Detecting Replica Node in Distributed Mobile Wireless Sensor Networks

Sujihelen L (sujihelen@gmail.com)
Sathyabama Institute of Science and Technology https://orcid.org/0000-0001-6596-8205
C Senthilsingh
Shadan Womens College of Engineering and Technology

Research Article

Keywords: Node Replication Attacks, HIP-HOP, History of Neighbor Node, Replica Node, Detection Accuracy.

Posted Date: April 28th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-233955/v1

Detecting Replica Node in Distributed Mobile Wireless Sensor Networks

L.Sujihelen[1],C.Senthilsingh[2]
[1]*Sathyabama Institute of Science and Engineering,Chennai,*
[2] *Shadan Women's College of Engineering,Hyderabad*
[1]sujihelen@gmail.com

Abstract

Security is an important problem in wireless sensor networks. There are more attacks in WSN. Node replication attack is an important attack in wireless sensor networks which can be easily captured by adversaries. In this attack, the node will behave as an original node and collect all the information which is transferred in the network and passes to the attacker node. Some existing schemes are proposed for predicting the replica nodes. In existing method, the detection rate is less, communication cost is high. To increase the detection accuracy and to increase the communication cost, a History of Neighbor Node (HNN) method is proposed. The proposed HNN approach detects the replicated node locally and globally. The HNN method detection accuracy is high in any speed limit. Another approach also proposed for static mobile sensor networks, FEC approach, the replicated node is detected based upon the speed, direction and location. In random time the base station verifies the node with the observed speed and direction. The verification is conducted by the SPRT technique. The SPRT technique tests the node which should be rejected (clone node) or accepted (genuine node). Once the clone node is found quickly, then it is removed from the network. The proposed system has high detection accuracy and less communication cost and less energy efficiency when compared with the existing system.

Keywords- Node Replication Attacks, HIP-HOP, History of Neighbor Node, Replica Node, Detection Accuracy.

1. Introduction

Node Replication attacks is an active attack in WSN [1][6]. The node replication attack is the root cause of many attacks in wireless sensor networks. In node replication attack, the replica node will behave likes a genuine node and sense all the confidential information from the sensor nodes [2][3]. The sensed information is transferred to the attacker node or attacker base station [4][9]. More researchers have proposed to detect the replica node in wireless sensor networks [7][8]. The main drawback is less detection rate and high communication overhead. Few existing system techniques are discussed in this section. Extremely Efficient Detection (XED), EDD[11] scheme is to detect the clone nodes from the mobile sensor networks [10][5]. If any sensor node meets the other sensor node at any time, then it shares a random number. If it happens to meet the node again then it should be check for replica which is discussed in XED approach. If the network is without a replicating node, then the number of times visiting the node should be limited in a given time interval. UTLSE and MTLSD protocol is detect the replica node based on location and time[12]. SDD-LC a technique employed to share information to mobile node is verified with the local memory data. SDD-LWC in which the nodes exchange information is common in both their locally maintained tables [13].In SEDD[11] scheme is to monitor all nodes in a particular time interval. Another approach suggested mainly for securing the nodes and detecting clone nodes in MWSN [14]. Another approach is to detect the replica node using HIP/HOP method [15].

HIP/HOP method is the modification of the existing work [16]. In this scheme, implied methodology is to divide the time into different rounds. The sensor nodes send their location claim to neighbor node in every round. The neighbor node will compare their own history log for duplication. If the duplication occurs, then the location is verified. If there is a location conflict then the identified node will be assigned as a clone node. The HIP verifies with all the logs received and identify the duplications. It has less storage requirement compared to the existing detection technique. In HIP/HOP approach, the same technique will be challenging for global detection. To detect the replica node globally another approach is introduced [17]. This approach is for detecting hybrid and global detection method. The time slot is calculated as rounds. When the round is less, the detection accuracy is less. The existing system has more false positives and less detection rate. To improve the detection accuracy, a HNN approach is proposed. This paper is arranged as Introduction in section 1, proposed system in section 2, HNN approach in section 3, Results and Discussion in section 4, simulation results in section 5, conclusion in section 6 and references in section 7.

2. Proposed System for Distributed Mobile Sensor Networks

HNN approach is the modification of HIP/HOP approach. The HNN approach detect replica node by detecting clone node on its own log, detect clone node by neighbor log and detect clone node globally by the field key and speed. The overview of HNN Architecture diagram is Fig. 1.

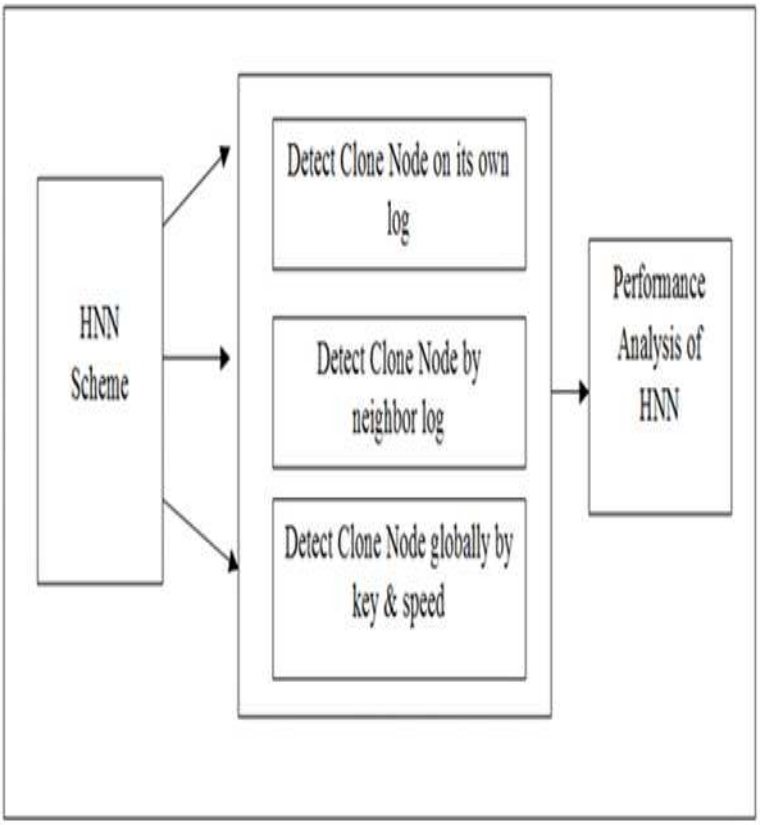

Fig.1 Overview of HNN Architecture

3. HNN Method

Assume the network has N nodes with ID's. The nodes are deployed randomly in the network. Assume the replica nodes (R) with same node id, location id and time. Each node communication radius is assigned as r. The sensor nodes are moving randomly [18]. The nodes speed limit in the interval (T_{min}, T_{max}). At a random time t, a node is selected randomly and a message is broadcast to all the nodes to share the neighbor logs to its nearest neighbor node. The neighbor log has node id, location id and time shown in Fig. 2.

Node ID	Location ID	Time

Fig.2 Neighbor log Field

The HNN method follows three steps: In the first step, each node monitors their own log. If the log has the duplicate node with same location id with different time then the node should be validated by verifying the distance. The distance of the node is calculated in different time during verification.

$Dj >= Dk$ if $tj < tk$ (1)

$\frac{dk-dj}{tk-tj} \notin (T_{min}, T_{max})$ if $tj < tk$, $dj < dk$ (2)

$V \in (T_{min}, T_{max}]$, $d \in (1, \sqrt{x^2 + y^2}]$ (3)

$$P(v,d) = \frac{1}{(Tmax - Tmin)\sqrt{x^2+y^2}-1} \quad (4)$$

If any deviation in the distance is sensed, it is assigned as a clone node. The distance travel by a node and the replica node distance travelled will never be same. In the second case, at a random time each node verifies the nearest neighbor node log history. If the duplicate is present, the location id may be different at the same time. Then check for the replication for verifying the node id, location id, speed and energy level. Each node checks the log of all nearest nodes and verifies the log details. For example, A is the random node selected; it checks the neighbor node B, C, D, E, F logs in Fig. 3.

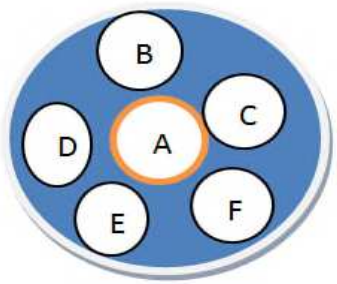

Fig. 3 Neighbor Node

Suppose R is the replicated node present nearer to the node F. The neighbor node B holds the log list as { {R, L1, t1},{B, L1,t2}} , F has the log list as {{A, L2,t1},{C,L1,t2}} and A has the log as {{d,L1,t1}, {e,L2,t2}}. A verifies the neighbor list of B and F with their own log. The duplicate is not detected if the neighbor log is verified with own log. The history of all neighbor logs will be combined and check for replicated node. To reduce the energy consumption, the logs will be cleared in FIFO order. The overview algorithm of the HNN is shown in the Fig.4.

```
Input: Position the node at time t.
        History Log M.
  1.Check the duplication  with its own log.
    If ( dup (node)) then
       check for replica in  lid and t.
       if(dup(node(lid[i],t[i])) != dup(node(lid[j],t[j]))
              report 'not clone'
              else
              report 'clone'
    2.Check the duplicate with neighbor logs
       M← Receive from neighbors
       For each(msg[i],msg[j] !=M) do
          If(msg[i]==msg[j]) then
            If(lid[i],t[i]==lid[j],t[j])
              Report 'clone'
              Else
              Report 'not clone'
       3.  Check the node globally
       M=log (node id,t)
        If dup(M) then
         if (locid and key)
          Report clone
```

In the third case, a node is randomly selected as verifier node. The verifier node verifies the entire sensor node in the network. Each node sends the speed and key to the verifier node. If the verifier node finds the mismatch in speed and key, then it will be assigned as a replica node. The speed limit of the mobile node is fixed.

<IdB, LocB, speed,signed(K Priv A) > (5)

4. Proposed System for Static Mobile Sensor Networks

The proposed Fast, Efficient Centralized scheme can identify the clones with better communication cost and energy consumption.

FEC Approach

A novel detection scheme for static mobile nodes based on the FEC approach is proposed and compared with the existing SPRT [16] method. The detection uses speed, location, direction and tested by using a SPRT. The various cases to be followed are for detecting replica node.

Case 1:

An attacker node moves in exceeding configured maximum speed(S_{max}). An attacker node's speed can exceed the deployement speed in speed measurement [17][18]. If the node mobility speed is high, check for the presence of nodes with the same identity.

The speed is calculated based upon the smooth random mobility model[19]. The speed is assigned the range as $(0,S_{max})$[20][21]. If the node has the set as $\{0, 0.4S_{max}, S_{max}\}$, the probability distribution is in Equation 6.

$$P(s)=\begin{cases} P(s=0)\delta(s) & s=0 \\ P(s=0.4Smax)\delta(s-0.4Smax) & s=0.4Smax \\ P(s=Smax)\delta(s-Smax) & s=Smax \\ 0 & otherwise \end{cases} \quad (6)$$

where $P(s = 0) + P(s = 0.4S_{max}) + P(s= S_{max}) < 1$

The new speed s(t) is taken from the probability distribution between $(0, t_{max})$and(t_{min},0).

$$P(t)=\begin{cases} \frac{1}{t_{max}} & for\ accelertion\ \ 0 < t \le t_{max} \\ \frac{1}{t_{min}} & for\ decleration\ t_{min} \le t < 0 \\ 0 & otherwise \end{cases} \quad (7)$$

A new speed of the node is computed as Equation 7.

$s(t)=s(t-\Delta t)+a(t)\ \Delta t(3)$

Speed of the node increases than the previous speed of the node then the node should be monitored.

Case 2:

If the speed is fixed for long time then the FEC approach is activated then it is in equation 8.

$$S1(t)=s(t-\Delta t)+a(t)\ \Delta t \quad (8)$$

If S1(t)=S(t) then check for the speed at time (t-1). If the speed S1(t)=S(t-1) then the node should be monitored for replica node.

Case 3:

Direction is assumed in the interval $(0,2\Pi)$as Equation 9.

$$P_{\emptyset}(\emptyset) = \frac{1}{2\Pi} \quad for\ 0 \le \emptyset < 2\Pi \quad (9)$$

The direction of the node changes the new direction, it is calculated as Ø(t) and Ø(t') which is represented in Equation 10.

Ø(t) =new direction, Ø(t')-old direction

$$\Delta\emptyset(t)=\begin{cases} \emptyset(t)-\emptyset(t')+2\Pi & \text{for } -2\Pi<\emptyset(t)-\emptyset(t')\leq-\Pi \\ \emptyset(t)-\emptyset(t') & \text{for } -\Pi<\emptyset(t)-\emptyset(t')<\Pi \\ \emptyset(t)-\emptyset(t')-2\Pi & \text{for } \Pi<\emptyset(t)-\emptyset(t')\leq 2\Pi \end{cases} \quad (10)$$

The movement direction should be smooth and small direction changes have to be recorded. The direction value should be very small as $\Delta\varphi(t)$.

Case 4:

The node moves and change its location at time(T, T-i) . The mobile node never moves faster than S_{max}. Then it is computed by Equation 11.

$$\left|\frac{\|L1-L2\|}{\|T1-T2\|-int}\right|\leq Smax \quad (11)$$

The algorithm about the proposed in Fig.4.

```
Initialization: n=0,
Input: Node id ID, Location information L, Time information T
Output: Replicated node or not Replicated node.
Curloc=L
Curtime=T
If n>0
Compute Speed from target and time s(t)=s(t-Δt)+a(t) Δt.
Formulate H0 and H1, and specify α
Check the value of the test statistics falls, reject the null hypothesis.
If n is reject
    Compute the direction from cur loc and pre loc.
    Perform hypothesis test.
    If n is reject
        Check the Virtual Certificate
        If not match then
            Assign n as replicated node
End if
  n=n+1
end
```

Fig.4 Algorithm for FEC Approach

4. RESULTS AND DISCUSSION

4.1 HNN Approach

The maximum distance is MD and if the replica node is present in one slot is assigned as MD+r. Suppose R and R' are the replicas present in the network. Neighbors of the node and the replicas are present in the circle is assigned as MD+r. In a random time t1, a replica node with different location id is present in the neighbor P. ϵ indicates the number of elements of e are hosted in the node. If d nodes can locate in d cells and event e exactly in different nodes is discussed in equation 12.

$$P(D') = \sum_{i=1}^{d} P(\epsilon | ei) \quad (12)$$

The probability is that at least one replica node should be in the network.

$$P(D)=1-P(D') \quad (13)$$

$$=1-(\sum_{i=1}^{d}\frac{(q-i)^d}{q}P(wi])^j \quad (14)$$

4.1.1 Detection Probability

The detection accuracy of the proposed work HNN is compared with the existing system EHDM [17] and HIP-HOP [15]. When d=4 the HOP and EHDM detection rate is 88.7 and 64.86. When a node verifies with its neighbor at one slot it identifies only 88.7% of clone node. If the d value increases, the clone detection rate is also increasing. The HOP method detection rate increases if the speed and the slot value increase resulting in the increase of detection rate. In the proposed HNN approach the mobile node is assigned as fixed and if the d value increases the detection rate also increased and achieved 100% detection accuracy shown in Fig. 5. The detection accuracy for one slot is discussed in the Table 1.

D	4	6	8	10	12	14	16	18
HNN(proposed)	88.7	99.5	100	100	100	100	100	100
EHDM	64.86	92.48	99.20	99.95	100	100	100	100
HOP	7.93	7.93	31.06	44.96	58.40	70.24	79.8	87.13

Table 1 Detection Probability in one slot

If the slot is five then the detection rate is 100% for all the d values 4,6,8,10,12,14,16,18 shown in Table 2. In EHDM approach the detection accuracy is 100% from d=10. The proposed approach detection rate is high when compared with the existing approach HIP-HOP and EHDM approach. If the slot is 10 and d=4 the HNN approach produce 100% detection accuracy, EHDM approach produce 100% detection accuracy and HIP-HOP approach detection accuracy is 70.45% shown in Fig.5.

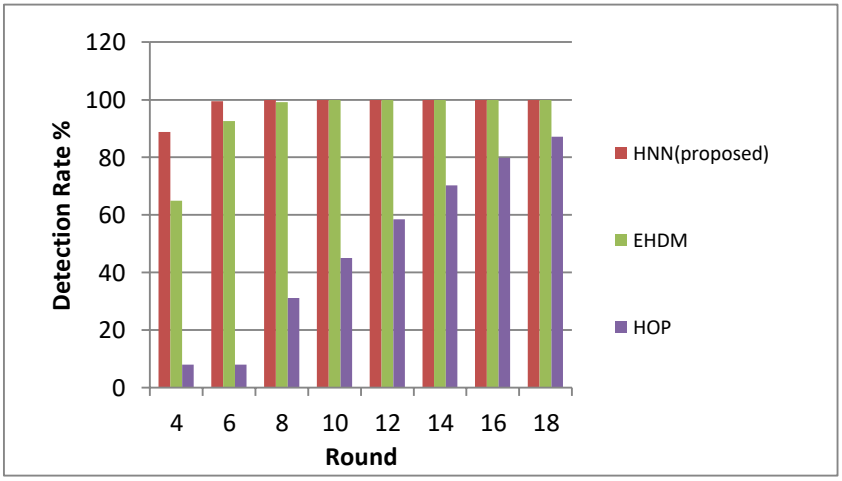

Fig.5 Detection Accuracy in slot one

d	4	6	8	10	12	14	16	18
HNN(proposed)	100	100	100	100	100	100	100	100
EHDM	79.44	97.92	99.93	100	100	100	100	100
HOP	33.83	63.32	84.42	94.95	98.75	99.97	99.97	99.97

Table 2 Detection Accuracy in slot 5

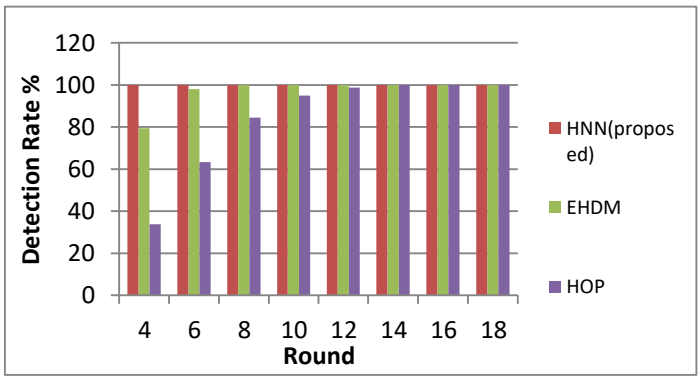

Fig. 6 Detection Accuracy in slot 5

4.1.2 Communication Overhead

During the detection, the nodes transfer the logs. Thus one node may send and receive a logs as (ld+1) per slot. The overhead for the HNN approach is $O(ld^2)$. The communication cost of the existing system HIP-HOP approach and EHDM approach is $O(fd^2)$.

4.2 FEC Approach

At random time t, a node x is selected and observed with the samples of speed and direction using SPRT [21]. Each samples are observed and verified using Bernoulli random variable in Equation 15.

$$E_i=\begin{cases}0 & if\ S(t)\trianglelefteq Smax\\ 1 & if\ S(t)\triangleright Smax\end{cases} \quad (15)$$

The success probability is calculated and assigned as λ, in Equation 16.

$$P(E_i=1)=1-P(E_i=0)=\lambda \quad (16)$$

A node x from the speed is utilized for estimations. The Log Probability ratio is calculated as Equation 10 and 17.

$$R_n=\ln\frac{(P(E1\ldots\ldots\ldots\ldots..En|H1)}{(P(E1\ldots\ldots\ldots\ldots\ldots En|H0)} \quad (17)$$

$$R_n=\ln\frac{\Pi_{i=1}^{n}(P(Ei|H1)}{\Pi_{i=1}^{n}(P(Ei|H0)}$$
$$=\sum_{i=1}^{n} ln\frac{P(Ei|H1)}{P(Ei|H0)} \quad (18)$$

SPRT for null hypothesis and alternate hypothesis is represented as α'

$R_{n\trianglelefteq\ln\frac{\beta'}{1-\alpha'}}$ accept Ho $R_{n\geq\ln\frac{1-\beta'}{\alpha'}}$ accept H1

$\ln\frac{\beta'}{1-\alpha'}<R_n<\ln\frac{1-\beta'}{\alpha'}$ with another observation α' and β' are false positive and false negative.

Packet Loss Rate

The Packet Loss Rate is to calculate by Equation 19.

$$PLR=\frac{\text{Total Data lost}}{\text{Total data}} \quad (19)$$

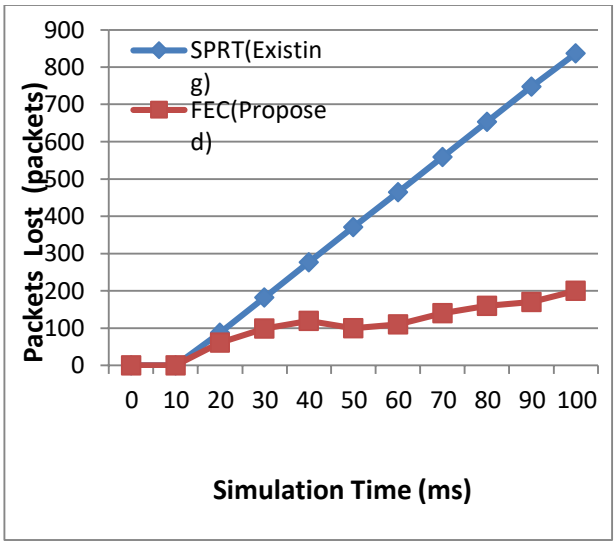

Fig. 7 Packet Loss Rate

PLR is lower for both static and mobile scenario than the existing methods in Fig. 7.

Average Delay

The average delay is measured by Equation 20.

$$D = \frac{\sum_0^n \text{Send Time} - \text{RecvdTime}}{\text{totaltime}} \quad (20)$$

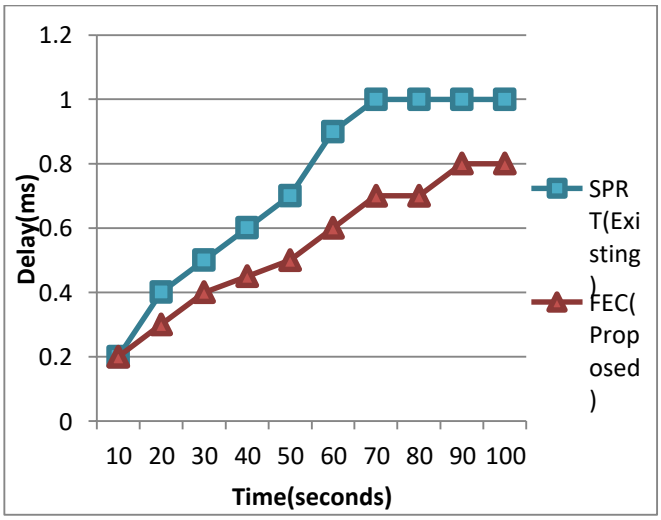

Fig. 8 Delay

Fig.8 discusses the delay for the proposed scheme for SPRT and FEC (proposed).

Detection Accuracy

The existing system has a drawback, if a clone node is less, the detection rate is less. The proposed system has 100% accuracy if the number of clone node is increasing above 6. The detection accuracy of the proposed system has 99.8% shown in fig.9.

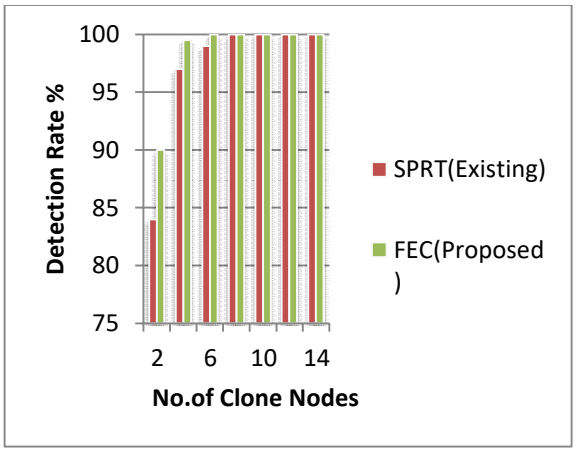

Fig. 9 Detection Accuracy

5 Conclusion

Replica node detection in distributed mobile WSN is more difficult to detect. The proposed system uses three methods to identify replica nodes. The first system uses node's own log list. The second method uses a neighbor node log list. In the third method, a node is selected as a verifier and a check for the replica. The methods are compared with the existing systems HIP-HOP, EHDM and their performance is analyzed. The proposed methods HNN have high detection rate and less communication overhead when compared with the EHDM and HOP. The FEC approach is to detect replica node. It uses SPRT technique to verify the proposed system. The FEC approach is compared with the existing systems. The FEC approach offer high detection rate and minimal communication overhead compared with the existing system.

Compliance with Ethical Standards:

Conflict of Interest: Authors has no conflict of interest.
Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Akyildiz, IF., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002), "A Survey on Sensor Networks", IEEE Communication Magazines, Vol.40, Issue.8, pp.102–114.
2. Osanaiye, O., Alfa, A. S., & Hancke, G. P. (2018). A statistical approach to detect jamming attacks in wireless sensor networks. Sensors, 18(6), 1691.
3. Han, G., Shen, W., Duong, T. Q., Guizani, M., & Hara, T. (2014). A proposed security scheme against denial of service attacks in cluster-based wireless sensor networks. Security and Communication Networks, 7(12), 2542–2554.
4. Brooks, R., Govindaraju, P.Y., Pirretti, M., Vijaykrishnan, N. and Kandemir, M.T. (2007), "On the Detection of Clones in Sensor Networks Using Random Key Predistribution" , IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews , Vol.37, No.6, pp.1246-1258.
5. Nurgaliyev, M., Saymbetov, A., Yashchyshyn, Y., Kuttybay, N., & Tukymbekov, D. (2020). Prediction of energy consumption for LoRa based wireless sensors network. Wireless Networks, 26(5), 3507–3520.
6. Conti, M., Di Pietro, R. and Spognardi A. (2014), "Clone wars: distributed detection of clone attacks in mobile WSNs", Journal of Computer and System Sciences, Vol. 80, No. 3, pp. 654–669.
7. W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A trust-based security system for data collecting in smart city," IEEE Transactions on Industrial Informatics, p. 1, 2020.
8. Heesook Choi,SencunZhu and La Porta, T.F. (2007), "SET: Detecting node clones in sensor networks", proceedings of the 3rdInternational Conference on Security and Privacy in Communications Networks and the Workshops, Vol.341, No.350, pp.17-21.

9. Ho, J.W., Wright, M. and Das, S. K. (2011), "Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing", IEEE Transactions on Mobile Computing, Vol. 10, No. 6, pp. 767–782.

10. Manjula, V., and Chellappan, C. (2011), "The replication attack in wireless sensor networks: analysis and defenses", Advances in Networks and Communications, pp. 169-178.

11. Yu, C. M., Lu, C. S. and Kuo, S. Y. (2008), "Mobile sensor network resilient against node replication attacks", proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '08), pp. 597–599.

12. Yu, C. M., Lu, C. S. and Kuo, S. Y. (2009), "Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks", proceedings of the 70th IEEE Vehicular Technology Conference (VTC Fall '09), pp. 20–23.

13. Deng, X., Xiong, Y. and Chen, D. (2010), "Mobility-assisted detection of the replication attacks in mobile wireless sensor networks", proceedings of the 6th Annual IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob, 2010), pp.225–232.

14. Xing, K., Cheng, X., Liu, F. and Du, D. H. C. (2008), "Real-time detection of clone attacks in wireless sensor network", proceedings of the 28th International Conference on Distributed Computing Systems , pp. 3–10.

15. Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu and Sy-Yen Kuo (2013), "Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Network", IEEE Transactions on Information Forensics and Security,Vol.8, No. 5.

16. Conti, M., Di Pietro, R. and Spognardi A. (2014), "Clone wars: distributed detection of clone attacks in mobile WSNs", Journal of Computer and System Sciences, Vol. 80, No. 3, pp. 654–669.

17. Zhou, C. and Wang, Z. (2014), "An two dimension detection to node replication attacks in mobile sensor networks", Proceedings of the 10th IEEE International Conference on Anti-Counterfeiting, Security, and Identification IEEE (ASID '16), Xiamen, China.

18. Wang, Ze, Zhou, Chang and Liu, Yiran. (2017), "Efficient Hybrid Detection of Node Replication Attacks in Mobile Sensor Networks", Mobile Information Systems, pp. 1-13.

19. Foh, C. H., Liu, G.,. Lee,B. S.,Seet, B.C., Wong, K.J. and Fu,C. P.(2005), "Network connectivity of one-dimensional MANETs withrandom waypoint movement", IEEE Communications Letters,Vol.9, No.1, pp.31–33.

20. Dhamodharan, U. S. R. K., Nagamani, M. and Krishnamoorthy, V. (2019). An Efficient Node Ranking Mechanism for Identifying Selective Forwarding Attacks in WSN. International Journal on Emerging Technologies, 10(4): 50–56.

21. Anitha, S., Jayanthi, P. & Thangarajan, R. Detection of Replica Node Attack Based on Exponential Moving Average Model in Wireless Sensor Networks. Wireless Pers Commun **115,** 1651–1666 (2020).

Figures

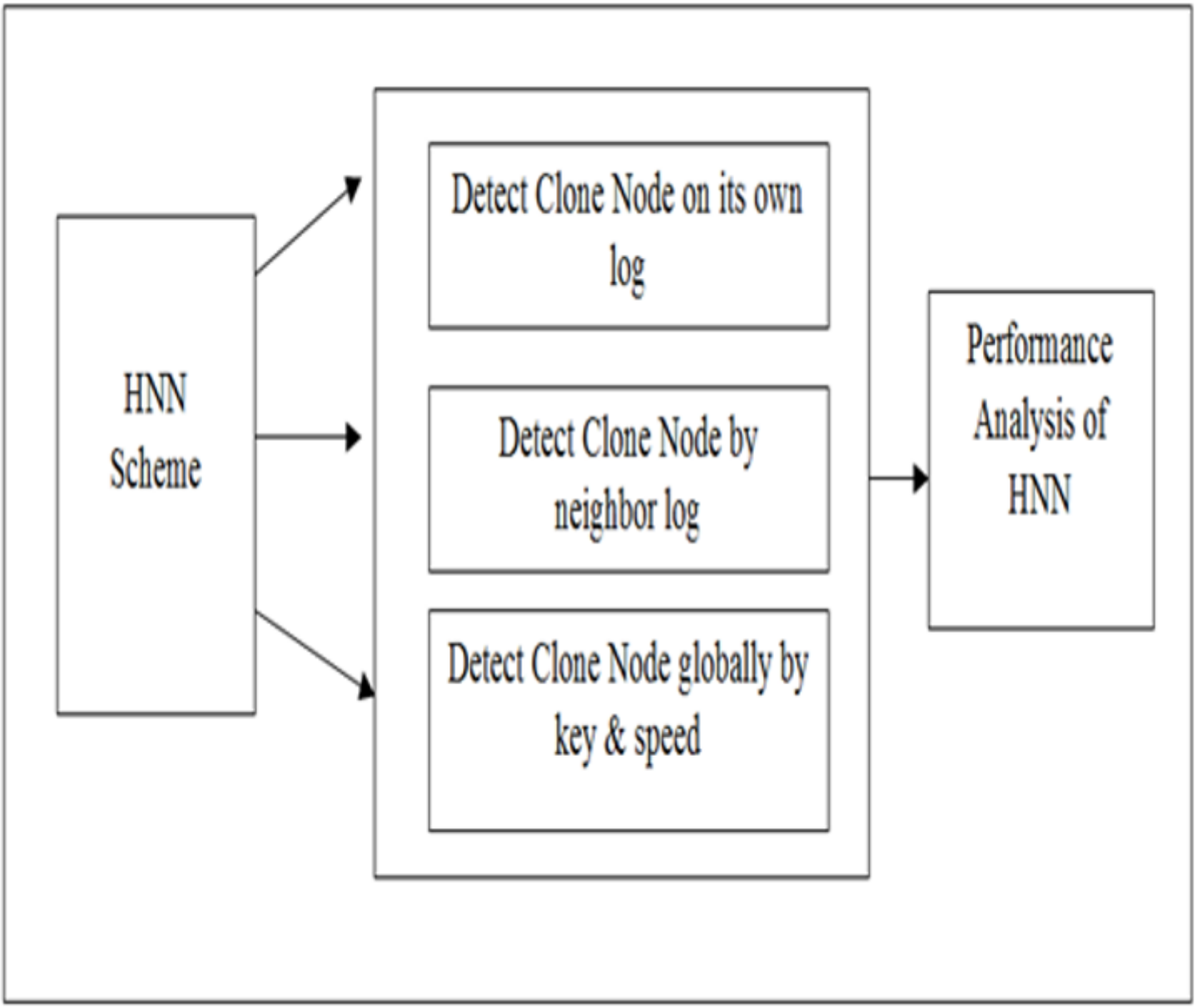

Figure 1

Overview of HNN Architecture

Node ID	Location ID	Time

Figure 2

Neighbor log Field

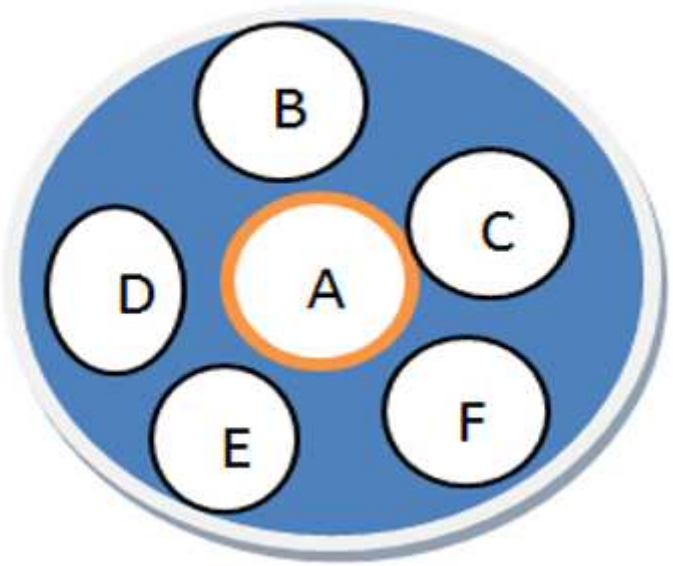

Figure 3

Neighbor Node

```
Initialization: n=0,
Input: Node id ID, Location information L, Time information T
Output: Replicated node or not Replicated node.
Curloc=L
Curtime=T
If n>0
Compute Speed from target and time s(t)=s(t-Δt)+a(t) Δt.
Formulate H0 and H1, and specify α
Check the value of the test statistics falls, reject the null hypothesis.
If n is reject
    Compute the direction from cur loc and pre loc.
    Perform hypothesis test.
    If n is reject
        Check the Virtual Certificate
        If not match then
            Assign n as replicated node
End if
  n=n+1
end
```

Figure 4

Algorithm for FEC Approach

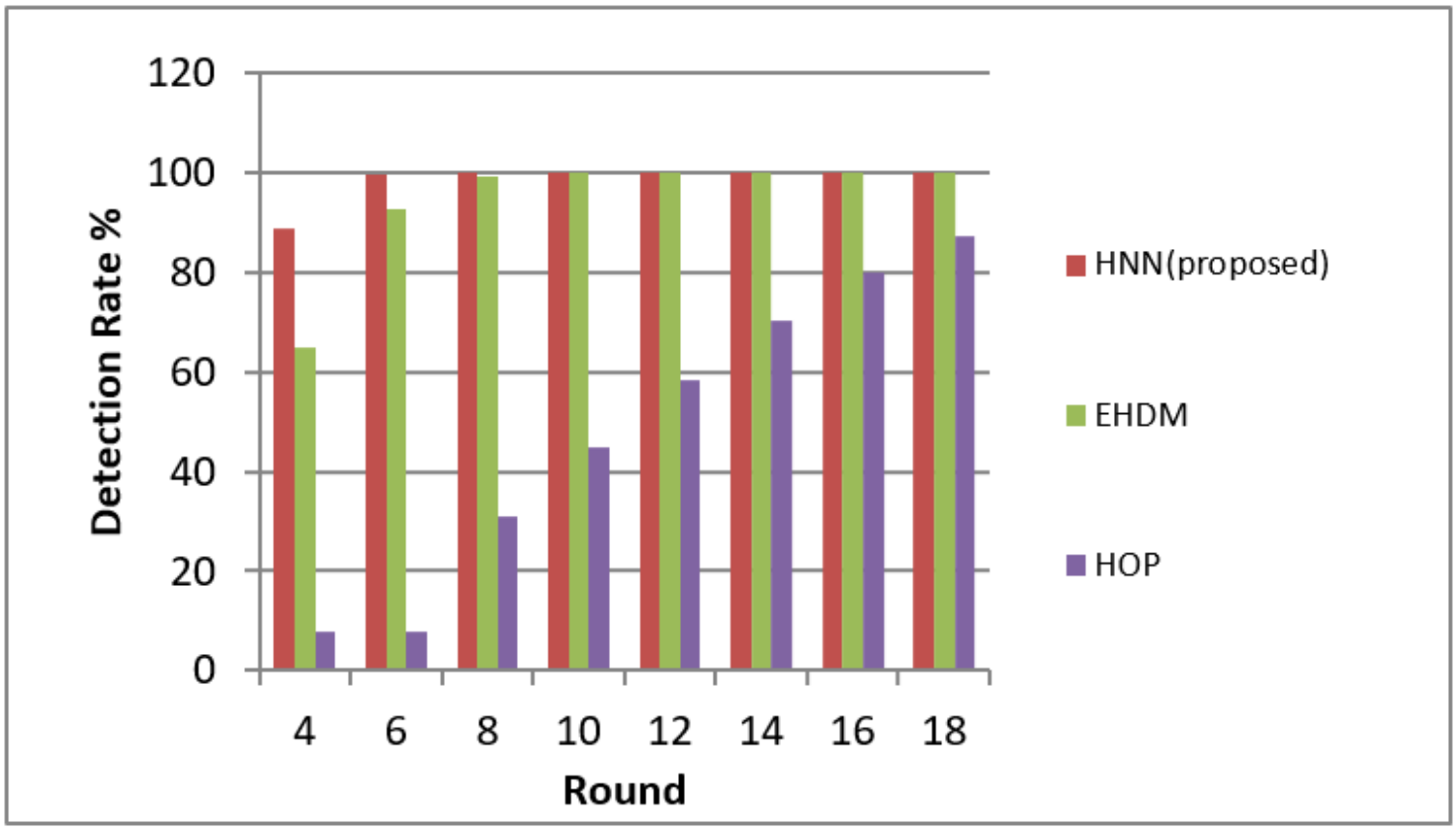

Figure 5

Detection Accuracy in slot one

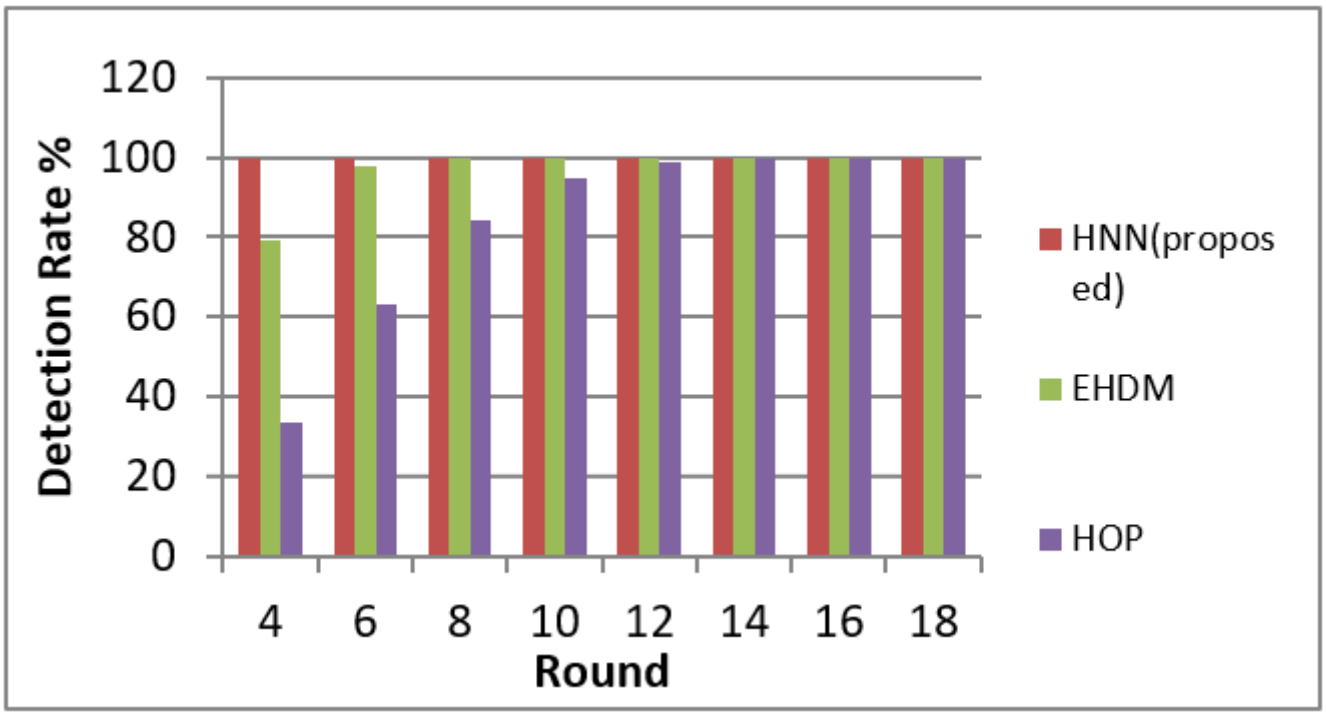

Figure 6

Detection Accuracy in slot 5

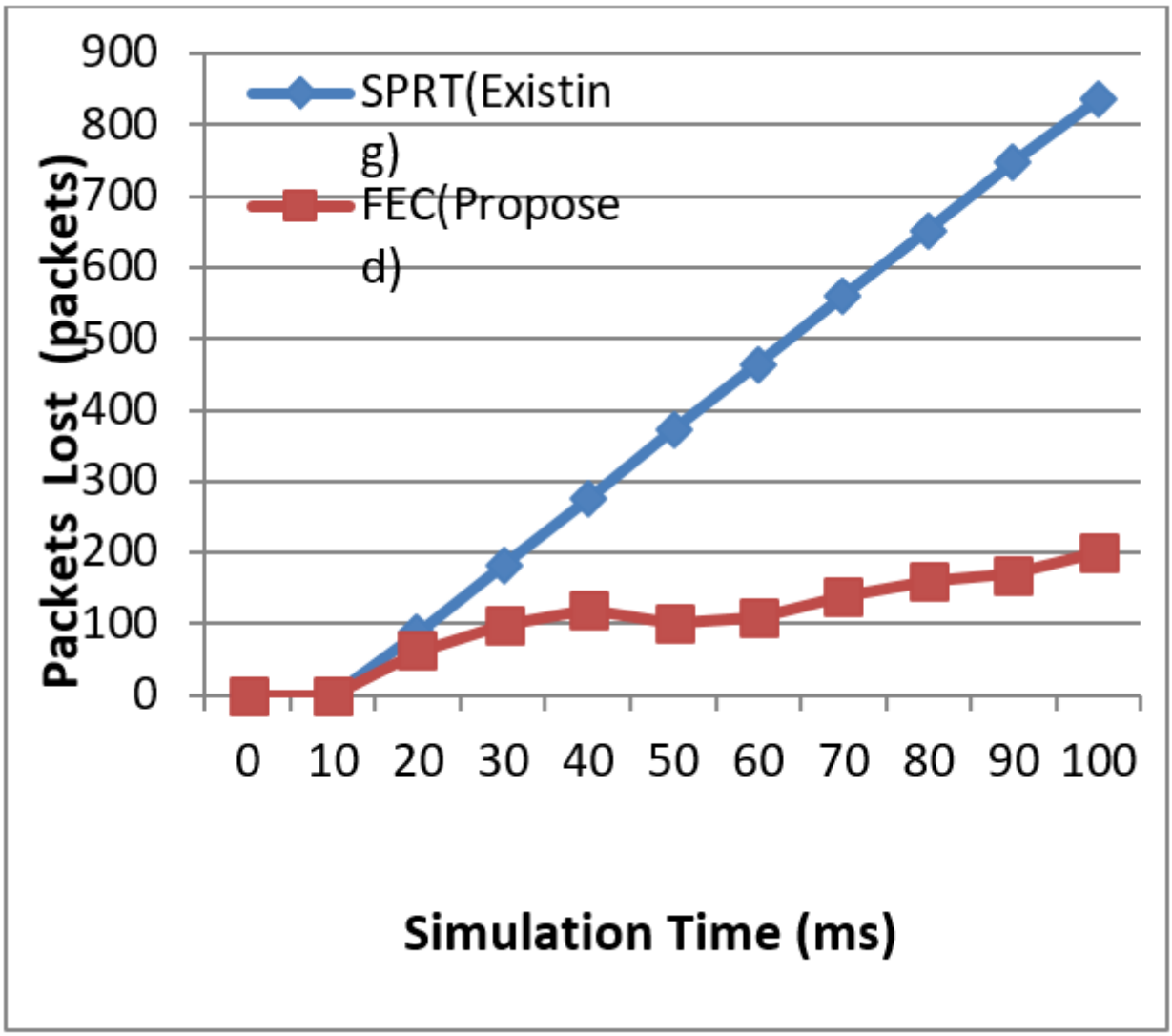

Figure 7

Packet Loss Rate

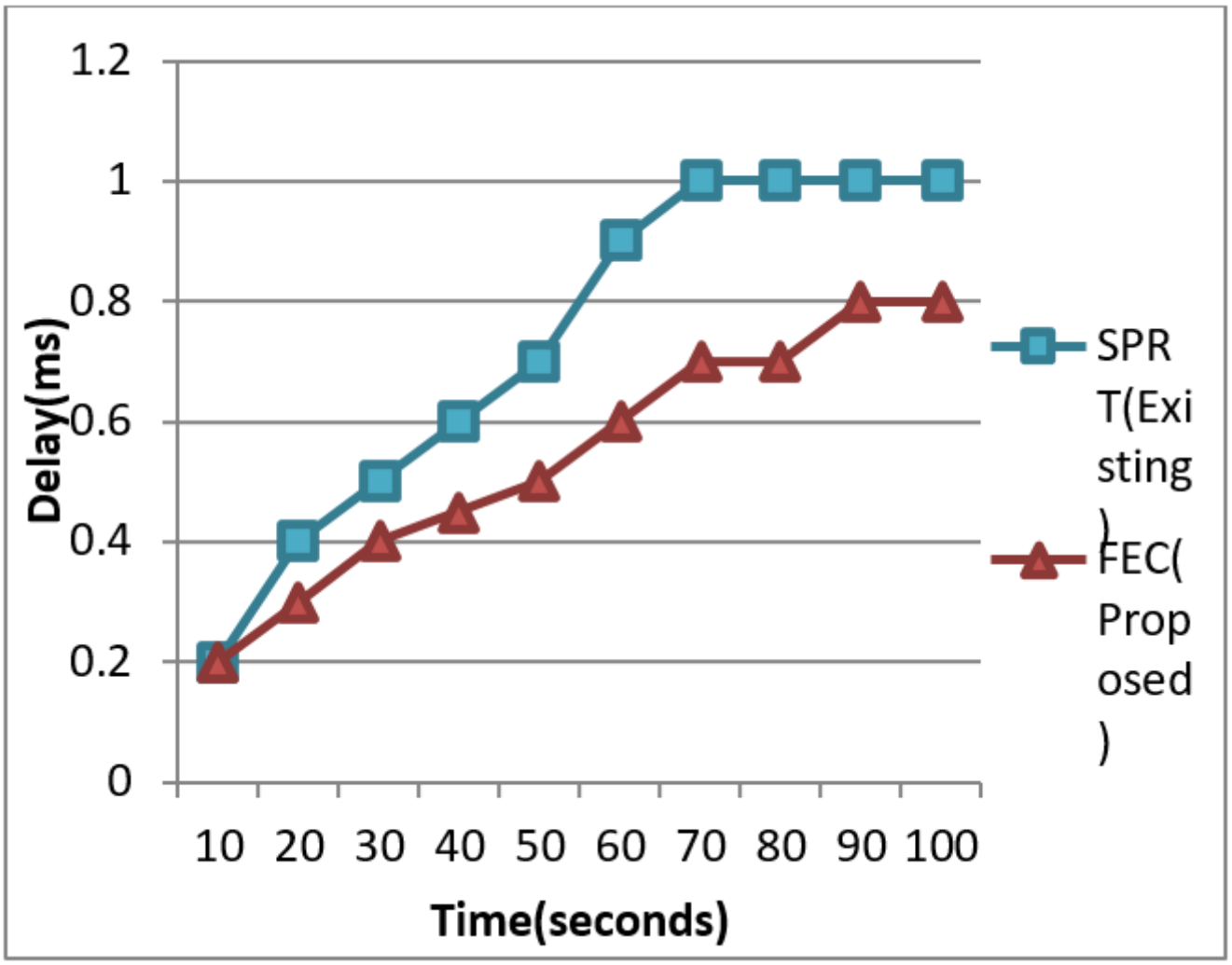

Figure 8

Delay

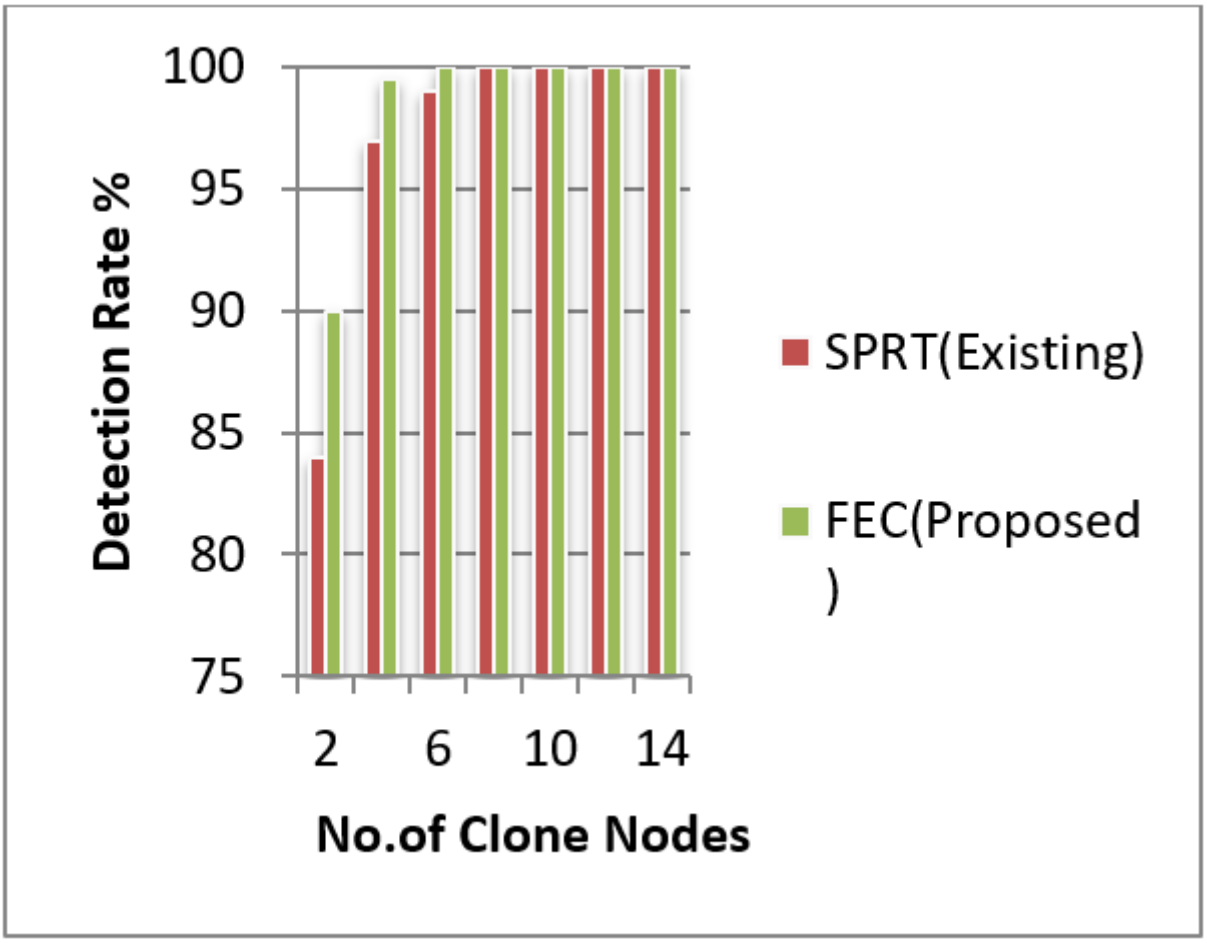

Figure 9

Detection Accuracy