REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

Development of a Lightweight Security Framework for Optimal Routing in Secure Wireless Sensor Networks

Dr. Manjunath B.E[1*], Dr. R. Divya[2], Dr. P. Vamsi Krishna[3]

[1*]Professor, Department of ECE, R K College of Engineering-Vijayawada, Andhra Pradesh, India
E-Mail: manjunathbe7666@gmail.com
[2]Assistant Professor, Department of ECE, R K College of Engineering-Vijayawada, Andhra Pradesh, India
E-Mail: sdivyareddy22@gmail.com
[3]Associate Professor, Department of ECE, R K College of Engineering-Vijayawada, Andhra Pradesh, India
E-Mail: pvk11278@gmail.com

Abstract-In the past recent years, WSN has progressively grown as an emerging technology. Various research efforts have been made in the literature to address the problem associated with WSN security. Based on the review analysis, it is found that the existing methods are mostly associated with complex security operations that are not suitable for resource constraint sensor nodes. The proposed paper has presented cost-effective modeling of the security framework that addresses the problem of security and energy in WSN. The proposed security framework implements two different protocols to attain maximum security services and optimizes the security operation of the proposed security models to achieve higher energy efficiency and privacy preservation against a majority of the lethal attacks. The first security model introduces a novel cost-efficient pair-wise key-based authentication mechanism to identify the availability of optimal routes under the presence of adversary in the network. The second security model introduces an integrated part of the first security model that optimizes security operation to perform secure communication using a lightweight encryption mechanism. Based on the experimental outcome and analysis, the proposed system attains a 60% performance improvement in terms of security and computational efficiency compared to the existing Sec-LEACH. The second security model has achieved a 50% improvement in terms of overall aspects like reduction in transmission delay, packet delivery ratio, remaining energy, and communication performance.

Keywords:-*WSN, Security, Routing, Energy Efficiency, Authentication and Encryption*

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have evolved due to their potential of supporting functions of data transmission within a cost-effectiveness manner where human intervention is quite difficult. WSNs widely deployed for enabling data collection services using small sensor nodes with self-configuring features that operate in areas of interest [1]. Although various commercial and industrial applications are mainly meant for event monitoring in multiple fields such as border security surveillance, residential area surveillance, patient activity monitoring, and home automation, etc. [2-3]. However WSNs mainly suffers by different aspects of operational constraints that have an adverse impact on the performance of the entire network [4]. One of the highly focused problems of WSN is security issues, which is a very hot topic in the research domain. If the security issues and the attackers are identified as early as possible, the adverse effects of threats and attacks can be reduced efficiently. Therefore, the Intrusion Detection System (IDS) emerged as the main security tool for identifying malicious activities in WSN [5]. The main feature of any IDS is to monitor the network traffic and nodes activity and identify malicious patterns and behavior. The adversary usually occurs where single nodes or multiple nodes can be compromised by the adversary where the attacker intends to disrupt the essential function and steal the confidential data from the network. However, in some cases the adversary intends just to steal some important information. The adversary in this type of attack does not disrupt the network operation therefore; identifying this kind of attack becomes quite challenging for many attack detection systems because the adversary initially, does not allow the captured nodes to show their intent. There have been lots of research studies done to address security issues in the WSNs [6-8]. However, many of the existing solutions are not much suitable for the resource constraint sensor-based wireless network. Existing security solutions are more likely to be robust against particular nature of the attacks and which fails when any unknown form of attack is introduced to the network. Another issue with the existing security solution is that they are mostly associated with performance issues due to the incorporation of the complex form of cryptographic operations. More specifically, it should be understood that the implementation of heavy encryption operations will gradually affect the overall communication performance, higher energy utilization, and computing requirements [9-10]. Therefore, an efficient security mechanism should be designed that considers all prominent constraints and parameters for ensuring maximum security requirements and maintains a balance between energy consumption and network performance.

In the proposed research paper, the study introduces a lightweight security mechanism that considers energy consumption and uncertain traffic condition as prominent constraint factors, thereby identifying the availability of secure and reliable routes for the data transmission in an efficient manner even though there is a presence of adversary in the network. The rest of the section is organized as follows: In section II, related work is discussed, section III presents a description of the

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

proposed system methodology, section IV implementation strategy and algorithm for the proposed security model and section V discusses performance analysis, and finally in section VI overall contribution is concluded.

II. RELATED WORK

This section presents a review of the existing research work carried out in the domain of WSNs security. There have been lots of research studies towards addressing security issues presented in the literature. One of the significant research works carried out by the Mahidhar, and Raut [11] have carried an investigative analysis towards identifying issues associated with existing packet scheduling methods. The authors have then used multilayer priority with the Bit rate division to overcome issues like transmission delay factor and network performance. Apart from this, the authors have used an encryption mechanism to protect the data transmission process. Another work in a similar direction is carried out by the Monika and Upadhyaya [12], where the authors have discussed enabling a secure communication environment in WSN based on DNA-cryptography. Kabaskin and Kundler [13] have presented an approach based on the Markov model to determine the reliability of WSN nodes. Lu et al. [14] has explored the effectiveness of various existing approaches for secure packet transmission and presented a digital signature security algorithm for secure communication in two steps. Ghosal et al. [15] have attempted to develop a robust and efficient security technique against a various adversary in WSN. The author utilizes an improved encryption mechanism to achieve maximum security requirements, such as confidentiality, authentication, availability, and integrity. Yu and Zhang et al. [16] have introduced a layered-oriented network model to achieve higher energy efficiency for monitoring for the smart grid application. Zhu et al. [17] explored the issues associated with the network performance and presented a cost-effective design considering uplink and downlink transmission links.

Teng et al. [18] have used cross-layer optimization to reduce the transmission delay and to improvise network efficiency. For data aggregation, the sensor nodes' energy consumption characteristics are obtained, and a cross-layer optimization method is used to make stable energy consumption in case of nodes nearer to sink node and other nodes. The study outcomes exhibit it achieves a reduction in data transmission delay. Chidean et al. [19] have introduced a combined approach of clustering and network processing technique boosting the performance of WSN. The study outcome reveals that a combined approach of processing technique and clustering technique can optimize energy utilization and reduce data transmission delay. Hu et al. [20] have developed a secure communication channel between the user and the sensor using encryption and digital signature algorithm. Biswas et al. [21] introduced an energy-efficient routing strategy using a cryptographic approach to achieve efficient energy utilization with maximum security services. Li et al. [22] used a certificate-less cryptographic approach to provide guaranteed security services in WSN. The study outcomes show that their approach has achieved confidentiality, authenticity, non-repudiation, and integrity, and it also reduces computational complexity. Manjunath B E and P V Rao [23] have carried extensive analysis on existing research work to explore recent trend and progress in the wireless network. Liu, Zhi-xin, et al.[24] presented an efficient routing approach for real-time applications in WSN, considering various constraints like node energy and dynamicity of the network. The simulation outcome shows that the presented approach attains reliability, with less delay factor. Mondal et al. [25] use a cryptographic approach to ensure data security while maintaining the authentication and integrity. Vaseghi et al. [26] used the chaos synchronization technique and applied a sliding mode controller to obtain the true synchronization value between the chaotic oscillators from both the base station and the sensor nodes. Another work carried out by Manjunath B E and P V Rao [27-28] where the authors have used hash-based authentication and lightweight encryption mechanism to perform Balancing Trade-off between Data Security and Energy thereby enabling secure communication in WSN to resist maximum security threats.Yu, Hong, et al.[29] proposed a scheme based on asymmetric encryption to perform the authentication process as well as symmetric keys and encryption for key management operations. Here, the authentication and access control functions are redistributed to the gateway between WSN and the Internet, thereby reducing the data processing burden and reducing energy consumption. The results show that the method achieves good results in extending the network's life, where the transmission process is reliable, with low computation cost and robust security mechanism.

III. RESEARCH PROBLEM

This research work attempts to address issues associated with existing research in domain of WSN security by analyzing the different forms of security vulnerabilities existing in existing systems. The followings are the research problem identified based on the review analysis.

- The security solutions currently used in WSN are only defensive against certain forms of attack scenarios, which makes it impossible to use when the attack scenario changes due to the use of other types of adversarial strategy.
- For time-based tracking, existing security methods cannot provide the best solution, which can lead to incorrect implementation in the WSN network environment.
- The encryption protocol adopted in most of the existing research work consumes a lot of resources during computation.
- Also, balancing of strong security requirements and energy efficiency under uncertain traffic pattern is also missing in the existing research works. Therefore, ensuring robust and efficient energy utilization in resource constraint sensor-based network is still a problem to be studied and resolved.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

Therefore, the problem statement for the proposed study can be expressed as "*Developing a lightweight robust security framework that can ensure comprehensive level of security as well as higher energy efficiency without compromising network performance is quite a challenging task*".

IV. PROPOSED SYSTEM

The current research study proposes a computational model for introducing the novel design of energy-efficient mechanism and security paradigm in the wireless sensor network. The prime focus of the proposed security model is considered in the direction of ensuring a secure association between the WSN nodes, and the selection of a reliable route for enabling secure data transmission till the network service duration. The study adopts an analytical research methodology to implement the introduced security system. The development of the proposed security modeling is carried out in such a way that it does not associate to a greater extent of use of complex security operations, it is highly functional that enhances network service duration, and even in the presence of adversary in the network, it provides a secure sensitive data transmission. In addition, the design of the proposed security model is most suitable for homogeneous and heterogeneous sensor networks, which will be robust to any attacker and will never allow any operational and effective lethal activities on homogeneous and heterogeneous networks. The modeling and design of the proposed security model are carried out in two implementation steps, as shown in figure 1.

In the first security model implementation step-*(security module-1*), the development of a security module is considered based on a probabilistic method to formulate an efficient and robust strategy that can resist security threats, thereby providing a comprehensive security environment for packet transmission and node communication. This part of the design and implementation aims to introduce a novel functional scheme for identifying the availability of the best route in the presence of an adversary without affecting network performance and not relying on a large number of node resources. The security module-1 also introduces an adversary modeling as a case of node capturing attack considering the incident of higher energy depletion by the compromised nodes. In this regard, the compromised nodes with less energy will be supposed to perform different behavior than compromised nodes with higher energy. The security module-1 also performs a secure authentication process using the installations of pair wise key between WSN nodes to check whether both the sensor node and routing path are spiteful or authentic based on positive and negative probability value. Therefore, in this way, the security module of the proposed system can efficiently identify attacker nodes.

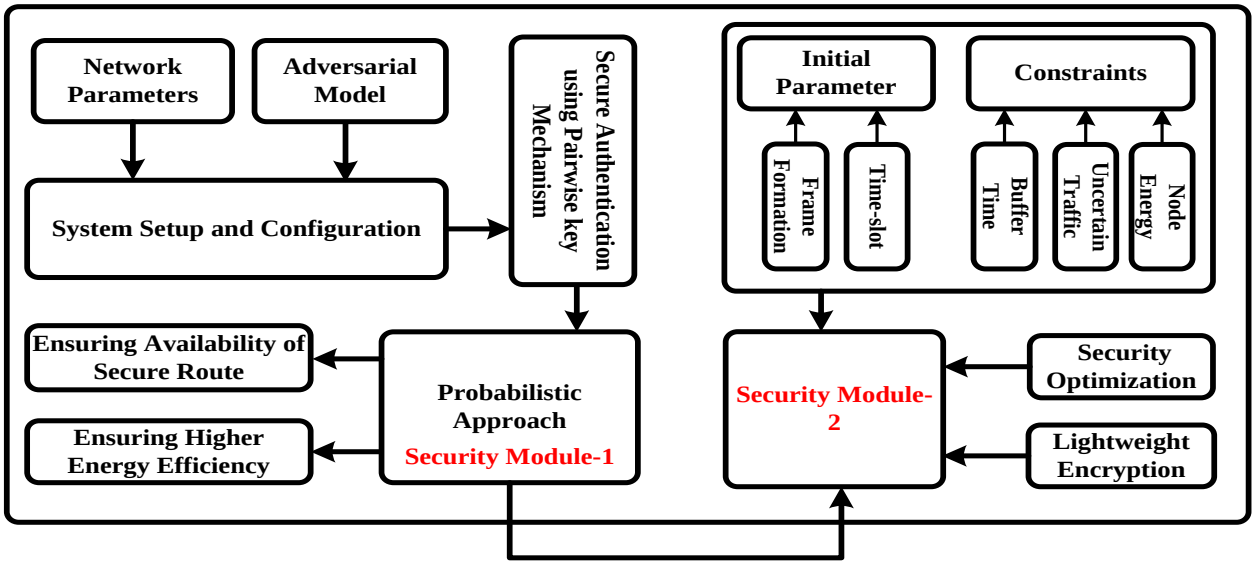

Figure 1 Schematic Architecture of Proposed System

The second security module-(Security Module-2) is a continuation of Security Module-1 and aims to provide a complementary layer of protection by optimizing various security operations in the network. The study assumes that the adversary may have full knowledge of the node's private data, allowing it illegitimate access to that confidential information. In this modeling, a decision strategy is established between nodes where it is also assumed that an attacker must also spend some amount of node resources to launch the attack. Therefore, an attacker can only launch an attack under favorable conditions, which means that if the attacker does not want compromised nodes to be identified as an adversary, then it must assist in the forwarding of packets in the network. The proposed model introduced a lightweight encryption mechanism and optimized security algorithm, which considers frame rate and time slots in uncertain traffic environments to ensure optimal utilization of the node resources, as well as ensures an effective balance between maximum security requirements and network performance.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

V. IMPLEMENTATION STRATEGY

This section presents the description about implementation strategies adopted for the Modelling of security system.

A. Security Module-1: Computational Modelling Approach for Identifying Best Secure Route

This phase of the proposed system aims to develop a novel strategic model to identify the availability of the optimal secure path in the presence of attackers. The detailed design and operational flow of this security model are shown in Figure 2. The system design stage includes several operational stages. Among them, in the initial stage, an adversary modeling is performed considering the situation of node capture attacks and the formation of heterogeneous networks, where the data transmission and communication processes follow the multipath propagation approach.

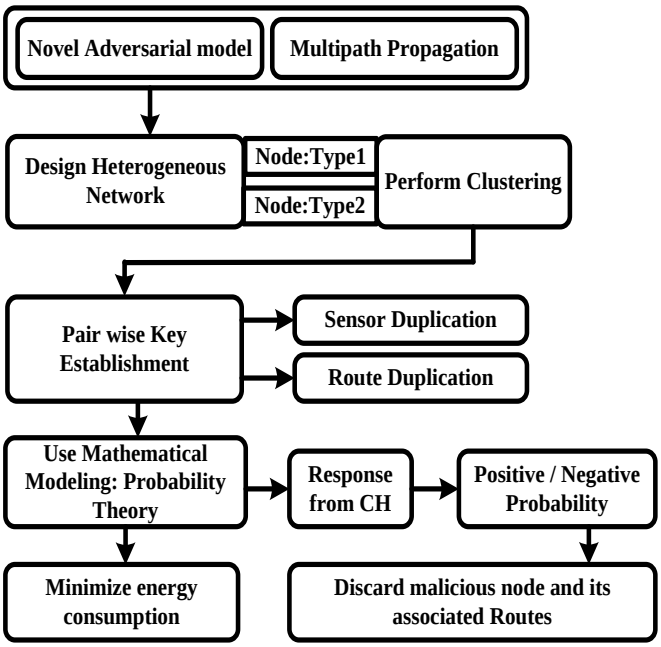

Figure 2 Security model for identifying secure and energy efficient route

The proposed system considers two different kinds of sensor nodes i.e., node type-1 and node type-2, to perform network formation in simulation boundary. The placement of both types of nodes carried out in mixed mode deployment modes, where node type-1 is considered as regular sensor nodes that sense the event in the surroundings and have less resource value. The node than node type-2 is the cluster head node having large resource value, which aggregates data from their member nodes-(node type-1). The mix-mode deployment strategy considered in the proposed system for network formation is depicted in figure 3. In addition, mixed-mode node deployments can ensure an optimal balance between energy consumption and security requirements by using secure and robust authentication mechanisms using Hash-based Message Authentication Codes (HMAC) during the execution of clustering operation and data aggregation. The study also introduces novelty in the clustering process. Unlike existing systems, this study introduces different strategies in the clustering operations i.e., in an asymmetrical manner in view of real-time implementation scenarios. In the proposed authentication mechanism, the system checks whether there is duplication on the WSN nodes and routing path. In this regard, the formulation of strategic models is carried out using probabilistic methods, where the system also verifies whether nodes and paths are malicious with positive and negative probabilities. Therefore, a distributed selection strategy is designed that can efficiently identify hostile nodes. This process is initiated by the CH nodes itself in the network by randomly choosing their adjacent nodes that are basically according to the transmission range of the sensor node. This operation is assisted by all CH nodes who shared their beacon messages to invite adjacent nodes to form a cluster using pair-wise keys. However, more than one response message is identified for particular member nodes, and then it will be considered a vulnerable node and will be immediately prohibited from participating in the communication process.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

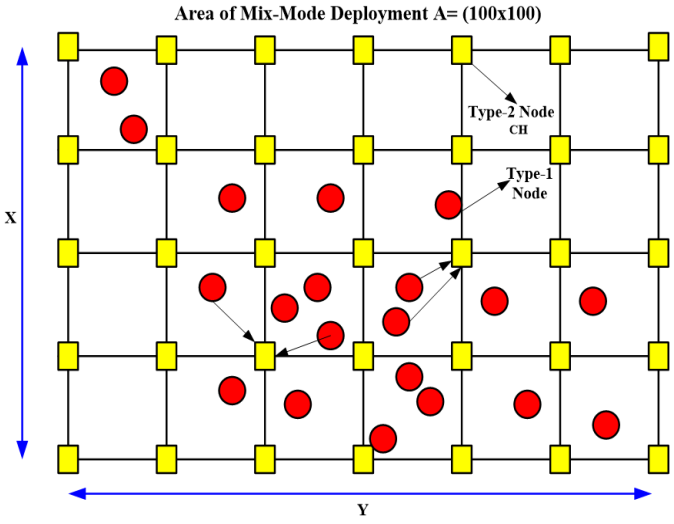

Figure 3 Mix-mode nodes deployment strategy

The modeling of pair-wise key generation uses different key parameters, such as the nodes key public key and encryption based secret key. The public keys are computed based on the product of the public key and Tuple elements. An empirical formulation is carried out to achieve multiple hash functions towards the computation of the pair-wise key. In this process, all WSN nodes must perform verification of their private keys. In addition to this, the CH node also performs cluster key generation process using the pair-wise mechanism for type - nodes that are considered to be members of a particular cluster. This process verifies the authenticity of participating in regular nodes. In this process, the member nodes have the freedom to leave, join a new cluster, or rejoin the same cluster that previously has left. However, when any node joins the new cluster, it must perform all necessary verification operations, which was executed during the initial cluster configuration setup. To maintain security, the CH node will periodically update its cluster key and update it to the base station. Here, the base station is responsible for maintaining the records of all true nodes and compromised nodes that are not supposed to be a part of further communication and other network operations. In this way, the proposed system detects suspicious nodes and secure routes with lower energy consumption.

Algorithm-1: Identification of secure route with higher energy-efficiency

The algorithm takes input as number of nodes and dimension of simulation area A. Then the algorithm executes pair-wise key generation process and clustering operation executed based on a fact where the node resides within a minimum distance. Finally, the algorithm performs the secure data aggregation process prior to the initialization performance metrics to assess efficiency of the proposed security module.

Input: Ntype1, Ntype2, A
Output: Secure DA and Energy Efficient Communication
START
1. Initialize Ntype1, Ntype2, A;
   a. Generate x, y localization under boundary;
   b. Generate coordinates of Type-1 nodes;
   c. Generate coordinates of Type-2 nodes;
2. Perform mixed mode deployment;
3. Perform, Initial KEY Setup;
   a. Init MPKEY, PUBKEY, Crypto(hash);
      i. Concatenate MP_{KEY}, PUB_{KEY}, Crypto(hash);
      ii. PLOT N;
      iii. Formation of a cluster
4. Perform pairing KEY set up
5. Compute pair of $PAR_{P\text{-}KEY}$, $PAR_{PUB\text{-}KEY}$
6. Generate individual node key randomly
7. Perform HMAC, SHA-1 on N_{type1} data.
   a. Perform pairwise KEY generation
      i. For (i←1: Ntype1)
8. COMPUTE Adv.msg
9. COMPUTE dist.
10. End
   a. Connect N_{type1} with N_{type2}
   b. Find out nodes within range
11. Set up communication
   a. Select CH based on proximity
   b. Select the node with minimum dist
12. Perform Data Aggregation
END

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

Initially, the algorithm takes no of Type-1 sensor nodes and type-2 sensor nodes for the deployment of network in simulation area A that exhibits mix mode network formation with different node capabilities to perform communication and data transmission operation in an efficient manner (Line1-2). The algorithm considers system and initial security parameters provided by bases station to perform pair-wise key. Further, it calls key parameter MP_{KEY}, PUB_{KEY} and a cryptography hash function Crypto (hash) to generate public key and encrypted secret key. A pair-wise key generation is carried out based on concatenation process over all the key attributes and then a communication link is established among the nodes that result in full functioning network parameters (Line: 3-10). The algorithm also executes a clustering operation for performing energy efficient and secure data aggregation based on mechanism of pairing KEY followed by computation of partial private and public key towards generation of cluster key. The proposed security model performs hash-based authentication scheme to validate each and every data packet during the data aggregation process and data transmission to base station (Line-10-12).

The descriptions of the symbols used in algorithm-1 are shown below.

Sl. No	Symbol	Description
1	A	Deployment Area
2	Ntype1	No of Sensor Node of Type-1
3	Ntype2	No of Sensor Node of Type-2
4	x, y	Localization of Sensor Nodes
5	DA	Data Aggregation
6	MPKEY	Master Private key
7	PUBKEY	Public Key
8	Crypto(hash)	Cryptographic HASH function
9	N	Network parameter
10	Adv.msg	Advertisement Message
11	dist	Distance
12	PARP-KEY	Partial Private key
13	PARPUB-KEY	Partial Public key
14.	D	DATA
15	MPKEY1	Secret key derived from original key
16	HMAC	Cryptographic Hash

B. Security Module-2 Analytical Model for Optimizing Security Operations

This security module offers an optimal form of strategy towards ensuring maximum security requirements in the network without affecting energy efficiency. It also provides a design of a lightweight encryption mechanism to resist dynamic malicious attacks operates in large-scale deployments. In this work, special consideration is given to the traffic dynamics and node resource to establish a secure communication route in WSN and balance the trade-off between energy demand and network performance. The system considers some initial parameters like time-slot and frame rate. The system also considers node energy, traffic, and buffer time three constraints for the modeling of the security system. In this, the frame rate considered for control message and the initialization of data required for communication. The time-slot attributes are considered to analyze different activities currently being performed within the network. The time slot function can also help recognize various activities in the network in the security view. The routing update process is also controlled and adjusted by the time slot frame, which maintains the maximum-security demands at every moment.

Algorithm-2: Optimizing Security Operations and maintains tradeoff between security needs and energy efficiency

The proposed algorithm performs different operation steps for optimizing security in WSN considering network traffic dynamicity and node energy as prominent constraints. The significant steps of the security module-2 are illustrated as follows:

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

```
Input: n, b, bt, sd
Output: encMsg
Start
    1.  For i=1: n If sd<sr
    2.  Rmat [(i, n+1) (n+1, i)] =1
    3.   [link]→f1(Rmat, α)
    4.  Init sg
    5.  For i=1: n
    6.   obtain secLink
    7.  If j<nsg
    8.   ind→f2(c.g(n)+1¦j.g(n))
    9.   Else
    10. ind→f2(c.g(n))
    11. Init Smsg
    12. msg→msgT
    13. For i=1:64: size(msg)
    14. [encMsg, skey]=f3(msg, skey)
    15. Init AP, sfrm, bt, β
    16. CAT→explore (Brate)
    17.  nβ→f3(size(CAT)* β/100)
    18. Apply encryption
    19. For i+1:n
    20.  h→argmin{ETX→f4(d, data)
    21.  Forward data
End
```

The proposed algorithm first executes the process of initiating communication among the nodes where the system considers number of nodes n, buffer time (bt), base station (b), sensing range (s_r), R_{mat} (structure matrix)and spatial distance ($S_{d)}$. For all sensor nodes in the network the algorithm checks a condition whether the spatial distance among nodes are with the sensing range. based on distance computation the algorithm constructs a connection matrix where information about each node and their neighbor are maintained to establish link between each node followed by another 2D matrix α is which holds information related to recent communication nodes a and node b (line 1-4). The next step of the algorithm is towards formation of secure group. The algorithm initializes a variable that holds parameter values of secure group after which it obtains secure links to form a secure association between nodes and base station. This step is carried out using a matrix which maintains the record of the initial link formation and extracts optimal secure group based on certain conditions. It further executes a condition to check interest of each group towards participating in data transmission process. It addresses the problems associated with a node when it is not found to be optimal for aggregation process; thereby such misbehaving nodes are assigned with an id belonging to particular group. A function f2(x) is applied for performing indexing in terms of a constant c and another function g(n) (line 5-10). After computing all optimal secure groups the algorithm then initiates the process of encrypting node message. In this process, initialization of another variable Smsg (message size) is carried out to store the message in the matrix format. Further, the algorithm computes the transpose of message (msgT)**.**In the next process the algorithm verifies the authenticity of message by checking the parity, where if the key size is found 64-bits, then the algorithm checks for its bit parities else it will additionally add extra bits of the parity check. Here, the significant fact is that the algorithm excludes 8-bit extra parity bits during the process of encryption and decryption which indicates that if a node compromises with this encrypted key of the considered bit size (e.g. 64-bit) then the adversary will always have to check for these additional 8-bit parity to generate the original data. The effort that it originally produces will be other 64-bit key units and mismatches with the original secure key that originated (Line 11-14). The next step of the algorithm is to execute secure communication process. For this process, the algorithm initializes a variables AP (active period), S_{frm} (size of frame), b_t(Secure buffer time), and β (percentage of message criticalness).In the next step the algorithm computes a connection matrix CAT, which is meant for connection arrival time for extracting exact B_{rate} (buffer rate). After which a computation is carried out for generating node identity with respect to size of the CAT (connection arrival time) which refers to message weight age or priority level of the message. In addition, the proposed algorithm also implements a light-weight encryption to protect all data packets shared between nodes in a secure manner. The algorithm also computes the transmittance energy of each sensor node E_{TX} to determine most optimal secure path for data transmission to final destination. Here it checks the two different conditions of distance and energy demand before performing communication.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

The descriptions of the symbols used in algorithm-2 are shown below.

Sl. No	Symbol	Description
1	n	Number of sensors
2	b	Base station
3	b_t	Secure buffer time
4	s_d	Spatial distance
5	s_r	Sensing range
6	R_{mat}	Structure matrix
7	α	2-D matrix
8	s_g	Secure group
9	nsg	Eligible secure groups
10	g(n)	function
11	S_{key}	Secret key
12	S_{frm}	Size of frame

VI. RESULT ANALYSIS

The proposed study has presented a cost-effective integrated framework of security for enabling secure environment for communication and data transmission considering dynamic attacking scenario also energy and uncertain traffic condition as prominent constraints. The study has used design of light-weight encryption mechanism and cryptography hash function based secure authentication. The design and implementation of the introduced system is carried out on numerical computing tool. This section presents quantified outcome analysis of the proposed system. The independent variables for the proposed systems outcome analysis is mentioned in table1.

Table 1Independent Variables and its values for Algorithm-1

Independent Variables	Values
No. of Type-1 nodes	100
No. of Type-2 nodes	16
$T_{backoff}$(0-20)	5
T_{hold}(0-1000)	500

The outcome of algorithm-1 for the identification of secure route with higher energy-efficiency is assessed in terms of processing time required for cluster key- update and energy consumption in the process of pair-wise key generation.

Table 2 Quantified Outcome Analysis for processing time required for cluster key update

Iteration	**Processing Time Required for Cluster Key Update**				
	V-1m/sec	**V-2m/sec**	**V-4m/sec**	**V-8m/sec**	**V-16m/sec**
0	1.09	1.86	2.96	4.8	8.68
20	1.2	1.81	3	4.75	8.5
40	1.98	1.87	3.06	4.5	4.16
60	1.19	1.70	2.8	3.39	3.19
80	1.1	1.64	2.5	2.5	2.49
100	1.09	1.61	2	2.1	2
120	1.06	1.59	2	1.8	1.59
140	1.08	1.51	1.7	1.7	1.54
160	1.03	1.48	1.71	1.7	1.71
180	1.02	1.29	1.29	1.29	1.3
200	1	1.29	1.3	1.3	1.31

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

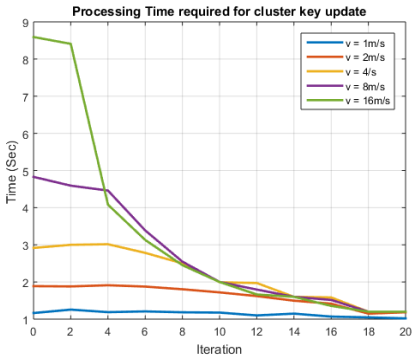

Figure 4 Iteration v/s Processing Time (Sec)

Table 2 shows the quantified value of the outcome for processing time performance of the proposed system for the cluster key update with different sensor node mobility speed. The closer analysis from figure 4 shows that even the mobility of nodes increases, the proposed system does not take much processing time over an increasing iteration, which indicates that better energy utilization by the system. The updating of the cluster-key process executes the member nodes of any cluster leaves or joins any cluster. However, neither any nodes leave or join the cluster then the CH itself executes periodic updates.

Table 3Quantified Outcome of Energy Consumption during Pair wise Key Establishment

Iteration	**Energy Consumption (Joule) Required for Pair Wise Key Establishment**				
	V-1m/sec	V-2m/sec	V-4m/sec	V-8m/sec	V-16m/sec
0	8	13.2	17	24	35
100	7.9	13.0	15	18	17
200	6	13	15	14	13
300	7	14	12.7	14	10.8
400	6	11	12.7	13	8.7
500	8	10.9	12.8	14	8.8
600	8	10.9	12	12	8.8

In table 2 and 3 V-1m/sec, V-2m/sec, V-4m/sec, V-8m/sec and V-16m/sec illustrates velocity of mobile sensor nodes.

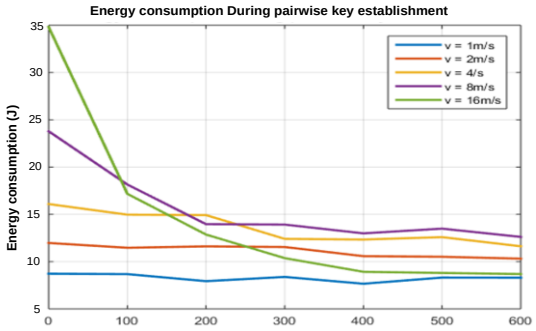

Figure 5 Iteration v/s Energy Consumption (J)

Table 3 exhibits the quantified values for assessing the performance of the proposed algorithm-1 in terms of energy consumption during the pair-wise key generation operation. A closer analysis from figure 5 shows that the introduced system security module-1 does not consume much energy for the pair-wise key generation and can process secure data transmission faster. The algorithm introduced can also achieve the optimal balance between security and energy consumption. The proposed algorithm does not involve any form of complex computations and does not include repetitive key-generation processes. Therefore, due to the lightweight security operation, the system only needs to store the key of the hash function in the sensor memory; therefore, the algorithm-1 responses faster. In order to justify this algorithmic response time, the study also carried a comparative assessment of algorithm processing time, considering comparison with the existing method Sec-LEACH.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

Table 4Quantified outcome for algorithm processing time assessment

Iteration	Algorithm Processing Time (sec)	
	Proposed System	Existing System
10	0.9	1
50	2	2
100	0.8	3
150	0.8	2
200	1.9	4
250	1	7.8
300	2	9.2
350	5	10
400	10	14

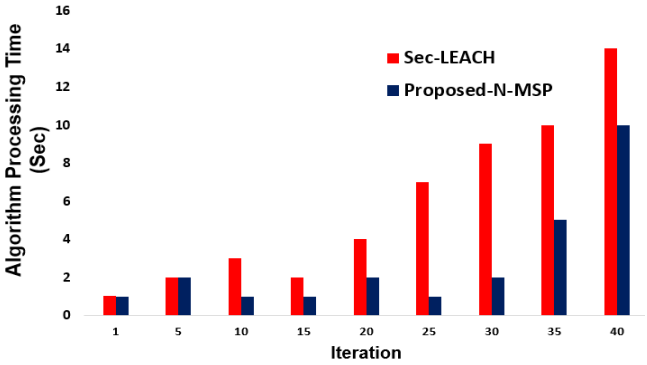

Figure 6 Analysis of Algorithm Processing Time (Sec)

Table 4 exhibits the quantified outcome for the assessment of the processing time performance of the proposed system. A closer analysis from figure 6 shows that proposed algorithm-1 attains good performance compared to existing Sec-LEACH. The system takes an average time of 2.71 seconds to execute security operations for identifying a secure and energy-efficient route, and the existing system takes 9.22 seconds to perform their operation.

Table 5Quantified outcome End-to-End Delay Analysis

Buffer Time	End-to-End Delay		
	Proposed System	SEEM	Flexi-Cast
1	26	28	37
2	13	14	16
3	7	10	12
4	6	7	8
5	5	6	7
6	4.5	5.8	6
7	4.2	5.2	5.9
8	4	5	5.2
9	3.5	4.9	5
10	3	4	4.9

The Table 5 shows quantified outcome of the proposed algorithm-2in terms of End-to-End delay.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org
Article Received: 26/08/2024 Revised: 10/09/2024 Accepted: 17/09/2024

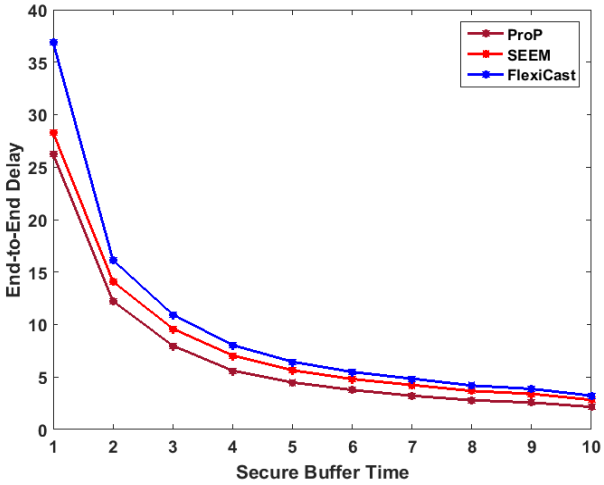

Figure 7Comparative Analysis of End-To-End Delay

A closer analysis from figure 7 can be analyzed that the proposed algorithm-2 (ProP) shows reduced delay with respect to Secure Buffer Time compared to the existing system. The existing method SEEM [30] associated with heavier and complex computations in the route maintenance process, which results in degradation of the communication performance. On the other hand, the existing method Flexi-Cast [31] uses the Bloom Filters by authenticating fingerprints with two-layer of validation procedures. Therefore, Flexi-Cast reaches to better security level compared to the existing method SEEM, but Flexi-Cast exhibits increased delay compared to SEEM and proposed algorithm-2.

VII. CONCLUSION

The proposed study has presented a computationally efficient model that provides lightweight security operations based on secure hash function based authentication and lightweight encryption based secure data transmission in the WSN. The proposed security model focuses on the security associations between WSN nodes and the selection of reliable routes for secure data transmission. The development of the proposed security model is carried out in such a way that it is not associated with greater use of complex security operations, robust and can extend the duration of network services, even in the presence of adversaries, thereby providing secure data transmission in the network. In addition, the design of the proposed security model is best suited for homogeneous and heterogeneous sensor networks, which will be robust to any attacking scenario.

REFERENCES

[1] Khan, S. &Pathan, A.-S.K. & Alrajeh, N.A (2016). Wireless sensor networks: Current status and future trends.
[2] S. R. Jino Ramson and D. J. Moni, "Applications of wireless sensor networks — A survey," 2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT), Coimbatore, 2017, pp. 325-329, DOI: 10.1109/ICIEEIMT.2017.8116858.
[3] Mohamed, Reem E., et al. "Survey on wireless sensor network applications and energy efficient routing protocols." *Wireless Personal Communications* 101.2 (2018): 1019-1055.
[4] BenSaleh, Mohammed Sulaiman, et al. *"Wireless Sensor Network Design Methodologies: A Survey"* Journal of Sensors 2020 (2020).
[5] Butun, Ismail, Salvatore D. Morgera, and Ravi Sankar. "A survey of intrusion detection systems in wireless sensor networks" *IEEE communications surveys & tutorials* 16.1 (2013): 266-282.
[6] Jain, Manoj Kumar. "Wireless sensor networks: Security issues and challenges." *International Journal of Computer and Information Technology* 2.1 (2011): 62-67.
[7] T. Azzabi, H. Farhat and N. Sahli, "A survey on wireless sensor networks security issues and military specificities," 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET), Hammamet, 2017, pp. 66-72, DOI: 10.1109/ASET.2017.7983668.
[8] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," in IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006, DOI: 10.1109/COMST.2006.315852.
[9] Gonçalves, Danilo De Oliveira, and Daniel G. Costa. "A survey of image security in wireless sensor networks" *Journal of Imaging* 1.1 (2015): 4-30.
[10] M. Ebrahim and Chai Wai Chong, "Secure Force: A low-complexity cryptographic algorithm for Wireless Sensor Network (WSN)," 2013 IEEE International Conference on Control System, Computing and Engineering, Mindeb, 2013, pp. 557-562, DOI: 10.1109/ICCSCE.2013.6720027.

[11]. Mahidhar, Rashmi, and Archana Raut. "A Survey on Scheduling Schemes with Security in Wireless Sensor Networks" *Procedia Computer Science* 78 (2016): 756-762.
[12]. Upadhyaya, Shuchita. "Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks." *Procedia Computer Science* 70 (2015): 808-813.
[13]. Kabashkin, Igor, and Jörg Kundler. "Reliability of Sensor Nodes in Wireless Sensor Networks of Cyber Physical Systems" *Procedia Computer Science* 104 (2017): 380-384.
[14]. Lu, Huang, Jie Li, and Mohsen Guizani. "Secure and efficient data transmission for cluster-based wireless sensor networks." *IEEE transactions on parallel and distributed systems* 25.3 (2014): 750-761.
[15]. Ghosal, Amrita, Sanjib Sur, and Sipra DasBit. "μSec: a security protocol for unicast communication in wireless sensor networks." *Data Privacy Management and Autonomous Spontaneous Security"*. Springer, Berlin, Heidelberg, 2013, pp258-273.
[16]. Yu, Jun, and Xueying Zhang. "A cross-layer wireless sensor network energy-efficient communication protocol for real-time monitoring of the long-distance electric transmission lines." Journal of Sensors 2015 (2015).
[17]. Zhu, Xiaojuan, et al. "Transmission reliability evaluation for wireless sensor networks." *International Journal of Distributed Sensor Networks* 12.2 (2016): 1346079.
[18]. Teng, Haojun, et al. *"Adaptive transmission power control for reliable data forwarding in sensor based networks*", Wireless Communications and Mobile Computing2018 (2018).
[19]. Chidean, Mihaela I., et al. "Energy efficiency and quality of data reconstruction through data-coupled clustering for self-organized large-scale WSNs." *IEEE sensors journal* 16.12 (2016): 5010-5020.
[20]. Hu, Chunqiang, et al. "Secure and efficient data communication protocol for wireless body area networks." *IEEE Transactions on Multi-Scale Computing Systems* 2.2 (2016): 94-107.
[21]. Biswas, K., Muthu Kumarasamy V., Sithirasenan, E., & Singh, K. Energy Efficient Routing and Secure Data Communication in Wireless Sensor Networks.
[22]. Li, Fagen, Yanan Han, and Chunhua Jin. "Practical signcryption for secure communication of wireless sensor networks" *Wireless Personal Communications* 89.4 (2016): 1391-1412.
[23] Manjunath B E and P V Rao, "Trends of Recent Secure Communication System and its Effectiveness in Wireless Sensor Network" in International Journal of Advanced Computer Science and Applications (IJACSA) Volume 7, No. 9, 2016, (Thomson Reuters Indexed).
[24]. Liu, Zhi-xin, et al. "Balance energy-efficient and real-time with reliable communication protocol for wireless sensor network." *The Journal of China Universities of Posts and Telecommunications* 20.1 (2013): 37-46.
[25]. Mondal, Satyajit, Sraban Kumar Mohanty, and Sukumar Nandi. "Energy efficient secure communication architecture for wireless sensor network" *Security and Communication Networks* 9.16 (2016): 3314-3323.
[26]. Vaseghi, Behrouz, Mohammad Ali Pourmina, and Saleh Mobayen. "Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control." *Nonlinear Dynamics* 89.3 (2017): 1689-1704.
[27] Manjunath B E and P V Rao, "Balancing Trade-off between Data Security and Energy Model for Wireless Sensor Network" in International Journal of Electrical and Computer Engineering (IJECE), Volume 8, No. 2, April 2018, pp. 1048-1055.
[28] Manjunath B E and P V Rao, "Unique Analytical Modelling of Secure Communication in Wireless Sensor Network to Resist Maximum Threats" in International Journal of Advanced Computer Science and Applications (IJACSA), Volume 10 Issue 2, March 2019.
[29]. Yu, Hong, et al. "Enabling end-to-end secure communication between wireless sensor networks and the Internet." *World Wide Web* 16.4 (2013): 515-540.
[30] N Nasser, Y. Chen, "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Elsevier, Vol. 30, pp. 2401-2412, 2007
[31] J. Lee, L. Kim and T. Kwon, "FlexiCast: Energy-Efficient Software Integrity Checks to Build Secure Industrial Wireless Active Sensor Networks," in IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 6-14, Feb. 2016.