ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

Inspired by Soldier Bees: A Defense Mechanism for Detecting Impersonated Sensor Nodes in Wireless Sensor Networks

Debnath Bhattacharyya, CSE, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

K saikumar, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

Abstract

Through the utilization of this mechanism, we can promptly notify the base station of any potentially malicious nodes within the network and continuously monitor their positional changes. In response to these security concerns, we have developed an advanced secure Artificial Bee Colony Optimizer algorithm, enriched with swarm intelligence. This algorithm facilitates comprehensive exploration of multiple data transmission paths from sensors to sink nodes, particularly when dealing with scenarios involving potential malicious nodes. In order to establish secure communication among nodes, we have seamlessly integrated the Elliptic Curve Digital Signature Algorithm (ECDSA) into our framework. This integration offers several key advantages, including the rapid identification of compromised nodes, a reduction in authentication delays, and the minimization of packet loss. The core strengths of our algorithm encompass swift detection and isolation of compromised nodes, resulting in improved overall network security. Importantly, this process is executed without causing harm to the other nodes in the network. As a result, our scheme significantly enhances energy efficiency, boosts packet delivery ratios, and maximizes throughput within the Wireless Sensor Network (WSN).

Introduction

The role of wireless sensor networks (WSNs) in various felds is becoming famous, by providing multiple results to various gathered data. The WSN forms a topology according to the environment and there are some factors to be predefned to create a proper wireless topology [1]. The key factor to be noted while deploying WSN is security, where the lack of security in wireless network creates many issues. If the scheme or network topology strategy is missing the safety factor, the attackers will create a severe issue by

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

staging their attacks inside and outside of the network [2]. The positioning of sensor nodes in the forbidden zone needs to have more near of security to avoid several attacks. To provide efcient solutions for the requested queries, the design of the network should have a proper secured data transfer [3]. Mostly, the sensor networks are implemented for monitoring purpose [4].

4 Experimentation and result analysis

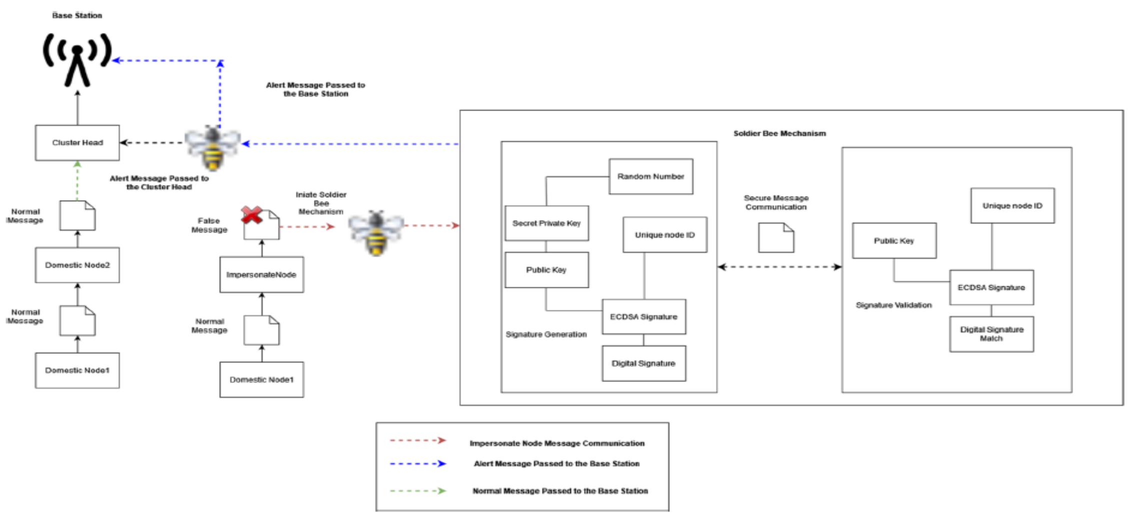


Fig. 1 Workflow of soldier bee defence mechanism

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021**

Algorithm 1. Key feature selection using RSVM

Input: Dataset F with n features

BEGIN
Let $F = \{f_1, f_2, f_3 \dots \dots, f_n\}$//where n represents the number of features in the data set
Let $K = \{F\}$
    $\forall_{i-1}^{n} F$: ***do***
    Remove f_i from F
    $K = K - f_i$//restore feature subset
    Apply SVM classifier
    Remove f_i from F
end
    Based on the accuracy of the classifier the features are sort
    if$((eff > eff\_thersold)\&\&(\det\_rate > \det\_rate\_thersold))$**Then**
      {
        $K = K - f_i$//choosing Key features
      }
Else
      {
        Search for high efficiency feature
      }
END

Output: Key Feature Selection

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021**

Algorithm 2. Soldier bee defence mechanism.

Input: #Population $P = [x_1, x_2, \ldots, x_n]$
fitness function f(),CL is the cluster
DN_{cl} *is the noraml node in the cluster cl*
Cluster head in the network CH
EN_G *Gateway Node*
M is the message
$\oplus$ Concatenation of message is expressed
U Universal Point in ECC
N_B Base station BS

1:Initalize the Population
$p \leftarrow [x_1, x_2, \ldots, x_n]$
Where $x_i \leftarrow \{f_1, f_2, f_3 \ldots \ldots, f_n\} \forall f \in \{0,1\}$
Initialize the cluster BS generates signature (r, s)
M is the message private key is D
NV is nonce value
D (m) duplicate message. // Broadcast from Base Station to Cluster heads
2: Calculate the fitness $f(p)$
3:t← 1
4:Repeat
5:**Employee Bee Phase**
6:**For** each$x_i \in P$ do
7: Old $\_x_i \leftarrow x_i$
8: **If** (rand>rand)
9: Soldier Bee Defence Mechanism Signing the broadcast message(R,S)
10: R=$x_1 mod\ n$ KP= (x_1, x_2) //K∈(1,n-1), P is a point on curve
11: S=$k^{-1}\{h(m \oplus R) + dr\}\ mod\ n$ // h is SHA-1, n is large prime
12: Gateway nodes forward it to the cluster heads.
13: BS→ $EN_G : EK_{KBS,ENG}\ ((r, s) \oplus m \oplus NV)$ //BS sends a pair of signature (*r; s*)
14: EN_G → CH: $EK_{K-ENG,CH}\ ((r, s) \oplus m \oplus NV)$// message (*m*) with random nonce (*NV*) toEN_G
15: Verifying the broadcast message.
16: *CH*←signed (M)//Verifies the message by comparing v and r
17: v=$x_1 mod\ n$,$u_1 * G + u_2 * P_{BS}$=(x_1, y_1)
18: $u_1 = \{h(m \oplus R) * c\}\ mod\ n$
19: $u_2 = r * c\ mod\ n$
20: c=$\frac{1}{s}$ mod n
21: Calculated (v) is same as the received (r),
22: **if** (v==r)
23: CH accepts m
24: CH→ $\boldsymbol{DN}$: $E_{KC}(m)$
25: **else**
26: CH rejects the message
27: DN does the assigned work
28: end
29:Broadcast from CH to BS
30: Signing the broadcast message
31: *CH*←$\boldsymbol{DN_{CL}}$
32: CH→ $EN_G : EK_{Kc,ENG}\ ((r', s') \oplus m' \oplus NV')$//CH sends a pair of signature $r', s'$and m' to a EN_G
33: EN_G → $\boldsymbol{BS}$: $EK_{ENG,BS}\ ((r', s') \oplus m' \oplus NV'$//$EN_G$ forwards the pair to the BS through other CL.
34: ***Verifying the broadcast message****.*
35: BS← CH//BS can verify the m from CH because it maintains the public keys of CH
36: D(m) is rejected
37: Calculate $E_{ef} = \frac{E_{node\_out}}{E_{node\_in}}$
38: **if** signature is accepted
39: BS accept the message
40: **else**
41: Messages is rejected

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

Table 1 Literature study comparison table

S. no	Author	Methodology	Pros	Cons
1	Pang, Ce, Gongguo Xu and Yunpu Zhang [25]	Enhancing the supervision scheme, extending the time recess between two adjacent annotations, improved lion algorithm combined with the logistic chaos sequence	Energy saving	Not providing any countermeasures if it is exposed to network attacks
2	Zhang, Xiu [46]	Evolutionary computing (EC) algorithms. Such as genetic algorithms (gas), differential evolution (DE), particle swarm optimization (PSO), artificial bee colonies (ABCs) and neighbourhood field optimization (NFO)	Enhancing lifespan of WSNs	The stated methods are only for increasing the lifespan of the network when they are malicious free
3	Saad, Eman, Mostafa A [31]	Culture algorithm and artificial bee colony CB-ABC	Searching procedure of food sources in WSN perspective identifying the node position	The algorithm fails to identify the node position when they have impersonated nodes which will create a heavy damage, if it enters the WSN
4	Mehmood Amjad [18]	ICMDS (Inter-Cluster Multiple Key Distribution Scheme for Wireless Sensor Networks	Two-phase secured mechanism	Even though it provides a secured mechanism using data protection, it needs to be considered which is not a part of this secured mechanism
5	Di Pietro, Roberto [6]	Authentication techniques, permits an UWSN	High performance at the time of message communication	Proper mechanism for UWSN usage of cryptographic to protect the data is not proposed
6	Maerien, Jef [17]	SecLooCI	Better security	The security process has lots of pros and less cons by not demonstrating with attacks
7	Wang, Ding [42]	Hierarchical wireless sensor networks (HWSN)	XOR operations	Cryptographic functions are explaining fine
8	Mohd Anuar Mat [12]	Diffie-Hellman communication protocol model	Easy design for automata machine	Not for secure mechanism
9	Tripathi [38]	Black hole and grey hole attacks with LEACH	Efficiency of the network	Black hole and grey hole attacks with LEACH (primitive method which is not providing full fledge communication)
10	Patil, Shital [27]	Denial-of-Service (DoS)	Accuracy rate	General description of DOS attack does not have the ability to handle different qualities of attacks
11	Amish, Parmar [3]	AOMDV (Ad hoc On demand Multipath Distance Vector)	Handle the attack in an effective way	Suitable for carrying the data from one layer to other with less security
12	Shashi Kant [34]	Elliptic Curve Cryptography (ECC)	Identify replay attack	The procedure is for normal data encryption and decryption
13	Patil, Ashish and Rahul Gaikwad [26]	Lightweight secure mechanism and energy weight monitoring system	Network lifetime of the network by giving protection from the DOS attack	The lifetime of the network increases when this strategy is adopted, but if the attack is indicated, the stability will be degraded
14	Moon, Ayaz Hassan Digital [21]	Cryptographic algorithms	Improving the authentication of the data	Without incorporating any types of attacks, a normal mechanism is presented

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

Table 2 Without soldier bee defence mechanism

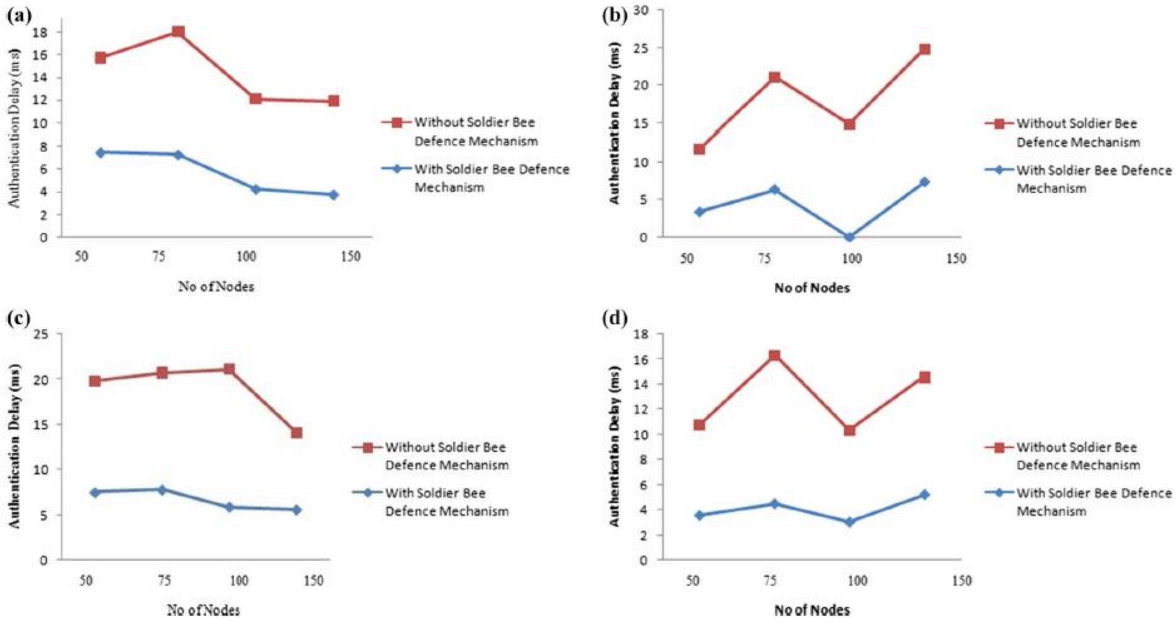
No of nodes	Authentication delay (ms)	PDR	Communication overhead	Packet loss	Throughput	Hit ratio
50	8.2	49.3	8.6	19.32	70.15	0.2
	12.3	55.2	6.9	21.02	71.36	0.6
	8.4	43.7	7.8	18.72	69.54	0.1
	7.2	59.3	7.6	12.35	75.16	0.3
75	10.7	45.2	7.1	17.9	70.21	0.4
	12.9	57.5	7.5	22.12	72.83	0.3
	14.7	59.32	8.2	25.31	69.31	0.47
	11.8	54.7	6.3	22.1	69.9	0.2
100	7.8	47.3	8.1	26.2	60.5	0.6
	15.2	59.71	9.5	33.7	69.7	0.4
	14.9	58.2	5.3	32.9	59.1	0.1
	7.3	60.21	9.3	14.2	79.7	0.5
150	8.1	48.5	8.4	26.2	68.3	0.2
	8.5	48.9	9.9	25.1	67.01	0.5
	17.4	59.3	8.8	13.7	75.2	0.4
	9.37	49.2	10.2	28.9	68.4	0.1

Table 3 With soldier bee defence mechanism

No of nodes	Authentication delay (ms)	PDR	Communication overhead	Packet loss	Throughput	Hit ratio
50	6.56	70.5	4.7	14.24	147.25	0.6
	7.5	70.6	1.7	13.2	137.9	0.9
	3.4	84.5	1.0	8.02	174.3	1.0
	3.6	77.7	3.62	4.58	148.61	0.5
75	7.3	73.9	5.3	10.2	154.4	1.0
	7.8	71.3	1.81	13.5	128.6	0.6
	6.39	56.2	3.47	9.25	152.2	0.9
	4.53	62.10	6.89	8.65	150.85	0.7
100	4.28	69.2	4.0	9.54	124.4	0.6
	5.9	72.6	3.02	10.35	147	0.9
	6..82	60.7	2.67	10.14	156.4	0.4
	3.07	69.4	2.25	7.24	154.5	0.8
150	3.8	75.2	2.7	11.4	160.24	0.9
	5.6	76.2	1.5	5.1	184.5	0.7
	7.4	87.10	4.35	9.43	179.6	1
	5.24	93.75	7.42	11.36	187.21	1

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021**



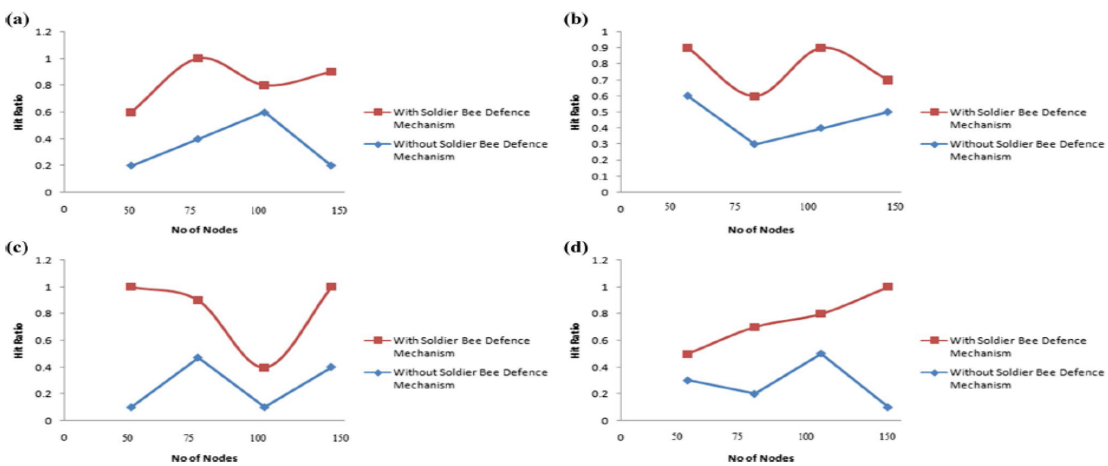


Fig. 3 **a** Hit ratio, malicious node = 5; **b** hit ratio, malicious node = 10; **c** hit ratio, malicious node = 15; **d** hit ratio, malicious node = 20

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

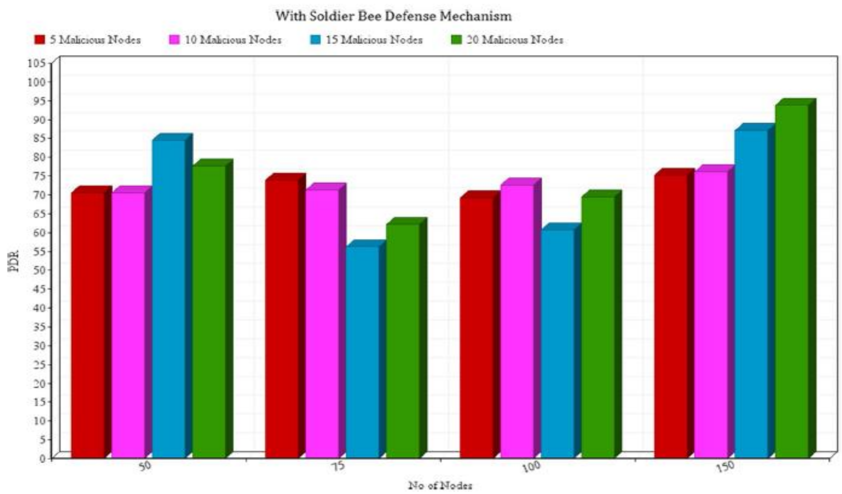


Fig. 4 PDR with soldier bee defence mechanism

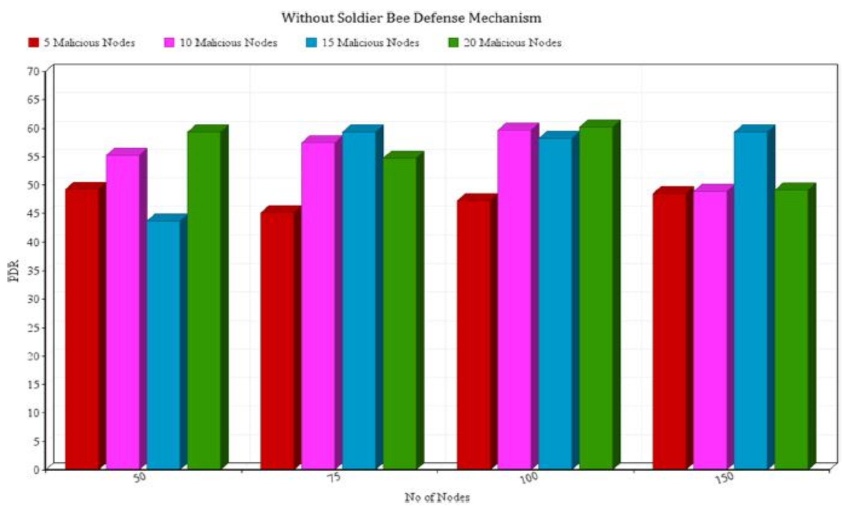


Fig. 5 PDR without soldier bee defence mechanism

5 Result analysis and discussion

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

Fig. 6 Packet loss with soldier bee defence mechanism

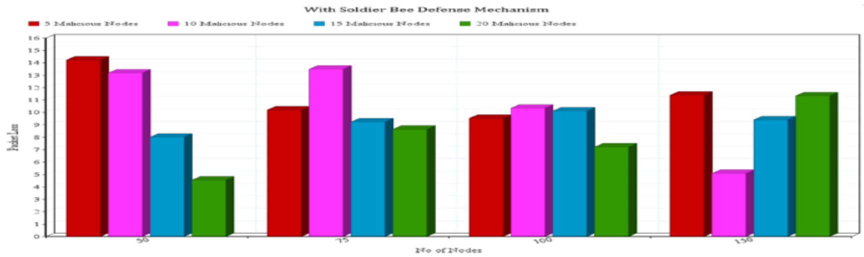
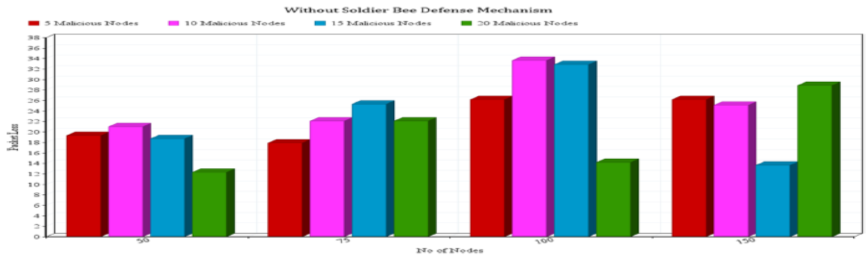


Fig. 7 Packet loss without soldier bee defence mechanism



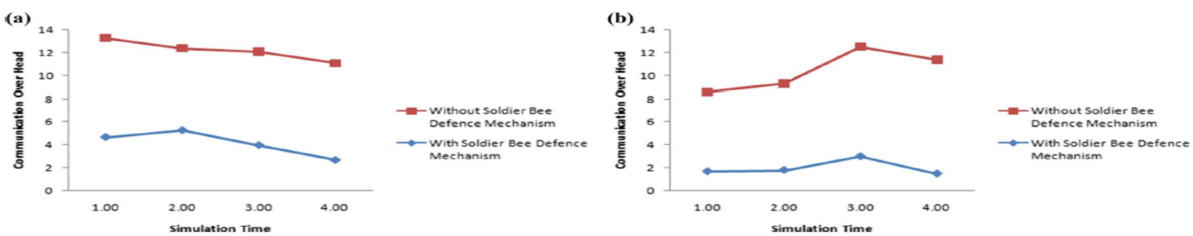
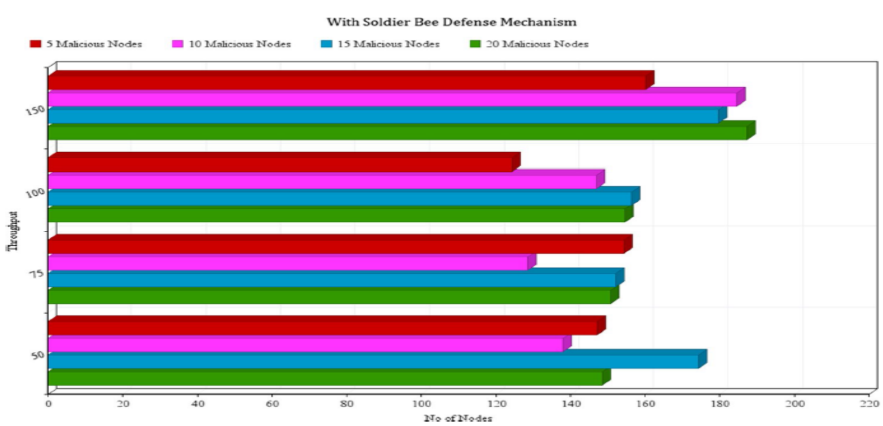


Fig. 8 **a** Communication overhead, malicious node = 5; **b** communication overhead, malicious node = 10; **c** communication overhead, malicious node = 15; **d** communication overhead, malicious node = 20

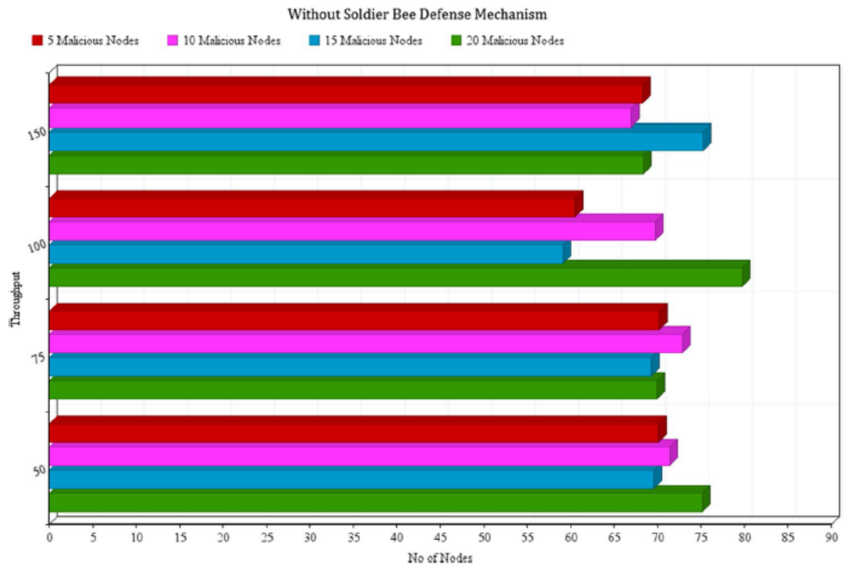
Fig. 9 Throughput with soldier bee defence mechanism

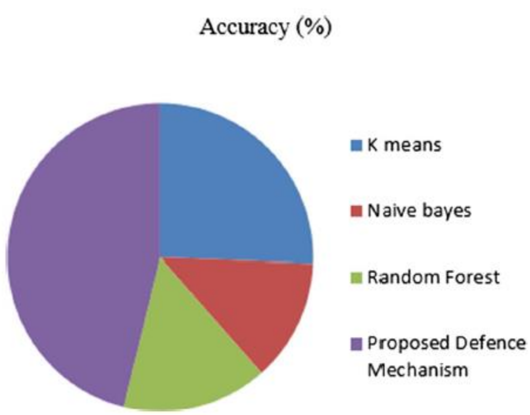


ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021**

Fig. 10 Throughput without soldier bee defence mechanism





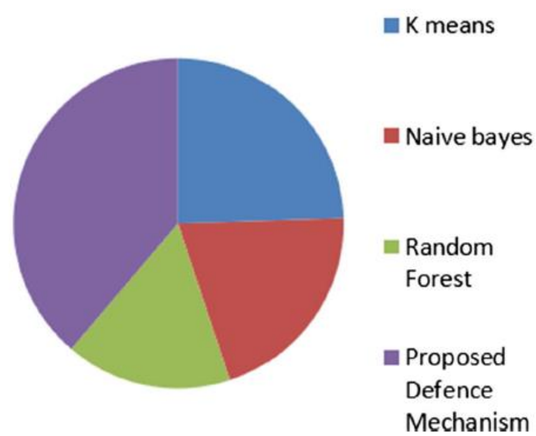


Fig. 11 Comparison on accuracy using proposed scheme

Fig. 12 Comparison on detection rate using proposed scheme

6 Conclusion and future work

This research paper introduces a robust defense mechanism designed to mitigate a significant threat known as the sensor node impersonation attack in Wireless Sensor Networks (WSN). The paper provides an in-depth exploration of the nature of this attack and the adverse consequences it inflicts on nodes within the network. To accurately detect node impersonation attacks, we employ a meticulous feature selection process, focusing on key features known for their high detection rates. These chosen features are subsequently compared against other feature selection methods to highlight their effectiveness in identifying such attacks.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

References

1. Abirami R, Premalatha G (2014) Depletion of vampire attacks in medium access control level using interior gateway routing protocol." Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE

2. Achuthan E, Kishore R (2014) A novel anti jamming technique for wireless sensor networks." Communications and Signal Processing (ICCSP), 2014 International Conference on. IEEE

3. Amish Parmar, Vaghela VB (2016) Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. Procedia Comput Sci 79:700–707

4. Amudha P, Karthik S, Sivakumari S (2015) A hybrid swarm intelligence algorithm for intrusion detection using significant features. Sci World J 2015