous applications in areas like smart healthcare, smart grids, VANETs, and smart shipping systems. Many approaches have been projected to report these challenges, such as sensing black holes and wormhole attacks[(15,16)]. Yang et al.[(17)] suggested a pattern that integrates Block chain and deep learning to sense active and attacker nodes in WSNs. However, their method showed problems such as amplified delay and compact packet delivery ratio, so restraining its efficiency in improving network security. Ankur and Amit[(18)] showed relative investigations of several security devices designed for WSNs, contribution appreciated visions into their relevant assets, and faintness in encouraging network security. Despite expansions, these methods repeatedly face difficulties that can hamper network procedures and decrease overall system efficiency. Ahmed et al.[(19)] anticipated energy constraints to support WSN security. However, the self-directed environment of WSNs leads to certain challenges that can bind the usefulness of this approach in safeguarding healthy security. Elizabeth et al.[(20)] suggested an approach using key sharing for MANET security. However, the vital nature of MANETs, where nodes can freely join or leave could negotiate the consistency of key sharing and possibly decrease overall network output. In[(21,22)], the authors led a detailed review and relative investigation of security methods designed for 4G wireless networks. Alnoor et al.[(23)] presented an Artificial Intelligence-based approach designed to enhance trust in social networks. However, the verification and privacy methods used in this approach are not adequate for safe wireless sensor networks efficiently. Jaiswal and Dwivedi[(24)] projected a complete safety model to WSN applications, which, even though, familiarizes difficulties that may cause delays and present possible security risks.

Moreover, current security protocols considered for Mobile and ad hoc networks (MANETs) and IoT procedures have restrictions in safeguarding complete security in autonomous network settings[(25)]. Hence, there is a crucial requirement to improve particular security prototypes explicitly for 5G-based WSNs. This approach supports multifaceted security methods through different network levels. The aim is to preserve privacy and maintain data integrity during the data broadcast process.

The Existing investigation highlights numerous approaches such as energy-based approaches, key distribution, simple digital codes, and SDNs designed to strengthen security. Still, these methods have limitations and may not apply to 5G Wireless Sensor Networks (WSNs), particularly when combined with IoT. Therefore, need to develop an innovative security model for 5G

WSNs. Here we are proposing a novel approach that has the property to execute several layers of security at various network levels and communication hops, thus employing strong authentication, confidentiality, and data integrity during the entire communication process.

The paper is designed as follows: In Section 2 we present the methodology of the work. In Section 3, we showed the results and discussed our paper. Moreover, in section 4, we conclude our paper, and finally reference section has been added to the manuscript

2 Methodology

2.1 Proposed approach

The primary decimal values that are used to create a hexadecimal string (i.e. 4-bit representation) are expanded from 0-15 decimal numbers and must follow the equal-weight rule i.e., the same number of zeros and ones are present in the code word while signifying in hex-code. Furthermore, it must satisfy the following equation.

$$P_{dv} = \prod_1^t 3x\, 1 \leq x \leq t \,\&\, t = 4 \;\forall\; + ve\, integers \tag{1}$$

where 'P_{dv}' is the primary decimal value and can be represented as 3, 6, 9, and 12 (see Equation (1)), and also the binary hex values of the above decimal numbers are represented in (Equation (2)).

$$H_V = \begin{cases} 3 = 0011 \\ 6 = 0110 \\ 9 = 1001 \\ 12 = 1100 \end{cases} \tag{2}$$

Now to generate the security code words from (Equation (2)), we use a restoring algorithm with multiple criteria. To improve security a simple rule is applied to each code as follows:

Rule: If the digital code word obtained has four consecutive 1's or 0's then the third bit is complemented (i.e. '1' is changed to '0' and '0' is changed to '1').

The initial code word can be generated by dividing each number of (Equation (2)) by '3' using the Restoring algorithm. In the next step, we merge the bits of Accumulator 'A' and Quotient 'Q' row-wise

Figure 1 represents the flow chart of the proposed approach using the restoring algorithm. To understand the concept of the presented algorithm, let us consider the first number of the series i.e. '3' and divide it with '3' (such as 3/3) using the restoring algorithm to create an initial code word (see Table 1).

Table 1. Generation of initialcodeword using Restoring Algorithm

n	M	Accumulator bits (A)			Quotient bits (Q)		Action
					Q_1	Q_0	
2	011	0	0	0	1	1	Initialization
-	-	0	0	1	1	-	SL- AQ
		1	1	0	1	-	A= A-M
1		0	0	1	1	0	Q0 = 0, as MSB of A =1, restore A
		0	1	1	0	-	SL - AQ
		0	0	0	0	-	A = A-M
0		0	0	0	**0**	1	Q0 =1, as MSB of A= 0, No restore A

Initially accumulator 'A' contains '000' bits and Quotient 'Q' contains '11' bits, then as per the restoring algorithm, the one-bit left shift is provided to get the current elements of 'A'. Here n=2, because the number of bits in Q = 2 (i.e.,11).

Later in the next step A = A – M and the value of 'Q_0' is '0' because the most significant bit of 'A' =1, therefore according to the restore algorithm, the elements of 'A' will be restored, hence again A = 001 and the process will be continued till the iteration will be '0'. To get the value of '-M' we are using 2's compliment of 'M' (i.e. 011 can be written as 100+ 1= 101), therefore A = A-M = 001+ 101= 110. (See final step of iteration 2). So, the initially generated code word has a length of '31' bits (i.e. all the bits of the restoring algorithm row-wise) and can be represented as

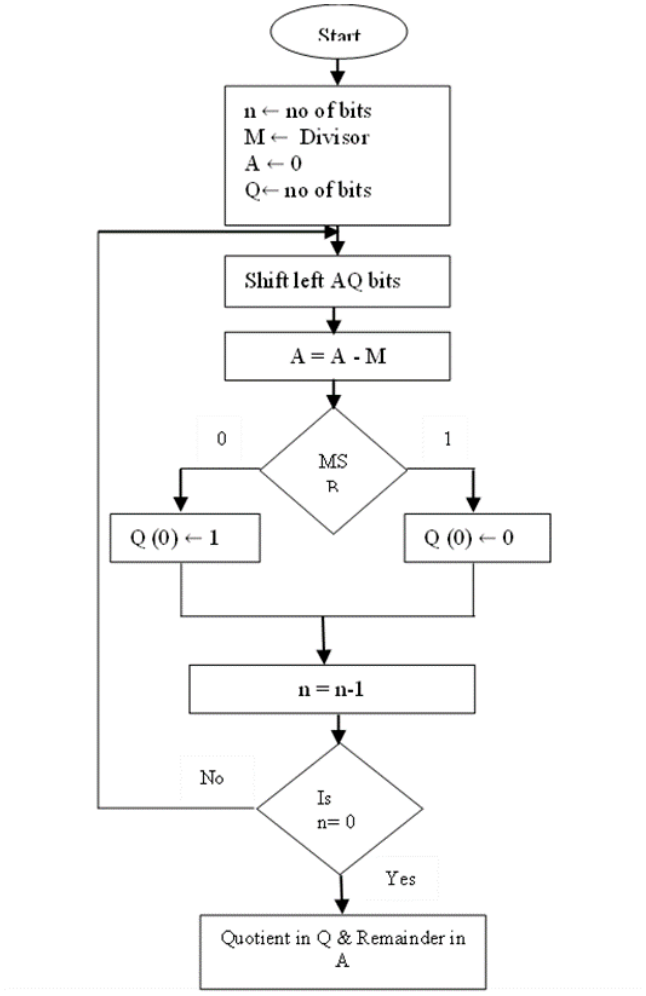

Fig 1. Flowchart of the initial Security code generation using Restoring Algorithm

I_{CW} = 00011001111010011001100000000001

However, to make the length in a standard form we are using even and odd parity, which can be symbolized as

The odd parity string is 00011001111010011001100000000011

Even the parity string is 00011001111010011001100000000010

For simplicity purposes, we choose here only 3/3, and the remaining series elements ofEquation (2) are divided by '3' (i.e. 6/3, 9/3, and 12/3) to generate more code words similarly to enhance the 5G security.

2.2 3/3 using Restoring Algorithm

3(Dividend) and 3(Divisor) => 1(quotient) and 0(remainder)

The codes obtained in this process are (as discussed in section 3.1)

I_{CW} = 00011001111010011001100000000001 (31-bit code)

32-bit code can be generated by using odd parity and even parity to make the number of bits in the code word in a standard form

The odd parity string is 00011001111010011001100000000011

Even the parity string is 00011001111010011001100000000010

After applying the rule these codes can be presented as

$$\begin{aligned} {}_1 &= 00011001111010011001100100100011 \\ {}_2 &= 00011001111010011001100100100010 \end{aligned} \tag{3}$$

Where C_z represents the final code and z=1, 2.

At Level 1, our approach will secure the Physical layer by employing security code words, as outlined in Equation (3), to authenticate active nodes. This ensures that only authorized nodes can enter the network, so all attacker nodes can be easily judged and will be eliminated from the network.

Similarly, at Level 2, the codes obtained from the 9/3 using the restoring algorithm will boost the privacy in the Network layer. The generated codewords from the above operation will also be employed to encode the data transmissions and protect sensitive data information, which is being snooped by malicious nodes.

Level 3 phase, strengthen the safety of the Application layer by making use of codes created from 12/3 restoring operation. These codes will guarantee the reliability and validity of the data. To do this operation we can easily notice and avoid any interference to the data, therefore preserving the complete safety and consistency of the 5GWSNs applications and rest areas. In overall response the designed security method, using restoring methodology at different levels of the network design, deals ample security. The Physical layer (L1) will stress on node verification, the Network layer (L2) on data privacy, and the Application layer (L3) on data reliability and validity. This approach considerably improves the elasticity and strength of the 5G WSNs from a wide range of security concerns.

2.3 Node Matching Process

Figure 2 represents the assumed geographical area of WSN to validate the proposed approach. In this setup, 'S' stands for the source node, 'A' signifies an active node, and 'M' represents a malicious node. While we illustrate only one attacker node ('M') for simplicity, this model can include multiple active and attacker nodes.

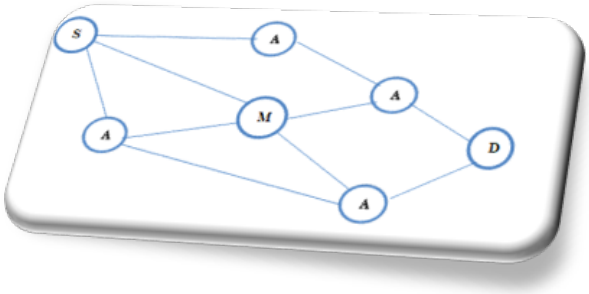

Fig 2. Geographical location of WSN

Initially, the source node (S) broadcasts a request signal to all neighboring nodes, to initiate the Level 1 communication. At this stage, only active nodes ('A') can access the information. They do this by matching the provided code words and performing the necessary mathematical operations to reproduce the same code word generated by the source node.

In the first hop, two types of code words are distributed: one for privacy (odd parity) and one for security (even parity), as described in Equation (3). From the second hop and further, nodes must match both the initial and final code words to maintain access to the data. Nodes that fail to match these code words are considered attacker nodes and are denied access to the data.

At any point during the communication process, if the privacy and security codewords generated from the ratios 3/3, 6/3, 9/3, and 12/3 do not match with those from the source node, the node is identified as a malicious node and removed from the communication path between the source and destination.

This method offers strong safety through various levels. At Level 1, it certifies that simply active nodes can enter the network by confirming the code words allotted at the transmission side. In succeeding hops, nodes must have continuous authorization both at the first and modified code words, to firmly uphold the safety checks during the data communication procedure. Moreover, any node deteriorating to meet such measures is recognized simply and omitted from the network. Accordingly, shielding the network from safety concerns and certifying data transmission security between end nodes.

3 Results and Discussion

Table 2 signifies the simulation parameters employed in the presented approach, in which we gauge the efficiency of the presented method concerning Elizabeth [24], Ahmad [19], and Dwivedi approaches by the application of Network Simulator 2 (NS2). These constraints comprise nodes employed in the network, range of communiqué, simulation time, size of packet, pattern of traffic type, and movement of the nodes, These parameters played a vital role in constructing a geographical network environment. The valuation focuses on key presentation measures, including packet delivery ratio (PDR), latency, security, throughput, and efficiency. Exploiting NS2 certifies that the simulations are directed in a careful, reproducible atmosphere which simplifies a detailed and impartial assessment of each method. This study shows how every method pays to refine the safety and efficiency of the designed network, furthermore delivering a strong consideration of their benefits and limits.

Table 2. Simulation Parameters

S. No	Parameters	Values
1	Simulation time	6os
2	Node count	0-290
3	Hope Count	6
4	Link Layer	Logical Link
5	MAC Type	802.11
6	Traffic type	variable
7	Area	1200mx1200m
8	mobility	3,4,5,6 and 7m/s
9	Pause time	0,35,45,55,65,150ms
10	Size of packet	1.5kb

Figure 3 represents the response of the overall Packet Delivery Ratio (PDR) between the source and destination. From the figure we observe that the proposed method attains more throughputs when equated with other approaches, suggesting its competence in effectively distributing packets across the network.

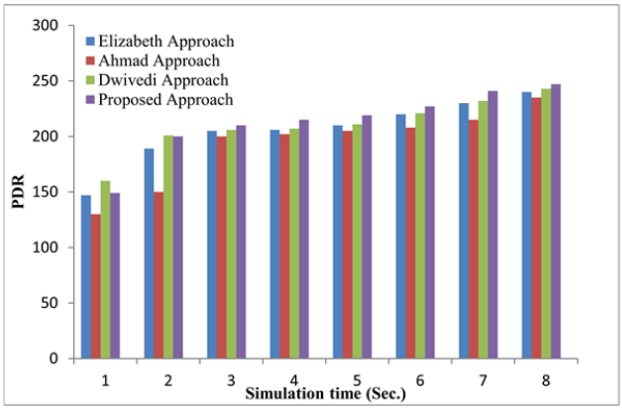

Fig 3. Variation of PDR with Simulation Time

The PDR plays a vital role in computer networks, as it calculates the output response of total packets transmitted and received, with a more PDR representing higher reliable network connection. The proposed method improves network security in terms of efficiency in packet management and delivery. The proposed method reduces packet loss and snooping from malicious nodes, these points to an additional stability and secure network connection. Therefore, the higher PDR and throughput obtained by applying our approach prove that our technique successfully improves both safety and network performance.

But from the figure, we observed that at the initial phase, few existing approaches show improved response when compared to our method. Since these approaches frequently sense attacker nodes initially, if the energy levels of nodes are similar. However, after time elapses, these approaches encounter issues when attacker nodes enter the network with varying energy levels, as a result of which these methods reduce the effectiveness and overall efficiency.

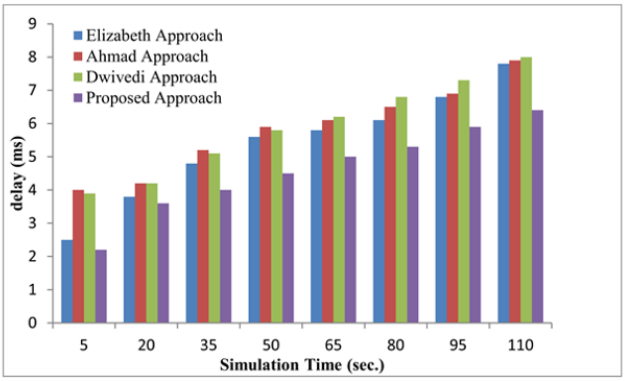

Fig 4. Variation of Delay with Simulation Time

Figure 4 shows the deviation in delay concerning the simulation time. Our projected method reliably illustrates minimum delay when related to the existing approaches. Primarily, the Dwivedi approach achieves well in handling delay. However, its competence drops as the number of hops grows. As a result, the delay will increase concerning time due to facing certain challenges to preserve an ideal path between source-destination pairs. In divergence, the suggested method upholds a minimum delay reliably during the entire simulation. This shows that the capability of our method to enhance communication paths effectively is better when compared to existing approaches

4 Discussion

The security problems associated with the 5G systems show a substantial security threat to network confidentiality and security. The suggested approach discusses these security concerns successfully and certifies protected communication between sink and destination. To clear the concept let us consider an example of a snooping attack, where attackers try to disturb and change data between end nodes. The presented approach provides distinctive codes at every individual node (such as at level 1 and level 2). The security codes presented at these layers do not allow the attacker nodes to enter the network and maintain the reliability of the data. Moreover, confirmation codes at level 3 increase security by stopping illegal data altering and successfully recognizing the attacker nodes to remove them from the communiqué path. In recurrence attacks, in which attacker nodes retain and repeat data between neighboring nodes, the proposed method provides a dynamic code generation technique at every node. Moreover, at each node, this procedure avoids the entertainment of interrupted data on consecutive communication links, which strengthens network security.

Also, the presented approach successfully removes maximum attacks from the network and improves the performance of the designed system. Among common attacks the well-known attacks are Sybil attacks which comprise the formation of numerous false identities to suppress genuine nodes; while the DoS attack's purpose is to overload the network with unnecessary traffic. By executing privacy and validation concerns at every layer and hop, the presented approach successfully senses and minimizes these threats, confirming continuous and safe network action. Additionally, the suggested approach exhibited healthy safety against a varied range of confidentiality and safety threats in 5G networks. By combining the dynamic and layered safety protocols, we detect as well as effectually mitigate attacks, avoiding the reliability and privacy of communicated data across the complete network.

5 Conclusion

The presented approach presented an innovative solution to 5G WSN security by employing the Restoring Algorithm and mathematical logic to justify numerous attacks across various network layers. Also, the presented approach can vigorously produce different code words at each hop. This confirms resilient node verification by consistently proving digital codes across the network, which shows the novelty of the presented approach. The security codes obtained at each hop count expand node trust and flexibility against possible vulnerabilities in the network. Furthermore, the presented approach is very simple to implement, energy efficient, and has the prospective to inspire the progression of healthy safety frameworks for 5G networks. Finally, this method provides the basic knowledge to researchers to enhance the security of 5GWSNs.

References

1) Sullivan S, Brighente A, Kumar SAP, Conti M. 5G Security Challenges and Solutions: A Review by OSI Layers. *IEEE Access*. 2021;p. 116294–116314. Available from: https://doi.org/10.1109/ACCESS.2021.3105396.
2) Szymoniak S. Key Distribution and Authentication Protocols in Wireless 'Sensor Networks: A Survey. *ACM Computing Surveys*;56. Available from: https://doi.org/10.1145/3638043.
3) Farooq MS, Riaz S, Alvi. . Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review. *Electronics*. 2023;12. Available from: https://doi.org/10.3390/electronics12143077.
4) Polat H, Polat O, Cetin A. Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models. *Sustainability*. 1035;2020. Available from: https://doi.org/10.3390/su12031035.
5) Zhu Y, Jia G, Han G, Zhou Z, Guizani M. An NB-IoT-based smart trash can system for improved health in smart cities. *Proc IEEE 15th Int Wireless Commun Mobile Comput Conf (IWCMC)*. 2019;p. 763–768. Available from: https://doi.org/10.1109/IWCMC.2019.8766748.
6) Zhang R, Cui S, Zhao C. Design of a data acquisition and transmission system for smart factory based on NB-IoT. *Proc Int Conf Commun Signal Process Syst*. 2020;p. 875–880. Available from: https://doi.org/10.1007/978-981-13-6508-9_107.
7) Zhang J, Cui J, Zhong H, Chen Z, Liu L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans Depend Secure Comput*. 2021;18(2):722–735. Available from: https://doi.org/10.1109/TDSC.2019.2904274.
8) Wang P, Chen CM, Kumari S, Shojafar M, Tafazolli R, Liu YN. HDMA: Hybrid D2D message authentication scheme for 5G-enabled VANETs. *IEEE Trans Intell Transp Syst*. 2021;22(8):5071–5080. Available from: https://doi.org/10.1109/TITS.2020.3013928.
9) Karthikeyan M, Manimegalai D, Rajagopal K. Firefly Algorithm-based WSN-IoT security enhancement with machine learning for intrusion detection. *Sci Rep*. 2024;14:231–231. Available from: https://doi.org/10.1038/s41598-023-50554-x.
10) Faris M, Mahmud MN, Salleh M, Alnoor A. Wireless sensor network security: A recent review based on state-of-the-art works. *International Journal of Engineering Business Management*. 2023;15. Available from: https://doi.org/10.1177/18479790231157220.
11) Ambika N. Securing the IoT-Based Wireless Sensor Networks in 5G and Beyond. In: Bhushan, B, Sharma, K S, Kumar, R, et al., editors. 5G and Beyond. Springer Tracts in Electrical and Electronics Engineering. Springer. 2023. Available from: https://doi.org/10.1007/978-981-99-3668-7_10.
12) Sahoo SS, Mohanty S, Sahoo KS, Daneshmand M, Gandomi AH. A Three-Factor-Based Authentication Scheme of 5G Wireless Sensor Networks for IoT System. *IEEE Internet of Things Journal*. 2023;10(17):15087–15099. Available from: https://doi.org/10.1109/JIOT.2023.3264565.
13) Sall S, Bansode R. Lightweight Cryptography Using Pairwise Key Generation and Malicious Node Detection in Large Wireless Sensor Network. *Indian Journal of Science and Technology*. 2023;16(36):3002–3008. Available from: https://doi.org/10.17485/IJST/v16i36.2503.
14) Stergiou C, Psannis KE, Kim BG, Gupta B. Secure integration of IoT and cloud computing. *Future Gener Comput Syst*. 2018;78:964–975. Available from: https://doi.org/10.1016/j.future.2016.11.031.
15) Ahmad ISJ, Unissa M, Ali A, Kumar. Enhanced security to MANETs using digital codes. *Journal of Information Security and Applications*. 2022;66. Available from: https://doi.org/10.1016/j.jisa.2022.103147.
16) Garg R, Gulati T, Kumar S. Range free localization in WSN against wormhole attack using Farkas' Lemma. *Wireless Netw*. 2023;29:2029–2043. Available from: https://doi.org/10.1007/s11276-023-03279-8.
17) Yang J, He S, Xu Y, Chen L, Ren J. A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for. *Wireless Sensor Networks Sensors*. 2019;19. Available from: https://doi.org/10.3390/s19040970.
18) Sirohi A, Agarwal AK. Security in Wireless Sensor Network (WSN): A Detailed Survey. *International Journal of Advanced Science and Technology*. 2020;29:376–387. Available from: http://sersc.org/journals/index.php/IJAST/article/view/7172.
19) Ahmed A, Abu Bakar K, Channa MI, Haseeb K, Khan AW. A trust aware routing protocol for energy constrained wireless sensor network. *Telecommunication Systems*. 2016;61(1):123–140. Available from: https://dx.doi.org/10.1007/s11235-015-0068-8. doi:10.1007/s11235-015-0068-8.
20) Elizabeth NE, Subsree S, Radha S. Enhanced security key management scheme for MANETS. *WSEAS Transactions on Communication*. 2014;13:15–25. Available from: https://doi.org/10.1007/s11235-015-0068-8.
21) Faris M, Mahmud MN, Salleh MFM, Alnoor A. Wireless sensor network security: A recent review based on state-of-the-art works. *International Journal of Engineering Business Management*. 2023;15:1–29. Available from: https://doi.org/10.1177/18479790231157.
22) Ahmad R, Wazirali R, Abu-Ain T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. *Sensors*. 2022;22(13):4730–4730. Available from: https://dx.doi.org/10.3390/s22134730. doi:10.3390/s22134730.
23) Alnoor A, Al-Abrrow H, Halbusi HA, Khaw KW, Chew X, Al-Maatoq M, et al. Uncovering the antecedents of trust in social commerce: an application of the non-linear artificial neural network approach. *Competitiveness Review: An International Business Journal*. 2022;32(3):492–523. Available from: https://dx.doi.org/10.1108/cr-04-2021-0051. doi:10.1108/cr-04-2021-0051.
24) Jaiswal SK, Dwivedi AK. A Security and Application of Wireless Sensor Network: A Comprehensive Study. In: 2023 International Conference on IoT, Communication and Automation Technology (ICICAT). IEEE. 2023;p. 1–5. Available from: https://doi.org/10.1109/ICICAT57735.2023.10263644.
25) Dwivedi AK, Sharma AK, Kumar R. Dynamic Trust Management Model for the Internet of Things and Smart Sensors: The Challenges and Applications. *Recent Advances in Computer Science and Communications*. 2021;14(6):2013–2022. Available from: https://dx.doi.org/10.2174/2213275912666190823103344. doi:10.2174/2213275912666190823103344.