

## Chapter 2

# QoS as Means of Providing WSN Security

### 2.1 Introduction

WSN are being increasingly used in applications where QoS and low cost are the overriding considerations. With increased use, their reliability, availability and serviceability need to be addressed from the outset. Conventional schemes of using sensor nodes and incorporating these three phenomenons (reliability, availability and serviceability—RAS) to attain QoS can effectively improve not only the reliability of the overall WSNs but security as well. We discuss the reverse look of QoS and hence present mathematically the three significant quality factors that should currently be taken into account in developing WSNs application services and security availability, reliability and serviceability. We also discussed specific characteristics and constraints of WSN, QoS factors when developing security applications for such networks. The security of WSNs has been addressed by providing the flow models and simulations testing using individual sensor nodes on our experiment. To evaluated possibility of establishing secure WSN through QoS we have used Hawk nodes to demonstrate our approach experimentally. The flow models show how the QoS can be integrated to increases the security of applications running under WSNs.

Sensor network communications must prevent disclosure and undetected modification of exchanged messages. Due to the fact that individual sensor nodes are anonymous and that communication among sensors is via wireless links, sensor networks are highly vulnerable to security attacks. If an adversary can thwart the work of the network by perturbing the information produced, stopping production, or pilfering information, then the perceived usefulness of sensor networks will be drastically curtailed. Thus, security is a major issue that must be resolved in order for the potential of WSNs to be fully exploited.

Several researchers have discussed QoS problems in WSN, but they have not focused on the availability, reliability and serviceability together as means of providing security integrity in WSN.

QoS is an overused term with multiple meanings and perspectives from different research and technical communities [1]. Perillo et al. [2] have defined QoS as measurements of application reliability with a goal of energy efficiency. An alternative definition equates QoS to spatial resolution [3]. This latter work also presented a QoS control strategy based on a Gur game paradigm in which base stations broadcast feedback to the network's sensors. The former work [2] refers to QoS parameters specific to the application, such as sensor node measurement, deployment, and coverage and number of active sensor nodes. The latter refers to how the supporting communication network can meet application needs while efficiently using network resources such as bandwidth and power consumption.

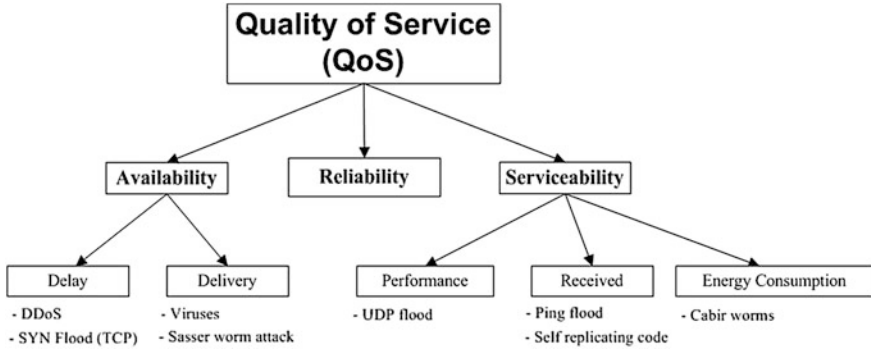
As WSNs are expected to be adopted in many industrial, health care and military applications, their reliability, availability and serviceability (RAS) are becoming critical. In recent years, the diverse potential applications for WSNs have been touted by researchers [4, 5] and the general press [6]. In many WSNs systems, to provide sufficient RAS can often be absorbed in the network cost. Nevertheless, as noticed early [7], network designers face "two fundamentally conflicting goals: to minimize the total cost of the network and to provide redundancy as a protection against major service interruptions".

To the best of our knowledge our approach is different from most of the existing works and on going research which deal with WSNs strategy to achieve QoS, we extend our finding to QoS as a support to security model we have designed by introducing a number of active security requirements distributed in a gradient fashion based on their logical connection to the QoS requirements.

Traditional QoS mechanisms used in wired networks aren't adequate to support WSNs because of constraints such as resource limitations and dynamic topology. So we build the middleware that provide new mechanisms to maintain QoS over an extended period and even adjust itself when the required QoS and the state of the application changes. That middleware had been designed based on trade-offs among performance metrics such as network capacity or throughput, data delivery delay, and energy consumption. We have considered QoS with new point of view, i.e. QoS as means of providing security mechanism in WSN. From combined availability, reliability and serviceability volumes together, we estimated meaning of QoS for WSN and then analyze it through our models.

WSNs are prone to security problems such as the compromising, tampering and malicious intrusions, eavesdropping of sensor data and adversarial packet injection, DoS attacks [8]. With this awareness in mind, integration of Security analysis with QoS design needs to meet both defense from these attacks and satisfy certain QoS requirements simultaneously from long view.

We examine WSNs nodes and propose the necessary QoS required for increasing both the availability and serviceability of the system, also as a way of intensify security within WSNs. Conventional schemes of using sensor nodes and incorporating these three phenomena (reliability, availability and serviceability) to attain QoS can effectively improve not only the reliability of the overall WSNs



**Fig. 2.1** Integration of security analysis with QoS

but also security. We present specific characteristics and constraints of WSNs QoS factors when developing security applications for such networks. The flow models show how the QoS can be integrated to increase the security of applications running under WSNs.

For better understanding, our approach is clearly mapped to our model where the model is merging to QoS as Fig. 2.1 indicates. A secure model is proposed with flow of security classes providing different levels of security using QoS. We assume that security context is not a precise technical specification; rather, it is a set of security-related factors narrowing down the WSNs security design to the region. Evidently, we describe the security context in terms of three related groups of factors and WSNs application: (1) Availability Motivation; (2) Reliability and (3) Serviceability.

## 2.2 QoS in Wireless Networks

### 2.2.1 QoS Concept

Quality-of-Service is “a set of service requirements to be met by the network while transporting a flow” [9]. Here a flow is “a packet stream from source to a destination (unicast or multicast) with an associated QoS” [9]. In other words, QoS is a measurable level of service delivered to network users, which can be characterized by packet loss probability, available bandwidth, end-to-end delay, etc. Such QoS can be provided by network service providers in terms of some agreement (Service Level Agreement, or SLA) between network users and service providers. For example, users can require that for some traffic flows, the network should choose a path with minimum 2 Mbit/s bandwidth.

### 2.2.2 QoS Metrics

To be implemented, service requirements have to be expressed in some measurable QoS metrics. Well-known metrics include bandwidth, delay, jitter, cost, loss probability, etc. Different metrics may have different features. The most commonly used functional forms of QoS-metrics are additive, multiplicative, and concave [10], classified according to an arithmetic relationship between the associated path-metric and link-metric. They are defined as follows.

For a path  $P = (n_1, n_2, \dots, n_n)$  of network nodes  $n_i, i = 1, 2, \dots, n$ , a metric  $m$  is:

**1. Additive**, if  $m(P) = m(n_1, n_2) + m(n_2, n_3) + \dots + m(n_{n-1}, n_n)$

Examples are delay, jitter, cost and hop-count. For instance, the delay of a path is the sum of the delay of every hop.

**2. Multiplicative**, if  $m(P) = m(n_1, n_2) \times m(n_2, n_3) \times \dots \times m(n_{n-1}, n_n)$

Example is reliability and loss probability.

**3. Concave**, if  $m(P) = \min\{m(n_1, n_2), m(n_2, n_3), \dots, m(n_{n-1}, n_n)\}$

Example is bandwidth, which means that the bandwidth of a path is determined by the link with the minimum available bandwidth.

### 2.2.3 Security and QoS

WSN is only as good as the information it produces. In this respect, the most important concern is information security. Indeed, in most application domains sensor networks will constitute a mission critical component requiring commensurate security protection. Sensor network communications must prevent disclosure and undetected modification of exchanged messages. Due to the fact that individual sensor nodes are anonymous and that communication among sensors is via wireless links, sensor networks are highly vulnerable to security attacks.

Being widely deployed in domains that involve sensitive information, for example, healthcare and rescue; the untethered and large deployment of WSNs in harsh environments increases their exposure to malicious intrusions and attacks such as DoS [8]. In addition, the wireless medium facilitates eavesdropping and adversarial packet injection to compromise the network's functioning. All these factors make security extremely important. Furthermore, sensor nodes have limited power and processing resources, so standard security mechanisms, which are heavy in weight and resource consumption, are unsuitable. These challenges increase the need to develop comprehensive and secure solutions that achieve wider protection, while maintaining desirable network performance. Middleware efforts should concentrate on developing and integrating security in the initial phases of software design, hence achieving different security requirements such as confidentiality, authentication, integrity, freshness, and availability.

### 2.2.4 QoS Challenges in Sensor Networks

Different from IP network, Sensor network naturally supports multiple service types, thus provides different QoS. The service types range from CBR (Constant Bit Rate) which guarantees bandwidth, delay and delay jitter, to UBR (Unspecified Bit Rate) which virtually provides no guarantees (just like today's "best-effort" IP network). While sensor networks inherit most of the QoS issues from the general wireless networks, their characteristics pose unique challenges. The following are an outline of design considerations for handling QoS traffic in WSNs.

**Bandwidth limitation:** A typical issue for general wireless networks is securing the bandwidth needed for achieving the required QoS. Bandwidth limitation is going to be a more pressing issue for WSN. Traffic in sensor networks can be burst with a mixture of real-time and non-real-time traffic. Dedicated available bandwidth solely to QoS traffic will not be acceptable. A trade-off in image/video quality may be necessary to accommodate non-real-time traffic. In addition, simultaneously using multiple independent routes will be sometime needed to split the traffic and allow for meeting the QoS requirements. Setting up independent routes for the same flow can be very complex and challenging in sensor networks due energy constraints, limited computational resources and potential increase in collisions among the transmission of sensors.

**Removal of redundancy:** Sensor networks are characterized with high redundancy in the generated data. For unconstrained traffic, elimination of redundant data messages is somewhat easy since simple aggregation functions would suffice. However, conducting data aggregation for QoS traffic is much more complex. Comparison of images and video streams is not computationally trivial and can consume significant energy resources. A combination of system and sensor level rules would be necessary to make aggregation of QoS data computationally feasible. For example, data aggregation of imaging data can be selectively performed for traffic generated by sensors pointing to same direction since the images may be very similar. Another factor of consideration is the amount of QoS traffic at a particular moment. For low traffic it may be more efficient to cease data aggregation since the overhead would become dominant. Despite the complexity of data aggregation of imaging and video data, it can be very rewarding from a network performance point-of-view given the size of the data and the frequency of the transmission.

**Energy and delay trade-off:** Since the transmission power of radio is proportional to the distance squared or even higher order in noisy environments or in the non-flat terrain, the use of multi-hop routing is almost a standard in WSNs. Although the increase in the number of hops dramatically reduces the energy consumed for data collection, the accumulative packet delay magnifies. Since packet queuing delay dominates its propagation delay, the increase in the number of hops can, not only slow down packet delivery but also complicate the analysis and the handling of delay-constrained traffic. Therefore, it is expected that QoS routing of sensor data would have to sacrifice energy efficiency to meet delivery requirements. In addition,

redundant routing of data may be unavoidable to cope with the typical high error rate in wireless communication, further complicating the trade-off between energy consumption and delay of packet delivery.

**Buffer size limitation:** Sensor nodes are usually constrained in processing and storage capabilities. Multi-hop routing relies on intermediate relaying nodes for storing incoming packets for forwarding to the next hop. While a small buffer size can conceivably suffice, buffering of multiple packets has some advantages in WSNs. First, the transition of the radio circuitry between transmission and reception modes consumes considerable energy [11] and thus it is advantageous to receive many packets prior to forwarding them. In addition, data aggregation and fusion involves multiple packets. Multi-hop routing of QoS data would typically require long sessions and buffering of even larger data, especially when the delay jitter is of interest. The buffer size limitation will increase the delay variation that packets incur while traveling on different routes and even on the same route. Such an issue will complicate medium access scheduling and make it difficult to meet QoS requirements.

**Support of multiple traffic types:** Inclusion of heterogeneous set of sensors raises multiple technical issues related to data routing. For instance, some applications might require a diverse mixture of sensors for monitoring temperature, pressure and humidity of the surrounding environment, detecting motion via acoustic signatures and capturing the image or video tracking of moving objects. These special sensors are either deployed independently or the functionality can be included on the normal sensors to be used on demand. Reading generated from these sensors can be at different rates, subject to diverse QoS constraints and following multiple data delivery models, as explained earlier. Therefore, such a heterogeneous environment makes data routing more challenging.

## 2.3 Effect of Security on QoS

Security services provide information secrecy, data integrity and resource availability for users. Information secrecy means to prevent the improper disclosure of information in the communications, while data integrity is to prevent improper modification of data and resource availability is considered to preventing improper DoS [12, 13].

All these attacks are aiming at one or more [14–16]. Although, security concerns in mobile traditional networks apply to sensor networks, the solutions are not the same. Sensor nodes are tightly constrained in terms of energy, processing, and storage capacities. Once deployed, it is often very difficult to change or recharge batteries for such nodes. This constraint limits the number of conventional techniques that can efficiently be adapted to sensor networks. Wireless communication makes information more vulnerable to attacks. Sensor nodes placed into the physical environments; therefore it is often easy to compromise by an attacker.

In addition, it is effortless to capture them physically and ruin them. However sensors networks composed of heterogeneous nodes with different capabilities.

Security is an overhead to the existing network QoS measurements therefore it has a strong influence on QoS of a network as well as providing (RAS). QoS metrics such as authentication delay, mobility, cost, call dropping probability and throughput of communication due to authentication overhead has to be affected. Typically authentication delay causes a pause for data transmission which decreases the throughput. Moreover length of keys and complexity of algorithm used has an adverse effect. Also size of packets transmitted is increased to include security parameters which affect the payload of messages.

Identifying the possible threats that may face sensor networks will help in designing secure WSNs as these threats are the ones hindering QoS. However in case of a WSNs longer keys would have a disastrous effect on the QoS of the network therefore it is important to classify security levels based on information secrecy, data integrity and resource availability. These aspects can be design into the system with variations of security strength classes.

Security classes indicate the level of protection provided by the QoS for analysis of security.

*Class 1, No Authentication:* Since no encryption is applied therefore secrecy of data and resource protection is not provided.

*Class 2, MAC verification only:* No encryption is applied therefore secrecy and resource protection is not provided. However this class provides slight bit of security by MAC authentication whereas a MAC address can be easily hacked.

*Class 3, Encrypted Challenge/Response without keys:* Encryption is applied only to verify user identity, therefore only legitimate users are allowed to have access to a resource. However since data transmission is not encrypted therefore there is a chance of data being compromised.

*Class 4, Encrypted transmission with  $K$ -length keys:* This class provides the highest level of security. However the length of the key could increase the overall authentication cost in terms of processing time. Higher security level is achieved by using complex cryptographic techniques which involve operations that increase the overhead of transmission and affects the QoS parameters such as authentication cost, authentication delay and packet dropping probability.

We investigated the problems of designing the accelerate block ciphers in Chap. 4 and establishment of distributed signature scheme in Chap. 5. The problem of reliable data transferring was considered in Chap. 6. We made a research about the influences of probabilities of stable system working and system breaking on QoS in Chap. 3.

Effects of security metrics place a lot of burden on the QoS of the overall system thus decreasing performance. Commonly used WSN protocols cannot be used for many reasons. Therefore a new secure transmission protocol, which has been proposed in Chap. 6, is required providing optimal transmission control and bandwidth utilization.

Integration of Security analysis with QoS design needs to meet both security and satisfy certain QoS requirements simultaneously from long view. Different from

most of the existing works which deal with WSNs strategy to achieve QoS, on Fig. 2.1, we extend QoS support to the model by introducing a number of active security requirements distributed in a gradient fashion based on their logical connection to the QoS requirements.

## 2.4 Reliability, Availability and Serviceability (RAS)

For availability and serviceability, remote testing and diagnostics is needed to pinpoint and repair (or bypass) the failed components that might be physically unreachable. Severe limitations in the cost and the transmitted energy within WSNs negatively impact the reliability of the nodes and the integrity of transmitted data. The application, itself, will greatly influence how system resources (namely, energy and bandwidth) must be allocated between communication and computation requirements to achieve requisite system performance. Furthermore, although performance of wireless communication systems and communication networks is well understood due to decades of research, the present body of knowledge regarding the performance of WSNs is limited.

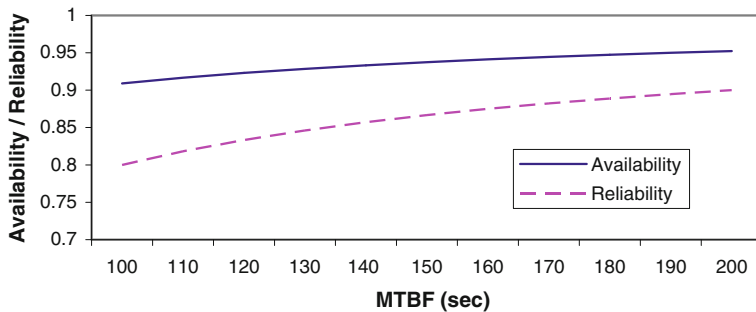
However, we examine WSNs nodes and propose the necessary QoS required for increasing both the availability and serviceability of the system, also as a way of intensify security within WSNs. Our approach is service oriented and was particularly motivated by recent proposals of defining QoS for WSNs in previously works.

QoS control is required for the assumption in sense that the number of sensors deployed exceeds the minimum needed to provide the requisite service. It presents two new techniques to maintain QoS under a variety of network constraints [2, 3]. The papers propose a new, extremely low-energy control strategy based on individual feedback in a random access communication system.

With the similar approach on QoS we present a primary application of this phenomenon, to explore and understand a security in WSNs as far as reliability, availability and serviceability are concerned as the indications for DoS detections. In particular, our work is applicable to sensor networks that are deployed in remote, hostile environments e.g., space applications and so on. Such networks are constrained by (1) high die-off rates of nodes and (2) inability to be replenished. The performance of the proposed approach is demonstrated throughout using numerical examples. Reliability of a system is defined as the probability of system survival in a period of time. Since it depends mainly on the operating conditions and operating time, the metrics of Mean Time Between Failure (MTBF) is used. For time period of duration  $t$ , MTBF is related to the reliability as follows [17]:

$$Reliability = 1 - \frac{t}{Mean\_time\_between\_failure} \quad (2.1)$$





**Fig. 2.2** Dependence availability and reliability on MTBF

Availability of a system is closely related to the reliability, since it is defined as the probability that the system is operating correctly at a given time. Dependence availability and reliability on MTBF presented on Fig. 2.2. Calculating availability is related to MTBF and Mean Time To Repair (MTTR) by the following relation [17]:

$$Availability = \frac{Mean\_time\_between\_failure}{Mean\_time\_between\_failure + Mean\_time\_to\_repair} \quad (2.2)$$

Considering availability of each node in isolation, from Eq. (2.2), the MTTR should be minimized, while MTBF should be maximized. While MTBF is given by manufacturing practices and components used, the value of MTTR can be controlled by both individual node and network design.

$$M\% = \frac{m \times 100\%}{n}$$

where  $m$  is a number of failed nodes within WSN,  $n$  is number of nodes within WSN and  $M\%$  is possible percentage of failed nodes within given WSN.

Serviceability of a system is defined as the probability that a failed system will restore to the correct operation. Serviceability is closely related to the repair rate and the MTTR [17].

$$Serviceability = 1 - \exp \times \left( -\frac{t}{Mean\_time\_to\_repair} \right) \quad (2.3)$$

A fundamental service in sensor networks is the determination of time and location of events in the real world. This task is complicated by various challenging characteristics of sensor networks, such as their large scale, high network dynamics, restricted resources, and restricted energy. We use Hawk sensor nodes for determination time of data transmitting in fulfilling the QoS under these constraints. We illustrate the practical feasibility to our approaches by concrete application of real sensor nodes (Hawk Sensor Nodes) to our experiments section.

In any system one must consider the reliability of its components when ascertaining overall system performance. Thus our question was whether the proposed strategy performed adequately for various levels of sensor reliability. Equation (2.1) does not include any information regarding expected sensor life and thus assumes static network resources, which is clearly not the case in WSNs. For example, sensors may fail at regular intervals due to low reliability, due to cost driven design choices, environmentally caused effects (especially in harsh environments), loss of energy, etc.

## 2.5 Calculating Availability and Probability Within WSN

What we discuss in this section is about achieving two primary factors of dependability in WSNs applications, namely availability and reliability. In the classical definition, a system is highly available if the fraction of its downtime is very small, either because failures are rare, or because it can restart very quickly after a failure [18]. If the application does not require all this redundant information, it would be desirable to conserve energy in some sensors by allowing them to sleep, thereby lengthening the lifetime of the network. For example, as sensors use up their limited energy, the application would like to use different sets of sensors to provide the required QoS (in this case, minimum sensor coverage area). This requires that the application manage the sensors over time. Such management can be as simple as turning sensors on and off, or as complex as selecting the routes for data to take from each sensor to the collection point in a multi-hop network. Furthermore, the needs of the surveillance application may change as a result of previously received data. For example, if the application determines that an intrusion has occurred, the application may assume a new state and require more sensors to send data to more accurately classify the intrusion.

The availability of several implementations is derived from Eq. (2.2) above for MTBF and MTTR. Due to the power issue and the unpredictable wireless network characteristics, it is possible that applications running on the sensor nodes might fail. Thus, techniques to improve the availability of sensor nodes are necessary. Estimated MTBF in our sensor nodes is based on the individually calculated failure rates for each component and the circuit board. Next, for the redundant system versions, if the failure rates ( $\lambda$ ) of each redundant element are the same, then the MTBF of the redundant system with  $n$  parallel independent elements ( $i$ ) [19] are taken as:

$$Mean\_time\_between\_failure = \sum_{i=1}^n \frac{1}{i\lambda} \quad (2.4)$$

The MTTR can be estimated by the sum of two values, referred to as Mean Time to Detect (MTTD) the failures and the Time to Repair (TTR) ( $MTTR = MTTD + TTR$ ). Notice that this part might be severely affected by the network connections.

Considering the technique [17], where the consumer starts the reparation mechanism by activating the local functional test. Once it completes, the test result is sent back to the consumer for analysis. If a failure occurs, the consumer will send the repair message to the sensor node and initialize the backup component. Acknowledgement is sent back to the consumer once the reparation is completed. If the message latency from the consumer to the target node is  $d$  seconds and the test time is  $c$  seconds, then we calculate MTTR as Eq. (2.5):

$$\text{mean\_time\_to\_repair} \sim 4d + c \quad (2.5)$$

For the sensor node without the Test Interface Module [17], consumer sends the measured data request command to the suspected sensor node. In order to check the data integrity, same request command will also send to at least two other nearby sensor nodes. The consumer compares the three collected streams of data and pinpoints the failed node. Once the failure is confirmed, consumer will notify the surrounding sensor node to take over the applications of the failed node. Once the failure is confirmed, consumer will notify the surrounding sensor node to take over the applications of the failed node. Again if the message latency from the consumer to the target node is  $d$  seconds, then MTTR is:

$$\text{Mean\_time\_to\_repair} \sim 8d \quad (2.6)$$

To estimate realistic MTTR numbers, we use study [20], where for WSNs Thermostat application with 64 sensor nodes is simulated. Due to the power and protocol requirements, the average latency of related messages is 1522 s. By applying this to our MTTR estimations, the test time  $c$  is much smaller and can be neglected.

Reliability of a system is defined as the probability of system survival (Fig. 2.6) in a period of time. Therefore, using Poisson probability [21] implemented for WSNs we have as well estimate probability of “failed” situation for whole WSN in given time interval, e.g. for one day (24 h) to demonstrate the reliability of our presented approach.

$$\text{probability}(r) = \frac{m^r \times e^{-m}}{r!} \quad (2.7)$$

where  $\text{Probability}(r)$  is a probability of failure system working with “ $r$ ” failed nodes within WSN for given time interval,  $r \geq 0$ ,  $m$  is a average number of failed nodes within WSN and  $e = 2.718...$

For example, in average there are 3 failed nodes in WSN for 24 h. Then we calculate Probabilities of failure system working as:

$$\text{Probability}(\text{“}r\text{”fails\_for\_24\_hours}) = \frac{3^r \times e^{-3}}{r!}$$

$$Probability(0\_fails\_for\_24\_hours) = P(0) = \frac{3^0 \times e^{-3}}{0!} = 0.0498$$

$$Probability(1\_fails\_for\_24\_hours) = P(1) = \frac{3^1 \times e^{-3}}{1!} = 0.1494$$

$$Probability(4\_fails\_for\_24\_hours) = P(4) = \frac{3^4 \times e^{-3}}{4!} = 0.1680$$

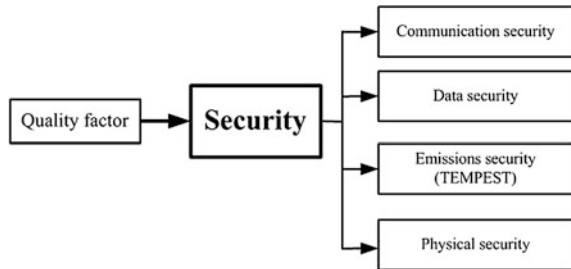
From this example, we can see that with progressive increase of fail nodes quantity of a WSN, the risk of unstable work also increases.

## 2.6 Proposed Security Models

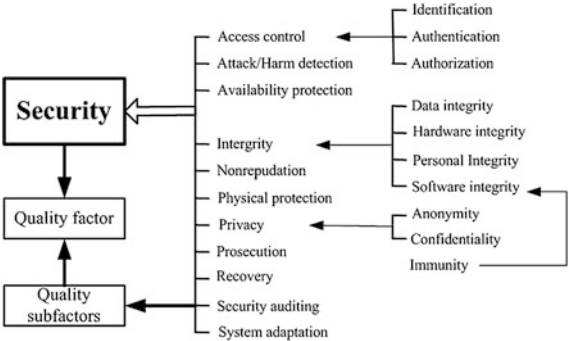
We have proposed thought model, in which things interact once they reach detailed proximity to each other. Here we clarify our assumptions about the flow the QoS uses to map Security. Specifically, the flow model needs to take care of two issues: (1) how to model the relationship between Security instances and QoS; (2) what are the quality factors and sub factors keep track to source QoS. There are of course many options for how to do this; but as far as our approach is concerned in the following part we discuss two reasonable flow ways in Figs. 2.3 and 2.4 for more clarity.

Our model is concern with properties that, such applications must have included availability, reliability, safety and security. The notion of dependability captures these concerns within a single conceptual framework, making it possible to approach the different requirements of a critical system in a unified way as can be seen in Fig. 2.1. We assume that application performance can be described by the quality factor of different variables of interest to the application, where the QoS of the different variables depends on which sensors provide data to the application. For example, in the personal health monitor, variables such as blood pressure, respiratory rate, and heart rate may be determined based on measurements obtained from any of several sensors. Each sensor has a certain QoS in characterizing each of the application's variables. For example, a blood pressure sensor directly measures

Fig. 2.3 Flow model



**Fig. 2.4** Amalgamation of QoS in WSN security coverage flow model



blood pressure, so it provides a quality of 1.0 (Quality is mapped to a specific reliability in determining the variable from the sensor’s data, with 1.0 corresponding to 100 % reliability) in determining this variable. In addition, the blood pressure sensor can indirectly measure other variables such as heart rate, so it provides some quality, although less than 1.0, in determining these variables (data security, communication security, physical security). The quality of the heart rate measurement would be improved through high-level fusion of the blood pressure measurements with data from additional sensors such as a blood flow sensor.

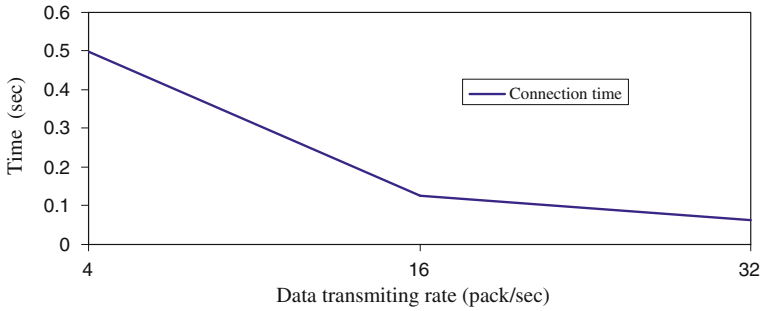
This can be modeled as the application changing state based on Quality factor. For different security states, different sets of sensors should be activated to provide the greatest benefit to the security application.

Figure 2.4 illustrates the important variables to monitor when determining a security condition and indicates the security types that can provide at least some quality to the measurement of these security types. Each line between a security type and a variable is labeled with the quality factor can provide to the measurement of that security.

2.7 Experiment Evaluation

To assess our techniques against traditional security approach in terms of three aspects Reliability, Availability, and Serviceability (RAS) we have implemented various experiments to Pentium III Computer processor and 512 MB memory was used. We measured the processing throughput, i.e., the number of data transmitted events that each phase is able to process per second and time taken to transmit these data within selected sensor nodes, as can be seen in graph presentation in Fig. 2.5.

To simplify the process, we suppose all services share the same QoS as defined formerly. We consider that the element QoS\_prediction\_input has four properties: Availability, Reliability, Bandwidth, and Request time. Availability measures whether or not the client can connect to the service (i.e., web service, SN service). It takes a value of 0 (can not connect) or 1 (be able to connect). Reliability refers to

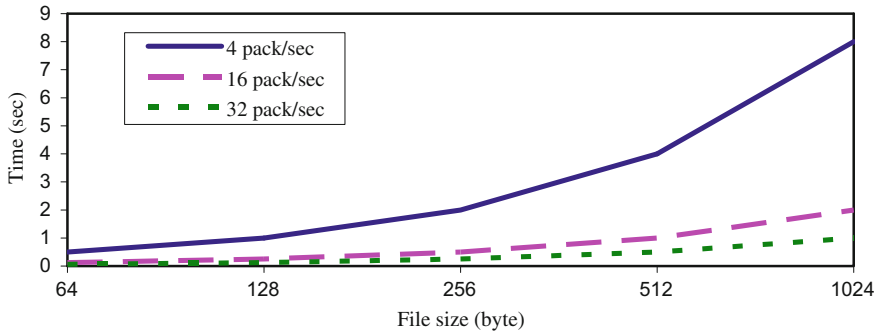


**Fig. 2.5** Connection time for 4/16/32 pack/s

whether the operation the client wishes to perform can be performed. It takes a value of 0 (unable to perform the operation) or 1 otherwise. If a service is not reachable, the Reliability is assumed to be 0 for that interaction. Bandwidth is used to measure the network condition, and Request\_time is the moment a user requests a particular service. As to the QoS output parameters, we mainly consider two QoS criterions: connection time and transmittion\_time. The former measures the expected delay between the moments a request is sent and the moment the result is brought back; the latter reflects whether the transmittion process has performed properly or not, where 1 means transmittion was well performed and 0 means otherwise. The Service's QoS prediction results are given as below however; this methodology requires increased computational complexity.

Notice that the performance of the communication channel is not taken into considerations in the above calculations for single node availability. With channels used for WSNs, packets losses are common. They increase the message latency and can ultimately affect the MTTR. We analyzed further the influence of the network to the availability. We plot the node availability versus average latency, which lumps together the characteristics of the channel, the number of retransmission retries on the failure, as well as the node-dependent features such as retransmission timeouts in Fig. 2.6.

In Fig. 2.6, we examine WSNs nodes to transmit the data in evaluating (RAS). Two sensor nodes with 32 size byte were used for estimating connection time with different transmitting rate. With 0.0625 t/s we were able to connect 32 packets. To ask one sensor node to transmit the data we need 2 data packets (one for asking, another one for receiving the answer). To estimate Time to connection we have to transmit only two packets. *Number of packets = file size / packet size*. *Time = number of packets / data transmitting rate*. This can be used to propose the necessary infrastructure required for increasing both the availability and serviceability of the system, in spite of the absence of a reliable transport layer. Hence this can be used to analyze and detect delay, delivery, performance or energy consumptions caused by different attacks as elaborated in Fig. 2.1.



**Fig. 2.6** Transmitting time in different number of packets to access (RAS)

## 2.8 Summary

In this chapter, security of WSN is considered through QoS. Using QoS components, we evaluated models and system-level test using sensor nodes.

One primordial issue is to satisfy application QoS requirements while providing a high-level abstraction that addresses WSN security. Notice that although we consider primarily testing in the lab, the proposed solutions can easily be applied to testing in factory with large size of Sensor network applications. With the proposed approach, such tests can be easily parallelized by applying wireless broadcast to many nodes at once. As a result, the proposed approach can be used in variety of testing scenarios.

Security issues in a health monitoring system utilizing Wireless Sensors in a WSN have been discussed precisely with data integrity in security aspects. A secure model is proposed with flow of security classes providing different levels of security using QoS. However our finding found that effects of security metrics place a lot of burden on the QoS of the overall system thus decreasing performance.

## References

1. Chen, D., Varshney, P.K.: QoS support in wireless sensor networks: A survey. In: Proceedings of International Conference on Wireless Networks, vol. 13244, pp. 227–233 (2004)
2. Perillo, M., Heinzelman, W.: Providing application QoS through intelligent sensor management. In: 1st Sensor Network Protocols and Applications Workshop, pp. 93–101 (2003)
3. Iyer, R., Kleinrock, L.: QoS control for sensor networks. In: IEEE International Conference on Communications, vol. 1, pp. 517–521 (2003)
4. Pottie, G., Kaiser, W.: Wireless integrated network sensors. *Commun. ACM* **43**(5), 51–58 (2000)
5. Estrin, D., Girod, L., Pottie, G., Srivastava, M.: Instrumenting the world with wireless sensor networks. In: Proceedings of International Conference on Acoustics, Speech and Signal Processing, vol. 4, pp. 2033–2036 (2001)

6. MIT Technology Review: 10 emerging technologies that will change the world. MIT Technology Review, Cambridge (2003)
7. Rey, R.F.: Engineering and Operations in the Bell System. Bell Labs, New Jersey (1977)
8. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. *Commun. ACM* **47**(6), 53–57 (2004)
9. Crawley, E., Nair, R., Rajagopalan, B., Sandick, H.: A framework for QoS-based routing in the Internet. Internet informational RFC 2386, 37. <http://wUHHUwww.ietf.org/rfc/rfc2386.txt> (1998)
10. Chen, S.: Routing support for providing guaranteed end-to-end quality-of-service. Ph.D. thesis, UIUC, 207. <http://cairo.cs.uiuc.edu/publications/papers/SCthesis.ps> (1999)
11. Min, R., Bhardwaj, M., Cho, S.H., Shih, E., Sinha, A.: Low power wireless sensor networks. In: *Proceedings of International Conference on VLSI Design*, pp. 205–210 (2001)
12. Stallings, W.: *Network security essentials. Applications and standards*. Prentice Hall, Upper Saddle River (2000)
13. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's Ad hoc Netw. J. Spec. Issue Sens. Netw. Appl. Protoc.* **1**(2–3), 293–315 (2003)
14. Kargl, F., Schlott, S., Klenk, A., Geiss, A.: Michael weber. Securing ad hoc routing protocols. In: *IEEE EUROMICRO*, pp. 514–519 (2004)
15. Undercoffer, J., Avancha, S., Joshi, A., Pinkston, J.: Security for sensor networks, wireless sensor networks, pp. 253–275 (2004)
16. <http://www.csee.umbc.edu/cadip/2002Symposium/sensorids.pdf>
17. Chiang, M.W., Zilic, Z., Radecka, K., Chenard, J.S.: Architectures of increased availability wireless sensor network nodes. In: *ITC International Test Conference*, vol. 43(2), pp. 1232–124 (2004)
18. Knight, J.C.: An introduction to computing system dependability. In: *Proceedings of the 26th International Conference on Software Engineering*. IEEE Computer Society, pp. 730–731 (2004)
19. Callaway, E.H.: *Wireless sensor networks architectures and protocols*. Auerbach Publications, UK (2004)
20. Headquarters, Department of the Army, TM-5-698-1: *Reliability/Availability of Electrical & Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance Facilities* (2003)
21. Eddousm, M., Stansfield, R.: *Methods of decision making*. Unity press, Leicester, pp. 50–52 (1997)



Security in Wireless Sensor Networks

Oreku, G.S.; Pazynyuk, T.

2016, XVII, 87 p. 20 illus., 7 illus. in color., Hardcover

ISBN: 978-3-319-21268-5