IJASRM

International Journal of Advanced Scientific Research and Management, Special Issue II, Oct 2018

www.ijasrm.com

ISSN 2455-6378

An Optimum Rejuvenation Strategy for Maximizing Reliability of Wireless Sensor Networks

Vandana Gupta[1] and Gulshan Chauhan[2]

[1,2]Department of Operational Research,University of Delhi,
Delhi 110 007, India

Abstract

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. It incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. A WSN should be capable of fulfilling its mission, in a timely manner, in the middle of intrusion, attacks, accidents and failures in a hostile environment. This paper addresses the issues of security breaches in a WSN, and is intended to analyze its effect on the reliability of WSN. For this purpose a framework of reliability model for WSN is proposed. The performance of the WSN in the existence of security breaches is modeled as a stochastic process based on continuous time Markov chain (CTMC) to study the system reliability. From the CTMC the mean time to failure (MTTF) is obtained as a system reliability measure. To help avert failures in a WSN and to improve its comprehensive reliability, software rejuvenation procedure is adopted. In addition to framework of reliability model, an optimal rejuvenation strategy is also proposed for achieving the best attainable value of MTTF with respect to the parameters involved in the reliability model. The model analysis with numerical illustration indicates the feasibility of the proposed approach.

Keywords: *WSN, system reliability, continuous time Markov chain, software rejuvenation, optimal rejuvenation strategy.*

1. Introduction

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. The development of WSNs was motivated by military applications such as battlefield surveillance. Today engineers have created WSN applications for areas including health care, utilities, and remote monitoring. In health care, wireless devices make less invasive patient monitoring and health care possible. For utilities such as the electricity grid, streetlights, and water municipals, wireless sensors offer a lower-cost method for collecting system health data to reduce energy usage and better manage resources. Remote monitoring covers a wide range of applications where wireless systems can complement wired systems by reducing wiring costs and allowing new types of measurement applications.

In typical application scenarios, sensor nodes are spread randomly over the terrain under scrutiny and collect sensor data. In WSNs critical event data collected by the sensor nodes need to be reliably delivered to the sink for successful monitoring of an environment. Therefore, given the nature of error prone wireless links, ensuring reliable transfer of data from resource constrained sensor nodes to the sink is one of the major challenges in WSNs. Reliable transfer of data is the surety that the packet carrying event’s information arrives at the destination. Hence, a WSN should be capable to fulfill its mission, in a timely manner, in the face of intrusions, attacks, accident and failures in hostile environment.

2. Related Work

Significant research has been done in the area of reliability of WSNs. In (Hosam, 2006) authors defined a WSN reliability measure that considers the aggregate flow of sensor data into a sink node (gateway or cluster head). The paper (Pereira, 2007) presents a survey on transport and routing protocols for wireless sensor networks (WSN). Research challenges regarding the problem of end-to-end reliability are addressed in particular in this paper. In (Mahmood, 2015) also a survey on reliability protocols in WSNs is presented. Several reliability schemes based on retransmission and redundancy techniques using different combinations of packet or event reliability in terms of recovering the lost data using hop-by-hop or end-to-end mechanisms are reviewed in this paper. In (Antônio, 2014) a model for evaluating the reliability of WSNs considering the battery level as a key factor is proposed, and the proposed model is based on routing algorithms used by WSNs. In (Kim, 2006), a framework of survivability model for WSN is proposed in which software rejuvenation methodology is implemented to improve the survivability measures. Software rejuvenation is a type of defensive maintenance that proactively restarts a system or an application in order to evade an unprepared failure due to software aging.

Performing rejuvenation consists of cleaning the internal state of a system resulting in returning the system at the initial state or at a previously check pointed state. Software rejuvenation has been comprehensively studied in the past years. The effects of software rejuvenation on systems like AT&T billing applications (Avritzer & Weyuker, 1997), web server Apache (Li et al., 2002) have been studied. Furthermore, software rejuvenation performed on cluster systems (Koutras & Platis, 2006), (Park & Kim, 2002), on systems that allocate free memory whenever an application is initiated (Koutras & Platis,2005), have been also studied. In (Huang et al., 1995; Koutras & Platis, 2009), homogeneous continuous time Markov chains (CTMCs) have been used to model rejuvenation. However to the best of our knowledge, an optimal rejuvenation strategy for maximizing the survivability measures of WSN has never been proposed. This motivated me to formulate an optimization problem to propose an optimal rejuvenation strategy.

With the purpose of improving system reliability of a WSN, a framework of reliability model for a WSN is presented here in this paper. As a defensive course of action, software rejuvenation is implemented to avert or suspend software failures in a WSN which is applicable in security and also less expensive. In practical situations, majority of the failure and repair times follow time-dependent probability distributions such as Weibull, Pareto or lognormal. But, by and large analytical models with non-exponential distributions are not mathematically well-mannered, and it is very difficult to obtain the closed form or numerical solution. For this reason phase-type distribution, which is a convolution of many exponential phases is used for approximating many general distributions (Osogami and Harchol-Balter, 2006). In view of the fact that exponential distribution is a special case of phase-type distribution and it makes the analysis mathematically tractable, in this paper it is considered that the time to move from one system state to other follows exponential distribution, and a stochastic model for the reliability analysis of a WSN with software rejuvenation methodology is proposed. The proposed model utilizes a hierarchical cluster based sensor network, which has advantages in terms of cost and energy. Each single cluster is modeled as a stochastic process based on a CTMC. As a reliability measure, system mean time to failure (MTTF) is obtained from the CTMC. An optimal software rejuvenation strategy which leads to increased system reliability is also proposed.

The remainder of this paper is structured as follows: In Section 2 the software rejuvenation model for a WSN is described, and a reliability study in terms of system MTTF is discussed. In addition, an optimal rejuvenation scheme is proposed with the purpose of improving system MTTF. In Section 3, a numerical example is presented in order to illustrate the study. In the numerical example the proposed optimization problem is solved and the graphical results for the sensitivity analysis are presented.

3. SOFTWARE REJUVENATION MODEL

3.1 MODELDESCRIPTION

In this section the software rejuvenation model for a WSN is proposed. Figure 1 represents the state transition diagram of the proposed model in which circles correspond to the *states* and directed arcs correspond to the *transitions*. The various states of the model are described as follows:

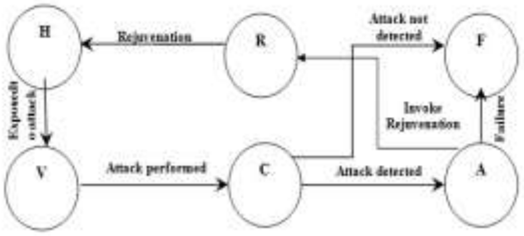

Figure1. Software rejuvenation model of a WSN

Healthy state (H): This is the exceedingly proficient and extremely robust implementation stage. The system operates faultlessly in this state. The purpose of the defense mechanism is to make the system stay in this state for so long as viable. After a breakdown, both rejuvenation and a repair take the system back to this state.

Vulnerable state (V): If any kind of penetrations into the resistance mechanisms is occurred using known or unknown vulnerabilities, the cluster enters vulnerable state V. This is a susceptible stage where the system is prone to security breaches. This stage is extremely crucial for the reason that attackers and mischievous users would like to take advantage of the vulnerabilities and attempt to make a successful attack.

Compromised state (C): A successful exploitation of the vulnerable state V by the attackers causes the system to enter compromised state C, and then unwanted damage follows.

Adaptation state (A): If the Intrusion Detection System (IDS) can recognize the compromised state C, or some other function can change its state, it triggers the transition from compromised state C to adaptation state A. This is a decision making state and it assesses the impact of damages occurred and determines the appropriate strategies for recovery. The actions to be taken depend on the requirements of the types of attack detected. If the critical requirements of the system are integrity and confidentiality, then system is switched to rejuvenation state R.

Rejuvenation state (R): At this stage, the system's operations are suspended for a short time, and software rejuvenation procedure is implemented on the system. We adopt software rejuvenation to counteract the adversary's actions by killing or resetting the malicious node(s) and/or compromised node(s) online and brought the cluster to healthy state. It is noted that only illegitimate nodes are killed or reset.

Failed state (F): The system completely breaks down at this stage, and is sent for total repair or reconfiguration.

As mentioned before, we consider that the time to move from one system state to other follows exponential distribution, and hence the underlying CTMC is given as below:

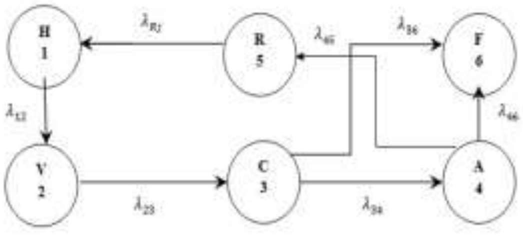

Figure 2. Underlying CTMC of software rejuvenation model

The system begins with the robust state H. The WSN can be bared to security intrusions at any moment. For this reason, while the system is in state H, and if any sort of infiltration takes place into the resistance scheme, the system moves to the vulnerable state V with rate $\lambda_{12.}$ A successful exploitation of the vulnerable state V by the attackers causes the system to enter compromised state C with rate λ_{23}. If the IDS can recognize the compromised state, it triggers the transition from compromised state to adaptation state A with rateλ_{34}. In contrast, if the attack made in state V goes unidentified even in state C, then the system completely breaks down and moves to state F with rate λ_{36}. While the system is instate A, the after-effects of the security attack are analyzed and the damages are calculated. Based on the impacts of the attack some revival schemes are proposed. The revival strategies depend on the demand of the resources and the nature of attacks detected. If the crucial needs of the system are reliability and confidentiality, the system goes to the rejuvenation state R with rate λ_{45}. Or else, if the system can no longer sustain because of the after-effects of the security attack, then it moves to the down state F with rate λ_{46}. From the rejuvenation state R system moves back to healthy state with rate λ_{51} after successful software rejuvenation.

3.2 Reliability Study

Having already described the software rejuvenation model and the underlying CTMC, next purpose is to study system reliability of WSN in the sense of MTTF. For this, a stochastic process$\{X(t), t \geq 0\}$is defined which represents the evolution of the system with time. Here $X(t)$ is a homogeneous CTMC. In order to determine the system MTTF, the time that the process spends at each state is needed. From Figure 2 the transition rate matrix $Q$of the CTMC $X(t)$can be determined. In Q the rows and the columns represent states $\{H, V, C, A, R, F\}$ correspondingly, and the elements of Q represent the transition rates between the above states.Hence elements q_{ii}, $i, j \in \{H, V, C, A, R, F\}$,of the transition matrix denote the transition rate from state i to state j.

Let the state space of the process defined by E, which is decomposed into subsets U and D such that $U \cup D = E$ and $U = \emptyset, U = E$. Subset U contains the up states, and correspondingly D contains the down states. In the model presented subset D contains only the absorbing state F. The transition rate matrix is given now by

$$Q = \begin{pmatrix} Q^U & Q^{UD} \\ Q^{DU} & Q^D \end{pmatrix}$$

Hence, $Q^U$is the matrix Q limited to the operational states.$Q^D$is the transition rate matrix inside the non-operational subset D and Q^{UD}, Q^{DU} are the transition rate matrices from subset U to subset $D$and from subset $D$to subset U correspondingly (Platis et al., 1998).

Let $\boldsymbol{\pi}^{\boldsymbol{U}}(\boldsymbol{0}) = \Pr(X(0) = i), i \in \{H, V, C, A, R\}$ sub-vector of the initial distribution vector $\boldsymbol{\pi}^{\boldsymbol{U}}(\boldsymbol{0})$,be the initial distribution constrained in the operating states (upstate). In order to derive the timeτ_i^Uspent at each state i, the following system of equations has to be solved:

$$\boldsymbol{\tau}^{\boldsymbol{U}}.Q^U = -\boldsymbol{\pi}^{\boldsymbol{U}}(\boldsymbol{0}) \qquad (1)$$

where $\boldsymbol{\tau}^{\boldsymbol{U}} = [\tau_H^U \tau_V^U \tau_C^U \tau_A^U \tau_R^U]$ is the vector representing the time spent at each state (Trivedi 2001). In the study presented, it is assumed that the initial distribution sub vector is:

$$\boldsymbol{\pi}^{\boldsymbol{U}}(\boldsymbol{0}) = [1\ 0\ 0\ 0\ 0\ 0\ 0] \qquad (2)$$

The MTTF can now be computed (Trivedi K. S., 2001) using the following equation:

$$MTTF = \tau_H^U + \tau_V^U + \tau_C^U + \tau_A^U + \tau_R^U \qquad (3)$$

which represents the time that the process spends at all states before entering the absorbing failure state F.

After obtaining the system MTTF, next objective is to establish an optimal rejuvenation scheme which maximizes the system reliability of WSN in terms of system MTTF. With this purpose we now present a mathematical programming formulation for optimizing the system MTTF. As far as the constraint for the mathematical programming formulation is concerned, the time that the stochastic process spends at the rejuvenation state cannot go beyond the time spent at the other functional states. Consequently, the constraint obtained by this supposition is given by the following equation:

$$\tau_R^U \leq \tau_H^U + \tau_V^U + \tau_C^U + \tau_A^U \qquad (4)$$

Therefore the mathematical programming problem that ultimately has to be solved with the aim of achieving the maximum value of MTTF and thus improving system reliability of WSN is:

$$maximize\text{MTTF} = \tau_H^U + \tau_V^U + \tau_C^U + \tau_A^U + \tau_R^U \qquad (5)$$
$$subject\ to \tau_R^U \leq \tau_H^U + \tau_V^U + \tau_C^U + \tau_A^U$$

Now, deducing vector $\boldsymbol{\tau}^{\boldsymbol{U}}$by solving equation (1) points out that the time spent at each state excluding the rejuvenation state R is a constant. The time spent only at the rejuvenation state depends on λ_{Rj}. Hence the objective function in the above optimization problem, MTTF, apparently is a function of the rejuvenation rate λ_{Rj} only. Furthermore, the rejuvenation rate λ_{Rj} is also involved in the constraint since the time that the stochastic process $X(t)$spends at the rejuvenation state is also a function of λ_{Rj}. The optimization is therefore carried out with respect to the decision variable λ_{Rj} . And establishing the optimal rejuvenation scheme consists of solving the mathematical programming problem in equation (5), and finding out that value of the rejuvenation rate λ_{Rj} which maximizes the MTTF with respect to the constraint mentioned. Thus, in order to establish the optimal rejuvenation scheme, rejuvenation action has to be carried out as often or as rarely as the solution of the problem indicates.

3. NUMERICAL ANALYSIS

In order to illustrate the above study, it is necessary to provide a numerical example based on experimental data. The aim of this example is to provide the optimal rejuvenation strategy consisting of the value of the rejuvenation rate λ_{Rj}, which maximizes the MTTF. In this section, a numerical example is presented to demonstrate the same. For the purpose of numerical illustration, we set the parameter values of several components of network elements as given by (Gupta & Dharmaraja, 2009). The parameter values are given in Table 1.

Table 1. Model Parameters

Parameters	**Values (in years^{-1})**	**Parameters**	**Values (in years^{-1})**
λ_{12}	1.5	λ_{36}	2
λ_{23}	4	λ_{45}	3
λ_{34}	4	λ_{46}	2

Figure 3 shows behavior of system MTTF for different values of λ_{12}.The graph also depicts the optimal values of the rejuvenation rate λ_{Rj} which maximizes the MTTF. It can be observed from the graph that the MTTF increases with decrease in λ_{12}as anticipated. Moreover, as λ_{12} increases, the system needs to be rejuvenated more often. And this is very much apparent from the graph that as λ_{12} increases λ_{Rj} also increases.

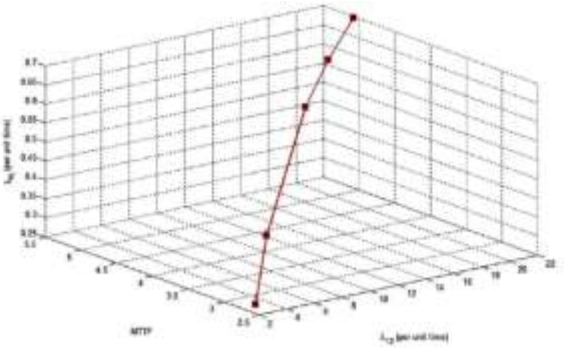

Figure 3. MTTF vs$\boldsymbol{\lambda_{12}}$

Figure 4 shows the behavior of system MTTF for different values of λ_{34}, i.e., rate of moving from the compromised state to adaptable state. The graph also portrays the optimal values of the rejuvenation rate λ_{Rj} which maximizes the MTTF. It can be observed from the graph that the MTTF increases with increase in λ_{34} as predicted. In addition, as λ_{34} increases, the system needs to be rejuvenated more frequently. And this is very much noticeable from the graph that as λ_{34} increases λ_{Rj} also increases.

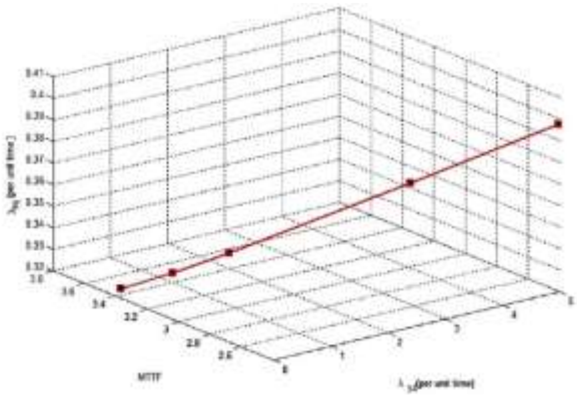

Figure 4. MTTF vs$\boldsymbol{\lambda}_{34}$

4. Conclusion

The paper discusses and optimizes the system reliability of a WSN system using optimal rejuvenation scheme taking into consideration the effects of resource exhaustion and security attacks. An analytical model is presented using a CTMC to find out the system MTTF and study the behavior of WSN tolerance in the presence of security breaches.

From the CTMC, the MTTF is obtained as a reliability measure. An optimization problem isthen formulated with respect to a constraint about the time invested at the rejuvenation state of the model. The solution of the optimization problem provides the maximum MTTF for the system. An optimum rejuvenation scheme concerning how often rejuvenation should be performed is proposed for achieving the maximum MTTF with respect to the parameters involved. The rejuvenation scheme therefore gives the optimum rejuvenation time interval that maximizes MTTF which sprightly affects the QoS. The discussed optimal rejuvenation scheme can hence be used to prevent performance degradation and other associated failures in a WSN.

References

[1] M.f. AboelfotohHosam, S. Elmallah Ehaband S. Hassanein Hossam.On the Reliability of Wireless Sensor Networks, *IEEE International Conference onCommunications*(2006).

[2] Paulo Rogério Pereira, AntónioGrilo, Francisco Rocha, MárioSerafimNunes, AugustoCasaca, Claude Chaudet, Peter Almströmand Mikael Johansson.*End-to-end reliability in wireless sensor networks: Survey and research challenges*, *EuroFGI Workshop on IP QoS and Traffic Control, Lisbon, Portugal*, December 6-7(2007).

[3] Muhammad AdeelMahmood, Winston K.G.Seah and IanWelch.Reliability in wireless sensor networks: A survey and challenges ahead.*Computer Networks*79(2015) 166-187.

[4] AntônioDâmaso, Nelson Rosa and Paulo Maciel.Reliability of Wireless Sensor Networks.*Sensors* 14(2014) 15760-15785.

[5] Dong Seong Kim, Khaja Mohammad Shazzad and Jong Sou Park. A Framework of Survivability Model for Wireless Sensor Network.*First International Conference on Availability, Reliability and Security (ARES'06)*(2006).

[6] A. Avritzer and E. J. Weyuker. Monitoring smoothly degrading systems for increased dependability.*Empirical Software Engineering*2(1)(1997)59-77.

[7] L. Li, K.Vaidyanathan and K. S. Trivedi. An approach for estimation of software aging in a web server. *IEEE International Symposium on Empirical Software Engineering* (2002)91-100.

[8] V. P. Koutras andA. N. Platis. Applying software rejuvenation in a two node cluster system for high availability. *International Conference on Dependability of Computer Systems (DEPCOS-RELCOMEX06)* (2006) 2285-2290.

[9] K. Park and S. Kim. Availability analysis and improvement of active/standby cluster systems using software rejuvenation. *Journal of Systems and Software* 61 (2) (2002) 121-128.

[10] V. P. Koutras and A. N. Platis. Optimizing the amount of free resources on a computer system using software rejuvenation, *Advances in Safety and Reliability, Kołowrocki (ed.), 2005 Taylor & Francis Group, London* (2005) 1187-1192.

[11] Y.Huang, C. Kintala, N. Kolettis, and N. D. Fulton. Software rejuvenation: Analysis, module

and applications. *25th IEEE International Symposium on Fault-Tolerant Computing, FTCS-25, Digest of Papers* (1995) 381-390.

[12] V.P. Koutras, C.-P.S .Salagaras and A. N. Platis. Software rejuvenation for higher levels of VoIP availability and mean time to failure. *International Conferenceon Dependability of Computer Systems* (2009) 99-106.

[13] V. Gupta and S. Dharmaraja. Semi-Markov modeling of dependability of VoIP network in the presence of resource degradation and security attacks. *Reliability Engineering and System Safety* 96 (2011) 1627–1636.