Vol. 9(33), Jul. 2019, PP. 4271-4286

Contents list available at IJMEC

International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)

Journal Homepage: www.aeuso.org

PISSN: 2411-6173 - EISSN: 2305-0543

A New Markov-Based Survivability Model for Wireless Sensor Networks

Athareh Shahabinejad, Reza Javidan* and Manijeh Keshtgari

Department of Computer Engineering and IT, Shiraz University of Technology, Shiraz, Iran

Phone Number: *+98-7137261391*

****Corresponding Author's E-mail:*** *reza.javidan@gmail.com*

Abstract

Network survivability is one of the main design challenges in Wireless Sensor Networks (WSNs). In this paper, a survivability model for WSN is proposed that is based on network availability. In this work, because of its advantages in terms of cost and energy, cluster-based topology for WSNs is selected. In the proposed method, first survivability of a single cluster of WSN is modeled as a continuous time Markov chain. This model is based on software rejuvenation and recovery mechanisms. To apply recovery mechanism, a special WSN model is considered in which each node has a spare one which becomes active when the original one turns into inactive. Afterward, a survivability analysis based on Markov chain on a WSN is presented which consists of multiple clusters. Without loss of generality, a WSN with ten clusters is used as a case for this analysis. Finally a comparative analysis of survivability between two previous works and the proposed model is performed. Results showed that the proposed model improves survivability of cluster by 14% and 3.7% and survivability of WSN by 12.4% and 3.1% in terms of rejuvenation rate, also average improvement of 5.3% is obtained in terms of recovery rate. Previous works addressed survivability of WSNs just for a single cluster while the proposed model in this paper is more general and more accurate. SHARPE simulation tool is used to validate the survivability mathematical evaluations in terms of availability. The results show the superiority of the proposed model.

Keywords: *Survivability, Availability, Software Rejuvenation, Markov, Recovery, WSNs.*

1. Introduction

Wireless Sensor Networks (WSNs) consist of a large number of small sensor nodes which are battery-operated and have capabilities of data processing and short-range radio communications [19]. WSNs have a wide range of applications in agricultural, environmental monitoring, healthcare, traffic control, national defense, homeland security, safety, medical and military applications [6],[7]. The reliance on these WSNs causes their presence to be mission critical. Survivability of a system can be defined as the capability of system to complete its mission, in a timely manner, in the presence of attacks, failures or accidents [6]. Over the past few decades studies have done on survivability of conventional networks[10],[13],[15]. Resource constraints on sensor nodes such as memory, processing power etc. make solutions that are suitable for traditional computer systems; not applicable to WSNs [17]. Survivability in WSNs has several challenges such as wireless nature of communication, resource limitations on sensor nodes, very large and dense WSNs, lack of fixed infrastructure, data redundancy, limited energy, unknown network topology prior to deployment and high risk of physical attacks to unattended sensors. Moreover, in some deployment scenarios sensor

Article History:
Received Date: Dec. 08, 2018
Accepted Date: May. 23, 2019
Available Online: Jul. 01, 2019

nodes need to operate in hostile environments making them susceptible to failures and security attacks [4], [6], [17],[22].

In this paper a new Markov Based survivability model for WSNs is proposed that is based on software rejuvenation and recovery mechanisms. Denial of service and physical attacks are considered and the status of WSN is modeled as a stochastic process. In the proposed model cluster-based topology [6],[22] for WSNs is selected because of its advantages in terms of cost and energy. In the proposed method, survivability of a single cluster of WSN with spare nodes is modeled as a continuous time Markov Chain. Afterward, a survivability analysis based on Markov Chain on a WSN consists of multiple clusters is presented. The simulation results on prototype data show the effectiveness of the proposed method.

The main contributions of this paper can be summarized as follow:

- We takes three mechanisms of rejuvenation, recovery and graceful degradation together that is not the same as stated in other works which usually just use one mechanism of rejuvenation.
- Our work generalizes the approach for the first time and considers WSN as a whole. In all of the previous works that were based on Markov model, survivability was analyzed only for on cluster of WSN.
- Finally, extensive simulation experiments in comparison with other two well-known methods showed effectiveness of the proposed approach.

The rest of this paper is organized as follows. In Section 2, a brief review on related works is presented. The framework for the survivability model of WSN is explained in Section 3. In Section 4 the survivability model for a WSN comprised of duplex sensor nodes is presented. In this section first survivability of a single cluster of WSN is modeled, and then survivability model of a WSN that consists of 10 clusters is presented and analyzed. Section 5 presents performance analysis of the proposed approach for both, a single cluster and the WSN whole self. In addition, a comparative survivability analysis of the proposed topology and a topology with simple nodes is presented. Finally in Section 6 conclusion and remarks are outlined.

2. Related works

Network survivability of WSN has recently attracted considerable attentions [3]. Rejuvenation is the process of roll backing of a program to avoid failures in the future using irregularly terminating, cleaning its internal state and restarting it [23]. It was shown that for most of life-threatening applications rejuvenation is effective to enhance system performance [17]. Kim et. al [6] for the first time presented a framework of survivability model for WSN with software rejuvenation methodology which is applicable in security field and also was less expensive. They showed that software rejuvenation and adaptation mechanisms can increase the probability of the system being stayed in healthy state. Despite of the subject of their paper, they didn't define survivability clearly and didn't present a mathematical formula for analyzing. Moreover, because in state of rejuvenation, system is not survivable and doesn't perform its main task; just being in a healthy state does not determine degree of survivability.

In [21] one method to increase survivability of WSNs with biological characters is suggested. This method is based on semi-Markov process and did not provide a clear mathematical framework for survivability analysis. The authors only considered failures of WSNs base stations; while node faults

are the most common faults in WSNs [12]. Because it considered only base station failures, it cannot be compared with our work.

As another work, Parvin et.al [17] presented a survivability evaluation model for WSNs by a continuous time Markov chain that describes the status of real WSNs. They also modeled and analyzed survivability of WSNs under key compromise. They also presented a complete analytical model and validated their results using simulations. However, the decreasing state of availability in key management schemes does not show a good result.
Liu et. al [22] developed a model to evaluate the tradeoffs between the cost of WSN defense mechanisms and the expected survivability after an attack. They defined survivability as a measurement of performance levels. Their model showed a relationship between the cost of defense mechanisms of the system and the transition probabilities of the state transition matrix where the transition probabilities are functions of the type of incident and the defense mechanism. Their work seems to be hard to understand clearly. Moreover, their mathematical framework is ambiguous and is an arduous work.

Chang et.al [4] proposed a survivability model for WSN based on semi-Markov process (SMP) and Discrete Time Markov Chain (DTMC). In their model, the isolation problem of head cluster node is also included for analyzing. However, their validation step was vague.

Kumar et. al [16] evaluated survivability of WSN by simulating a DDoS attack on a WSN-gateway to highlight how the services on the system will be affected. In this work, the ability of WSN for data collection is selected as a metric to measure survivability. Regarding to enhance fault tolerance to remove vulnerabilities related to the WSN-gateway; they proved that WSN-gateway is a single point of failure. They did not consider WSN survivability in the presence of fault tolerance that they claimed and did not compare its improvement in survivability.

Yi et. al [24] developed a framework that provides security and survivability features that are crucial in many WSN applications. To understand the interactions between security and survivability, they also designed and analyzed a key management scheme. They proposed a secure and survivable WSN architecture which have the requirements and services of reliability, availability, energy efficiency, confidentiality, authentication, integrity and secure management. They mentioned that the security requirements can be described by the metrics of scalability, efficiency, resilience and reliability. To measure reliability and resilience they considered a key connectivity of the new schemes in normal conditions and attack conditions, respectively. Their work mainly considers security and survivability of WSN could be considered in which that availability or energy efficiency be considered.

As another work, Thein et. al [20] proposed a recovery model to increase the availability and survivability of dual cluster-head in WSNs. They found that proactive rejuvenation and recovery mechanisms might have a significant effect on availability and survivability of cluster head of WSN. However, this model has some drawbacks. There should be a possible transition from infected state and rejuvenation state to failure state. Moreover, they should consider a situation when head node and its redundant node fail simultaneously. Since only one duplex head node is included in each cluster, a new head node is simplex and it is in danger of being failed very soon. In addition with a high risk attack when many primary sensor nodes are defected, the limited remained healthy duplex head nodes cannot do the task of a cluster or entire WSN very Well.

Masoum et.al [2] used connectivity and coverage concepts to reduce the permanent failures and improve WSN survivability. In another work [1], they also analyzed survivability of WSN with transient

faults based on network availability model and showed frequent availability of a route. Their works have strong mathematical analysis and proper simulations to validate results.

Finally, Petridou et.al [19] evaluated survivability of WSNs using probabilistic model checking. They considered all types of failures and modeled WSN with a continuous Time Markov chain (CTMC) and then injected faults and attacks in the developed CTMC to study their impact on WSNs. In the work of ref [19], sensors are divided into critical and noncritical nodes. The authors assumed that node fault is dedicated only to critical sensor nodes and typical sensor nodes are considered to just lead data delay, because of losing link connection to critical sensor nodes. Moreover, the impact of failures is considered to be data loss; while if we add recovery mechanisms, this effect can be minimized while in this paper no repair or recovery mechanism is considered with this type of failure. Generally, such assumption that dedicating node faults to critical sensor nodes is not a realistic assumption. Since node fault is the most common among all types of faults [3], our work doesn't consider link failures. We made node fault for all of the nodes: critical or typical sensor nodes and a clear Markov model is presented to analyze the results. Therefore our work outperforms the work of ref. [19] because of its unrealistic assumption.

In addition to methods mentioned so far, some of the Markov-based methods [6],[17],[20] analyzed survivability just for a single cluster of WSN. In addition, in their Markov models, some of possible transitions between states were ignored. Finally, in some cases such as [6],[20], no proper simulation is performed to validate their results.

In this paper a survivability model for WSN is proposed that is based on software rejuvenation and recovery mechanisms. First a new model for survivability of a single cluster of WSN is presented and then this model is applied to the entire WSN. Results are validated using simulations. Finally a comparative survivability analysis is performed between the proposed topology and a WSN with non-redundant nodes. All the results showed the effectiveness of the proposed model.

3. The framework for survivability modeling in WSNs

A topology for survivability modeling is depicted in Fig.1. Cluster-based topology is selected because of its advantages in terms of cost and energy [6],[17]. In this topology, all nodes are duplex sensor nodes. One is active sensor and another is inactive spare sensor. When the active sensor fails, the spare becomes active. Heartbeat mechanism in WSN is proposed to detect node fault. In this mechanism spare sensor sends periodically a packet named heartbeat to its host node. When host receives the heartbeat packet, will send the same packet to the spare node. If this response packet cannot be received in a predefined amount of time, the host node will be considered as faulty node [12]. This framework is hierarchical and one or more clusters are managed by a base station with good CPU power and memory than typical sensor nodes [6]. Each sensor node transfer the collected data to its cluster head node, and the cluster head node sends the collected data to the Base Station (BS) [17]. The BS is connected to the access point of a legacy network such as Internet or satellite communication. This collaborative cluster model provides an abstraction to the framework [6], [17]. Each collaborative cluster can be modeled as a stochastic process which is presented in next section.

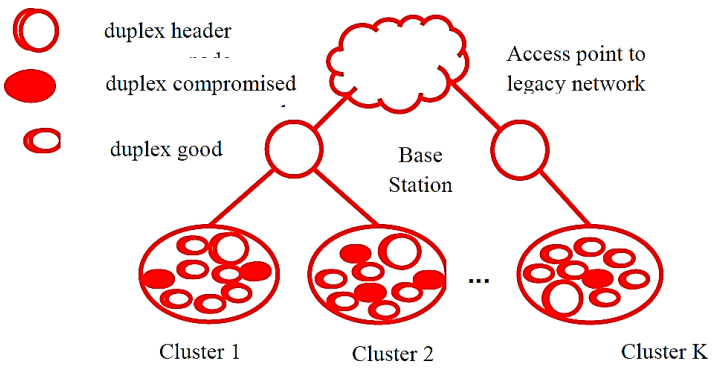

Figure 1: A Topology for Redundant Node Cluster-Based WSN

4. The proposed approach for survivability analysis

In complex systems in which failure rates are assumed to be constant, Markov models can be used for deriving expressions for the system reliability. They also include repair process. In this section to analyze the reliability [8], the proposed survivability model based on the framework presented in previous section is introduced. The proposed model is a stochastic model with multiple states with state transition diagram which is shown in Fig. 2. A stochastic process at time t, X(t), is an infinite number of variables. Process X(t) is called a Markov chain if:

$$Prob\{X(t_n)=j \mid X(t_0=i_0),X(t_1=i_1),\ldots,X(t_{n-1}=i_{n-1})\}=Prob\{\{X(t_n)=j \mid X(t_{N-1}=i_{N-1})\} \quad (1)$$

for every $t_0<t_1<\cdots<t_{N-1}<t_n$

If *X(t)=i* it means that the chain at time *t*, is in state *i* [24].

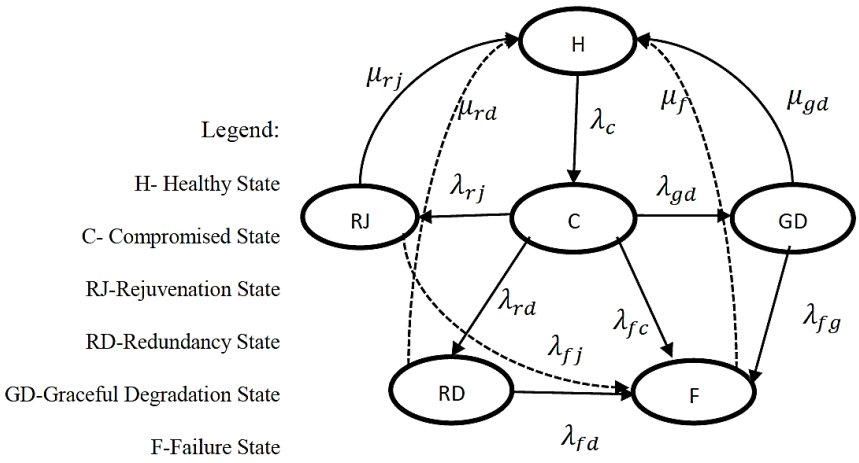

Figure 2: State Transition Diagram of a Single Cluster of WSN

4.1. The System Model

In this section the system model which is proposed in Fig. 2 will be described and analyzed. In this model, at first the cluster is in the healthy state H. As expressed in reference [14], if the number of compromised nodes being infected by an adversary exceeds from a predetermined threshold value, the system switches to the compromised state C. The attack's behavior can be represented by the states {H, C}. In the compromised state, system has to determine whether should rejuvenate the compromised nodes or switch into the spare sensor nodes or provide minimum services. If critical requirements of the system are defined to be integrity and confidentiality, then system switches to

rejuvenation state RJ. On the other hand, if system needs to be available to satisfy minimum services, it switches to graceful degradation state GD. If it is necessary that the system accomplishes full services as in the healthy state or if the impact of the damage is high and it is not suitable to rejuvenate the nodes, system switches to redundancy state RD. In this state all of the compromised nodes are replaced with their redundant spare nodes. If the system does not successfully switch into one of these states, it goes to failure state. In the RJ, GD and RD states if proper action is performed successfully, system recovers to the healthy state; otherwise it goes to the failure state F. Therefore, system responses during and after attack can be represented by the states {GD, RJ, RD, F}. Operating system parameters and their descriptions and values are represented in Table 1. Random system operation parameter values are mostly used to perform experiment [6], [17], [20]. Moreover, in this work random system operation parameter values in Table 1 are used for executing the equations. The state transition diagram in Fig. 2 can be described by the Markov process.

Table 1: Steady state parameters of stochastic approach

Parameter	Description	value
λ_c	Compromised rate	1 time/hr
λ_{rj}	Rejuvenation rate	0, 1/15, 1/10, 1/5, 1/3 (per min)
λ_{gd}	Switch over to graceful degradation rate	1/3(per min)
λ_{rd}	Switch over to redundancy rate	1/3(per min)
λ_{fc}	Unsuccessful compromised switching rate	1/5(per min)
λ_{fj}	Unsuccessful rejuvenation rate	1/5(per min)
λ_{fd}	Unsuccessful redundancy rate	1/5(per min)
λ_{fg}	Unsuccessful graceful degradation rate	1/5(per min)
μ_{rj}	Recovery rate of rejuvenation	0.8 (per sec)
μ_{rd}	Recovery rate of redundancy	0.2, 0.4, 0.6, 0.8, 1(per sec)
μ_{gd}	Recovery rate of graceful degradation	1 (per sec)
μ_f	Recovery rate of failure state	2 times/ hr

The steady-state probabilities are computed by writing down the balance equations. πi means the probability of being in state *i*.

$$
\begin{aligned}
&H: \mu_f\pi_f + \mu_{gd}\pi_{gd} + \mu_{rd}\pi_{rd} + \mu_{rj}\pi_{rj} = \lambda_c\pi_h \\
&C: \lambda_c\pi_h = \left(\lambda_{rj} + \lambda_{rd} + \lambda_{fc} + \lambda_{gd}\right)\pi_c \\
&GD: \lambda_{gd}\pi_c = (\mu_{gd} + \lambda_{fg})\pi_{gd} \\
&RJ: \lambda_{rj}\pi_c = (\mu_{rj} + \lambda_{fj})\pi_{rj} \\
&RD: \lambda_{rd}\pi_c = (\mu_{rd} + \lambda_{fd})\pi_{rd} \\
&F: \lambda_{fc}\pi_c + \lambda_{fg}\pi_{gd} + \lambda_{fj}\pi_{rj} + \lambda_{fd}\pi_{rd} = \mu_f\pi_f
\end{aligned}
\tag{2}
$$

And general equation:

$$\pi_h + \pi_c + \pi_{rj} + \pi_{gd} + \pi_{rd} + \pi_f = 1 \tag{3}$$

Combining these equations and solving them, the following expressions for the steady-state probabilities are obtained:

$$\pi_c = \frac{\lambda_c}{(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})}\pi_h$$

$$\pi_{gd} = \frac{\lambda_{gd}\lambda_c}{(\mu_{gd}+\lambda_{fg})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})}\pi_h$$

$$\pi_{rj} = \frac{\lambda_{rj}\lambda_c}{(\mu_{rj}+\lambda_{fj})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})}\pi_h$$

$$\pi_{rd} = \frac{\lambda_{rd}\lambda_c}{(\mu_{rd}+\lambda_{fd})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})}\pi_h$$

$$\pi_f = \left(\frac{\lambda_{fc}\lambda_c}{\mu_f(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{fg}\lambda_{gd}\lambda_c}{\mu_f(\mu_{gd}+\lambda_{fg})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{fj}\lambda_{rj}\lambda_c}{\mu_f(\mu_{rj}+\lambda_{fj})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{fd}\lambda_{rd}\lambda_c}{\mu_f(\mu_{rd}+\lambda_{fd})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})}\right)\pi_h$$

$$\pi_h = \left(1 + \frac{\lambda_c}{(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{gd}\lambda_c}{(\mu_{gd}+\lambda_{fg})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{rj}\lambda_c}{(\mu_{rj}+\lambda_{fj})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{rd}\lambda_c}{(\mu_{rd}+\lambda_{fd})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{fc}\lambda_c}{\mu_f(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{fg}\lambda_{gd}\lambda_c}{\mu_f(\mu_{gd}+\lambda_{fg})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{fj}\lambda_{rj}\lambda_c}{\mu_f(\mu_{rj}+\lambda_{fj})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})} + \frac{\lambda_{fd}\lambda_{rd}\lambda_c}{\mu_f(\mu_{rd}+\lambda_{fd})(\lambda_{gd}+\lambda_{rj}+\lambda_{rd}+\lambda_{fc})}\right)^{-1} \quad (4)$$

The availability and survivability of system can be defined as follows:

$$availability = 1-\pi_f \quad (5)$$

It means that availability of a system is the probability of system being in every state except failure state.

$$survivability=availability-(\pi_{rj}+\pi_{rd}) \quad (6)$$

According to Eq. (5) and Eq. (6), survivability of the system depends on the probability that the cluster is in the failure, rejuvenation and redundancy states. Therefore, it is necessary to minimize the time being in failure, rejuvenation, and redundancy states. This means that the actions should be performed and the system should be recovered from the failure state, quickly. Notice that in the GD state, system is available and survivable because it is doing its main task but in a degraded state. In addition, in work [6], it is mentioned that if availability is needed, system goes to the GD state. The effect of rejuvenation and recovery on the availability and survivability of system can be determined. Therefore, availability and survivability of the system are calculated using the operation system parameter values in Table. 1, Eq. (5) and Eq. (6).

4.2. Survivability Model for WSN

In this section, the model for WSN is presented. It is assumed that the WSN consists of 10 clusters and it completely fails to accomplish its task, when all of the clusters fail. Fig. 3 shows the state transition diagram of the assumed WSN. It is obvious that when a cluster fails with rate λ_{Cr}, the state changes to the state with one cluster lesser; for example from state 10 to state 9. If the system is repaired, it returns to higher number state with rate μ_{Cr}.

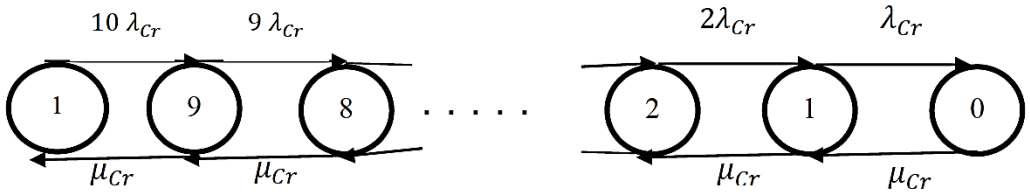

Figure 3: State Transition Diagram of WSN

Differential equations of the WSN cluster model which is described in Fig. 2 are:

$$\frac{dp_h}{dt} = \mu_{rj}p_{rj}(t) + \mu_{rd}p_{rd}(t) + \mu_{gd}p_{gd}(t) - \lambda_c p_h(t)$$

$$\frac{dp_c}{dt} = \lambda_c p_h(t) - \left(\lambda_{rj} + \lambda_{rd} + \lambda_{gd} + \lambda_{fc}\right)p_c(t)$$

$$\frac{dp_{rj}}{dt} = \lambda_{rj}p_c(t) - (\mu_{rj} + \lambda_{fj})p_{rj}(t)$$

$$\frac{dp_{rd}}{dt} = \lambda_{rd}p_c(t) - (\mu_{rd} + \lambda_{fd})p_{rd}(t)$$

$$\frac{dp_{gd}}{dt} = \lambda_{gd}p_c(t) - (\mu_{gd} + \lambda_{fg})p_{gd}(t)$$

$$\frac{dp_f}{dt} = \lambda_{fc}p_c(t) + \lambda_{fg}p_{gd}(t) + \lambda_{fd}p_{rd}(t) + \lambda_{fj}p_{rj}(t) \quad (7)$$

Solving the above set of differential equations with initial conditions $p_h(0)=1, p_c(0)=0, p_{rj}(0)=0, p_{rd}(0)=0, p_{gd}(0)=0, p_f(0)=0$, and keep in the mind that to calculate reliability, the edge from a failure state to a healthy state; the edge with label μf, should be ignored. Reliability of a cluster is obtained by Eq. (8) [24].

$$R(t)=1-pf(t) \quad (8)$$

Therefore MTTF of a cluster ($MTTF_{Cr}$) of WSN is obtained.

$$MTTF_{Cr}=\int R(t)dt \infty 0 \quad (9)$$

Solving Eq. (9) and differential equation set (7) using random system operating parameters in Table 1 and finally by solving Eq. (10) the value of failure rate of WSN, λCr is obtained as:

$$\lambda_{Cr} = \frac{1}{MTTF_{Cr}} \tag{10}$$

The state transition diagram in Fig. 3. can be modeled by the Markov process. The stationary probabilities are computed by writing down the balance equations. By solving the balance equations of state transition diagram of Fig.3 which are obtained as in Eq. (2) , the probability of being in state *i*, is obtained from Eq. (11):

$$\pi_i = \frac{i!(\frac{\mu_{Cr}}{\lambda_{Cr}})^i}{\sum_{k=0}^{10} \frac{(\frac{\mu_{Cr}}{\lambda_{Cr}})^k}{k!}} \tag{11}$$

Availability of WSN can be defined as the probability of being in each state except state 0; because in this state no cluster is available and all of them are failed.

$$availability = 1 - \pi_0 = 1 - \frac{1}{\sum_{k=0}^{10} \frac{(\frac{\mu_{Cr}}{\lambda_{Cr}})^k}{k!}} \tag{12}$$

Eq.(12) with the help of Eq. (8)-(11) show that availability of the system depends on rejuvenation rate and recovery rate of the cluster which are variables in our experiments.

In addition, WSN is survivable if none of active clusters are in the rejuvenation or redundancy states. This is satisfied by Eq.(13):

$$Survivability = Availability - \sum_{i=1}^{10} \binom{10}{i} (\pi_{rj} + \pi_{rd})^i \pi_f{}^{10-i} = Availability - \left(10(\pi_{rj}+\pi_{rd})\pi_f{}^9 + 45(\pi_{rj} + \pi_{rd})^2\pi_f{}^8 + \cdots + 10(\pi_{rj} + \pi_{rd})^9\pi_f + (\pi_{rj} + \pi_{rd})^{10}\right) \tag{13}$$

Eq.(13) shows that survivability like availability depends on both rejuvenation rate and recovery rate. Using random system operation parameters in Table 1 and assuming that μCr=1 $times/hour$, availability and survivability of the system are calculated using Eq. (12) and Eq. (13) and the effect of recovery and rejuvenation on availability and survivability of WSN can be shown.

5. Discussion

In this section, availability and survivability of the system will be analyzed. Table 2 shows parameters that will be evaluated and analyzed.

Table 2: Parameters of evaluation

parameter	In terms of
Availability of a single cluster-Availability of WSN	Rejuvenation rate(λ_{rj})-recovery rate(μ_{rd})
Survivability of a single cluster-Survivability of WSN	Rejuvenation rate(λ_{rj})-recovery rate(μ_{rd})

5.1 Performance analysis of the model of the single cluster

Figs. 4 and 5, according to Eq. (5) and Eq. (6), show that as the rejuvenation rate (in terms of number of nodes that are rejuvenated per second) increases, availability and survivability of system increase.

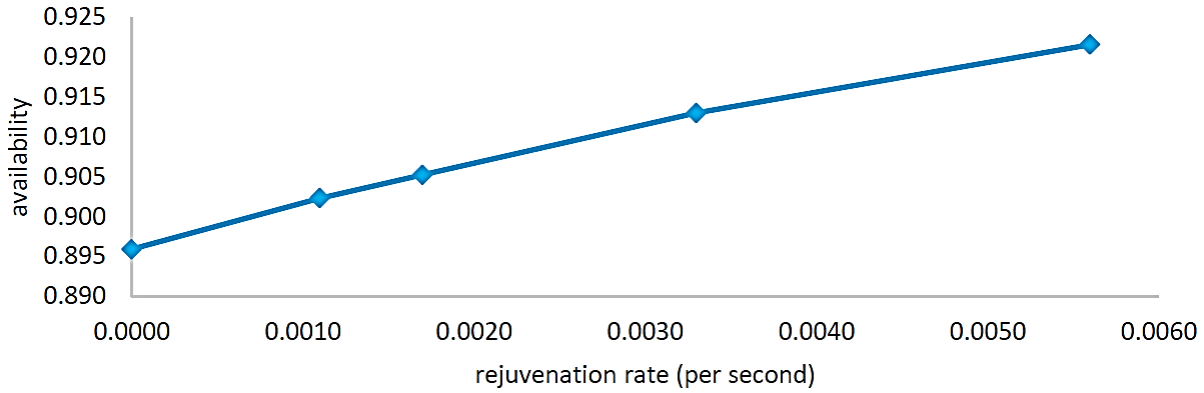

Figure 4: Availability vs. Rejuvenation Rate

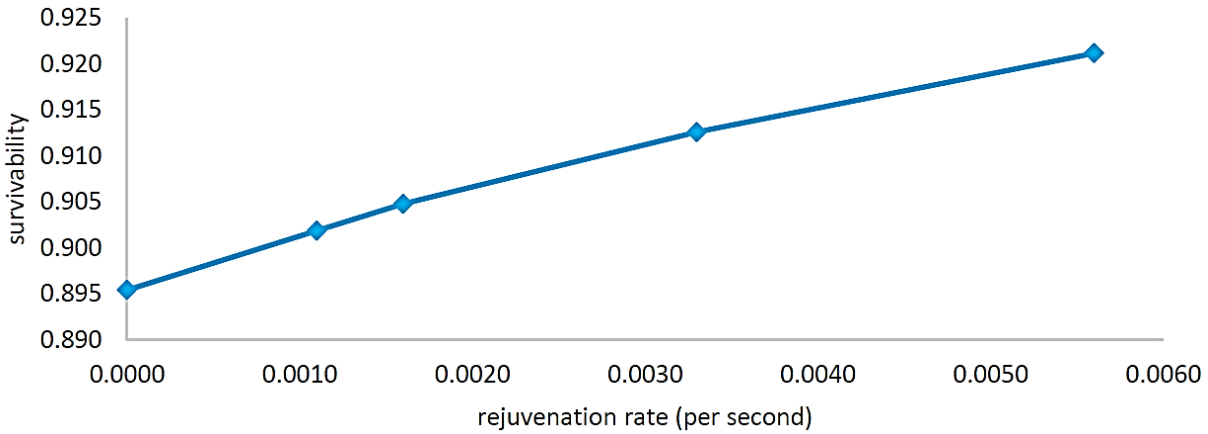

Figure 5: Survivability vs. Rejuvenation Rate

Figs. 6 and 7 show changes in availability and survivability of the system versus increasing the recovery rate (in terms of number of nodes that can be recovered per second). Fig. 6 shows that availability of the system increases with increasing in the recovery rate. Fig.7 shows that if recovery strategy is applied, survivability of the system will be increased. The proposed model is validated using SHARPE (Simulated Hierarchical Automated Reliability and Performance Evaluator) which is the most widely used simulator for measuring reliability and performance of networks. It allows the users to analyze the stochastic models [5 ,11]. The rates of simulation are adjusted according to Table 1 to be the same as mathematical analysis. It is obvious that as recovery rate increases, the result of simulation and mathematical analysis match. And this shows the correctness of the mathematical analysis.

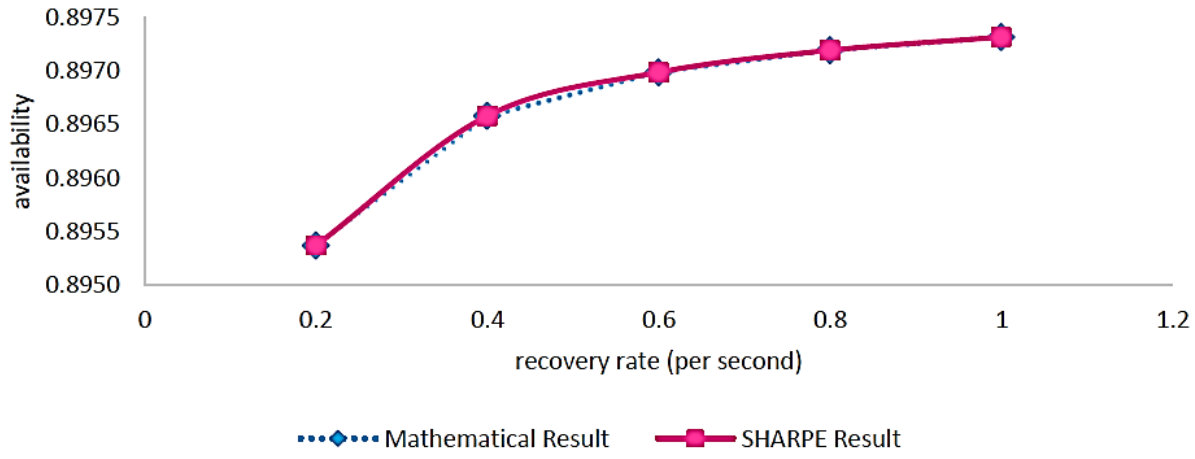

Figure 6: Availability vs. Recovery Rate

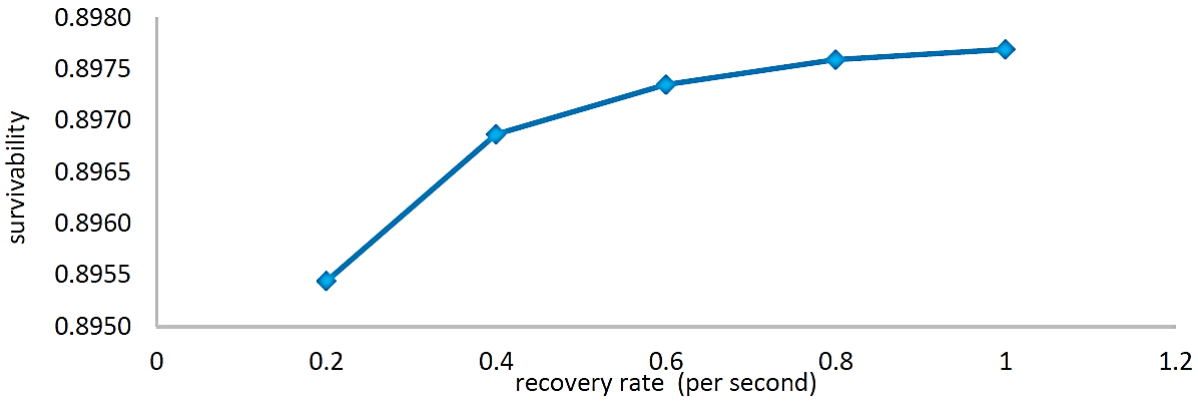

Figure 7: Survivability vs. Recovery Rate

5.2 Performance analysis of the WSN

Figs. 8 and 9, according to Eq.11 and Eq.12, show that by increasing the rate of rejuvenation, availability and survivability of WSN increase.

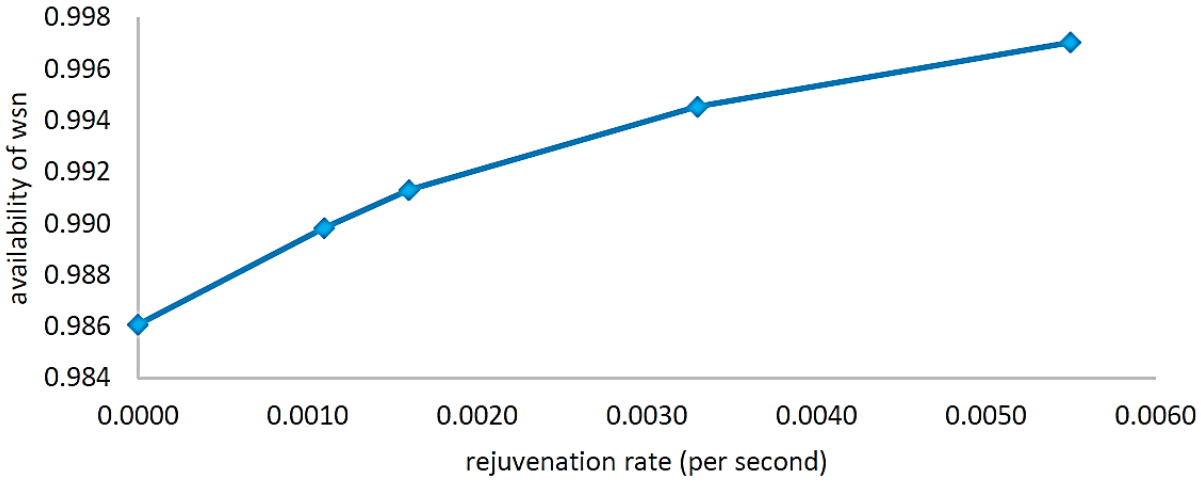

Figure 8: Availability of WSN vs. Rejuvenation Rate

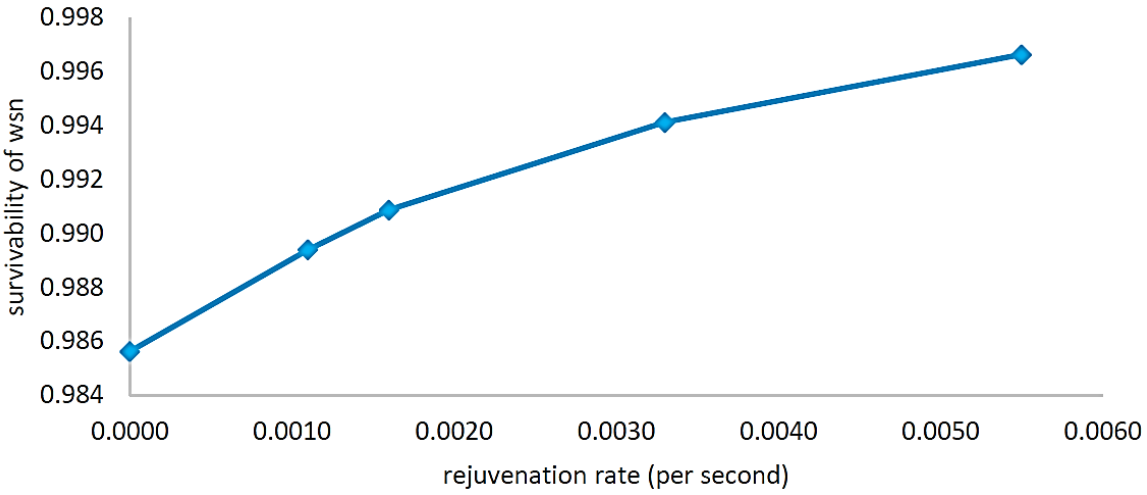

Figure 9: Survivability of WSN vs. Rejuvenation Rate

In Fig. 10, it is shown that by increasing the rate of recovery, availability of WSN increases. In addition, Fig. 6 and Fig. 10, respectively show that the results obtained from mathematical analysis and SHARPE simulation are almost the same. This shows the correctness and robustness of the proposed approach. Finally, Fig.11 represents that survivability of WSN increases as the rate of applying the recovery mechanism increases.

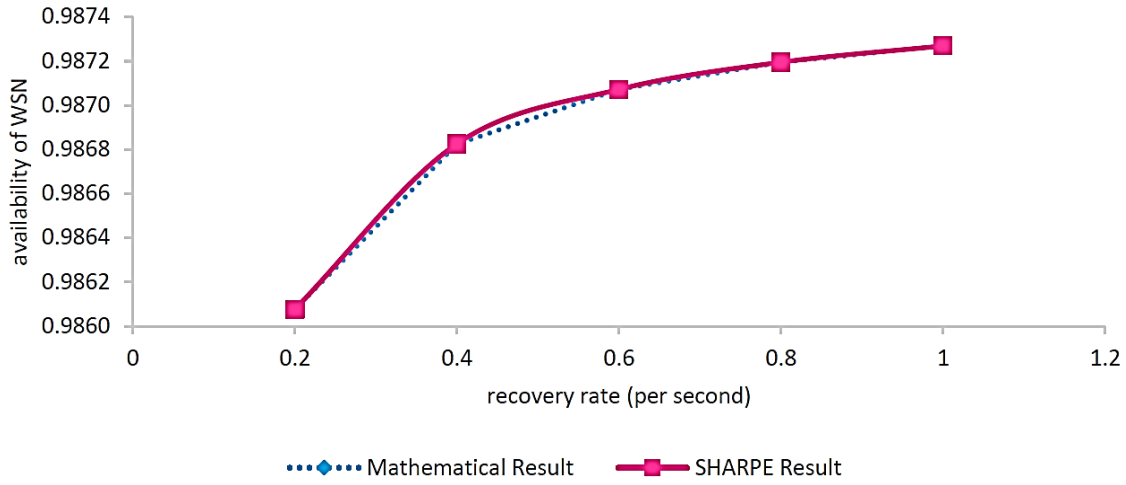

Figure 10: Availability of WSN vs. Recovery Rate

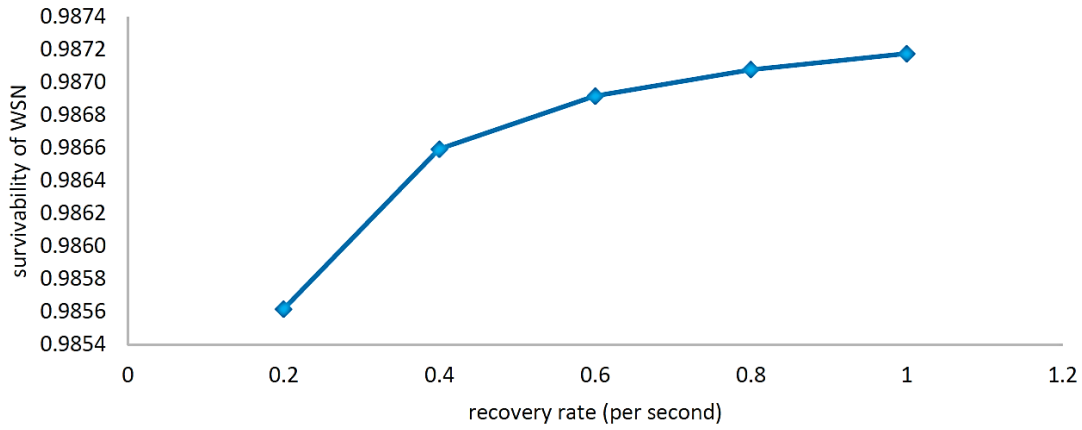

Figure11: Survivability of WSN vs. Recovery Rate

5.3. Comparative Analysis

In this section, a comparative analysis is presented. This is a comparison between the proposed model in this paper and two previous models [17, 20].The model in [20] is incomplete because there should be possible transitions from infected state and rejuvenation state to failure state. To perform this comparison these transitions are added to the original model. Fig .12 shows the results. Average improvement of 14% and 3.7% are obtained from the proposed model in this paper over two previous works [17] and [20] respectively.

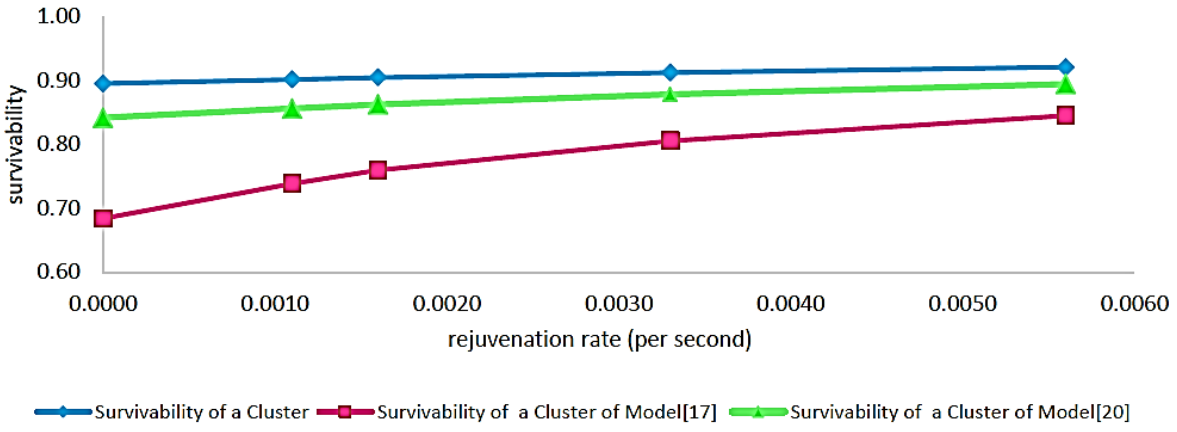

Figure 12: Comparative Results of Survivability of Cluster vs. Rejuvenation Rate

Fig.13 shows the comparative analysis of survivability of WSN between three schemes: the model presented in this paper and models proposed in [17] and [20]. The models in [17,20] were presented for only one cluster, so firstly, they are extended to the WSN according what is presented in previous sections. Results show average improvement of 12.4% and 3.1% over WSN of models [17] and [20] respectively.

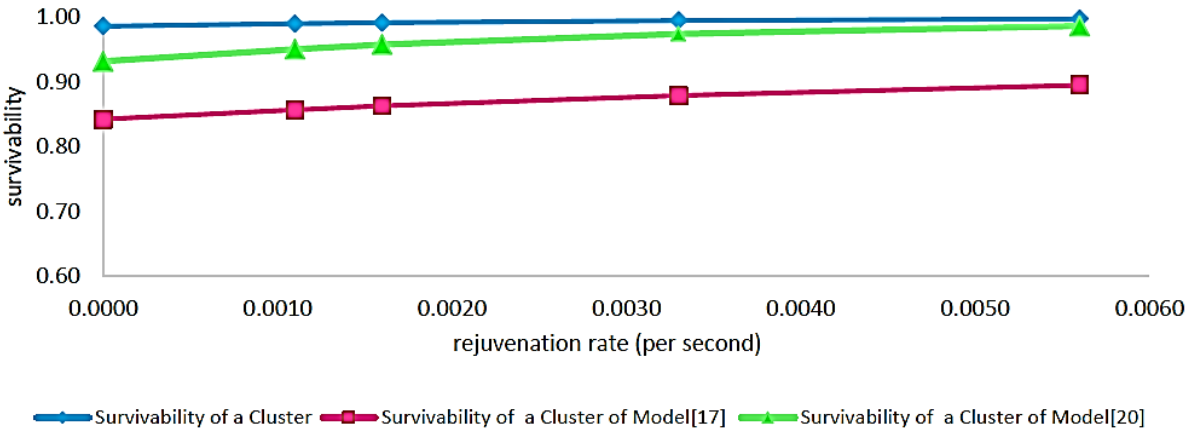

Figure 13: Comparative Results of Survivability of WSN vs. Rejuvenation Rate

Figs.14 and 15 show that model presented in this paper improves survivability by 5.3% both in the case of cluster and WSN. Only model [20] is used in this analysis because it uses recovery mechanism using spare head nodes.

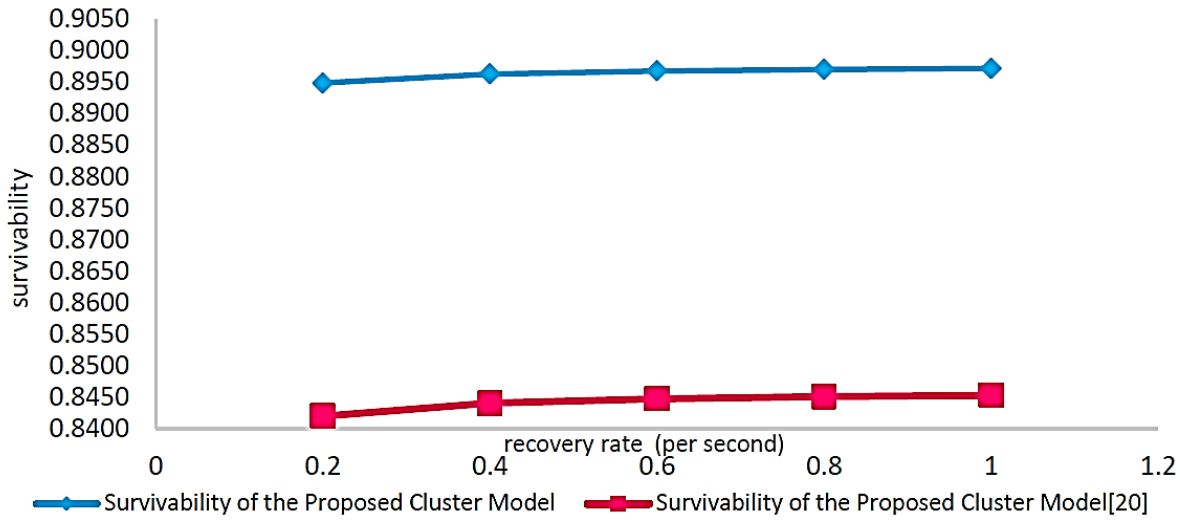

Figure 14: Comparative Results of Survivability of Cluster vs. Recovery Rate

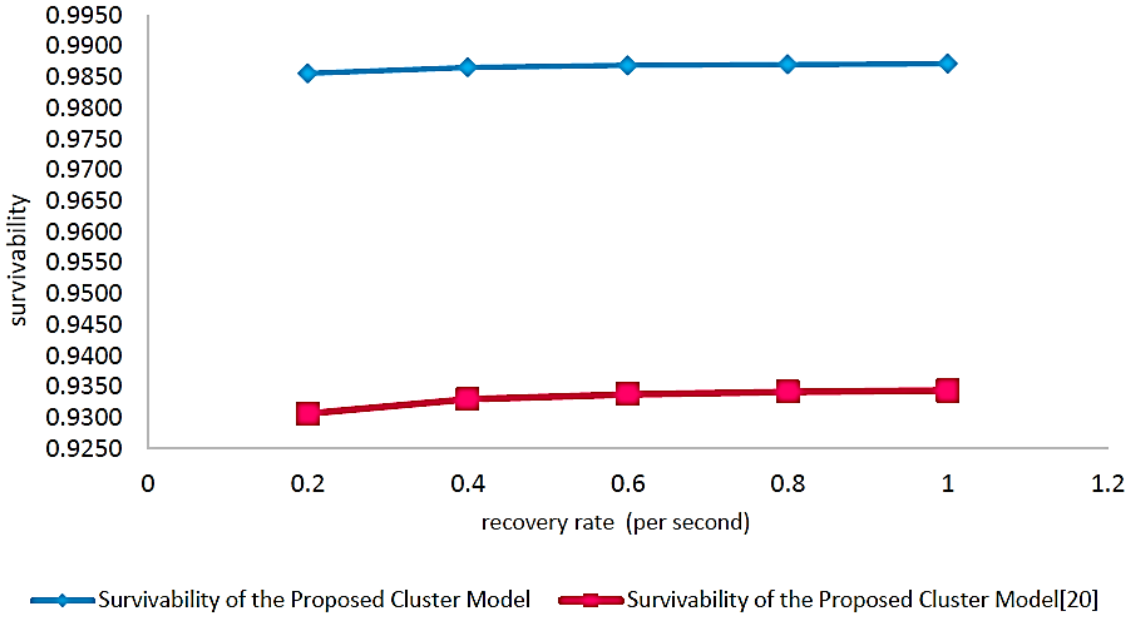

Figure15: Comparative Results of Survivability of WSN vs. Recovery Rate

CONCLUSION

In this paper**,** a new survivability model in Wireless Sensor Networks (WSNs) is presented. This model is based on software rejuvenation and recovery mechanisms. To apply recovery mechanism, it is assumed that all nodes of WSN are duplex sensor nodes; one is active and another is spare sensor node. In addition, two survivability models are proposed: one for a single cluster of WSN and the other for the whole WSN. To do this, first survivability of a cluster of WSN is modeled as a state transition diagram to reflect the status of real clusters of WSNs. Mathematical analysis is performed to show the feasibility of this work. Then, a survivability model for the whole WSN is presented. Previous works addressed survivability of WSNs just for a single cluster of WSN. The proposed model in this paper is more general and accurate. Finally, a comparative analysis of three designs is presented: the design in this paper and two previous works [17],[20]. Results show that the proposed framework in this paper

has better survivability values than a framework with simple nodes. One may think that this scheme has much cost because of spare sensor nodes but in mission critical applications, which if system fails, the impact of damage is high, the proposed topology is recommended to reach better survivability. Moreover some works have done on designing a low cost wireless sensor node or network. To overcome cost overheads it is suggested to use these WSNs or WSN nodes [9], [14]. For Future work, modeling survivability of WSN in the presence of link failures can be considered.

References

[1]. R. Masoum, A. H. Jahangir, Z. Taghikhaki, A. Masoum, Survivability Modeling of Wireless Sensor Networks, International Symposium on Wireless Communication Systems, IEEE ISWCS '08, Reykjavik Iceland, 593-597, 2008.

[2]. R. Masoum, Z.Taghikhaki, A. H. Jahangir, Survivability Analysis of Wireless Sensor Network with Transient Faults, International Conference on Computational Intelligence for Modeling Control & Automation, IEEE Computer Society, 975-980, 2008.

[3]. A.Stanoev, S.Philiposka, V.In, L.Kocarev : Cooperative Method for Wireless Sensor Network Localization, International Journal of Ad-Hoc Networks, Vol. 40, 61-72, 2016.

[4]. Chang, C. Zhu, H. Wang, C. Pei, Survivability Evaluation of Cluster-Based Wireless Sensor network under DoS Attack, Springer-Verlag Berlin Heidelberg. IOT Workshop 2012, CCIS 312, pp. 126-132, 2012.

[5]. Hirel, R. Sahner, X. Zang, K.S.Trivedi, Reliability and Performability Modeling Using SHARPE 2000, Computer Performance Evaluation/TOOLS 2000, 11th International Conference, TOOLS 2000 Schaumburg, IL, USA, March 25-31, 2000 Proceedings, pp. 345–349, 2001.

[6]. S. Kim, Kh.M.Shazad, J. S. Park, A Framework of Survivability Model for Wireless Sensor Network, The First International Conference on Availability, Reliability and Security, ARES2006, IEEE Computer Society, 2006.

[7]. G. Han, J. Jianga, L.Shu, J.Niu, H. Chao, Management and applications of trust in Wireless Sensor Networks: A survey, Journal of Computer and System Sciences, Vol. 80, pp. 602-617, 2014.

[8]. Koren, C. M.Krishna, "Fault Tolerant Systems, *"Morgan Kaufmann Publishers*, pp. 33-36, 2007.

[9]. I.Muller, E.P.de Freitas, A.A.Susin, C.E.Pereira, Namimote: A Low-Cost Sensor Node for Wireless Sensor Networks, International Conference on Internet of Things, Smart Spaces, and Next Generation Networking, pp.391-400, 2012.

[10]. J. C. Acosta, B. G. Medina, Survivability Prediction of Ad Hoc Networks under Attack, military communications conference, IEEE computer society, 2012.

[11]. K.S.Trivedi, SHARPE 2002: Symbolic Hierarchical Automated Reliability and Performance Evaluator, Proceedings of the 2002 International Conference on Dependable Systems and Networks. DSN 2002: 544, 2002.

[12]. M.Chuang, L.H. Wei, Zh.H. Ying, W.Z.bo, Y.X.Zong, X.X.Bo, A New Fault-Tolerant Method for Wireless Sensor Network Design, Proceedings of 2010 Conference on Dependable Computing, CDC'2010, IEEE, 2010.

[13]. M. Keshtgari, A. H. Jahangir, F. A. Al-Zahrani, A. P. Jayasumana, Survivability Performance Evaluation of WDM Networks with Wavelength Converters, Vol. 11, No. 1, Photonic Network Communications, pp. 15-27, 2006.

[14]. O.Rorato, S. Bertoldo, C.Lucianaz, M. Allegrreti, G.Perona, A Multipurpose Node for Low Cost Wireless Sensor Network, IEEE-APS Topical Conference on Antennas and Propagation in Wireless Communications (APWC), 2012.

[15]. P. E. Heegaard & K. S.Trivedi, Network Survivability Modeling, Computer Networks, pp. 1215-1234, 2009.

[16]. S. Kumar, R. Valdez, O. Gomez, and S. Bose, Survivability Evaluation of Wireless Sensor Network under DDoS Attack. International Conference on Mobile Communications and Learning Technologies, IEEE computer society, 2006.

[17]. S. Parvin, F. KH. Hossain, J. S. Park, D.S. Kim, A Survivability Model in Wireless Sensor Network, Journal of Computers and Mathematics with Applications, Vol. 64, No. 12, pp. 3666–3682, 2012.

[18]. S. Petridou, S. Basagiannis, M. Roumeliotis, Survivability Analysis Using Probabilistic Model Checking: A Study on Wireless Sensor Networks, IEEE systems journal, Vol. 7, No. 1, 4-12, 2013.

[19]. S. Sirsikar, S.Anavatti, Issues of Data Aggregation Methods in Wireless Sensor Network: A Survey, Procedia Computer Science, Vol. 49, 2015, 194-201.

[20]. T. Thein, S. Chi, J. S. Park, Increasing Availability and Survivability of Cluster Head in WSN, The 3rd International Conference on Grid and Pervasive Computing, GPC.WORKSHOPS.2008.44, IEEE Computer Society, 281-285, 2008.

[21]. W.Wei, Y.Qi, X.He, W.Wang, R.Li, H.He, Improving the Survivability of WSNs with Biological Characters Based on Rejuvenation Technology, IEEE Asia-Pacific Services Computing Conference, 2008.

[22]. X. Liu, J. Ning, J. Li, J. Yin, M. Li, Model for Survivability of Wireless Sensor Network, Springer-Verlag Berlin Heidelberg, MSN 2007, LNCS 4864, 705-714, 2007.

[23]. Y. Huang, C. Kintala, N. Kolettis, N. Fulton, Software Rejuvenation: Analysis, Module and Application, In Proceeding of the International Symposium on Fault Tolerant Computing, 330–381, 1995.

[24]. Y.Qian, K.LU, D. Tipper, A Design for Secure and Survivable Wireless Sensor Networks, Security in wireless mobile ad hoc and sensor networks, IEEE wireless communications, 2007.