electronics

Article

An Energy-Efficient Secure Forwarding Scheme for QoS Guarantee in Wireless Sensor Networks

Dongwan Kim [1], Jaekeun Yun [2,*] and Daehee Kim [3,*]

[1] Department of Electronics Engineering, Dong-A University, Busan 49315, Korea; dongwankim@dau.ac.kr
[2] Division of Vehicle Component, LG Electronics, Seoul 07795, Korea
[3] Department of Internet of Things, Soonchunhyang University, Asan 31538, Korea
* Correspondence: novaroot82@gmail.com (J.Y.); daeheekim@sch.ac.kr (D.K.); Tel.: +82-10-9392-5711 (J.Y.); +82-10-2547-3751 (D.K.)

Received: 13 August 2020; Accepted: 31 August 2020; Published: 1 September 2020

Abstract: Many wireless sensor network (WSN) applications require both security and quality-of-service (QoS) to be guaranteed simultaneously. However, ensuring both security and QoS is not trivial in WSNs since security normally has bad impact on QoS. In this paper, we propose an energy-efficient secure forwarding method that minimizes energy consumption while meeting both security and QoS requirements at the same time. To accomplish this goal, we alternatively use hop-by-hop security for conserving energy through data aggregation and end-to-end security to satisfy the QoS requirement. We further analyze why hop-by-hop security with data aggregation provide better energy efficiency than end-to-end security without aggregation in detail. The simulation result shows that our proposed method outperforms other scheme in terms of energy efficiency while meeting both QoS and security.

Keywords: wireless sensor networks; secure forwarding; quality-of-service; data aggregation; hop-by-hop security; end-to-end security

1. Introduction

Wireless sensor networks (WSNs) generally consist of numerous distributed sensor nodes and several base station (BS). Sensor nodes detect the events and gather the environment information, and this information is then delivered to the BS over multi-hop. Recently, WSNs are getting attentions as an essential component of the Internet of Things (IoT), which can be applied to various applications such as environmental monitoring, patient monitoring, and industrial fields [1–4]. The important thing to note is that these applications must guarantee quality-of-service (QoS) requirement, especially *delay*. For example, when sensor nodes detect a fire in the mountain, it must be notified to the BS as soon as possible. If the detection information is delivered to the BS late, it becomes useless [4]. Thus, a lot of works have been focused on the QoS in WSNs [5–12].

As deployment of WSNs increases, security threats to WSNs are also increasing. However, ensuring security in WSNs is not so trivial because sensor nodes have very low computation capability and limited energy, and thus cannot apply general security technology such as public key cryptography. Furthermore, sensor nodes are subject to node compromise attacks where the adversary can physically compromise sensor nodes and extract all information such as key materials from them. Lots of research on security in WSNs have been done in the field of efficient and lightweight key management, data encryption, and authentication [13–22].

On the other hand, in a variety of wireless sensor networks applications such as the intruder detection system and the remote patient monitoring system, the sensory data must be delivered to the BS while ensuring both security and QoS. For example, the information of the intruder in the intruder detection system must not only be forwarded to the BS within the predefined time budget, but also be protected by security primitives such as confidentiality, integrity, and authentication. However, ensuring both security and QoS is challenging in WSNs since it takes non-trivial time a resource-constrained sensor node to perform security operations such as encryption and decryption. Thus, security and QoS have been studied independently as mentioned above.

Only very few works have focused on both security and QoS [23–26]. Xu et al. [23] tried to optimize security and QoS at the same time using both connection outage probability and secrecy outage probability, but it does not take energy efficiency into account. Rachedi et al. [24] focused on maximizing the security level without sacrificing QoS, thus it can be vulnerable to security attacks when congestion happens. Rathee et al. [25] attempted to find a balance among security, QoS, and energy efficiency by employing a multi-objective function. However, they do not guarantee security strictly. Rachedi et al. [26] proposed a genetic algorithm based on optimization method for security, QoS and energy efficiency. They also fail to satisfy security requirements because of the priority to QoS and energy efficiency.

In this paper, we propose a secure forwarding scheme whose goal is to minimize energy consumption while satisfying the requirement of both QoS and security in WSNs. It is important to note that among many QoS parameters, we especially focus on delay which is the most critical parameter in a variety of WSNs applications such as the intruder detection system and the remote patient monitoring system. Furthermore, we focus on three security requirements of confidentiality, authenticity, and integrity which are fundamental in most WSNs applications. Confidentiality is guaranteed by encryption and decryption, and authenticity and integrity are achieved by authentication tokens such as message authentication code (MAC). To accomplish our goal, we alternatively use hop-by-hop security and end-to-end security according to the remaining time budget. Hop-by-hop security implies that each node shares a key with its neighbor and the data are decrypted and encrypted in every hop. Thus, hop-by-hop security has computation delay in each hop that aggravates QoS. However, hop-by-hop security gives an opportunity to perform in-network data aggregation [27–29] using spatial and temporal correlations among sensed data from nearby sensors, thereby reducing the energy consumption. On the other hand, end-to-end security performs encryption and decryption in the source node and the BS only, not in the intermediate nodes, and thus have no computation delay in each hop. However, end-to-end security does not provide data aggregation since intermediate nodes do not know a key between the source node and the BS. Thus, we use hop-by-hop security to conserve energy through data aggregation as long as the time budget is sufficient. When estimating that the sensor node does not have enough time with hop-by-hop security, it switches into end-to-end security in order to reach the BS within deadline. Our main contributions are as follows.

- We propose a secure forwarding scheme with QoS assurance which tries to minimize energy consumption. Given QoS requirements, our scheme performs data aggregation as many times as possible by preferring hop-by-hop security.
- We analyze the relation between QoS and security in terms of energy efficiency in detail and prove that hop-by-hop security with data aggregation provides better energy efficiency than end-to-end security without data aggregation.
- We evaluate our proposed scheme through a variety of simulations in terms of energy efficiency and packet delivery ratio under a variety of scenarios. The result shows that our proposed scheme guarantees security and security at the same time while minimizing energy consumption.

The remainder of the paper is organized as follows. Section 2 provides related works on QoS and security. In Section 3, we propose our secure forwarding scheme with QoS guarantee, and we analyze the energy consumption in hop-by-hop security and end-to-end security in Section 4. After Section 5 presents and discusses the performance evaluation about our scheme, Section 6 concludes the paper.

2. Related Works

In this section, we thoroughly investigate a variety of related works on energy efficiency, QoS, and security in WSNs since our goal is to minimize energy consumption while satisfying both QoS and security simultaneously. We further present several related works on data aggregation which motivate our proposed scheme. After we emphasize the importance of energy efficiency in WSNs, we look into several works on QoS and security separately. Finally, a few schemes aiming to guarantee both QoS and security are followed by works on data aggregation.

Since sensor nodes are generally deployed in the unattended environment, they are equipped with batteries with limited capacity. Obviously, the most important goal in WSNs is to conserve energy in sensor nodes. This is why most existing research on WSNs has been focusing on energy efficiency while considering other factors such as routing, QoS, security, and data aggregation [30].

There have been a lot of research on QoS in WSNs which are mainly combined with routing. Xu et al. [5] proposed an energy-efficient clustering routing protocol based on a high-QoS node deployment with an inter-cluster routing mechanism that extends the network lifetime by selecting the cluster head based on the residual energy and the distance of the nodes to the BS. Gao et al. [6] presented a statistical QoS-driven power control scheme while maximizing energy efficiency. They selected best power control policy under different QoS constraints. Zhang et al. [7] proposed a QoS-aware and energy-efficient routing algorithm in industrial WSNs by selecting the optimal relay node in terms of real-time and reliability. Hasan et al. [8] proposed multipath QoS routing algorithms by adaptively switching QoS paths whereby significantly improving packet delivery ratio, energy efficiency, and end-to-end delay. Genta et al. [9] presented a meta-heuristic optimization based on routing algorithm by considering minimum distance and least energy dissipation in order to provide QoS and energy efficiency. QoS-aware and heterogeneously clustered routing protocol was proposed in [10] which provides the dedicated paths for satisfying QoS requirements. Wu et al. [11] proposed a novel delay-aware routing algorithm that achieves energy efficiency by employing a location-based forwarding scheme. Faheem et al. [12] proposed a cross-layer QoS-aware routing protocol for the underwater acoustic sensor networks. All of these works provided novel approaches on QoS in WSNs, but they only focused on QoS and energy efficiency without taking security into account.

Since security in WSNs is of paramount importance, many researchers have been focusing on tailoring existing security methods into resource-constrained WSNs in terms of key management, encryption/decryption, integrity, and authentication. Liu et al. [14] proposed a lightweight pseudo-random encryption scheme to ensure confidentiality over insecure wireless links. Hayajneh et al. [15] proposed a security protocol for WSNs with cooperative communication, thereby improving the network reliability and resilience. Hasseb et al. [16] developed a secure and energy-efficient routing protocol for avoiding intrusion. They ensure the integrity and reliability of the sensory data by exploiting Shamir secret sharing scheme [17]. Hussein et al. [18] provided a scalable group key management scheme and a secure communication method based on elliptic curve cryptography. Yu et al. [19] presented a novel authentication protocol for vehicular communications in WSNs which can guarantee mutual authentication, session key management, and privacy. Jung et al. [20] proposed an authenticated key agreement protocol which provides enhanced features such as anonymous authentication, resistance to session key compromise, and energy efficiency. Gope et al. [21] proposed a lightweight mutual authentication protocol with privacy-preserving which are secure against physical node compromise attacks and energy efficiency. Energy-efficient and secure path optimization protocol was proposed in [22] where security and energy efficiency are accomplished by binary hop count and security code using Huffman coding. All of above works guaranteed effective security and energy efficiency for WSNs, but they do not consider QoS at all.

Even though a lot of attentions have been paid to QoS and security as mentioned above, there have been very few works which considers both QoS and security simultaneously. This is because security gives adverse effect on QoS in terms of processing time and transmission time. In other words, sensor nodes must perform encryption/decryption for confidentiality or generate security tokens for authentication, and then deliver these security tokens to the destination node. Xu et al. [23] proposed a secure optimal QoS routing protocol (SOQR) which attempts to optimize both security and QoS at the same time using both connection outage probability and secrecy outage probability. Even though SOQR achieves a balance between QoS and security, but it does not take energy efficiency into account. Rachedi et al. [24] proposed a new integration scheme of QoS and security based on the PID controller. Given QoS requirements, they try to maximize security by considering resource availability and residual energy. This scheme is very novel in that it gracefully integrates security with QoS using the PID controller, but it can be vulnerable to security attacks when congestion happens since it does not sacrifice QoS instead of security. Rathee et al. [25] proposed a QoS aware energy balancing secure routing (QEBSR) protocol based on ant colony optimization. QEBSR selects a routing path according to the metric of energy cost, end-to-end delay and the trust factor computed by enhanced heuristics. QEBSR attempts to make tradeoffs among security, QoS, and energy efficiency by employing a multi-objective function, but it does not guarantee security strictly. Rachedi et al. [26] proposed a genetic algorithm based on optimization method for security, QoS, and energy efficiency. They accomplish to find a balance among them, but also fail to satisfy security requirements due to the priority to the QoS and energy efficiency.

Data aggregation in WSNs is a good technique to save energy by aggregation multiple packets into one packet [27]. This effectively reduces the amount of transmitted data and helps to improve the lifetime of sensor nodes. Li et al. [28] proposed a differentiated data aggregation routing protocol in order to conserve energy. Zhang et al. [29] proposed a novel data aggregation scheme based on rings which provides reliability and energy efficiency. In this paper, we utilize data aggregation to conserve as much energy as possible while delivering data to the BS. Data aggregation can have negative or positive impacts on QoS. If each sensor node waits for a long time to aggregate more packets, it will affect QoS badly. However, if each sensor node waits for a short time, it gives better QoS since data aggregation reduce the amount of data to be transmitted. In this paper, we try to aggregate as many packets as possible in order to reduce energy consumption by considering the QoS requirement.

3. Proposed Secure Forwarding Scheme with QoS Guarantee

3.1. Overview

The goal of our proposed scheme is to deliver the sensed data collected from the sensor nodes to the BS securely within deadline while minimizing energy consumption. To achieve this goal, we take advantage of the fact that the sensed data has spatial and temporal correlation. Instead of forwarding the received sensed data directly, each node waits for another sensed data for some time and aggregates them into one packet by removing the redundant data and header overhead. The aggregated packet is then forwarded to the next sensor node. This process is repeated until the packet arrives at the BS. Since energy consumed by communication is most significant in WSNs, hop-by-hop security must be used to enable data aggregation in secure forwarding. Unfortunately, the waiting time and hop-by-hop security for data aggregation have an adverse effect on the QoS requirement. Thus, we adaptively adjust the waiting time for data aggregation using fully distributed hop count and average transmission time at each node. Adaptive waiting time increases the probability of data aggregation and reduces energy consumption. Energy consumption in hop-by-hop security with data aggregation and end-to-end security without data aggregation is analyzed in detail in Section 4.

3.2. Assumptions

We first assume that WSNs consists of resource-constrained sensor nodes with limited resources and one BS with infinite resources. Our goal is to minimize energy consumption of sensor nodes while ensuring QoS and security. We assume that each packet has a predetermined QoS requirement ($T_{deadline}$) according to the applications and every packet can be delivered to the BS successfully if we do not perform data aggregation and do not have collisions during transmission. We assume that symmetric key cryptography, especially AES-128 for encryption/decryption and hash-based MAC (HMAC) for authenticity and integrity, is used for WSNs and parameters related to security, including key materials and cryptographic algorithms, are established in each node by using existing key establishment scheme such as COKES [31]. It is important to note that security in our scheme is provided with the help of existing security algorithms using symmetric key cryptography. We focus on how to balance between QoS and energy efficiency by alternately using existing secure hop-by-hop security and end-to-end security. Each sensor node is assumed to be synchronized with the BS using existing synchronization protocols such as SETB [32] and transmit the collected information to the BS through multi-hop communication.

3.3. Database Component (DC)

The database component (DC) stores the information, obtained from the information exchange component (IEC), for forwarding the sensing data as shown in Figure 1. When requested, the DC provides the information to the IEC or the decision making and forwarding component (DMFC). The DC consists of two tables; the forwarding table (FT) and the average transmission time table (ATTT).

The FT stores the information of one neighboring node to be forwarded, which has the smallest hop count to the BS, including the ID, the hop count to the BS, and the average transmission time as shown in Figure 2. If a better neighbor, which has the smaller hop count than the current one, is discovered through a beacon message, the FT is updated accordingly. The ATTT is a table that stores the average transmission time that it takes to deliver a message from each neighboring node to itself. Whenever receiving the sensing data from the neighbor node, each node obtains the real transmission time from the timestamp of the received packet and updates the average transmission time of the neighboring node in the ATTT using exponentially weighted moving average. Furthermore, the ATTT of each node is exchanged with the neighbor nodes via a beacon message in order to inform the neighboring nodes of the average transmission time to the sender of the beacon message. The structure of FT and ATT is shown in Figure 2.

3.4. Information Exchange Component (IEC)

The IEC periodically transmits a beacon message which contains the ID of the sending node, the minimum hop count to the BS, the ID of the neighbor nodes, and the corresponding average transmission time from each neighbor node to the sending node. Upon receiving the beacon message from the neighboring node, the IEC compares the hop count in the beacon message with that of the FT, and updates the FT with the received information if the hop count in the message is smaller than that of the FT. It is important to note that the overhead due to beacon messages can be negligible since sensor nodes in WSNs already use beacon messages for the neighbor discovery. To avoid collision with neighboring nodes, each node sends a beacon message after random waiting.

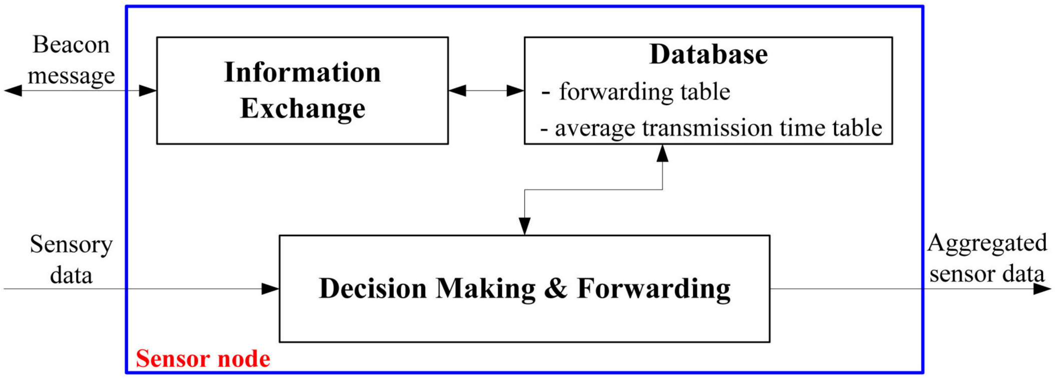


Figure 1. The architecture of the proposed scheme.

3.5. Decision Making and Forwarding Component (DMFC)

The DMFC is responsible for making forwarding decision of either hop-by-hop with data aggregation or end-to-end security without data aggregation.

When selecting to perform hop-by-hop security with data aggregation, the total time spent in the intermediate node i is expressed as

$$t_{tot}(i) = t_{dec}(i) + t_{agg}(i) + t_{enc}(i) + t_{tx}(i) \tag{1}$$

where $t_{dec}(i)$ is the time taken to decrypt the data and authenticate the data, $t_{agg}(i)$ is the time taken to wait and perform data aggregation, $t_{enc}(i)$ is the time to encrypt the data and generate an authentication token, and $t_{tx}(i)$ is the time to transmit the data to the next-hop node. $t_{tx}(i)$ includes all possible delay such as queueing delay, transmission delay, propagation delay, and delay due to collision and contention.

Without data aggregation at intermediate nodes, the following equation is always satisfied from our assumption.

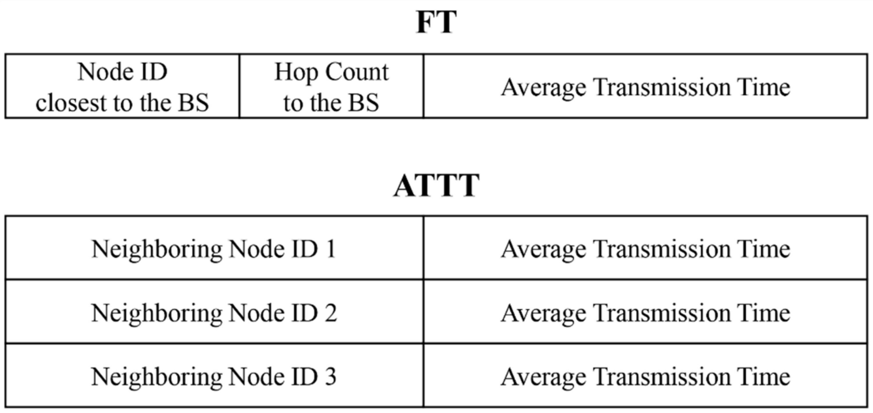
$$\sum_{i=1}^{h} (t_{dec}(i) + t_{enc}(i) + t_{tx}(i)) \leq T_{deadline} \tag{2}$$

where h is a hop count from the source node to the BS.

When performing data aggregation to conserve energy, each intermediate node spends additional time, $t_{agg}(i)$, for waiting and processing data aggregation. Thus, we need to guarantee the following equation.

$$\sum_{i=1}^{h} (t_{dec}(i) + t_{agg}(i) + t_{enc}(i) + t_{tx}(i)) \leq T_{deadline} \tag{3}$$

In Equation (3), each node knows h via a periodic beacon message. t_{dec} and t_{enc} is predetermined by the performance of the sensor node. For example, it takes 1.53 ms and 3.52 ms for TelosB, widely used in WSNs, to perform encryption and decryption using AES-128, respectively [33]. Since the sum of t_{dec} and t_{enc} is five times longer than the time taken to send a 28-byte packet using CC2420 RF transceiver (250 kbps), which is 28 bytes/250 kbps = 0.896 ms, t_{dec} and t_{enc} must be taken into account. t_{agg} is the time we can adjust to improve the energy efficiency while satisfying the QoS. t_{tx} is the most difficult part to predict accurately because of queueing delay and retransmission from collision and contention. To estimate t_{tx}, each node updates the average transmission time whenever sensing data is received. Upon receiving sensing data, the receiving node obtains the time taken for the actual transmission and updates the average transmission time using exponentially weighted moving average. The updated average transmission time is then delivered to the neighboring node through a beacon message and used for forwarding.



FT

Node ID closest to the BS	Hop Count to the BS	Average Transmission Time

ATTT

Neighboring Node ID 1	Average Transmission Time
Neighboring Node ID 2	Average Transmission Time
Neighboring Node ID 3	Average Transmission Time

Figure 2. The structure of forwarding table (FT) and average transmission time table (ATTT).

Algorithm 1 shows the operation of our proposed scheme. When the sensing data are received from node *A*, the receiving node *B* computes the time taken for the real transmission through timestamps of the packet (step 1, 2), and updates the average transmission time (step 3). Node B then calculates the remaining time (step 4) and adaptively adjusts the time when the received data is forwarded to the next node. If the remaining time is equal to or less than 0, the data are discarded since the deadline is exceeded so that it is no longer useful (step 5). If the remaining time is larger than y and the current security mode is hop-by-hop security, node B first computes RT_1 to check whether data aggregation can be enabled (step 6). We use the reserved bit in the Frame Control field of the 802.15.4 MAC header to denote the current security mode where "0" is hop-by-hop security and "1" is end-to-end security. We ignore the switching time because it consists of a few computations. If the current security mode is end-to-end security, the node just records a timestamp and relay it to the next node without modification (step 9). The term of y is a margin for the QoS requirement. Since the estimated average transmission time and the actual transmission time can be different, we add the term of y to enhance delivery ratio. As y increases, t_{agg} decreases, thereby enhancing the probability of meeting the QoS requirement. However, the term of y has an adverse impact on the energy consumption by reducing t_{agg}. Thus, we try to balance between the delivery ratio and the energy consumption by multiplying *rand*() with y where *rand*() is a uniformly random value between 0 and 1. If *rand*() returns 0, the actual margin is 0. If *rand*() returns 1, the actual margin becomes y. RT_1 is the estimated remaining time when intermediate nodes perform data aggregation. If RT_1 is larger than y which means that node *B* has sufficient time for aggregation, node *B* computes the aggregation time, t_{agg}, as shown in step 7. The term of $h/\sum_{i=1}^{h} i$ makes t_{agg} become larger in the node with a larger hop count since the nodes near the event have more probability for aggregation due to spatial correlation. Once node *B* computes t_{agg}, it waits for t_{agg} in order to perform data aggregation and send the sensing data using hop-by-hop security as explained in step 7.

Algorithm 1 Operations of node *B* upon receiving sensing data from node *A*.

```
1:  Record a timestamp of data reception, $t_{rx}^{B}$.
2:  $t_{real\_trans}^{AB} = t_{rx}^{B} - t_{tx}^{A}$        // AB means "from node A to node B"
3:  $t_{avg\_trans}^{AB} = (1-\alpha)t_{avg\_trans}^{AB} + \alpha \cdot t_{real\_trans}^{AB}$
4:  $T_{deadline} = T_{deadline} - t_{real\_trans}^{AB}$
5:  if $T_{deadline} <= 0$,
        Discard the data.
6:  else if hop-by-hop security
        Retrieve the information of the neighbor node C with the smallest hop h in the FT.
        $RT_1 = T_{deadline} - (t_{dec} + t_{avg\_trans}^{BC} + t_{enc}) \times h$
7:      if  $RT_1 > y$,        // in case of data aggregation (hop-by-hop security)
            $t_{agg} = (RT_1 - rand() \times y) \times \frac{h}{\sum_{i=1}^{h} i}$   , Unit of $RT_1$ and $y$ : ms
            Wait for $t_{agg}$ to perform data aggregation.
            Record a timestamp, $t_{tx}^{B}$ in the data packet.
            Send node C the data encrypted by a key shared with node C.
8:      else               // in case of no data aggregation (end-to-end security)
            $RT_2 = T_{deadline} - (t_{dec} + t_{avg\_trans}^{BC} \times h + t_{enc})$
            if  $RT_2 > y$, $t_{agg} = RT_2 - rand() \times y$
              Wait for $t_{agg}$ to perform data aggregation.
            Record a timestamp, $t_{tx}^{B}$ in the data packet.
            Mark end-to-end security in the Frame Control field of the MAC header.
            Send node C the data encrypted by a key shared with the BS.
9:  else if end-to-end security
        Record a timestamp, $t_{tx}^{B}$ in the data packet.
        Send node C the data without modification.
```

If RT_1 is smaller than y, node B cannot use hop-by-hop security in the subsequent sensor nodes. Thus, node B decides to use end-to-end security instead of hop-by-hop security. Node B then calculates RT_2 which is the estimated remaining time when end-to-end security is adopted. If RT_2 is larger than y, node B has a chance for data aggregation, thus node B waits for t_{agg} after it sends the sensing data using end-to-end security as shown in step 8. It is important to note that node B does not perform aggregation if RT_2 is equal to or less than y.

4. Analysis on Energy Consumption of Hop-by-Hop Security and End-to-End Security

In this section, we analyze energy consumption of hop-by-hop security with aggregation and end-to-end security without aggregation in detail. We first assume a very simple topology as shown in Figure 3 where each circle is a sensor node and arrows denote the direction of transmission. Each node is denoted as S_x which is a sensor node x hops away from the BS. We focus on the effect of data aggregation in a specific node, S_h, which is an intermediate node h hops away from the BS. S_h receives data from downstream nodes and can aggregate them into one packet, which is then transmitted to the upstream node S_{h-1}.

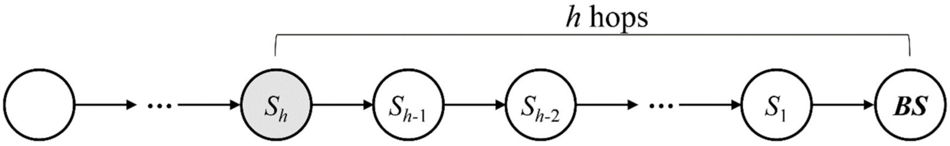


Figure 3. An example of simple topology in wireless sensor networks (WSNs).

We assume that the size of a packet is the sum of a header, H, and a payload, P. We refer to E_{enc}, E_{dec}, and E_{auth} as the energy consumed by encryption, decryption, and authentication. Authentication adds a HMAC of size T to the packet in order to guarantee authenticity and integrity. E_{agg} is the energy consumed by aggregating one byte, and E_{byte} is the energy consumed by transmitting one byte and receiving one byte. We finally assume that S_h has N packets in the buffer.

Under these assumptions, total energy consumption to deliver N packets from S_h to the BS with end-to-end security without aggregation is

$$E_{tot}^{no\_agg} = h \times N \times (H + P + T) \times E_{byte} \tag{4}$$

It is worth noting that intermediate nodes do not perform encryption and decryption since they use end-to-end security.

Data aggregation can reduce energy by taking advantage of redundancy which means that sensor nodes can send identical packet when they detect the same event. We assume that S_h aggregate N packets received from downstream nodes into one packet. In the worst case, all N packets are different and thus all packets must be delivered to the upstream node. Even with this situation, we can make the size of a packet transmitted shorter by aggregation them into one packet. More specifically, the size of N packets is $N \times (H + P + T)$ which becomes $H + N \times P + T$ as Figure 4.

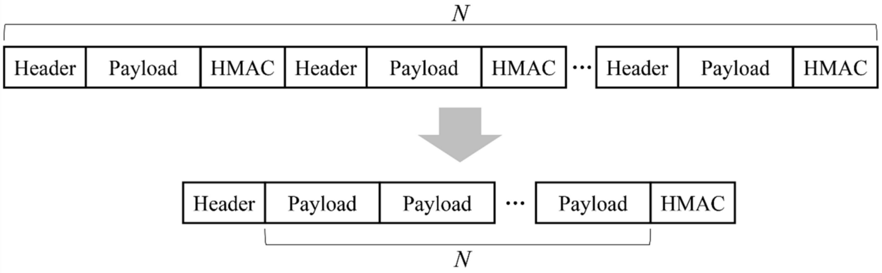


Figure 4. An example of data aggregation in the worst case.

Thus, in the worst case, total energy consumption to transmit N packets from S_h to the BS with hop-by-hop security with aggregation is

$$E_{tot}^{agg\_worst} = h \times \{(H + N \times P + T) \times (E_{byte} + E_{agg}) + (E_{enc} + E_{dec} + E_{auth})\} \tag{5}$$

In this case, energy consumption by communication is reduced by performing data aggregation but energy consumption by encryption and decryption is added due to hop-by-hop security. Obviously, the best case using data aggregation is that all N packets are identical, i.e., redundant, thus S_h can aggregate N packets into only one packet whose size is $H + P$. In this case, total energy consumption becomes

$$E_{tot}^{agg\_best} = h \times \{(H + P + T) \times (E_{byte} + E_{agg}) + (E_{enc} + E_{dec} + E_{auth})\}. \tag{6}$$

With above equations, we compare end-to-end security without aggregation to hop-by-hop security with aggregation by setting the parameters as shown in Table 1. We assume that the number of packets to be aggregated is 5. "Data aggregation (best)" and "Data aggregation (worst)" show even smaller energy consumption than no data aggregation by 35.5% and 72.7%, respectively.

Table 1. Parameter values used in the simulation.

Parameter	Value
Communication range	20 m
Beacon interval	1 s
Packet size	39 bytes (header: 19, data: 20)
Energy consumed by transmission of one byte	5.76 µJ
Energy consumed by reception of byte	6.48 µJ
Energy consumed by encryption	39.08 µJ
Energy consumed by decryption	89.9 µJ
Energy consumed by authenticating a HMAC	62.15 µJ
Energy consumed by aggregation of one byte	5 nJ
Size of a HMAC	4 bytes
Deadline ($T_{deadline}$)	1 s, 2 s
Decryption Time (t_{dec})	1.53 ms
Encryption Time (t_{enc})	3.52 ms
Simulation time	1000 s
α (for EWMA)	0.5
margin (y)	0 ms, 10 ms, 20 ms

From the analysis in this section, we can conclude that hop-by-hop security with data aggregation gives much better energy efficiency than end-to-end security with no data aggregation since energy consumed by communication is much better than energy consumed by encryption, decryption, authentication, and data aggregation.

5. Evaluation

In this section, we compare our proposed scheme to one with no data aggregation at all in terms of energy consumption and packet delivery ratio since we focus on how to balance between energy efficiency and QoS, especially delay, by alternately using hop-by-hop security and end-to-end security. Packet delivery ratio is the ratio of packets received by the BS within deadline over total packets sent by sensor nodes. It is worth noting that it is impossible to compare our scheme with other existing schemes [23–26] that consider both QoS and security since they focus on different metrics from ours as introduced in Section 2. We perform simulations with MATLAB where one BS, located at the center, and 400 sensor nodes are deployed randomly in a field of 200 m × 200 m. The event occurs every second and the event location is uniformly random. When an event occurs, every node within the range of 10 m can detect the event and send the event to the BS according to IEEE 802.15.4. Each node performs data aggregation by discarding data when receiving the same event data or by compressing headers when receiving different event data, and each node is assumed to have infinite energy since nodes near the sink usually spend much more energy, thus fail earlier which makes the entire WSN disabled. We also perform simulations with several margins, y, in order to identify the influences of y on energy consumption and delivery ratio. We finally set the deadline to 1 s and 2 s. For more accurate result, we derive an average result based on ten times. The remaining parameters for the simulation based on TelosB platform with TinyOS employed from [33–36] are summarized in Table 1.

Figure 5 shows the energy consumption of both the no data aggregation forwarding method and our proposed method with three different margins when the deadline is 1 s. The proposed method is better than no data aggregation method in terms of energy efficiency by approximately 73.2%, 67.5%, and 63.6% in case of y = 0, 10, and 20, respectively. This is because the proposed scheme sends a small number of packets by effectively aggregating payloads and HMACs through hop-by-hop security. It is important to note that even though hop-by-hop security consumes more energy to encrypt, decrypt, authenticate, and aggregate data in each hop, this is much smaller than the energy for communicating more data without data aggregation. Figure 5 also shows that the margin value has an adverse impact on energy consumption. When the margin value increases, t_{agg} is shortened and the opportunity for data aggregation is reduced, thereby increasing energy consumption slightly.

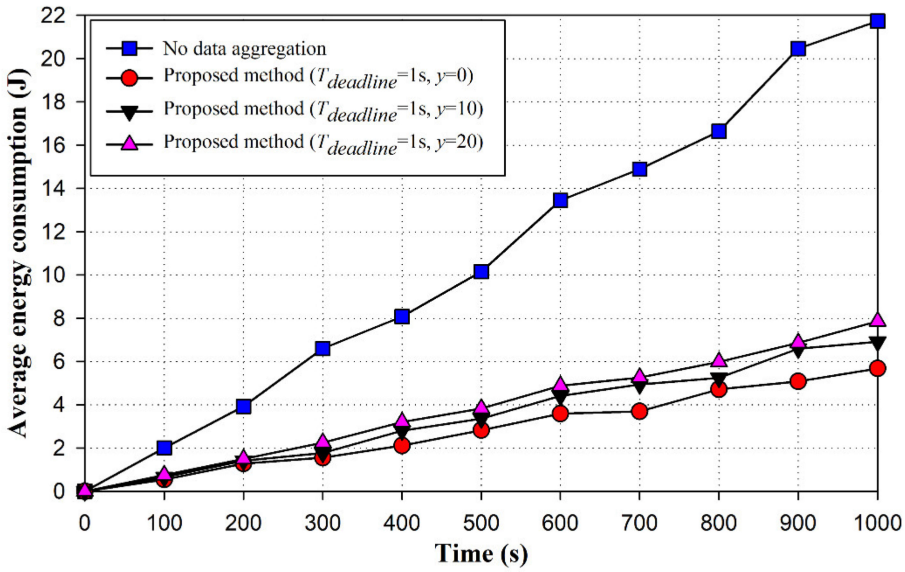


Figure 5. Average energy consumption with the deadline of 1 s.

Figure 6 shows the packet delivery ratio within the deadline of both no data aggregation method and our proposed method with three different margins. Our proposed method with a margin of 20 and the no data aggregation scheme delivered every packet within deadline successfully. In contrast, our proposed method with a margin of 0 and 10 shows lower packet delivery ratio by approximately 3.01% and 2.01%, respectively. It is because additional delay due to data aggregation is introduced when sending data after waiting for t_{agg}, thereby exceeding the deadline of the data. More specifically, our proposed scheme predicts the transmission time by averaging the actual transmission time as shown in line 3 of algorithm 1. Hence, if congestion in each node occurs, packets cannot be delivered to the BS within the deadline because it takes more time than predicted for the congested sensor node to send data. Even though our proposed method with a margin of 0 and 10 shows lower packet delivery ratio than one with no data aggregation, it is very important to note that our proposed method with a margin of 20 can achieve 100% of delivery ratio with much lower energy consumption by 63.6% than one with no data aggregation. This is because adding a fixed margin value to each hop is good for not violating the deadline and still helps nodes with larger hops to perform sufficient data aggregation.

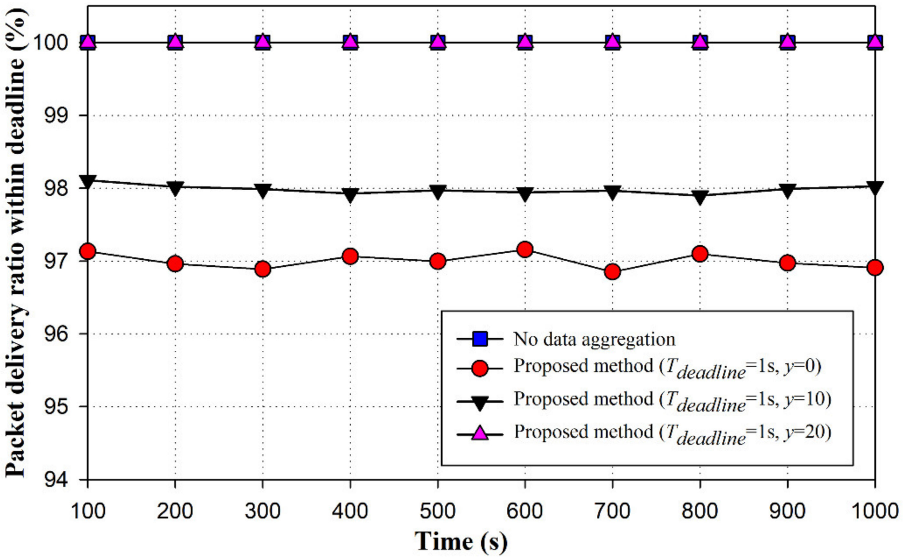


Figure 6. Packet delivery ratio with the deadline of 1 s.

Figure 7 shows the average energy consumption within the deadline when the deadline is 2 s. In this case, each node waits for longer time, thus it can have more opportunity to aggregate packets. As a result, it shows slightly smaller energy consumption than the case with deadline of 1 s. However, no data aggregation is not affected by the deadline because it does not perform data aggregation. Thus, we can find that our proposed scheme conserves much more energy than one with no data aggregation by approximately 76.2%, 70.1%, and 65.6% in case of y = 0, 10, and 20. It is worth noting that we can reduce more energy if we have longer deadline. We show the packet delivery ratio with the deadline of 2 s in Figure 8. You can verify that packet delivery ratio is almost the same as the case with deadline of 2 s because we spend additional time for data aggregation, not for transmitting faster. Compared with Figure 6, similar percentage of packets exceed the deadline due to congestion in Figure 8.

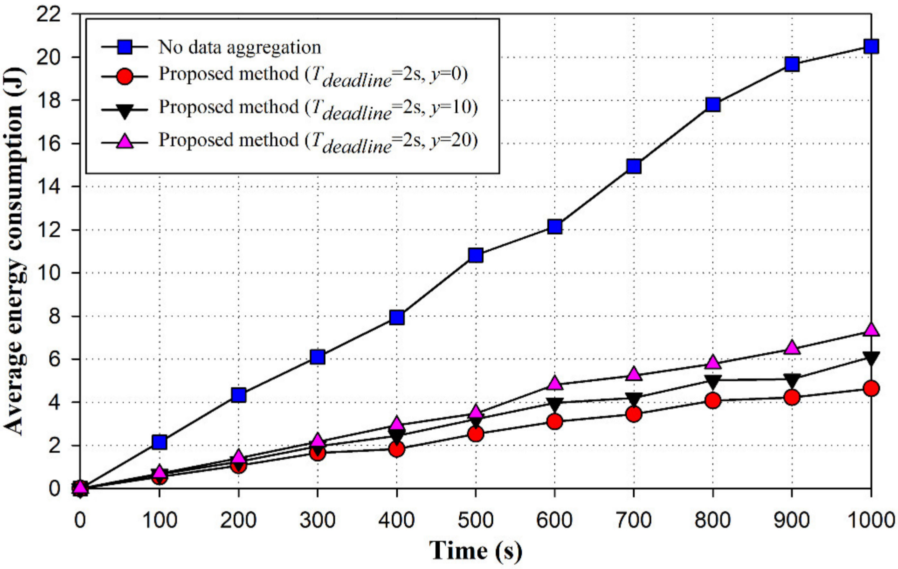


Figure 7. Average energy consumption with the deadline of 2 s.

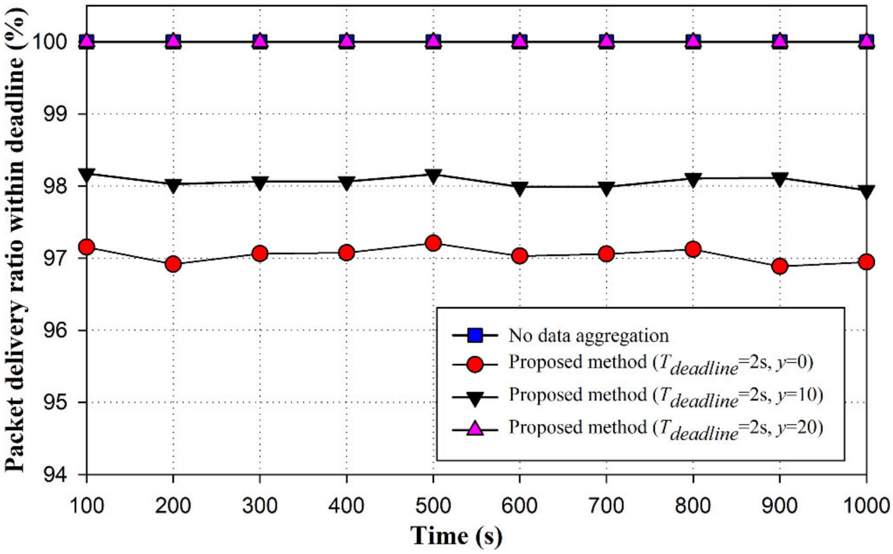


Figure 8. Packet delivery ratio with the deadline of 2 s.

Figure 9 shows the average energy consumption when the number of nodes increases. In no aggregation case, the energy consumption increases rapidly since more sensor nodes detect the same event and they send all information individually. On the contrary, energy consumption in our proposed method increases more slowly as the number of nodes increases. This is because more redundant packets are aggregated in the intermediate node when more sensor nodes detect the same event. It is worth noting that our proposed scheme outperforms one with no data aggregation by about 89.1% in the case that y is 0 and the number of nodes is 2000.

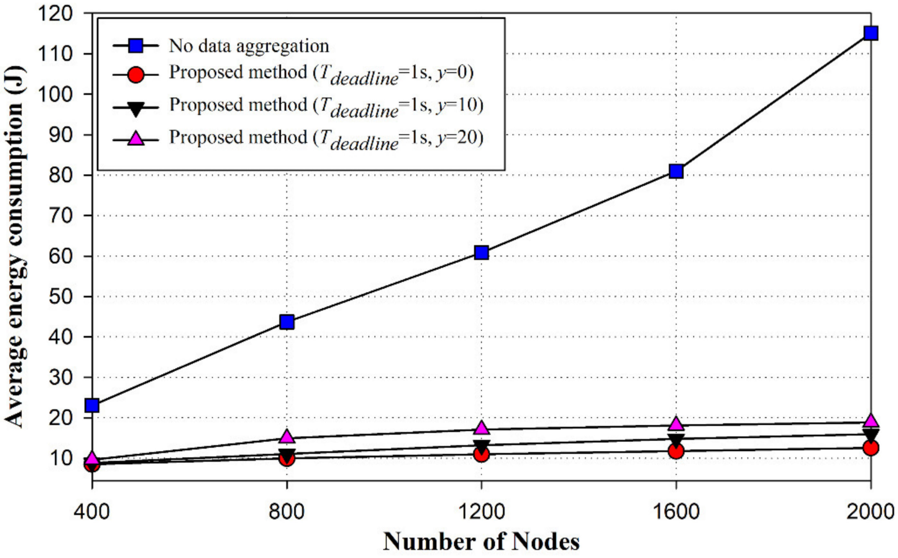


Figure 9. Average energy consumption according to the number of sensor nodes.

In Figure 10, we finally show the tradeoffs between the average energy consumption and the deadline violation probability when the margin value changes. As the average energy consumption increases from 5.68 J to 7.87 J, the deadline violation probability decreases from 0.301 to 0. Thus, with our proposed scheme, we can obtain no deadline violation by sacrificing approximately 28.9% of energy consumption. However, it is important to note that our proposed scheme still consume less energy than one with no data aggregation by 63.6%.

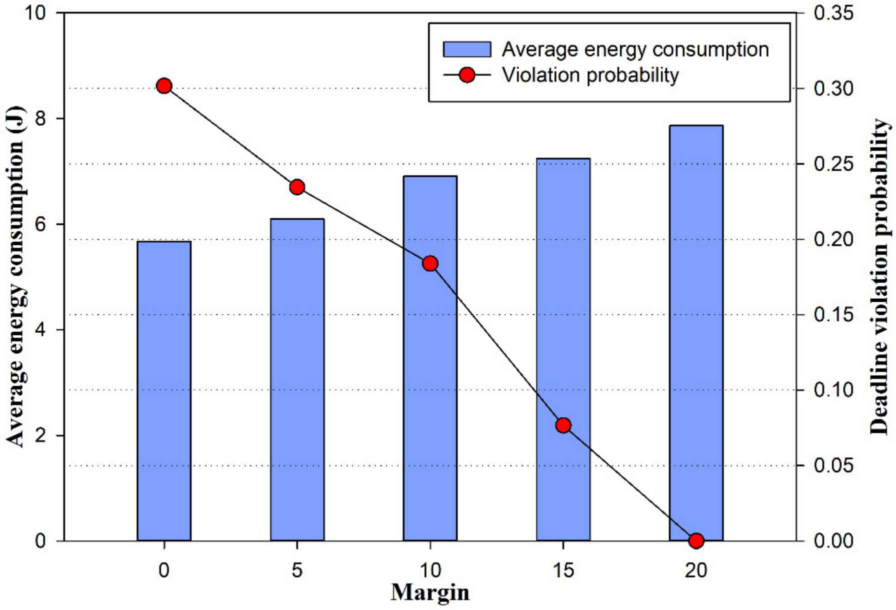


Figure 10. Tradeoffs between average energy consumption and deadline violation probability.

6. Conclusions

In this paper, we proposed an adaptive energy-efficient secure forwarding method with QoS assurance. In order to reduce energy consumption while meeting both security and QoS requirements, we use hop-by-hop security to conserve energy through data aggregation as long as the delay budget is sufficient. When estimating not to meet the delay budget with hop-by-hop security, we switched to end-to-end security in order to reach the BS within deadline. The simulation result showed that our proposed method with a margin of 20 can achieve 100% of delivery ratio with lower energy consumption by 63.6%. In our future work, we will try to improve the accuracy of the average transmission time estimation by taking into account other factors such as queue lengths and channel conditions. Accurate estimation gives us an enhanced delivery ratio within deadline. In addition, we will try to implement our proposed scheme in real motes to reflect real environments such as channel conditions and energy consumption for better evaluation in a variety of WSN applications.

Author Contributions: D.K. (Daehee Kim) devised the basic concept of the proposed scheme. J.Y. supervised the whole procedure related to this paper. D.K. (Dongwan Kim) performed simulations, validated the result, and wrote the original draft. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Soonchunhyang University research fund and this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2020R1F1A1048664).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kandris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of Wireless Sensor Networks: An Up-to-Date Survey. *Appl. Syst. Innov.* **2020**, *3*, 14. [CrossRef]
2. Haque, M.; Asikuzzaman, M.; Khan, I.U.; Ra, I.-H.; Hossain, S.; Shah, S.B. Comparative Study of IoT-Based Topology Maintenance Protocol in a Wireless Sensor Network for Structural Health Monitoring. *Remote Sens.* **2020**, *12*, 2358. [CrossRef]
3. Kim, B.-S.; Kim, S.; Kim, K.H.; Sung, T.-E.; Shah, B.; Kim, K.-I. Adaptive Real-Time Routing Protocol for (m,k)-Firm in Industrial Wireless Multimedia Sensor Networks. *Sensors* **2020**, *20*, 1633. [CrossRef] [PubMed]
4. Xu, Y.-H.; Sun, Q.-Y.; Xiao, Y.-T. An Environmentally Aware Scheme of Wireless Sensor Networks for Forest Fire Monitoring and Detection. *Future Internet* **2018**, *10*, 102. [CrossRef]

5. Xu, K.; Zhao, Z.; Luo, Y.; Hui, G.; Hu, L. An Energy-Efficient Clustering Routing Protocol Based on a High-QoS Node Deployment with an Inter-Cluster Routing Mechanism in WSNs. *Sensors* **2019**, *19*, 2752. [CrossRef]
6. Gao, Y.; Cheng, W.; Zhang, H. Statistical-QoS Guaranteed Energy Efficiency Optimization for Energy Harvesting Wireless Sensor Networks. *Sensors* **2017**, *17*, 1933. [CrossRef]
7. Zhang, W.; Liu, Y.; Han, G.; Feng, Y.; Zhao, Y. An Energy Efficient and QoS Aware Routing Algorithm Based on Data Classification for Industrial Wireless Sensor Networks. *IEEE Access* **2018**, *6*, 46495–46504. [CrossRef]
8. Hasan, M.Z.; Al-Turjman, F.; Al-Rizzo, H. Optimized Multi-Constrained Quality-of-Service Multipath Routing Approach for Multimedia Sensor Networks. *IEEE Sens. J.* **2017**, *17*, 2298–2309. [CrossRef]
9. Genta, A.; Lobiyal, D.K.; Abawajy, J.H. Energy Efficient Multipath Routing Algorithm for Wireless Multimedia Sensor Network. *Sensors* **2019**, *19*, 3642. [CrossRef]
10. Amjad, M.; Afzal, M.K.; Umer, T.; Kim, B.-S. QoS-Aware and Heterogeneously Clustered Routing Protocol for Wireless Sensor Networks. *IEEE Access* **2017**, *5*, 10250–10262. [CrossRef]
11. Wu, S.; Chou, W.; Niu, J.; Guizani, M. Delay-Aware Energy-Efficient Routing towards a Path-Fixed Mobile Sink in Industrial Wireless Sensor Networks. *Sensors* **2018**, *18*, 899. [CrossRef] [PubMed]
12. Faheem, M.; Butt, R.A.; Raza, B.; Alquhayz, H.; Ashraf, M.W.; Shah, S.B.; Ngadi, A.; Gungor, V.C. QoSRP: A Cross-layer QoS Channel-Aware Routing Protocol for the Internet of Underwater Acoustic Sensor Networks. *Sensors* **2019**, *19*, 4762. [CrossRef] [PubMed]
13. Yu, J.-Y.; Lee, E.; Oh, S.-R.; Seo, Y.-D.; Kim, Y.-G. A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security. *IEEE Access* **2020**, *8*, 45304–45324. [CrossRef]
14. Liu, L.; Chen, W.; Li, T.; Liu, Y. Pseudo-Random Encryption for Security Data Transmission in Wireless Sensor Networks. *Sensors* **2019**, *19*, 2452. [CrossRef] [PubMed]
15. Al Hayajneh, A.; Bhuiyan, Z.A.; McAndrew, I. A Novel Security Protocol for Wireless Sensor Networks with Cooperative Communication. *Computers* **2020**, *9*, 4. [CrossRef]
16. Haseeb, K.; Almogren, A.; Islam, N.; Din, I.U.; Jan, Z. An Energy-Efficient and Secure Routing Protocol for Intrusion Avoidance in IoT-Based WSN. *Energies* **2019**, *12*, 4174. [CrossRef]
17. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
18. Hussein, S.M.; López-Ramos, J.A.; Álvarez-Bermejo, J.A. Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro. *Sensors* **2020**, *20*, 2242. [CrossRef]
19. Yu, S.; Lee, J.; Lee, K.; Park, K.; Park, Y. Secure Authentication Protocol for Wireless Sensor Networks in Vehicular Communications. *Sensors* **2018**, *18*, 3191. [CrossRef]
20. Jung, J.; Moon, J.; Lee, D.; Won, D. Efficient and Security Enhanced Anonymous Authentication with Key Agreement Scheme in Wireless Sensor Networks. *Sensors* **2017**, *17*, 644. [CrossRef]
21. Gope, P.; Das, A.K.; Kumar, N.; Cheng, Y. Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4957–4968. [CrossRef]
22. Alghamdi, T. Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method. *IEEE Access* **2018**, *6*, 53576–53582. [CrossRef]
23. Xu, Y.; Liu, J.; Takahashi, O.; Shiratori, N.; Jiang, X. SOQR: Secure Optimal QoS Routing in Wireless Ad Hoc Networks. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2017; pp. 1–6.
24. Rachedi, A.; Hasnaoui, A. Advanced quality of services with security integration in wireless sensor networks. *Wirel. Commun. Mob. Comput.* **2014**, *15*, 1106–1116. [CrossRef]
25. Rathee, M.; Kumar, S.; Gandomi, A.H.; Dilip, K.; Balusamy, B.; Patan, R. Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks. *IEEE Trans. Eng. Manag.* **2019**, 1–13. [CrossRef]
26. Rachedi, A.; Benslimane, A. Multi-objective optimization for security and QoS adaptation in Wireless Sensor Networks. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2016; pp. 1–7.
27. Dhand, G.; Tyagi, S. Data Aggregation Techniques in WSN: Survey. *Procedia Comput. Sci.* **2016**, *92*, 378–384. [CrossRef]

28. Li, X.; Liu, W.; Xie, M.; Liu, A.; Zhao, M.; Xiong, N.N.; Zhao, M.; Dai, W. Differentiated Data Aggregation Routing Scheme for Energy Conserving and Delay Sensitive Wireless Sensor Networks. *Sensors* **2018**, *18*, 2349. [CrossRef] [PubMed]
29. Zhang, J.; Hu, P.; Xie, F.; Long, J.; He, A. An Energy Efficient and Reliable In-Network Data Aggregation Scheme for WSN. *IEEE Access* **2018**, *6*, 71857–71870. [CrossRef]
30. Nakas, C.; Kandris, D.; Visvardis, G. Energy Efficient Routing in Wireless Sensor Networks: A Comprehensive Survey. *Algorithms* **2020**, *13*, 72. [CrossRef]
31. Kim, D.; Kim, D.; An, S. Communication pattern based key establishment scheme in heterogeneous wireless sensor networks. *KSII Trans. Internet Inform. Syst.* **2016**, *10*, 1246–1272.
32. Kim, D.; Kang, S.; An, S. Secure and Efficient Time Synchronization for Border Surveillance Wireless Sensor Networks. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2016**, *99*, 385–401. [CrossRef]
33. Lee, J.; Kapitanova, K.; Son, S.H. The price of security in wireless sensor networks. *Comput. Netw.* **2010**, *54*, 2967–2978. [CrossRef]
34. El Fissaoui, M.; Beni-Hssane, A.; Saadi, M. Energy efficient and fault tolerant distributed algorithm for data aggregation in wireless sensor networks. *J. Ambient. Intell. Humaniz. Comput.* **2018**, *10*, 569–578. [CrossRef]
35. Gupta, G.P.; Misra, M.; Garg, K. Towards scalable and load-balanced mobile agents-based data aggregation for wireless sensor networks. *Comput. Electr. Eng.* **2017**, *64*, 262–276. [CrossRef]
36. Islam, M.; Ali, G. Data Aggregation in Wireless Sensor Networks Using Firefly Algorithm. *Wirel. Pers. Commun.* **2019**, *104*, 307–324.