Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 5563-5579

Research Article

Kriging Regressive Pseudo Randomized Lamport Certificateless Signcryption based Replication Attack Detection for Secure Routing in WSN

[1]D.Sudhakar, [2]Dr.V.S.Meenakshi

[1]Asst.Prof, Bishop Appasamy College of Arts and Science, Coimbatore-18.
sudhakar.dr@gmail.com

[2]Asst.Prof, PG & Research Department of Computer Science, Chikkanna Govt. Arts College, Tirupur-2.
meenasri70@yahoo.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

ABSTRACT : A Wireless Sensor Network (WSN) includes small, low-cost, and resource-constrained sensor nodes to perform monitoring. Each node is free to move and susceptible to various attacks. Therefore, WSNs have huge attention to communication security. Identifying and monitoring attack node is complex in distributed network and creates node replication attacks in WSN. In order to improve secure routing, a novel technique called Kriging Regressive Attack Detection based Pseudo Randomized Lamport Certificateless Signcryptive Secure Routing (KRAD-PRLCSSR) is proposed. KRAD-PRLCSSR enhances the secure routing by detecting the replication attack in WSN. Initially, the neighbor discovery is performed using the Kriging Regression function. Energy of every sensor node is calculated and validates with threshold value. Based on estimated results, normal node or replica node is identified. Then the normal node is chosen as neighboring node. After that, secure transmission is performed using Pseudo Randomized Lamport one-time Generative Certificateless Signcryption. By applying the signcryption technique, Pseudo Randomized private and public keys are generated for each sensor node. After the key generation, the source node performs the encryption as well as a digital signature. The encrypted data and signature are sent to receiver. Finally, signature is verified at the receiver side to decrypt the data. This helps to increase the security of routing in WSN. The simulation analysis of KRAD-PRLCSSR technique is performed with the different metrics.

Keywords: WSN, secure routing, Replication Attack Detection, Kriging Regression, Pseudo Randomized Lamport one time Generative Certificateless Signcryption

1. INTRODUCTION

WSN comprises variety of nodes that mutually senses physical or environmental characteristics and that information is sending to sink node. It is applied in many applications namely health-care, battle-field, industry, and so on. Owing to dynamic broadcasting nature of WSN, it is vulnerable to various attacks. Among many attacks, one of the general attacks is a replica attack since it assists attackers to perform other attacks. Thus, it difficult to design an efficient security system in WSN. To resolve these issues, an efficient KRAD-PRLCSSR is proposed.

A lightweight replica node detection mechanism was developed in [1] using three-step process to discover the replica nodes with lesser false detection probability. However, the higher security of data delivery was not achieved. An Exponential Moving Average (EMA) model was introduced in [2] for replica node attack detection. But any cryptographic method does not enhance secure data delivery and reduce the packet loss.

A Localization technique uses received signal strength (RSSI) and the Triangulation method was introduced in [3] for Replica detection. But the performance of delay was not minimized. A location similarity-based detection method was introduced in [4] to find the node replica attack with lesser computational, and storage overhead. However, the attack detection accuracy was not improved. In [5], An Advanced eXtremely Effective Detection (AXED) of replica nodes was developed with lesser overhead. The designed algorithm detects the replica nodes faster but it failed to increase the security level.

A location and trust-based replica detection (LTBRD) technique was developed in [6] to find the replication attack. The designed technique increases the attack detection probability and minimizes the network delay. But, packet delivery ratio was minimal. A distributed replica detection scheme was introduced in [7] for MWSNs using the Sliding window concept. Through the designed technique increases the number of packets received, the performance of delay was not minimized.

A multi-tree architecture was designed in [8] for finding injected replica nodes to network through avoiding adversary. But architecture has more time for detecting the replication attack detection. Elliptical curve cryptography was developed in [9] to provide security by finding the replicated nodes for preventing the WSNs. However, the designed cryptographic algorithm failed to use the signature generation for achieving higher security. An efficient lightweight security mechanism was introduced in [10] to mitigate security issues by finding the replication attack node in WSNs. But it failed to explain how the source node finds out and select its immediate neighboring nodes.

1.1 Contributions

The major contributions of KRAD-PRLCSSR technique are given below,

- To increase the security of routing in WSN, a novel KRAD-PRLCSSR technique is introduced based on the Kriging Regression and Pseudo Randomized Lamport one-time Generative Certificateless Signcryption.
- The Kriging Regression function is applied to measure the energy level of the sensor node with the threshold value. Based on the estimated results, the normal node or attack node is detected. The source node finds the energy-efficient neighboring node for data transmission. This helps to increase the attack detection accuracy.
- To increase the packet delivery ratio, a Pseudo Randomized Lamport one-time Generative Certificateless Signcryption is applied. For each selected node, a key pair is generated based on the Pseudo-Random number. Then the encryption and signature generation is performed. At the receiver end, signature verification is performed to decrypt the original data. This helps to minimize the data loss of secure transmission.
- Finally, an extensive simulation is conducted to estimate the performance of our KRAD-PRLCSSR technique and other related works. The simulation result demonstrates that our KRAD-PRLCSSR technique is highly efficient than the other methods.

1.2 Paper organization

The rest of KRAD-PRLCSSR technique is categorized into different sections as below. Section 2 elaborates the existing works in identifying replication attack nodes in WSN. Section 3 describes the KRAD-PRLCSSR. Section 4 describes simulation settings followed by implementation procedure is presented. The result evaluation and discussion of outcomes are discussed in Sections 5, and KRAD-PRLCSSR is concluded in Section 6.

2. RELATED WORKS

In [11], a Secure Elliptic curve based chaotic key Galois cryptography-based Routing method was presented depends on Energy. The designed routing technique reduces the packet loss but the delay was not minimized. A hybrid local and global detection method was developed in [12] for increasing the detection probability of replication attack with lesser overhead. However, the performance security level was not improved. The hybrid clone node detection (HCND) method was introduced in [13] to identify the clone attack node with higher precision and lesser false positive rate. But the performance of packet loss rate was not minimized.

A comprehensive version of the multi-level replica detection method was developed in [14] based on danger theory. But, performance of delay was more. A secure random key distribution (SRKD) method was introduced in [15] for attack detection and improving security. However, energy-efficient attack detection was not performed.

A key management system was introduced in [16] to enhance security and reduces energy. However, it failed to increase the attack detection accuracy. An ant colony optimization technique [17] discovers the clone attack. But, delay was not reduced.

A novel distributed clone detection protocol was designed in [18] with lesser resource utilization. The designed protocol increases the detection probability, but the higher packet delivery ratio was not achieved. A convolutional technique (CT) was developed in [19] that increase the security using convolutional codes to avoid the attack node on WSNs. The designed technique reduces the computational complexity of attack detection but the accuracy was not improved.

An Enhanced Fuzzy C means and Adaptive Scheduling technique was developed in [20] to improve the energy-efficient secure routing. The designed technique enhances packet delivery ratio and minimizes delay.

3. PROPOSAL METHODOLOGY

WSNs consist of many small and inexpensive sensor nodes. In WSN, high-level security is an essential factor for both static and dynamic environments. But, WSN is highly vulnerable to numerous attacks owing to dynamic environment. Here the replication attack is considered for secure routing in WSN. Node replication attack is general attacks in WSNs. In replication attack, adversary captures sensor nodes which is deployed in the distributed network and extracts the entire significant information and functions to create replica nodes. The generated replica nodes include accurate information such as ID of captured sensor node. The adversary dispenses generated replica nodes in WSN. After that, it interrupts network transmission operation by creating several malicious nodes which include similar ID as that of captured nodes. Because malicious nodes (i.e., replica nodes) deliberately disturb the network operation and also introduce false data and destroy operation of normal sensor node operation, data aggregation, and so on.

When a node replication attack is initiated by an adversary the WSN in, the security of transmission is affected strictly based on two causes. First, if any efficient attack detection scheme is not employed to recognize replicas using an efficient encrypt, decrypt, and authentication. Next, when detection probability of conventional detection method employed is minimal to discover clones or replicas. Motivated by this, a novel KRAD-PRLCSSR technique is introduced to identify replica nodes with higher accuracy.

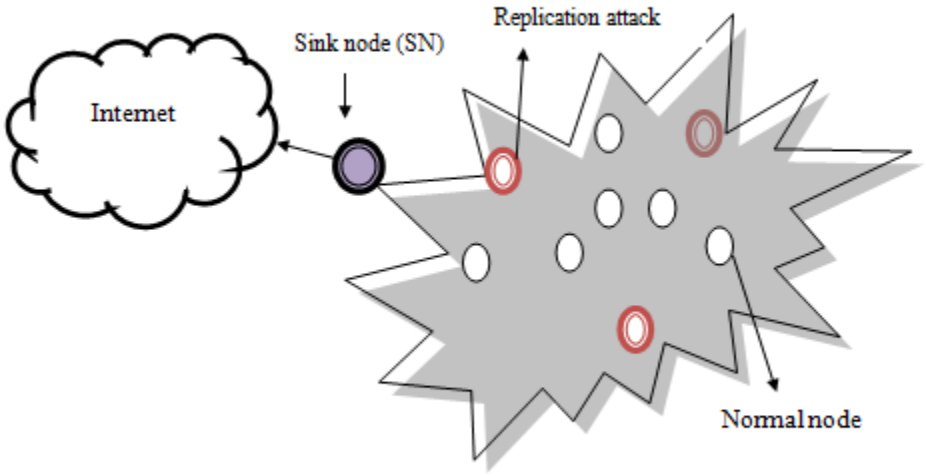


Figure 1 Wireless sensor network with replication attack

Figure 1 illustrates the architecture of the WSN with sensor nodes '$Sn_1, Sn_2, Sn_3, \ldots Sn_n$', one sink node '$SN$', replication attack node 'RN'. Therefore, a number of sensor nodes in distributed WSN connect to internet via sink node 'SN'. The WSN is organized in a graphical model '$G(v, e)$' where 'v' shows the vertices i.e. sensor nodes positioned in WSN and 'e' stands for connection between the sensor nodes in WSN. In WSN, defines source

node and transmits data packets '$d_1, d_2, .., d_m$' to sink via the energy-efficient neighboring nodes $Nn_1, Nn_2, Nn_3, \ldots Nn_b$ in a secured manner.

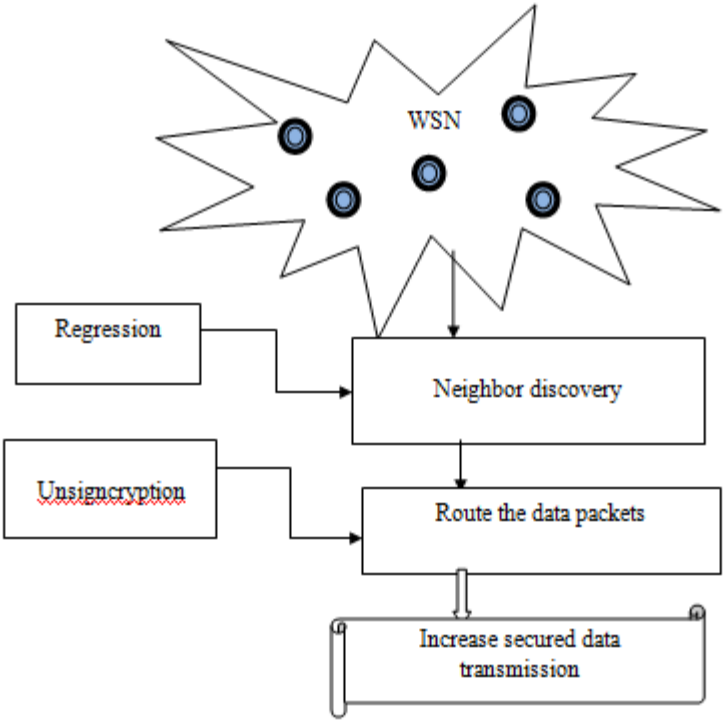


Figure 2 Architecture diagram of proposed KRAD-PRLCSSR technique

Figure 2 illustrates architecture diagram of proposed KRAD-PRLCSSR technique to perform accurate attack detection in WSN. The proposed KRAD-PRLCSSR technique performs two processes namely neighbor discovery and secure data transmission. At first, the neighbor discovery is performed by applying the kriging regression technique. Initially, the residual energy of sensor node is calculated. Node with higher energy nodes is called a normal node. The remaining nodes are said to be a replication node. Followed by, secure routing is performed through the Certificateless Signcryption. This helps to increase the replication node attack detection rate with minimal time. A brief description of KRAD-PRLCSSR is presented in below subsection.

3.1 kriging regression-based Replication attack detection

The proposed KRAD-PRLCSSR technique first performs the attack detection using the kriging regression function. The kriging regression analysis is a machine learning technique used for estimating the relationships between the variables. Initially, residual energy of node is measured. Firstly, entire sensor nodes have a similar energy level. Due to the sensing and monitoring nature of the nodes, the initial energy level gets reduced. The remaining energy is represented as below,

$$E_{RL} = [E_{TT}] - [E_C] \quad (1)$$

From (1), E_{RL} denotes residual energy of nodes ,E_{TT} shows total energy of node and E_C symbolizes consumed energy of nodes. Based on energy level, the neighboring nodes are identified as normal or replication attack node. The Kriging regression is the machine learning technique to analyze the respective feature values.

$$R_K = e^{\left(\frac{E_{RL}-E_{th}}{2d^2}\right)} \quad (2)$$

Where, R_K denotes a regression function, E_{RL} denotes a residual energy level, E_{th} denotes a threshold for residual energy, 'd' indicates a deviation. The regression provides the values ranges from 0 to 1

$$\boldsymbol{Y} = \begin{cases} R_K > Th\ ; & Normal\ node \\ Otherwise; & replication\ node \end{cases} \quad \textbf{(3)}$$

Where, Y denotes an output, R_K denotes a regression function, Th indicates the threshold. If the regression outcome is higher than threshold, then node is a normal node. Otherwise, the node is said to be a replication node. The Replica nodes with various fake identities utilize the extra energy than the normal sensor nodes. In case of periodic events, kriging regression differentiates the replica and normal sensor nodes depend on difference between residual energy and threshold residual energy. To initiate replica attack in WSN, extra energy is exhausted by replica nodes. While distributing the replica node, energy consumption is enhanced in creation of fake identity. Thus, when number of attacker node enhances, energy consumption is enhances. Therefore, the source node selects the normal node as a neighboring node to route the data packets.

// Algorithm 1: kriging regression based Replication attack detection

Input: Number of sensor nodes $Sn_1, Sn_2, Sn_3, \ldots Sn_n$

Output: Increase the attack detection accuracy

Begin

For each Sn

Measure residual energy 'E_{RL}'

Measure the Kriging regression 'R_K'

If $(R_K > Th)$ **then**

'Sn' is said to be a normal node

else

'Sn' is said to be a replication node

End if

Select the normal node as a neighboring node

End for

End

From above algorithm, the replication nodes among the entire nodes in WSN have identified accurately. The node replica is identified by using the kriging regression based on the residual energy. For each sensor node in WSN, residual energy is estimated and it verifies that the threshold value. Finally, the regression value is validated with the threshold. The regression value is higher than the threshold is said to be a normal node and the other nodes are said to be a replica node. In this way, the replication attacks and the normal nodes are correctly detected with higher accuracy. With the selected normal node, the secure data packet transmission is performed. This increases packet delivery and minimizes the packet loss.

3.2 pseudo-randomized Lamport one-time generative Certificateless Signcryption based secure routing in WSN

The secure routing is performed using pseudo-randomized Lamport one-time generative Certificateless Signcryption. A Certificateless signcryption is a relatively novel cryptographic technique that helps to perform the functions of a digital signature as well as encryption and it effectively decreases the computational costs

in comparison with the conventional signature-then-encryption methods. Certificateless is public-key cryptography where public key and private key is employed for encryption and decryption.

Signcryption is typically included three different processes namely Key Generation, Signcryption, and Unsigncryption. In the key generation, the private and public key of each sensor node is generated. Next, the signcryption process is carried out to perform both encryptions as well as digital signature generation. Finally, the unsigcryption is performed to decrypt the ciphertext after verifying the signature. Based on the above-said processes, secure routing is performed in WSN.

3.2.1 Pseudo randomized Key generation

Initially, the algorithm generates a pair of keys for each sensor node. The generated keys are used for both encryptions as well as decryption. The proposed algorithm uses positive random numbers for the key generation process. In other words, a different pair of keys is generated every time. It helps to improve the security of data transmission.

$$K_p = N = [a\ b\ c\ d] \qquad (4)$$

From (4),K_p represents a private key and it is chosen randomly. Here, $N\epsilon\ a\ b\ c\ d$ denotes different random integers. After generating the private key, the public key is generated as given below,

$$K_b = Q(N) \quad (5)$$

From (5),K_b indicates a public key, $Q(N)$ denotes a one-way function is a function that is simple to compute on every input as given below

$$Q(N) = N + (1\ mod\ 16) \quad (6)$$

The public keys are used as Node_ID and distributed but the private key is kept secret. In this way, the key pairs are generated for each node in routing process in WSN.

3.2.2 Signcryption

In this phase, both encryption and signature generation process is carried out for secure data transmission. Signcryption process performs both encryptions as well as digital signature generation. Encryption process is changing the input data into an unreadable format (i.e. ciphertext). A digital signature is created from data and secret key (i.e. private key) known only by the sender. The block diagram of these process are illustrated as given below,

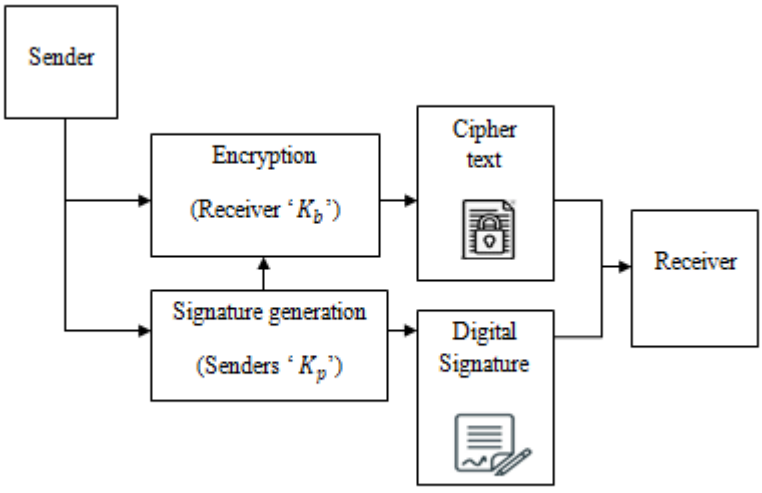


Figure 3 Block diagram of the encryption and digital signature generation

Figure 3 portrays the process of encryption as well as digital signature generation. Consider number of data packets $d_1, d_2, .., d_m$. The sender node performs the encryption with receiver's public key. Encryption process is obtained as follows,

$$C \leftarrow Ep\{K_b, d\} \quad (7)$$

Where C denotes a ciphertext, Ep represents encryption with the public key (K_b) of the receiver i.e. node_ID, 'd' indicates the data packets. Accordingly, a digital signature is generated for each data transmission with a sender's private key (i.e. secret key). A valid digital signature is used to believe that the data was created by an authorized sender (i.e. normal node). This helps to ensure that the transmitted data was not altered by any attacker nodes.

A signature is generated with the sender's private key. Let us consider, the data' 'be a positive integer and it converted into the binary string i.e. (0, 1) and the signature is generated as follows,

$$\varphi_d = [P_{ij}] \quad (8)$$

From (8),φ_d represents the signature of the data'd', P_{ij} indicates a position of the private key of the sender where 'i' varied from $(0 < i < r)$ where 'r' be a positive integer and $j \in (0,1)$. After generating the signature, the sender transmits the ciphertext and the signature to the next neighboring node.

3.2.3 Unsigncryption

Upon receiving the ciphertext, the unsigncryption is performed to attain the original data. At first, the signature verification is presented.

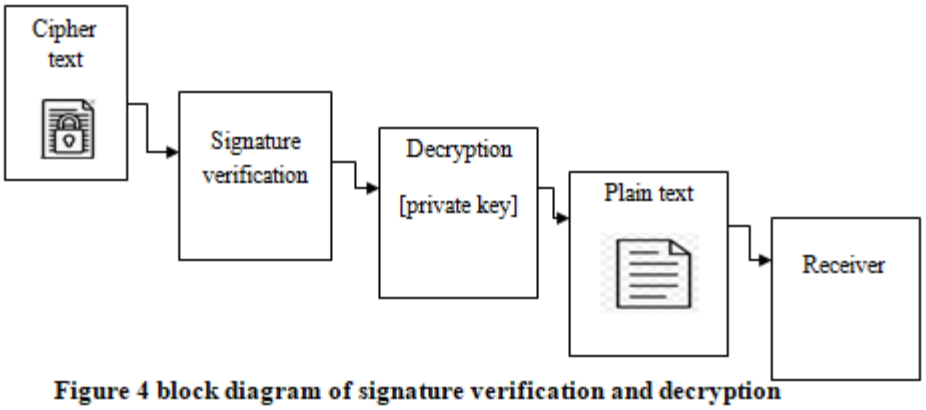


Figure 4 block diagram of signature verification and decryption

Figure 4 shows the block diagram of signature verification and decryption. At first, signature verification is presented with public key to obtain plain text. At the receiver side, the new signature is generated as given below,

$$\varphi_d(n) = Q(\varphi_d) \quad (9)$$

$$Q(\varphi_d) = \varphi_d + 1 \; mod \; 16 \quad (10)$$

From (9),$\varphi_d(n)$ denotes a newly generated signature at the receiver, $Q(\varphi_d)$ denotes a one-way function of the signature 'φ_d'. Finally, the generated signature is $\varphi_d(n)$ is verified with the public key K_b. When the signature

gets matched, it is valid and receiver node decrypts ciphertext. Or else, signature is not valid. In this case, receiver does not decrypt ciphertext,

$$d \leftarrow Dp\{K_p, C\} \quad (11)$$

Where,'d 'denotes original data, 'Dp' denotes decryption, K_p indicates private key of receiver, C represents ciphertext. As a result, the original data is obtained at the receiver. In this way, secure routing is performed among source and sink node.

// Algorithm 2 pseudo-randomized Lamport one time generative Certificateless Signcryption based secure routing in WSN

Input: Number of data $d_1, d_2, d_3, \ldots d_m$,

Output: Increase the security of routing

Begin

For each data transmission 'd_i'

For each sensor node 'Sn'

Generates a private and public key 'K_p and K_b

End for

// Signcryption

Encrypt the data using public key $C \leftarrow Ep\{K_b, d\}$

Generate digital signature 'φ_d'

Send to neighboring node

// Unsigncryption

Generate digital signature $\varphi_d(n) = Q(\varphi_d)$

Signature is verified with the public key

If the signature is valid **then**

Decrypt the data using private key $d \leftarrow Dp\{K_p, C\}$

Obtain original data 'd'

End if

End for

End

Algorithm 2 portrays the different processes of pseudo-randomized Lamport one-time generative Certificateless Signcryption based secure routing in WSN. At first, the private and public keys are generated for each sensor node. With the generated keys, the encryption and the signature generation is performed and sent to receiver. In receiver side, signature is again generated and verified with the public key. Finally, the receiver decrypts plaintext and attains original data. This enhances security of data transmission and minimizes packet loss.

4. SIMULATION SETTINGS

Performance of KRAD-PRLCSSR technique, Lightweight replica node detection mechanism [1], EMA model [2] is implemented in NS3. 500 sensor nodes are arbitrarily deployed over a squared area of A^2 (1100 m * 1100 m). In the simulation system, a random waypoint is employed as a mobility model to perform secure routing in WSN. The Ad hoc on-demand distance vector routing protocol (AODV) identify node replication attack in WSN. Simulation time is 300 seconds and sensor nodes' speed is varied from 0-20m/s. The various parameters are listed in table 1.

Table 1 Simulation Parameters

Simulation Parameters	Values
Simulator	NS3
Network area	1100 m * 1100 m
Number of sensor nodes	50,100,150,200,250,300,350,400,450,500
Mobility model	Random Waypoint model
Number of data packets	25,50,75,100,125,150,175,200,225,250
Speed of node	0 – 20 m/s
Simulation time	300s
Number of runs	10
Protocol	AODV

4.1 Implementation scenario

In this section, implementation of KRAD-PRLCSSR is discussed using a mathematical model. Let us consider the total energy of a single sensor node is $E_{TT} = 10 Joule$, Consumed energy $E_C = 3\ Joule$

$$E_{RL} = [E_{TT}] - [E_C] = 10 - 3 = 7\ Joule$$

. Based on the energy level, the neighboring nodes are identified as normal or replication attack node. The Kriging regression is the machine learning technique to analyze the respective feature values. Let us consider the residual energy$E_{RL} = 8 Joule$, threshold energy is $E_{th} = 8 Joule$

$$R_K = e^{\left(\frac{E_{RL}-E_{th}}{2d^2}\right)} = e^{\left(\frac{7-8}{2*1^2}\right)} = e^{\left(-\frac{1}{2}\right)} = e^{(-0.5)} = 0.606$$

Let us consider the threshold $Th = 0.5$

$$\boldsymbol{Y} = \begin{cases} R_K > Th\ ; & Normal\ node \\ Otherwise; & replication\ node \end{cases}$$

$$\boldsymbol{Y} = \begin{cases} 0.606\ > 0.5\ ; & Normal\ node \\ Otherwise; & replication\ node \end{cases}$$

If the regression outcome is higher than threshold (0.5), then the node is normal node. Then the source node considers the normal node as a neighboring node for data transmission.

Pseudo randomized Key generation

Initially, the algorithm generates a pair of keys for each sensor node. Let us consider the set of positive integer random numbers hence it is called a private key.

$$K_p = N = [a\ b\ c\ d\ ]$$

$$N = [2\ \ 5\ \ 6\ \ 0\ ]$$

After generating the private key, the public key is generated as given below,

$$K_b = Q(N)$$
$$Q(N) = N + (1\ mod\ 16)$$
$$N = [2\ \ 5\ \ 6\ \ 0\ ]$$
$$Q(N) = 2 + 1\ mod\ 16 = 2 + 1 = 3$$
$$Q(N) = 5 + 1\ mod\ 16 = 5 + 1 = 6$$
$$Q(N) = 6 + 1\ mod\ 16 = 6 + 1 = 7$$
$$Q(N) = 0 + 1\ mod\ 16 = 0 + 1 = 1$$
$$K_b = Q(N) = [3\ 6\ 7\ 1\ ] \dashrightarrow \text{Public key}$$

Signcryption

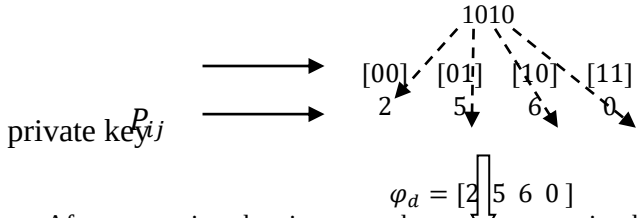
The encryption process is obtained as follows,

$$C \leftarrow Ep\ \{K_b, d\}$$

Where C denotes a ciphertext, Ep represents encryption with public key (K_b) of receiver i.e. node_ID,

A Lamport signature generation is carried out with private key. Let us consider the '10'be a positive integer i.e. data packets sent and it converted into the string i.e. (0, 1) and the
' = 10 and it converted into string 1010

$$\varphi_d = [P_{ij}\ ]$$



After generating the signature, the sender transmits the ciphertext and the signature to the next neighboring node.

Unsigncryption

At first, the signature verification is presented with public key to obtain plain text. At the receiver side, the new signature is generated as given below,

$$\varphi_d(n) = Q\ (\varphi_d) \quad (9)$$

$$Q\ (\varphi_d) = \varphi_d + 1\ mod\ 16 \quad (10)$$

Let us consider the received signature $\varphi_d = [2\ \ 5\ \ 6\ \ 0]$ and substitute it from the above equation,

$$Q\ (\varphi_d) = 2 + 1\ mod\ 16 = 2 + 1 = 3$$
$$Q\ (\varphi_d) = 5 + 1\ mod\ 16 = 5 + 1 = 6$$
$$Q\ (\varphi_d) = 6 + 1\ mod\ 16 = 6 + 1 = 7$$
$$Q\ (\varphi_d) = 0 + 1\ mod\ 16 = 0 + 1 = 1$$
$$\varphi_d(n) = [3\ 6\ 7\ 1\ ]$$

[00] [01] [10] [11]

Public key 3 6 7 1

$$\varphi_d(n) = [3\ 6\ 7\ 1\ ] = K_b$$

$\varphi_d(n)$ denotes a newly generated signature at the receiver and it is verified with the public key $K_b = [3\ 6\ 7\ 1\ ]$. These signatures get matched and it is valid and then receiver node decrypts ciphertext.

$$d \leftarrow Dp\left\{K_p, C\right\} \quad (11)$$

Where,'d 'denotes original data, 'Dp' denotes decryption, K_p indicates private key of receiver, C represent ciphertext

5. RESULTS AND DISCUSSION

Simulation outcome of three different methods such as KRAD-PRLCSSR technique, Lightweight replica node detection mechanism [1], EMA model [2] are discussed with various metrics. These metrics are described as given below.

- **Attack detection accuracy**

Attack detection accuracy is measured as ratio of number of sensor nodes which are correctly identified as normal or replica node. Attack detection accuracy is formulated as below,

$$ACC = \left[\frac{n_{CD}}{n}\right] * 100 \quad (12)$$

Where ACC denotes an attack detection accuracy, 'n' indicates number of sensor nodes, n_{CD} indicates number of sensor nodes correctly detected as normal of replication attack. Therefore, the attack detection accuracy is calculated in percentage (%).

- **Packet delivery ratio**

Packet delivery ratio is calculated as ratio of number of data packets correctly received at sink node to total number of data packets sent from source node. Packet delivery ratio is expressed as below,

$$R_{PD} = \left[\frac{Number\ of\ data\ packets\ correctly\ received}{Number\ of\ data\ packets}\right] * 100 \quad (13)$$

Where, R_{PD} denotes a packet delivery ratio. It is calculated in percentage (%).

- **Packet loss rate**

The packet loss rate is calculated as ratio of number of data packets lost to total number of data packets. It is measured using the following equation,

$$R_{PL} = \left[\frac{Number\ of\ data\ packets\ lost}{Number\ of\ data\ packets}\right] * 100 \quad (14)$$

Where, R_{PL} indicates a packet loss rate and it is measured in terms of percentage (%).

- **End to end delay**

It is measured as the difference between the actual arrival time of data packets and observed arrival time of the data packets at destination. Delay is calculated as follows,

$$Delay = [T_{act}\ ] - [T_{obs}\ ] \quad (15)$$

Where, T_{act} denotes an actual arrival time and 'T_{obs} ' indicates an observed arrival time. It is estimated in milliseconds (ms).

Table II attack detection accuracy

Number of sensor nodes	Attack detection accuracy (%)		
	KRAD-PRLCSSR	**Lightweight replica node detection mechanism**	**EMA model**
50	92	88	86
100	90	87	85
150	93	85	83
200	91	87	85
250	92	88	84
300	93	86	83
350	91	85	81
400	95	86	83
450	94	88	84
500	93	86	83

Table II demonstrates the performance of attack detection accuracy using three different methods namely KRAD-PRLCSSR technique, Lightweight replica node detection mechanism [1], EMA model [2]. As shown in Table II, ten runs are carried out for each method with different counts of input 50,100,150,200,…500. From table II, KRAD-PRLCSSR attains higher detection accuracy. This is proved through statistical analysis. Let us consider 50 sensor nodes for conducting the experiments. By applying the KRAD-PRLCSSR technique, 46 sensor nodes are accurately detected as normal or replica nodes hence the attack detection accuracy is 92%. Whereas, 44 and 43 nodes are correctly detected as a normal or attack by using the Lightweight replica node detection mechanism [1], EMA model [2]. The detection accuracy of the two existing methods is 88% and 86%. Among the three methods, the proposed KRAD-PRLCSSR technique achieves higher detection accuracy. The average of ten results provides the improvement of the KRAD-PRLCSSR technique than the conventional works. The attack detection accuracy is enhanced by 7% and 10% as compared to [1] and [2] respectively.

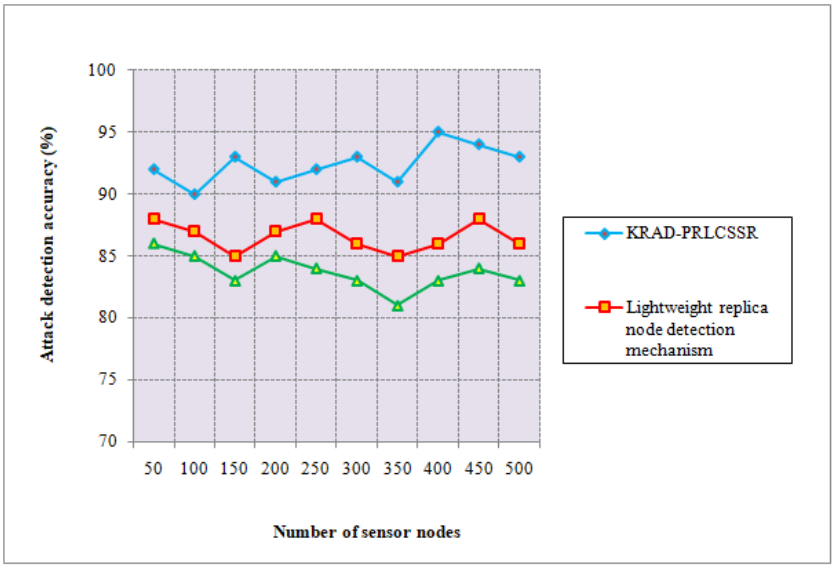


Figure 5 Performance results of attack detection accuracy

Figure 5 portrays outcomes of attack detection accuracy. The line chart indicates the accuracy of three namely KRAD-PRLCSSR, Lightweight replica node detection mechanism [1], EMA model [2] are represented by three different colors such as blue, red, green respectively. The plot notices that the proposed KRAD-PRLCSSR technique provides superior performance than conventional attack detection methods. This is because the KRAD-PRLCSSR technique uses the kriging regression for finding the neighboring node and detects the attacker node. The

regression function is analysis the residual energy of sensor node with threshold energy value. The sensor node which has higher residual energy than the threshold is said to be a normal node and the source node selects this node as neighbors'. The other higher energy nodes are called replica nodes. This helps to accurately find the normal or replica nodes with higher accuracy.

Table III packet delivery ratio

Number of data packets	Packet delivery ratio (%)		
	KRAD-PRLCSSR	Lightweight replica node detection mechanism	EMA model
25	88	84	80
50	90	86	84
75	89	85	83
100	92	87	85
125	91	86	83
150	90	85	82
175	89	84	81
200	88	85	82
225	90	84	81
250	89	86	80

Simulation results of the packet delivery ratio of three different techniques namely KRAD-PRLCSSR, Lightweight replica node detection mechanism [1], EMA model [2] are described in Table III. The delivery ratio is measured based on the number of packets taken in the ranges from 25 to 250. Ten iterations are performed for each method. The obtained performance results of KRAD-PRLCSSR achieve a higher packet delivery ratio. In first iteration, 25 data packets are sent from source. By applying KRAD-PRLCSSR technique, 22 data packets are received at sink node and packet delivery ratio is 88%. Similarly, 21 and 20 data packets are received and their delivery ratios are 84% and 80% using Lightweight replica node detection mechanism [1], EMA model [2]. Likewise, the remaining nine runs are performed with different counts of input. The average of ten results ndicates that packet delivery ratio is enhanced by 5% when compared [1] and 12% when compared to [2].

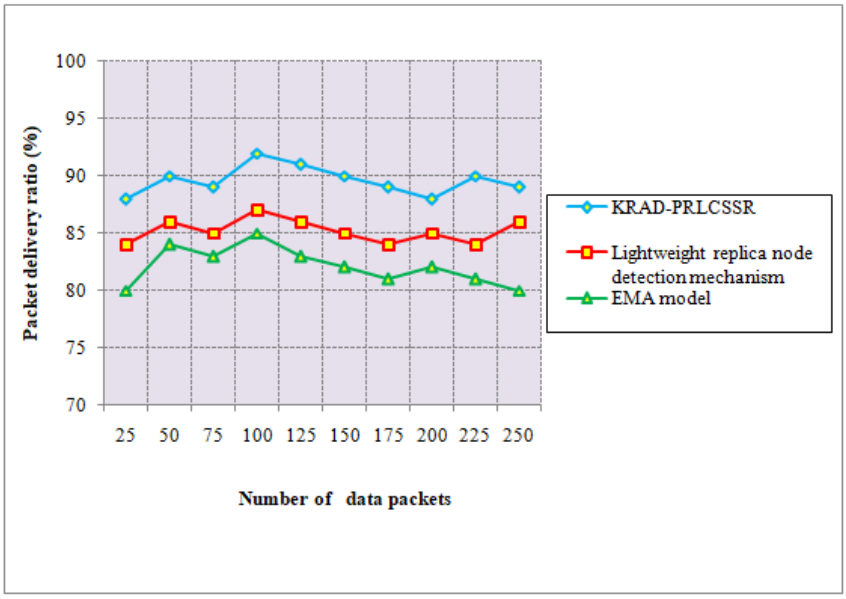


Figure 6 Performance results of packet delivery ratio

Figure 6 illustrates performance analysis of packet delivery ratio. As shown in figure 6, number of data packets is taken as input for calculating the packet delivery ratio. The different results are obtained on the vertical axis. From figure 6, KRAD-PRLCSSR technique achieves a higher delivery ratio. This is due to application of kriging regression and Pseudo Randomized Lamport one-time Generative Certificateless Signcryption. By applying the regression function, the node with higher residual energy is chosen for data delivery. In addition, the proposed signcryption technique is applied to securely transmit the data packets via the normal nodes. Besides, the

certificateless signcryption algorithm encrypts the data packets and sent to a sink node in the form of ciphertext to increase the security of data access. This assists to increase secure data delivery from source to sink node.

Table IV Packet loss rate

Number of data packets	Packet loss rate (%)		
	KRAD-PRLCSSR	Lightweight replica node detection mechanism	EMA model
25	12	16	20
50	10	14	16
75	11	15	17
100	8	13	15
125	9	14	17
150	10	15	18
175	11	16	19
200	12	15	18
225	10	16	19
250	11	14	20

Table IV describes the experimental outcomes of packet loss rate. Observed results demonstrate that the loss rate is considerably reduced using the KRAD-PRLCSSR technique than the other conventional attack detection methods. This is proved through the statistical measure. Let us consider 25 data packets for calculating the packet loss rate. By applying a KRAD-PRLCSSR, 3 data packets are lost and their loss rate percentage is 12%. Similarly, 4 and 5 data packets are lost using Lightweight replica node detection mechanism [1], EMA model [2] and the loss percentages are 16% and 20%. From above statistical measure, KRAD-PRLCSSR outperforms well in minimizing packet loss rate. Finally, the packet loss rate is reduced by 30% as compared to Lightweight replica node detection mechanism [1] and 42% when compared to the EMA model [2].

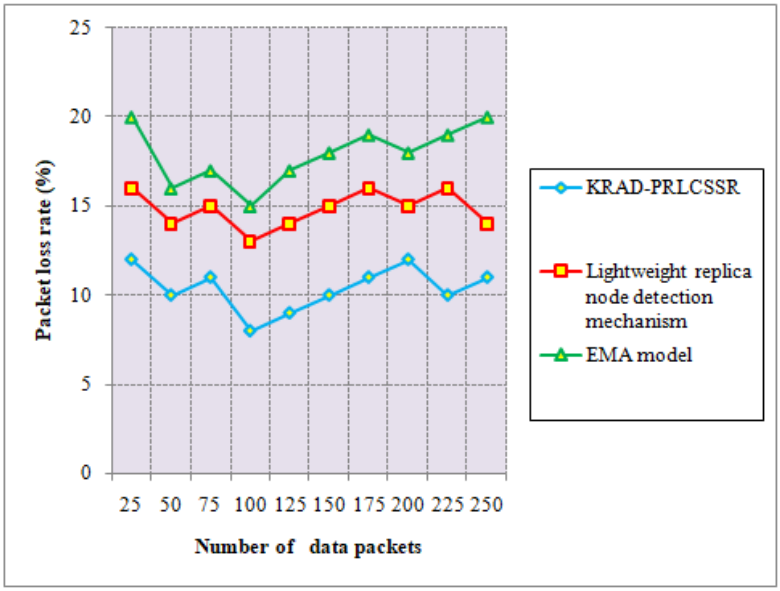


Figure 7 Performance results of packet loss rate

Figure 7 depicts the results of packet loss rate with number of data packets for different techniques. But the graphic representation indicates that the packet loss rate is comparatively minimized using the KRAD-PRLCSSR

technique than the other two existing techniques. The reason behind the pseudo Randomized Lamport one-time Generative Certificateless Signcryption effectively performs the key generation, signature generation, encryption, and decryption. Whenever the source node transmits the data packets, it generates the signature and generates the plain text. Then it sends to the other node resulting in it securely transmits the data packets and avoid the packet drop due to the attacker in WSN.

Table V End to end delay

Number of data packets	End to end delay (ms)		
	KRAD-PRLCSSR	Lightweight replica node detection mechanism	EMA model
25	10	12	14
50	11	14	16
75	13	15	17
100	15	17	20
125	17	19	21
150	19	21	22
175	21	23	25
200	22	25	27
225	24	26	28
250	25	28	30

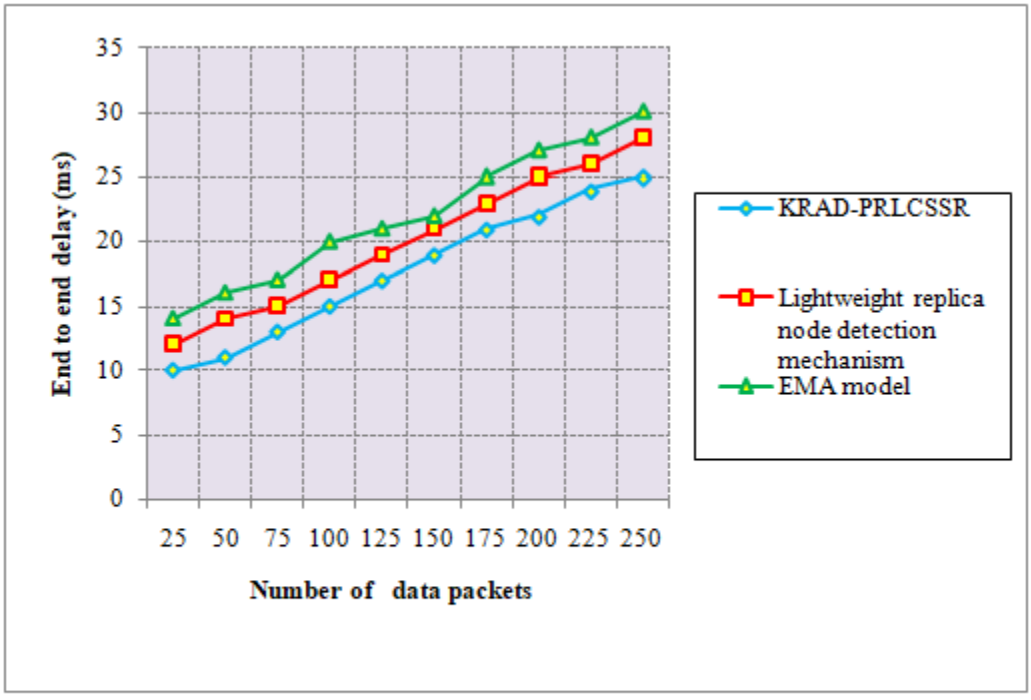


Figure 8 Performance results of end to end delay

Table V and Figure 8 demonstrates performance results of delay with number of data packets. From observed results, the delay is directly proportional to number of data packets. In other words, the delay of each method gets increased for each method while enhancing the data packets. But comparatively, delay is found to be lesser using the KRAD-PRLCSSR technique. The simulations are conducted for 25 data packets; the delay observed using proposed KRAD-PRLCSSR technique is $10ms$ whereas the delay of secure routing is $12ms$ and $14ms$ observed using Lightweight replica node detection mechanism [1], EMA model [2] respectively. Similarly, ten different runs are performed and the results are observed for each method. From the observed results, the proposed KRAD-PRLCSSR technique is reduced by 12% and 21% as compared to [1] [2]. This improvement is achieved by identifying the neighbor discovery and secure data transmission. The energy-efficient neighboring sensor node efficiently performs the data packet transmission with lesser time consumption.

6. CONCLUSION

An efficient KRAD-PRLCSSR technique is proposed to identify the replication nodes with higher accuracy. The technique is designed based on a kriging regression and Pseudo Randomized Lamport one-time Generative Certificateless Signcryption. The kriging regression is applied to find the neighbor node and avoid the replica node depends on residual energy analysis. With selected neighboring nodes, secure routing is performed to enhance delivery ratio and reduce packet loss. Signcryption technique performs the encryption, signature generation. Encrypted data is sent to receiver node where signature verification is carried out with public key. If signature is valid, then the receiver decrypts ciphertext and attains original data packets. This in turn improves security of data delivery in WSN. A simulation is conducted for the KRAD-PRLCSSR technique and existing with different metrics. The performance results in discussion indicates that the proposed KRAD-PRLCSSR technique achieved better performance in terms of achieving higher attack detection accuracy, packet delivery ratio, and minimum packet loss as well as delay than the other conventional methods.

REFERENCES

1. Mojtaba Jamshidi, Shokooh Sheikh Abooli Poor, Abbas Arghavani, Mehdi Esnaashari, Abdusalam Abdulla Shaltooki, Mohammad Reza Meybodi, “A simple, lightweight, and precise algorithm to defend against replica node attacks in mobile wireless networks using neighboring information”, Ad Hoc Networks, Elsevier, Volume 100, 2020, Pages 1-16
2. S. Anitha, P. Jayanthi & R. Thangarajan, “Detection of Replica Node Attack Based on Exponential Moving Average Model in Wireless Sensor Networks”, Wireless Personal Communications, Springer, Volume 115, 2020, Pages1651–1666
3. T.P.Rani and C.Jayakumar, “Unique identity and localization based replica node detection in hierarchical wireless sensor networks”, Computers & Electrical Engineering, Elsevier, Volume 64, November 2017, Pages 148-162
4. Chao Ding, Lijun Yang, and Meng Wu, “Localization-Free Detection of Replica Node Attacks in Wireless Sensor Networks Using Similarity Estimation with Group Deployment Knowledge”, Sensors, Volume 17, Issue 1, 2017, Pages 1-26
5. Mehdi Safari, Elham Bahmani, Mojtaba Jamshidi, Abdusalam Abdulla Shaltooki, “Advanced Extremely Efficient Detection of Replica Nodes in Mobile Wireless Sensor Networks”, International Journal on Informatics Visualization, Volume 3, Issue 4, 2019, Pages 337-342
6. G. Amudha & P. Narayanasamy, “Distributed Location and Trust Based Replica Detection in Wireless Sensor Networks”, Wireless Personal Communications, Springer, Volume 102, 2018, Pages 3303-3321
7. Alekha Kumar Mishra, Asis Kumar Tripathy, Arun Kumar, and Ashok Kumar Turuk, “A Replica Detection Scheme Based on the Deviation in Distance Traveled Sliding Window for Wireless Sensor Networks”, Wireless Communications and Mobile Computing, Hindawi, Volume 2017, January 2017, Pages 1-8
8. Mojtaba Jamshidi, Abdusalam Abdulla Shaltooki, Zahra Dagal Zadeh, Aso Mohammad Darwesh, “A Dynamic ID Assignment Mechanism to Defend Against Node Replication Attack in Static Wireless Sensor Networks”, International Journal on Informatics Visualization, Volume 3, Issue 1,2019, Pages 13-17
9. L. Sujihelen & C. Jayakumar, “Inclusive Elliptical Curve Cryptography (IECC) for Wireless Sensor Network Efficient Operations”, Wireless Personal Communications, Springer, Volume 99, 2018, Pages 893-914

10. Oladayo O. Olakanmi and Adedamola Dada, "An efficient point-to-point security solution for multihop routing in wireless sensor networks", security and privacy, Wiley, 2019, Pages 1-14
11. Geetika Dhand and Kavita Sheoran, "Protocols SMEER (Secure Multitier Energy Efficient Routing Protocol) and SCOR (Secure Elliptic curve based Chaotic key Galois Cryptography on Opportunistic Routing)", Materials Today: Proceedings, Elsevier, 2020, Pages 1-4
12. Ze Wang, Chang Zhou, and Yiran Liu, "Efficient Hybrid Detection of Node Replication Attacks in Mobile Sensor Networks", Mobile Information Systems, Hindawi, Volume 2017, August 2017, Pages 1-13
13. P.P.Devi and B.Jaison, "Protection on Wireless Sensor Network from Clone Attack using the SDN-Enabled Hybrid Clone Node Detection Mechanisms", Computer Communications, Elsevier, Volume 152, 15 February 2020, Pages 316-322
14. Haafizah Rameeza Shaukat, Fazirulhisyam Hashim, Muhammad Arslan Shaukat, and Kamal Ali Alezabi, "Hybrid Multi-Level Detection and Mitigation of Clone Attacks in Mobile Wireless Sensor Network (MWSN)", Sensors, Volume 20, Issue 8, 2020, Pages 1-23
15. Longpeng Li , Guangquan Xu, Litao Jiao , Xiaotong Li , Hao Wang , Jing Hu , Hequn Xian, Wenjuan Lian , Honghao Gao , "A Secure Random Key Distribution Scheme Against Node Replication Attacks in Industrial Wireless Sensor Systems", IEEE Transactions on Industrial Informatics , Volume 16, Issue 3, 2020, Pages 2091 – 2101
16. Erdong Yuan, Liejun Wang, Shuli Cheng, Naixiang Ao, and Qingrui Guo, "A Key Management Scheme Based on Pairing-Free Identity Based Digital Signature Algorithm for Heterogeneous Wireless Sensor Networks", Sensors, Volume 20, Issue 6, 2020, Pages 1-15
17. Anubha and R P S Bedi ,"Detection of Clone Attacks in Manets using Ant Colony Optimization", International Journal of Engineering and Advanced Technology (IJEAT), Volume 9, Issue 4, 2020, Pages 426-429
18. Zhihua Zhang, Shoushan Luo, Hongliang Zhu , and Yang Xin, "A Clone Detection Algorithm with Low Resource Expenditure for Wireless Sensor Networks", Journal of Sensors, Hindawi, Volume 2018, March 2018, Pages 1-16
19. Turki Ali Alghamdi, "Convolutional technique for enhancing security in wireless sensor networks against malicious nodes", Human-centric Computing and Information Sciences, Springer, Volume 9, 2019, pages 1-10
20. V. Kavidha and S. Ananthakumaran, "Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink", Peer-to-Peer Networking and Applications, Springer, Volume 12, 2019, Pages 881-892
21. Asraf Yasmin, B., Latha, R., & Manikandan, R. (2019). Implementation of Affective Knowledge for any Geo Location Based on Emotional Intelligence using GPS. International Journal of Innovative Technology and Exploring Engineering, 8(11S), 764–769. https://doi.org/10.35940/ijitee.k1134.09811s19