Improved Method for Secure and Survivable Wireless Sensor Networks

Thandar Thein, Sang Min Lee, and Jong Sou Park
Computer Engineering Department, Korea Aerospace University, Seoul, Korea
{thandar, minuri33, jspark}@kau.ac.kr

Abstract

The survivability of the wireless sensor network (WSN) is threatened by resource limitations and security attacks. Security and survivability of WSNs are receiving increasing attention, particularly critical infrastructure protection. Our goal is to develop a framework for secure and survivable WSN that can provide essential services in the presence of attacks and failures, and recovery of full services in a timely manner. To achieve such a goal, we propose a framework of survivability model with rejuvenation methodology for WSNs. This paper also outlines the interaction of survivability, security and fault tolerance, so that we can effectively analyze and design the secure and survivable WSNs. It will be one of the approaches for improving the survivability level in WSN environment.

Keywords: Fault tolerant, security, survivability, software rejuvenation, WSNs

1. Introduction

WSNs have received increasing attention in the recent years. A WSN [8] comprises hundreds of small battery powered sensor devices, each equipped with one or more sensors, an embedded processor, low power radio for wireless communication and the base station or information gateway to collect this information and process it further for that particular application. Applications of WSNs are numerous and growing, and range from indoor deployment scenarios in the home and office to outdoor deployment scenarios in natural, military and embedded settings [1]. With increasing interest and emphasis on WSN, it is important for such networks to possess the capability to overcome failures and provide secure and survivable services.

In WSNs, the sensor nodes can be deployed in controlled environment and uncontrolled environment. The survivability of the WSN is threatened by resource limitations and security attacks. Survivability [2], [4] implies that networks should have the capability to operate under node failures and attacks.

The survivability [3], [5] of a network is concerned with the ability of the network to provide a defined degree of assurance that the system will continue to function during and after a natural or man-made disturbance. With increasing interest and emphasis on WSN, it is important for such networks to possess the capability to overcome failures and provide secure and survivable services.

The goal of this paper is to study technologies for enhancing distributed WSN security and survivability that provides critical functions at all time, in spite of damage caused by unintentional errors or attacks. Our method is rejuvenation technique which provides a graceful degradation in the presence of malicious fault, intrusions, and attacks. This is meant that it will maintain safe operation as long as possible and in the end, fail in a predefined, safe mode operation.

Software rejuvenation [7] is a new concept of fault tolerant techniques in software engineering, and it is proposed as an intrusion tolerant technique in security engineering. Rejuvenation is a proactive fault management technique aimed at cleaning up the internal system state to prevent the occurrence of more severe future crash failures. This proposal is a novel approach to survivability.

The organization of this paper is as follows. Section 2 addresses the security and survivability requirements and presents the proposed framework. Section 3 presents the state transition model to describe the behaviours of WSN. The models are analyzed and experimental results are given in Section 4. Finally, we conclude with Section 5.

2. Security and Survivability Requirements for WSN

This subsection is focused on security and survivability requirements related with sensor network operation. The majority of the WSN applications should be reliable and run continuously without
interruptions. Hence, security and survivability should also be taken into account in developing WSNs [6]. In WSN, the security requirements that constitute fundamental objectives based on which every sensor application should adhere in order to guarantee an appropriate level of security. To protect WSNs from adversaries; confidentiality, authentication, integrity, freshness, secure management and availability are needed.

Survivability services can be organized into three general categories, namely: resistance, recognition, and recovery. Resistance refers to the capability of a system to deter attacks. Recognition refers to the capability to recognize attacks or to recognize the probing that may precede attacks. Recovery refers to a system’s ability to restore services after an intrusion has occurred and to improve its capability to resist or recognize future intrusion attempts.

2.1. Survivability, Security and Fault Tolerance for WSN

In this section, we consider the interaction of survivability, security and fault tolerance, so that we can effectively analyze and design secure and survivable WSNs.

Survivability can be defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. Security can be defined as the combination of availability, confidentiality, and integrity and focuses on “recognition of attacks” and “resistance of attacks”. Fault tolerance is the ability of a system to deliver a desired level of functionality in the presence of faults. Security attacks are a major concern for critical information systems of WSN.

It is important to recognize the relationship between survivability and security. WSN application may employ security mechanisms, such as passwords and encryption, and may still be very fragile. For instance, it may fail when a base station/gate-way or a communication link dies. On the other hand, a survivable application must be able to survive some malicious attacks. Therefore, survivability must involve security. The concept of survivability is broader than security and focuses on the “adaptation and evolution to attacks”. The requirements for recoverability are what most clearly distinguish survivable systems from merely secure systems.

Survivability is a dependability property; it is not synonymous with fault tolerance. Fault tolerance is a mechanism that can be used to achieve certain dependability properties. Since the sensor nodes are prone to failure, fault tolerance should be seriously considered in many sensor network applications.

Fault elimination and fault forecasting can be used as mechanisms to improve a system’s security and survivability. Survivability requirements and security requirements will be achieved by the fault tolerance mechanism, i.e., the secure and survivable system will have a fault tolerant design. Figure 1 shows the dependencies between survivability, security and fault tolerance.

2.2. Sensor’s State Diagram for Security and Survivability

Figure 2 depicts the sensor’s state diagram for security and survivability.

In this case, a sensor is active and pro-actively senses warnings. If the sensor senses warnings, the sensor transits from the normal state to the warned state. When the warning signal is ignored, the sensor will return to the normal state. A sensor is in the warned state and detects the intruder, the sensor transits to Attacked State. When the attack is unsuccessful (detection signal is ignore), the sensor will resume to normal state. In undetected situation, the sensor enters the compromised state.
2.3. Base’s State Diagram for Security and Survivability

The base station’s state diagram for security and survivability is shown in Figure 3. The base station is normal and received a warning alert from a sensor; the base transits from the normal state to the warned state. If the suspicion is not confirmed, the warning signal is ignored and then the base will return to the normal state.

In the warned state, the base will investigate whether the data from that sensor conflicts with data from other sensors. If there is a conflict, the base will transit to the attacked state.

When the attacked state of base station continues for a certain time, the base station damage will be accumulated. If the intrusion diagnosis module detects the meaningful performance degradation, it will trigger the defensive process. The main strategy of defensive process is application of rejuvenation methodology to provide essential services in the presence of attacks and failures, and to recover full services in a timely manner.

After successful rejuvenation process the base station will transit from the attacked state to the normal state. The main strategies of rejuvenation are occasionally stopping the executing software, cleaning the internal state and restarting by means of effectiveness of proactive managements, degrading mechanism, service stop, service restart, reboot and halt. If all of the above strategies fail then the base station enters the failure state and the system is suspended for repair. After repair process, the system will resume back to the normal state.

3. System Model

In this section, we are interested in determining how our proposed approach can enhance the availability of the base station. We construct the state transition model to describe the behavior of the base station as shown in Figure 4.

![Figure 4. State transition model of base station](image)

Let \( \{ X(t) = i, t \geq 0 \} \), \((i=0, 1, 2, 3)\) be the system state at time \( t \) with the transition probability

\[
Q_{ij}(t) = P_r \{ X(t) = j | X(0) = i \} (t \geq 0, j = 0,1,2,3).
\]
From an elementary probabilistic argument, the Kolmogorov’s differential equations which the transition probabilities have to satisfy are given by

\[
\frac{dQ_{0,0}(t)}{dt} = -r_1 Q_{0,0}(t) + r_4 Q_{0,2}(t) + r_2 Q_{0,1}(t) + r_5 Q_{0,3}(t)
\]

\(1\)

\[
\frac{dQ_{0,1}(t)}{dt} = -(r_2 + r_3 + \lambda_1)Q_{0,1}(t) + r_1 Q_{0,0}(t)
\]

\(2\)

\[
\frac{dQ_{0,2}(t)}{dt} = -(r_4 + \lambda_2)Q_{0,2}(t) + r_3 Q_{0,1}(t)
\]

\(3\)

\[
\frac{dQ_{0,3}(t)}{dt} = -r_5 Q_{0,3}(t) + \lambda_1 Q_{0,1}(t) + \lambda_2 Q_{0,2}(t)
\]

\(4\)

With the initial conditions:

\[Q_{0,0}(0) = 1, \quad Q_{0,1}(0) = 0, \quad Q_{0,2}(0) = 0, \quad Q_{0,3}(0) = 0\]

\(5\)

Suppose that the limiting transition probability \(P_j\) (\(j=0,1,2,3\)) exits, i.e.

\[P_j = \lim_{t \to \infty} Q_{0,j}(t), \quad j=0,1,2,3\]

\(6\)

By taking the limitation, since the Kolmogorov’s differential equations in (1) to (4) are reduced to the algebraic equations:

\[-r_1 P_0 + r_4 P_2 + r_2 P_1 + r_5 P_3 = 0\]

\(7\)

\[-(r_2 + r_3 + \lambda_1)P_1 + r_1 P_0 = 0\]

\(8\)

\[-(r_4 + \lambda_2)P_2 + r_3 P_1 = 0\]

\(9\)

\[-r_5 P_3 + \lambda_1 P_1 + \lambda_2 P_2 = 0\]

\(10\)

\[\sum_{j=0}^{3} P_j = 1\]

\(11\)

Solving the above equations, we obtain the following expressions for the steady-state probabilities:

\[P_0 = \frac{r_2 + r_3 + \lambda_1}{r_1 - r_5} P_1\]

\(13\)

\[P_2 = \frac{r_3}{r_4 + \lambda_2} P_1\]

\(14\)

\[P_3 = \left(\frac{\lambda_1}{r_5} + \frac{r_3 + \lambda_2}{r_5(r_4 + \lambda_2)}\right) P_1\]

\(15\)

The meanings of the probabilities are as follows:

\[P_0 : \text{The probability of the system is in the normal state}\]

\[P_1 : \text{Probability of the system is in the warned state}\]

\[P_2 : \text{Probability of the system is in the rejuvenation state}\]

\[P_3 : \text{Probability of the system is in the failure state}\]

Finally, by solving the above equations numerically, we can get the steady-state availability of the base station.

\[Availability = 1 - (P_2 + P_3)\]

\(16\)

The expected total downtime of the system in an interval of \(T\) time units is:

\[DownTime(T) = (P_2 + P_3) \times T\]

\(17\)

When a system is down, no service is provided and no revenue is received. Therefore, there is a business cost due to service being unavailable during downtime, and then the expected cost of downtime in an interval \(T\) time unit is:

\[DownTimeCost(T) = (P_3 \times C_f + P_2 \times C_r) \times T\]

\(18\)

4. Numerical Results

Consider a system with the following failure profile.

- The mean time between two consecutive failures is 3 months.
- The mean time between two consecutive failures from rejuvenation state to failure state is 6 months.
- The base longevity interval, which is the time for the system to go from normal state to warned state, is 15 days.
If rejuvenation is performed, the mean rejuvenation time is 10 minutes.
It takes 2 hours to recover from an unexpected failure.
It goes from the warned state to initial normal state with rate ($r_2=0.001$).
We perform software rejuvenation with the interval from 5 days to infinity (rate=0: no rejuvenation).
The average cost of unscheduled downtime due to a failure, $C_f$, is $1000 per hour.
The average cost of scheduled downtime during rejuvenation, $C_r$, is $50 per hour.

The influence of failure rates along with the different rejuvenation rates on availability is shown in Figure 6. Survivable systems require fewer failures and faster repair. We observe from Figure 6 that the failure rate of the system acts as an important factor in the availability of the system.
The influence of repair rates along with different detection rates on availability is shown in Figure 7.

The downtime cost of planned shutdown is much lower than that of an unplanned shutdown. Figure 8 shows the possibility of the practical use of our approach. The downtime cost of the system with our approach decreases as the detection rate increases.

5. Conclusion

In this paper, we have presented a framework of the security and survivability in WSN. We apply the software rejuvenation methodologies applicable in security and survivability fields. The rejuvenation methodology prevents the intruder’s attempts in various ways of attacks and the anticipated intrusions and protects unpredictable whole system failure by
detecting and monitoring the system in a timely fashion. In this paper, we have outlined the interaction of survivability, security and fault tolerance, so that we can effectively analyze and design the secure and survivable WSNs. Based on the studies of security requirements and survivability requirements, we have developed a framework for secure and survival WSNs through availability analysis.

As wireless sensor networks continue to grow, we expect that further expectations of security and survivability will be required of these WSN applications. This will be our future research for better improvement.

Acknowledgements

This research was supported by the Advanced Broadcasting Media Technology Research Center (ABRC) in Korea Aerospace University, Korea, under the Gyeonggi Regional Research Center (GRRC) support program supervised by Gyeonggi Province.

References


