Concealed data aggregation in wireless sensor networks: A comprehensive survey

Keyur Parmar*, Devesh C. Jinwala*

S. V. National Institute of Technology, Surat, India

Abstract

The objectives of concealed data aggregation are to provide end-to-end privacy and en route aggregation of reverse multicast traffic in wireless sensor networks. Privacy homomorphism has been used for realizing these objectives together. Although privacy homomorphism achieves the conflicting objectives, such as privacy and data aggregation, it negatively affects other security objectives such as integrity and freshness. Privacy homomorphism that protects sensor readings from passive adversaries makes them susceptible to active adversaries whose aim is to modify or inject malicious data packets in the network. In this article, we present a comprehensive survey of the state-of-the-art concealed data aggregation protocols in wireless sensor networks. We investigate the need for en route aggregation, encrypted data processing, en route and end-to-end integrity verification, and replay protection. We discuss the challenges and their proposed solutions for achieving the conflicting goals such as in-network aggregation, privacy, integrity, and replay protection. We comparatively evaluate the performance of concealed data aggregation protocols for measuring their respective strengths and weaknesses. In addition, we provide a detailed insight into the open research issues in concealed data aggregation and conclude with possible future research directions.

Keywords: Wireless Sensor Networks, Secure Data Aggregation, Privacy Homomorphism, Privacy, Integrity, Replay Protection

1. Introduction

Advances in Micro-Electro-Mechanical Systems (MEMS) technology have facilitated the development of tiny sensor devices. These sensor devices have escalating capabilities to perform sensing, processing, and transmission [1, 2]. The multitude of these devices can collaborate to form a network, commonly referred to as the Wireless Sensor Network (WSN) [1–5]. WSNs support a wide variety of applications in military and civilian environments such as battlefield surveillance, traffic regulation, home automation, environment & health care monitoring, and wildfire detection [3, 4, 6, 7]. One of the characteristic features that separate WSNs from the ad hoc networks is the scarce resources [4]. The tiny sensor devices are equipped with very limited resources such as memory, processor, bandwidth, and energy [8, 9]. Amongst these resources, non-replenishable energy has a direct impact on the longevity of WSNs. Therefore, there exists a need to reduce the energy consumption in WSNs. In WSNs, as shown by Hill et al. [10], transmission of a single bit over a meter range consumes the same amount of energy as required to execute a thousand CPU instructions. As the radio frequency (RF) operations consume far more energy than the CPU instructions, there exists a need to reduce the communication traffic for increasing the lifetime of WSNs. Although mechanisms, such as radio scheduling, control packet elimination, and topology control, help in reducing the energy consumption, one of the widely acknowledged approaches for reducing the energy consumption is in-network data aggregation [11–14]. In-network data aggregation performs en route aggregation of reverse multicast traffic in data-centric networks such as WSNs.

Although in-network data aggregation reduces

*Corresponding author

Email addresses: keyur.mtech@gmail.com (Keyur Parmar), dcjinwala@acm.org (Devesh C. Jinwala)

the redundant communication traffic, it is vulnerable to a wide range of attacks [15, 16]. Adversaries can compromise leaf/intermediate nodes and access the information stored therein. The compromised intermediate (aggregator) nodes can detriment the quality and accuracy of aggregated sensor readings. In addition, the lack of physical protection makes sensor nodes vulnerable to a wide variety of attacks [17–21]. The objective of secure data aggregation protocols [15, 16, 22–27, 27–34, 34–62] is to combine security and data aggregation together. Initial secure data aggregation protocols [15, 16, 23–27] tend to provide security in a hop-by-hop manner, where encryption and decryption operations are carried out at intermediate hops. However, in hop-by-hop secure data aggregation, sensor readings become vulnerable due to adversaries that have access to the compromised intermediate nodes. Therefore, the need to protect the privacy of sensor readings at intermediate nodes becomes imperative.

End-to-end secure data aggregation, also known as concealed data aggregation (CDA), achieves end-to-end privacy of reverse multicast traffic in WSNs [27, 28]. In the CDA protocols [27–44, 46, 47, 50–63], data once encrypted can only be decrypted at the base station. In addition, the CDA protocols support in-network data aggregation at intermediate nodes. Privacy homomorphism, introduced by Rivest et al. [64], enables the processing of encrypted data without decrypting them at intermediate nodes. Therefore, encrypted data processing help in protecting the privacy of sensor readings at (compromised) intermediate nodes. In addition, encrypted data processing not only reduces the security vulnerabilities but also reduces the extra computation overhead associated with the decryption and re-encryption of sensor readings.

Although privacy homomorphism protects sensor readings against passive adversaries, it makes them susceptible to active adversaries. Privacy homomorphism, used for protecting the privacy of sensor readings, is inherently malleable [65, 66]. Active adversaries can use the malleability property of privacy homomorphism for modifying or injecting malicious data in the network. Hence, the need to preserve the integrity of sensor readings and the need to ensure the freshness of sensor readings become imperative. The conventional security mechanisms assume that encrypted data are not supposed to be altered en route. However, in data-centric networks, the data are expected to be altered at intermediate nodes. Therefore, existing security mechanisms used for protecting the integrity of data are not viable in data-centric networks [59]. In addition, data freshness becomes another vital security objective for the CDA protocols. Data freshness has an immense impact on the accuracy of collected sensor readings. The conventional security mechanisms used to ensure the end-to-end data freshness are not viable in data-centric networks where the data are aggregated en route. In addition, the omnipresent threat of node capture attacks makes data freshness a vital security objective.

The comprehensive taxonomy of secure in-network data aggregation in WSNs is presented in Fig. 1. As shown in Fig. 1, there exist survey papers that discuss an overview of WSNs [3, 5], in-network data aggregation in WSNs [13, 14], and security issues in WSNs [19, 21]. In addition, there exist a few survey papers [24, 26, 27, 31, 47] that analyze secure data aggregation protocols in WSNs. Alzaid et al. [26] present a comprehensive survey of the hop-by-hop secure data aggregation protocols in WSNs. The surveys presented by Sang et al. [24] and Ozdemir et al. [27] analyze the hop-by-hop and end-to-end secure data aggregation protocols of WSNs. In addition, Mykletun et al. [31] and Peter et al. [47] provide a comprehensive analysis of asymmetric-key based privacy homomorphism techniques in WSNs. However, these surveys only consider homomorphic encryption techniques used for privacy protection in concealed data aggregation protocols. Therefore, there is a need to survey the state-of-the-art privacy preserving concealed data aggregation protocols along with the integrity and freshness preserving concealed data aggregation protocols of WSNs. As per our knowledge, this is the first survey that exclusively explores the state-of-the-art concealed data aggregation protocols in WSNs.

In this article, we investigate the impact of in-network data aggregation on vital security objectives such as confidentiality, privacy, integrity (message authentication), and freshness. We explore privacy homomorphism [64] and its variants such as homomorphic encryption [30, 42, 66–73], homomorphic hash functions [74, 75], homomorphic message authentication codes (MACs) [76, 77], and homomorphic digital signatures [78, 79]. We classify the CDA protocols based on their homomorphic features and provide an in-depth analysis of their strengths and weaknesses. We comparatively evaluate the performance of secure data aggregation protocols based on their respective security features.

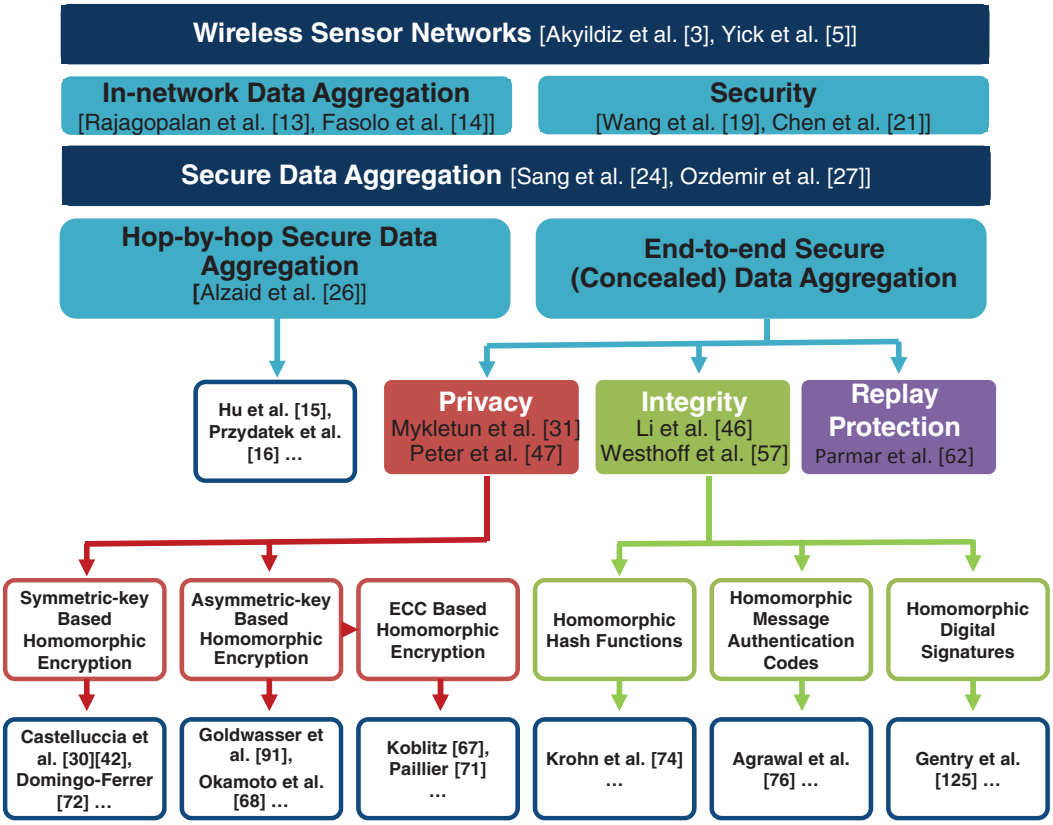

Fig. 1. The Taxonomy of Secure In-network Data Aggregation in Wireless Sensor Networks

The security strengths of the CDA protocols have been analyzed to recommend the security protocols that suits the requirements of sensor networks' applications. To the best of our knowledge, this is the first survey that exclusively explores the CDA protocols in WSNs. In addition, we recommend open research issues and future research directions to help in understanding the unique security challenges of data-centric networks along with the challenges that are imposed by constrained resources.

The organization of the rest of this article is as follows. Section 2 discusses in-network data aggregation and its impact on WSNs. In Section 3, we presents the security issues in WSNs. In addition, we present the impact of in-network data aggregation on the well-known security requirements. Section 4 explores different secure data aggregation protocols, namely, hop-by-hop secure data aggregation protocols and end-to-end secure data aggregation protocols. Section 5 describes the privacy homomorphism and its variants used for achieving different security objectives. In Section 6, we discuss the state-of-the-art CDA protocols that aimed at achieving the privacy of sensor readings. In Section 7, we discuss the state-of-the-art CDA protocols that incorporate integrity protection and replay protection along with the privacy protection at intermediate nodes. We comparatively evaluate the security strength of the CDA protocols in Section 8. In Section 9, we discuss the open research issues and provide future research directions. Section 10 concludes the article by emphasizing our contributions.

2. In-network data aggregation

Perrig et al. [80] implemented the RC5 cryptosystem and CBC MAC algorithm for analyzing the energy consumption incurred by computation and communication operations. As shown in Fig. 2, transmission of sensor readings is one of the most energy consuming operations in WSNs. The energy consumed by the CPU instructions is negligible compared to the energy consumed by the RF

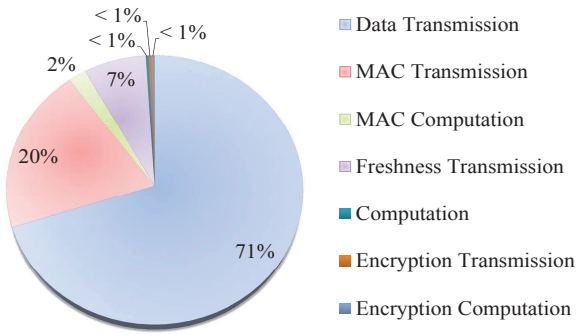

Fig. 2. Energy Consumptions in Wireless Sensor Networks [80]

operations. Therefore, in-network data aggregation have been employed to reduce the redundant communication traffic and to conserve the limited bandwidth and energy [11–13].

Fasolo et al. [14] define in-network data aggregation as, "the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime." As shown in Fig. 3 (A), the communication overhead increases when the data packets move upward in the hierarchy. The transmission of redundant sensor readings can impose an enormous communication overhead on the sensor nodes close to the base station. As shown in Fig. 3 (A), the convergecast communication creates an energy imbalance among nodes at different levels in the hierarchy. Due to energy imbalance, nodes closer to the base station have a shorter lifespan compared to the leaf nodes. However, as shown in Fig. 3 (B), if the data are aggregated en route, the communication traffic at intermediate (aggregator) nodes reduces drastically.

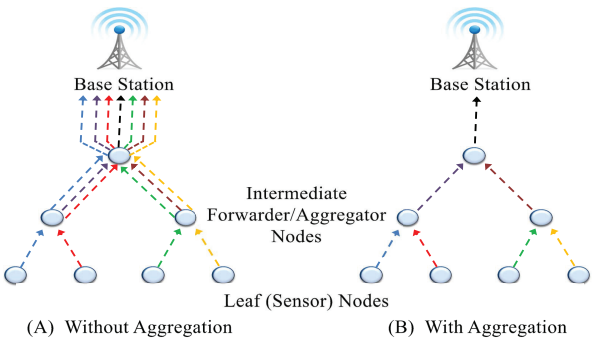

Fig. 3. Comparison of Communication Overhead

In-network data aggregation involves three vital ingredients, viz., routing protocols, aggregation functions, and data representation techniques [14]. Based on routing protocols, in-network data aggregation can be classified as follows: (1) tree based data aggregation [81, 82] (2) cluster-based data aggregation [83, 84] (3) hybrid data aggregation [85]. In addition to in-network data aggregation, there exist many in-network processing techniques, such as data fusion, data elimination, data filtering, and data compression, that reduces the communication overhead. However, the focus of this article is exclusively on in-network data aggregation.

2.1. Impact of in-network data aggregation on WSNs

Although in-network data aggregation helps in reducing the communication overhead, it adversely affects other performance metrics such as latency, accuracy, and security [86]. In this section, we discuss the impact of in-network data aggregation on vital performance metrics. In addition, the impact of in-network data aggregation on the essential security requirements will be discussed in Section 3.2.

2.1.1. Network lifetime

In-network data aggregation has a direct impact on the scarce resources, such as bandwidth and energy, of resource-constrained WSNs. Amongst these resources, the scarce energy has a direct impact on the lifespan of WSNs. Energy requirements of different sensor nodes at different levels in the hierarchy are different. The nodes closer to the base station have to forward far more data packets as compared to the leaf nodes. Hence, the objective of in-network data aggregation is to reduce the redundant communication traffic and to balance the energy expenditure among sensor nodes. The reduction in communication overhead can improve the energy efficiency and prolong the WSNs lifetime.

2.1.2. Latency

The latency can be measured as a time delay between the generation of sensor readings at leaf nodes and the reception of sensor readings at the base station [13]. In-network data aggregation increases the end-to-end latency. Therefore, it may not be a viable solution for the real-time systems that require the timely delivery of data packets. In addition, intermediate nodes that perform in-network data aggregation have to wait for a spe-

cific amount of time before the aggregation operation. The waiting time ensures that the packets forwarded by the child nodes can reach the intermediate nodes within that period. The reduction in waiting time increases the chances of an inaccurate aggregation due to non-availability of vital data packets while the longer waiting time increases the latency. Therefore, the trade-off is not only between the latency and network lifetime but also between the latency and accuracy.

2.1.3. Accuracy

Accuracy can be measured in terms of the difference between the result calculated using the original sensor readings and the result received/calculated by the base station. The variations in the results occur due to various factors such as aggregation functions, the wait time for performing data aggregation, and malicious adversaries. In-network processing techniques, such as lossy data compression, data aggregation, and data fusion, have a direct impact on the accuracy. In addition, different aggregation functions and compression techniques can also affect the accuracy of the result received by the base station.

3. Security in WSNs

Deployments in hostile and unattended environments, unreliable communication medium, and lack of tamper-resistant hardware make security a crucial design parameter for WSNs' protocols. However, the resource-constrained nature of sensor devices and the lack of physical security pose unique security challenges compared to the one found in conventional networks. As WSNs have some commonalities with conventional networks, such as wireless networks, the security requirements of WSNs remain similar to those found in conventional networks, such as confidentiality, integrity, freshness, etc. [6, 80]. However, the security requirements of WSNs have been affected by the in-network data aggregation [11, 14] and encrypted data processing [64]. In this section, we discuss an adversary model and the impact of in-network data aggregation on vital security primitives of WSNs.

3.1. Adversary Model

Sensor devices, such as the MICA2 mote [87], the MICAz mote [8], and the TelosB mote [9], are not equipped with tamper-resistant hardware. In addition, the deployment of sensor devices are not always in the physically secure locations. Hence, it is assumed that few sensor nodes may get compromised and leak the keys and data stored withing those nodes. In addition, cryptographic algorithms are publicly available, and the security should be dependent only on the secrecy of cryptographic keys.

In WSNs, there exist two types of nodes; the base station and the sensor nodes. The base station is assumed to be a trustworthy and resource-rich device. However, sensor devices are assumed to be resource-constrained devices. The adversaries in WSNs are classified as follows:

3.1.1. Insider versus Outsider Adversaries

An insider adversary is a captured node that remains a part of the attacked network [88]. An insider adversary can access the secret information stored within the compromised sensor node. While an outsider adversary is an entity that does not have access to the secret information stored within the sensor nodes. The outsider adversary analyzes the communication traffic to extract the secret information stored within the sensor nodes. In WSNs, an insider adversary is significantly powerful as compared to the outsider adversary.

3.1.2. Passive versus Active adversaries

The goal of a passive adversary is to analyze the communication traffic for extracting the meaningful information. The analysis may involve the data as well as the traffic patterns. While the goal of an active adversary is to create, modify, or inject malicious data packets in the network. An active adversary violates the integrity and freshness of sensor readings while a passive adversary violates the confidentiality and privacy of sensor readings (data, location, time, etc.).

3.1.3. Mote-class versus Laptop-class adversaries

The mote-class adversary possesses the sensor devices similar to the one found in the attacked network. The resource limitations of sensor devices affect the adversaries' capabilities to breach security. However, a laptop-class adversary is a powerful device (e.g., a laptop), and it is assumed to be much stronger than the devices used in the attacked network. A mote-class adversary is bounded by the energy limitations while a laptop-class adversary has unlimited energy supply.

3.2. Impact of in-network data aggregation on security requirements

Although in-network data aggregation reduces the communication overhead, it increases the security vulnerabilities. As sensor nodes are not equipped with tamper-resistant hardware, intermediate nodes that collect the sensor readings for further processing become a prime target for adversaries. In this section, we discuss the impact of in-network data aggregation on different security requirements.

3.2.1. Confidentiality and Privacy

Symmetric-key, asymmetric-key, and elliptic curve cryptography based encryption algorithms have been widely adopted for protecting the confidentiality of sensor readings during communication. However, data-centric networks, such as WSNs, require algorithms that ensure the confidentiality not only during communication but also at intermediate nodes where the sensor readings are processed. It is often being referred to as privacy of sensor readings at intermediate nodes. Moreover, the need to process the sensor readings at intermediate nodes and the need to ensure the privacy of sensor readings at intermediate nodes cannot be realized simultaneously using conventional encryption algorithms. Privacy homomorphism can provide the encrypted data processing, where data once encrypted can only be decrypted at the base station. However, intermediate nodes can process the data in order to reduce the communication overhead.

3.2.2. Message authentication/integrity

Although privacy homomorphism protects against passive adversaries, it increases vulnerabilities against active adversaries. The algorithms that support privacy homomorphism are inherently malleable. They allow not only intermediate nodes but also adversaries to manipulate encrypted sensor readings using public parameters. In addition, due to in-network data aggregation, identification of the malicious intermediate nodes becomes difficult. Although, conventional authentication mechanisms provide hop-by-hop message authentication, they are not viable in data-centric networks. In data-centric networks, data need to be verified at intermediate nodes as well as at the base station. The requirement of hop-by-hop, as well as end-to-end integrity verification, makes integrity preservation in WSNs a formidable challenge.

3.2.3. Data freshness

Data freshness is considered as an indispensable design characteristic for WSNs. Although the nonce and counter based mechanisms provide the replay protection against outsider adversaries, they are insufficient to provide the replay protection when there exist malicious insider nodes. In data-centric networks, data freshness needs to be protected from the insider, as well as outsider adversaries. In addition, encrypted data processing increases the challenges in verifying the data freshness at intermediate nodes. Due to encrypted data processing, compromised intermediate nodes can successfully aggregate any number of replayed (reused) packets without being detected. Hence, the need to ensure the accuracy of gathered information makes data freshness an imperative security objective.

4. Secure data aggregation

Security becomes an indispensable design issue for many WSNs protocols. In order to provide security in WSNs, one needs to consider the impact of security on the limited resources such as energy, memory, bandwidth, and processor [17–20]. Security attributes not only introduce significant computation overhead, but they also introduce enormous communication overhead. As shown in Fig. 2, transmission of security attributes consumes far more energy than energy consumed during the computation of security attributes. Although in-network data aggregation helps in reducing the redundant data traffic, it exacerbates security challenges. The conventional end-to-end security framework is no longer suitable due to en route aggregation of data packets. In addition, in-network data aggregation and security have conflicting requirements. The objective of in-network data aggregation is to reduce the communication overhead while the security attributes increase the communication overhead. Hence, the necessity to incorporate security and data aggregation together initiated research in secure data aggregation [24, 27]. Secure data aggregation protocols are categorized as either hop-by-hop secure data aggregation protocols or end-to-end secure data aggregation protocols [24, 27]. Hop-by-hop secure data aggregation protocols provide security in a hop-by-hop manner [15, 16, 26]. They assume that intermediate nodes are trustworthy. Hence, intermediate nodes can decrypt the encrypted sensor readings

and process the raw sensor readings before forwarding the result toward the base station.

Hu et al. [15] explore the feasibility of achieving hop-by-hop secure data aggregation in WSNs. Their solution involves delayed aggregation and delayed authentication. It uses a μTESLA protocol [80] for delayed authentication. Instead of relying on the costly cryptographic asymmetry (public and private keys), it uses the time asymmetry for providing authentication using symmetric keys. Przydatek et al. [16] use a random sampling and interactive proofs for verifying the correctness of aggregated sensor readings. Wagner [22] describes various attacks on data aggregation scenarios. In addition, author presents a mathematical way to quantify the robustness of an en route aggregation against malicious adversaries. One of the indispensable characteristics of the protocols mentioned above is hop-by-hop security.

Although Hu et al. [15], Przydatek et al. [16], and Wagner [22] provide secure data aggregation, they achieve only hop-by-hop security. Sang et al. [24], Alzaid et al. [26], and Ozdemir et al. [27] surveyed hop-by-hop secure data aggregation protocols and comparatively evaluated their performance. One of the key challenges with hop-by-hop security is the compromised intermediate nodes. If sensor network has compromised intermediate nodes, hop-by-hop security protocols cannot protect against malicious insider adversaries. Intermediate nodes consume a higher amount of energy as compared to the leaf sensor nodes, as they receive and process more data packets compared to individual sensor nodes. The decryption of encrypted sensor readings, processing of sensor readings, and re-encryption of processed sensor readings introduce latency. The delay introduced by the aggregator nodes affects the performance of the network that requires real-time data for analysis. One of the solutions that handle these issues (e.g., privacy at intermediate nodes, latency) is end-to-end secure data aggregation.

As opposed to the hop-by-hop secure data aggregation protocols, end-to-end secure data aggregation protocols provide end-to-end security using encrypted data processing at intermediate nodes [28, 89]. Wu et al. [89] introduce encrypted data processing in WSNs. In encrypted data processing, data encrypted at leaf nodes can be processed at intermediate nodes without the need for decryption. The protocol tackles the threat of insider adversaries by introducing encrypted data classification while supporting in-network data aggregation. The protocol ensures the classification of encrypted data at intermediate nodes without the need for decryption. The classifier matches the incoming encrypted message with a set of keywords and takes the appropriate decisions such as forwarding the message without aggregation, forwarding the message after aggregation, and dropping the duplicate messages. Such classifier helps in setting the threshold for processing only selected data, and hence, it reduces the computation and computation overhead. Here, the classifiers can only access the encrypted sensor readings and encrypted keywords. Hence, they cannot learn any information about the original sensor readings.

Girao et al. [28, 29] extend the idea of encrypted data processing to incorporate encrypted data aggregation. It supports the aggregation of encrypted data at intermediate nodes. The end-to-end secure (concealed) data aggregation ensures the privacy of sensor readings at intermediate nodes. The compromised intermediate nodes cannot view the raw sensor readings, as the sensor readings remain encrypted until they reach the base station. Hence, the data privacy remains unharmed. We will continue the discussion of end-to-end secure data aggregation in the upcoming sections.

5. Privacy homomorphism

The notion of "Privacy Homomorphism" was first introduced by Rivest et al. [64] for processing encrypted data. Privacy homomorphism can compute the function over encrypted data in the same way as it has been computed over unencrypted data. Formally, privacy homomorphism can be defined as follows:

Given an encryption of x, $\mathcal{E}(x)$, and an encryption of y, $\mathcal{E}(y)$, a function $\mathcal{F}$ can efficiently compute $\mathcal{E}_{\mathcal{K}}(x) \oplus \mathcal{E}_{\mathcal{K}}(y) = \mathcal{E}_{\mathcal{K}}(x \oplus y)$ such that the decryption $\mathcal{D}_{\mathcal{K}'}(\mathcal{E}(x \oplus y))$ yields the same result as computed by $x \oplus y$.

Any cryptosystem that supports privacy homomorphism either uses the same operator, $\oplus$, or uses different operators, $\oplus$ and $\otimes$. As shown in Eq.(1), Domingo-Ferrer's cryptosystem [72] uses the same operator $\oplus$ for processing encrypted data as well as for processing plain data. However, as shown in Eq.(2), Paillier's cryptosystem [70] uses different operators, $\oplus$ and $\otimes$, for processing encrypted data and for processing plain data. In addition, as shown in Eq.(1), symmetric-key cryptosystems use

the same key for performing encryption and decryption. However, as depicted in Eq.(2), asymmetric-key cryptosystems use different keys for encryption and decryption.

$$\mathcal{D}_{\mathcal{K}}(\mathcal{E}_k(x) + \mathcal{E}_{\mathcal{K}}(y)) \bmod n = x + y \bmod n \quad (1)$$

$$\mathcal{D}_{\mathcal{K}'}(\mathcal{E}_k(x) \times \mathcal{E}_k(y)) \bmod n = x + y \bmod n \quad (2)$$

Cryptosystems that support privacy homomorphism can perform either additive homomorphic operations or multiplicative homomorphic operations over encrypted data. Cryptosystems, such as the RSA cryptosystem [90] and the ElGamal cryptosystem [91], can support multiplicative privacy homomorphism. However, the majority of WSNs applications require to compute functions, such as sum, average, minimum, maximum, and movement detection, that can only be supported by the additive privacy homomorphism. Hence, in this article, we present the additive privacy homomorphism techniques that are adopted in WSNs. Cryptosystems that support additive privacy homomorphism can be categorized as either symmetric-key based privacy homomorphism [30, 43, 72] or asymmetric-key based privacy homomorphism [68–70, 92]. In addition, asymmetric-key based privacy homomorphism can further include elliptic curve cryptography based privacy homomorphism [67, 71, 73].

Privacy homomorphism, popularly known as homomorphic encryption, can support various other homomorphic primitives such as homomorphic hash functions [74, 75], homomorphic MACs [76, 77], and homomorphic digital signatures [78, 79]. Although privacy homomorphism can be advantageous in different circumstances, it is often being considered as an undesirable property. Cryptosystems that support privacy homomorphism are inherently malleable [65]. The property that helps in processing the encrypted data makes cryptosystems vulnerable against adaptive chosen-ciphertext attacks (CCA2) [93]. Therefore, cryptosystems that support privacy homomorphism can best be secure against non-adaptive chosen ciphertext attacks (CCA1). More discussion on the malleability property of privacy homomorphism and its impact on the CDA protocols will be discussed in Section 7.

6. Privacy protection with in-network data aggregation

Privacy in WSNs is categorized as either content-oriented privacy or context-oriented privacy [94, 95]. The goal of content-oriented privacy preservation is to ensure that the contents of packets are observable or decipherable only by intentionally authorized entities. While the goal of context-oriented privacy preservation is to ensure the protection of contextual information related to the sensed information such as location and time. In this article, we explore content-oriented privacy preservation techniques that ensure data privacy. The context-oriented privacy is not within the scope of this article. Henceforth, we use the term privacy to refer the data privacy.

In this section, we discuss the privacy preservation techniques used in WSNs. They are categorized as follows: (1) Symmetric-key based privacy homomorphism (2) Asymmetric-key based privacy homomorphism (3) Elliptic curve cryptography based privacy homomorphism.

6.1. Symmetric-key based privacy homomorphism

The use of symmetric-key cryptography has two indispensable advantages over asymmetric-key cryptography. First, symmetric-key based cryptosystems [42, 43, 72, 96] have a negligible message expansion. In symmetric-key based cryptosystems, ciphertext requires nearly the same number of bits as required by the plaintext. As communication in WSNs consumes far more energy compared to the computation [10, 97], the negligible message expansion not only saves bandwidth and energy but also increases the lifespan of WSNs. Second, the computation cost required to perform symmetric-key based operations is significantly less compared to the computation cost required by asymmetric-key based operations [15, 80]. Hence, symmetric-key based cryptosystems are preferable for resource-constrained devices due to their fewer communication and computation overhead. Although there have been numerous cryptosystems that support privacy homomorphism [66], very few of them are based on symmetric-key cryptography. In this section, we will discuss symmetric-key based privacy homomorphism techniques [30, 36, 72] used by the end-to-end secure data aggregation protocols.

6.1.1. Domingo-Ferrer's cryptosystem

Domingo-Ferrer's cryptosystem [72] is the first cryptosystem that supports full arithmetic operations (e.g., addition, subtraction, multiplication, and division) on encrypted data. It supports encrypted data processing if the data are encrypted

using the same secret key. Domingo-Ferrer's cryptosystem remains secure against known-plaintext attacks.

Domingo-Ferrer's Cryptosystem [72]

Public Parameters $\mathcal{P}$:

1. Select $d > 2$ and a large integer n

Secret Parameters: $\mathcal{S}$:

1. Select $n' > 1$ where $n' \mid n$;
2. Select a random integer r such that $r^{-1} \bmod n \in \mathbb{Z}_n$

Encryption $\mathcal{E}$:

1. Randomly split a plaintext $m \in \mathbb{Z}_{n'}$ such that $m = \sum_{j=1}^{d} m_j \bmod n'$ and each $m_j \in \mathbb{Z}_n$
2. Compute a ciphertext $c = \mathcal{E}(m) = (m_1 r \bmod n, \quad m_2 r^2 \bmod n, \quad \cdots, m_d r^d \bmod n)$

Ciphertexts Aggregation $\mathcal{A}$:

1. Given $c_1 = \mathcal{E}(m_1)$ and $c_2 = \mathcal{E}(m_2)$
2. Compute an aggregated ciphertext, $c = c_1 + c_2 \bmod n = \mathcal{E}(m_1 + m_2) \bmod n$

Decryption $\mathcal{D}$:

1. Compute the scalar product of the j^{th} coordinate of a ciphertext by $r^{-j} \bmod n$
2. $\mathcal{D}(c) = (m_1 r * r^{-1} \bmod n, \quad m_2 r^2 * r^{-2} \bmod n, \quad \cdots, \quad m_d r^d * r^{-d} \bmod n) = (m_1 \bmod n, m_2 \bmod n, \cdots, m_d \bmod n)$
3. Compute $\sum_{j=1}^{d} m_j \bmod n' = m$

Girao et al. [28, 29] investigated the need for privacy preservation at intermediate (aggregator) nodes and coined the term "concealed data aggregation (CDA)" to refer the encrypted data processing of reverse multicast traffic in WSNs. Girao et al. [28, 29] use the Domingo-Ferrer's cryptosystem [72] for computing over encrypted data at intermediate nodes. In their protocol, data encrypted at leaf sensor nodes are processed at intermediate nodes but decrypted only at the base station. They compared their end-to-end secure data aggregation protocol with hop-by-hop secure data aggregation protocol that uses RC5 cryptosystem [96] as an underlying encryption algorithm. However, their proposed protocol has a few limitations. They are as follows: (1) Domingo-Ferrer's privacy homomorphism [72] processes encrypted data only if the key used to encrypt the data remains the same. If sensor readings are encrypted with different keys, Domingo-Ferrer's privacy homomorphism cannot aggregate encrypted sensor readings. Moreover, if the same key is used for encryption across all nodes, it increases security vulnerabilities. A shared secret key used for performing encryption (as well as decryption) cannot help in preserving privacy at compromised sensor nodes. In addition, the use of a shared secret key across all nodes increases threats against the integrity of sensor readings. Any compromised node can use the shared secret key for decryption of sensor readings as well as for injecting malicious data into the networks. (2) Although Domingo-Ferrer's privacy homomorphism is a symmetric key based technique, it has significant message expansion. The message expansion in Domingo-Ferrer's privacy homomorphism is dependent on a public parameter, d. (3) Domingo-Ferrer's privacy homomorphism is insecure for some parameter settings [98]. Wagner [98] shows that if the factorization of n' is hard and $n < d$, Domingo-Ferrer's cryptosystem may remain secure. However, the restrictive parameter setting vastly affects the performance. Moreover, vulnerabilities against well-known cryptanalytic attacks [99] reduce the viability of Domingo-Ferrer's cryptosystem in real-world application scenarios. (4) The power consumption of Domingo-Ferrer's cryptosystem is considerably higher compared to the power consumption of RC5 cryptosystem. Authors claim that the use of Domingo-Ferrer's cryptosystem increases the overhead up to 22% compared to RC5 cryptosystem. Nevertheless, the additional overhead introduced at leaf nodes are compensated during the aggregation phase. In addition, the results show that end-to-end secure data aggregation balances the energy consumption across all nodes, unlike hop-by-hop secure data aggregation where the nodes nearer to the base station have to transmit more data packets compared to the nodes nearer to leaf nodes.

Westhoff et al. [32] improved their earlier work [28, 29] and incorporated a key pre-distribution scheme for reverse multicast traffic in WSNs. Authors comparatively evaluate their proposed protocol with a hop-by-hop security architecture of resource-constrained WSNs, namely, TinySec [100]. Although Domingo-Ferrer's [72] privacy homomorphism consumes more energy during CPU operations when compared to RC5 cryptosystem[96], it

helps in balancing the energy usage across all sensor nodes. In addition, the additive privacy homomorphism supported by Domingo-Ferrer's cryptosystem helps in achieving end-to-end security and energy efficiency in the real world application scenarios.

The need for a globally shared secret key, a significant message expansion, and a threat of cryptanalysis demanded the search for an efficient cryptosystem that can support encrypted data processing without having these limitations. One of the solutions that overcome these limitations is CMT cryptosystem [30, 42].

6.1.2. CMT cryptosystem

Castelluccia et al. [30, 42] proposed an efficient and provably secure additive aggregation scheme (CMT cryptosystem) for reverse multicast traffic in WSNs. They adapted the well-known Vernam cipher [101], also known as the one-time-pad, for the aggregation of plaintexts in a ciphertext domain. CMT cryptosystem introduces two simple but significant modifications in the original Vernam cipher. (1) CMT cryptosystem uses an addition operation instead of an exclusive-OR (X-OR) operation. (2) CMT cryptosystem uses a pseudo-random function [102] for generating the keys, instead of a random selection from the key space. Although a pseudo-random function makes CMT cryptosystem a viable alternative for real-world application scenarios, it reduces its security level. The original Vernam cipher is secure in an information-theoretic setting while CMT cryptosystem is secure in a computational-complexity theoretic setting. CMT cryptosystem provides the same level of privacy preservation as provided by the conventional end-to-end encryption (without aggregation) based approaches. In addition, CMT cryptosystem achieves the significant bandwidth gain compared to the no aggregation scenarios. However, as shown in Castelluccia et al. [42], CMT cryptosystem requires more bandwidth compared to the hop-by-hop secure data aggregation scenarios. Nevertheless, the higher bandwidth is compensated by much stronger level of security at intermediate nodes. CMT cryptosystem also helps in balancing the communication load evenly across all sensor nodes. The load balancing across WSNs eventually increases the network lifetime.

Peter et al. [36] suggested a way to combine Domingo-Ferrer's cryptosystem [72] and CMT cryptosystem [30] for increasing the overall security strength. As shown by Peter et al. [36], a simple additive aggregation approach makes CMT cryptosystem vulnerable to malleability issues. In CMT cryptosystem, an adversary can add any integer in the ciphertext without knowing the key or the plaintext. Peter et al. combine CMT cryptosystem with the Domingo-Ferrer's cryptosystem for reducing the malleability issues. The limitation with Peter et al.'s cryptosystem is that it not only combines the strengths of both the cryptosystem, but also combines the weaknesses of both the cryptosystems. In addition, Peter et al. discuss a need for the homomorphic MACs in the CDA. The working construction of the homomorphic MACs was later introduced by Agrawal et al. [76] for network coded systems.

CMT Cryptosystem [30, 42]

Key Generation $\mathcal{K}$:

1. Randomly select a decryption key $K \in \{0,1\}^{\lambda}$ for the base station.
2. Compute an encryption key of each node $i \in [1, 2, \cdots n]$ as, $k_i = \mathcal{F}_k(i)$. Here, $\mathcal{F}$ is a pseudo-random function (PRF) and $\sum_{i=1}^{n} k_i = K$.

Encryption $\mathcal{E}$:

1. Given an encryption key k_i, a nonce r, a modulus M, and a plaintext $m \in [0, M-1]$.
2. Compute a ciphertext at node i, $c = \mathcal{E}_{k_i}(m) = m + \mathcal{F}_{k_i}(r) \ \texttt{mod} \ M$.
3. Set the identity information (ID) of a node i as, $hdr_i = \{i\}$.
4. Forward an ID-ciphertext pair, (hdr_i, c).

Ciphertexts Aggregation $\mathcal{A}$:

1. Given $(hdr_1, c_1 = \mathcal{E}_{k_1}(m_1))$ and $(hdr_2, c_2 = \mathcal{E}_{k_2}(m_2))$.
2. Compute an aggregated ciphertext, $c = c_1 + c_2 \ \texttt{mod} \ M = \mathcal{E}_k(m_1 + m_2) \ \texttt{where} \ k = k_1 + k_2 \ \texttt{mod} \ M$.
3. Set $hdr = hdr_1 \cup hdr_2$.

Decryption $\mathcal{D}$:

1. Given an ID-ciphertext pair, (hdr, c) and a nonce r, generate $k_i = \mathcal{F}_k(i), \forall i \in hdr$.
2. Decrypt the ciphertext, $\mathcal{D}_k(c) = c - \sum_{i \in hdr} \mathcal{F}_{k_i}(r) \ \texttt{mod} \ M$.

In CMT cryptosystem, nodes' identity related information needs to be transmitted for performing the decryption at the base station. However, transmission of identity related information introduces significant communication overhead. Armknecht et al. [39] proposed an end-to-end secure data aggregation protocol using a symmetric-key cryptosystem. In the proposed cryptosystem, an encryption function is "bi-homomorphic" and provides a homomorphic transformation for data as well as the keys. One of the advantages of the proposed protocol compared to CMT cryptosystem is that it mitigates the requirement of nodes' identity transfer to the base station. Instead of transferring nodes' identity related information, the protocol uses dummy values, stored at each intermediate node, for representing the encryption of the child nodes. Hence, each intermediate node aggregates the dummy values of the nodes that do not respond to the base station's query. The protocol uses a counter to obtain the number of dummy values aggregated during the aggregation process. The dummy values are removed from the aggregated result at the base station.

Onen et al. [103] enhance the secure data aggregation using a layer-wise security mechanism and a key-attribution algorithm. The proposed protocol reduces the impact of well-known security threats such as node compromise attacks. The protocol combines the homomorphic encryption [104] with the multiple encryption mechanism. The homomorphic encryption function [104] used by the protocol is similar to the one found in Castelluccia et al. [30, 42] and a modified version of the Vernam cipher [101]. In addition, a key attribution algorithm is used to share a pair-wise key between the node and its m^{th} hop parent node. The pair-wise keys are used to add and suppress the encryption layers to/from the aggregated data while forwarding data towards the base station. A key pre-distribution mechanism, a re-keying requirement (due to exhausted parent nodes), a fixed network topology, and the reduced security are major limitations of Onen et al.'s protocol.

Di Pietro et al. [44] used CMT cryptosystem [42] for privacy protection in WSNs. Authors adapt a concept of delay aggregation and peer monitoring for integrity protection in WSNs. One of the features introduced by Di Pietro et al. is the ability to solve an identity management issue of CMT cryptosystem. In CMT cryptosystem, the secret key(s) is shared between the node(s) and the base station. However in Di Pietro et al.'s protocol, the secret key(s) is also shared with the neighboring nodes. The proposed key sharing with neighboring nodes helps in mitigating the effect of node compromise attacks and node failures. The aggregator nodes can use the information provided by their neighboring nodes during a node compromise attack or a node failure. Information provided by the neighboring nodes helps in preventing the identity transfer of the responding/non-responding nodes. One of the weaknesses of the proposed key sharing approach is that a compromised node can reveal not only its secret key but also helps in recovering the secret keys of the neighboring nodes. The key chains recovered from a large neighborhood can have a disastrous impact on the performance of WSNs.

Papadopoulos et al. [53] proposed a solution called SIES (Secure In-network processing of Exact SUM queries) to preserve privacy, integrity, authentication, and freshness of sensor readings using homomorphic encryption and secret sharing. They used a homomorphic encryption algorithm similar to the CMT cryptosystem for en route privacy protection.

Rafik et al. [58] proposed a security protocol that addresses end-to-end privacy and end-to-end integrity of the reverse multicast traffic in WSNs. Their protocol uses CMT cryptosystem and stateful public-key encryption [105]. Stateful public-key encryption can significantly reduce the computation cost associated with the public-key encryption algorithms. In stateful public-key encryption, the sender keeps track of the state information and re-uses this information across different encryptions. Stateful public-key encryption helps in periodically refreshing sensor nodes' keys required by CMT cryptosystem.

6.1.3. Summary of symmetric-key based cryptosystems

Girao et al. [28, 29], Westhoff et al. [32], Ren et al. [37], and Peter et al. [36] used the Domingo-Ferrer's privacy homomorphism [72] while Peter et al. [36], Rafik et al. [58], Papadopoulos et al. [53], and Di Pietro et al. [44] used CMT cryptosystem [30, 42] for privacy preservation at intermediate nodes in WSNs. In Table 1, we present symmetric-key based privacy homomorphism techniques with their strength and weaknesses.

Chan [43] proposed two different additive homomorphic encryption schemes, namely, an iterated Hill cipher and a modified Rivest scheme [64].

Table 1. Comparison of Symmetric-key Based Homomorphic Cryptosystems

Cryptosystem	Key Management	Homomorphic Operation(s)	Message Expansion
Castelluccia [30]	Each node shares a unique secret key with the base station.	$\oplus$ $\ominus$ $\otimes_c$	1
Domingo-Ferrer [72]	A global secret key is shared among sensor nodes and the base station.	$\oplus$ $\ominus$ $\otimes$ $\otimes_c$	$\frac{d \cdot n}{n'}$
Peter [36]	Each node possesses a secret key local to the node and a global secret key shared across sensor nodes (in the network).	$\oplus$ $\ominus$ $\otimes_c$	$\frac{d \cdot n}{n'}$

$\oplus$ - Homomorphic addition of ciphertexts
$\ominus$ - Homomorphic subtraction of ciphertexts
$\otimes$ - Homomorphic multiplication of ciphertexts
$\otimes_c$ - Homomorphic multiplication with a known constant
n - A randomly chosen large integer
n' - A randomly chosen $n' > 1$ such that $n' \mid n$
d - A plaintext is divided into $d > 2$ sub-parts

These schemes support additive and multiplicative homomorphism. The proposed schemes can provide security against ciphertext-only attacks. In addition, these schemes support the randomize zero encryption. Hence, an encryption of zero, $\mathcal{E}(0)$, can have several different representations in ciphertext domain, but all these representations can result in zero after decryption. The implementation of these schemes on sensor platforms, such as the TelosB mote [9] and the MICAz mote [8], and comparison with other symmetric-key based cryptosystems [30, 72] can further help to understand the viability of these schemes in WSNs. Zhou et al. [60] adopted a symmetric-key based encryption scheme of Chan [43] for privacy preservation in WSNs. They have combined homomorphic primitives, namely, homomorphic encryption and homomorphic MAC [76], for ensuring privacy and integrity of sensor readings.

6.2. Asymmetric-key based privacy homomorphism

Asymmetric-key based cryptosystems were initially considered as an expensive alternative for resource-constrained networks such as WSNs [15, 80]. However, Gura et al. [106], Wander et al. [107], and Malan et al. [108], implemented asymmetric-key based solutions, including those based on elliptic curve cryptography, on 8-bit micro-controllers used by sensor nodes [8, 9]. The performance results presented by them indicate that asymmetric-key cryptography is viable for resource-constrained devices even if implemented using software-based techniques. Mykletun et al. [31, 47] comparatively evaluate the viability of asymmetric-key based homomorphic cryptosystems in WSNs. Authors highlighted the desired characteristics of asymmetric-key based cryptosystems for use in the CDA protocols. The desired characteristics of asymmetric-key based cryptosystems for use in CDA are as follows:

- Aggregation - The CDA protocols perform en route data aggregation in a ciphertext domain. An aggregation of plaintexts in a ciphertext domain requires the cryptosystem to have an additive privacy homomorphism property.

- Security - Ciphertext indistinguishability is a common characteristic for the provably secure public-key based cryptosystems. Ciphertext indistinguishability ensures that given a public-key and a pair of plaintexts, any passive adversary cannot distinguish between a corresponding pair of ciphertexts with probability significantly greater than $\frac{1}{2}$.

- Overhead - The security features introduce computation and communication overhead. In asymmetric-key based cryptosystems, the size of a plaintext increases after encryption. Here, the increase in a ciphertext size compared to the plaintext size is commonly referred to as the message expansion. The CDA protocols should minimize the message expansion for preserving the performance gain achieved through data aggregation.

In this section, we discuss asymmetric-key based cryptosystems and their applications in CDA of WSNs.

6.2.1. Goldwasser-Micali's cryptosystem

Goldwasser-Micali's cryptosystem [92] is the first cryptosystem that is provably secure against chosen-plaintext attacks (IND-CPA). Security of the Goldwasser-Micali's cryptosystem is based on assumed intractability of the quadratic residuosity problem. The quadratic residuosity problem considers the hardness of distinguishing quadratic residues from quadratic non-residues modulo a composite number. In their seminal paper [92], Goldwasser et al. formalized the notion of semantic security. Semantic security ensures that the computationally bounded adversary cannot obtain any information about a plaintext given a corresponding ciphertext.

Goldwasser-Micali's cryptosystem supports privacy homomorphism with X-OR operations. During the aggregation phase, ciphertexts are multiplied to produce the X-OR effect on the underlying plaintexts. After decryption, an aggregated ciphertext results in a plaintext that is equal to the X-OR of the original plaintexts. One of the limitations of Goldwasser-Micali's cryptosystem is that it encrypts the data bit-by-bit, and each plaintext bit is converted to a corresponding ciphertext. Therefore, the substantial message expansion reduces its viability for real-world scenarios.

Samanthula et al. [109] employed Goldwasser-Micali's cryptosystem for computing the MIN/MAX functions at aggregator nodes in WSNs. For sensor readings without duplicates, their solution uses the X-OR homomorphic property of the Goldwasser-Micali's cryptosystem for finding the minimum/maximum of sensor readings. In addition, if there exist duplicate sensor readings, authors adopted a variant of the Goldwasser-Micali's cryptosystem, proposed by Sander et al. [110]. Sander et al. modify the Goldwasser-Micali's cryptosystem for incorporating the support for multiplicative homomorphic operations over encrypted data. Samanthula et al. [109] claim that although their proposed approaches introduce heavy computation and communication overhead, they reduce security vulnerabilities of the existing approaches used for MIN/MAX computations [38, 111]. Acharya et al. [111] suggested a way to perform secure comparison of encrypted data in WSNs. The order preserving encryption scheme (OPES) [112] is employed to perform the comparison operations such as minimum and maximum. The OPES preserves the order while transforming a plaintext to the corresponding ciphertext. However, the order preserving encryption leaks valuable information during the comparisons of encrypted data at intermediate nodes. In addition, the OPES

Goldwasser-Micali's Cryptosystem [92]

Key Generation $\mathcal{K}$:

1. Select large primes p and q, where, $p \neq q$
2. Choose a pseudo-square a such that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$
3. Compute, $n = p * q$

Encryption $\mathcal{E}$:

1. A plaintext, $m \in [0, 1]$
2. Choose a random integer r such that $1 < r < n$
3. Compute a ciphertext

$$c = \begin{cases} r^2 \mod n & \text{if } m = 0 \\ ar^2 \mod n & \text{if } m = 1 \end{cases}$$

Ciphertexts Aggregation $\mathcal{A}$:

1. Given $c_1 = \mathcal{E}(m_1)$ and $c_2 = \mathcal{E}(m_2)$
2. Compute an aggregated ciphertext, $c = c_1 * c_2 \mod n = \mathcal{E}(m_1 \oplus m_2)$

Decryption $\mathcal{D}$:

1. Decrypt the ciphertext, $\mathcal{D}(c) = \left(\frac{c}{p}\right) = c^{\frac{(p-1)}{2}} \mod p$

$$\text{A plaintext,} \quad m = \begin{cases} 0 & \text{if } \left(\frac{c}{p}\right) = 1 \\ 1 & \text{if } \left(\frac{c}{p}\right) = -1 \end{cases}$$

remains vulnerable to active insider adversaries (e.g., node capture attack). A compromised node can reverse the transformation using the (disclosed) mapping function and obtain information related to the encrypted sensor readings [38, 111]. In addition, if the domain of sensed values is known, any comparison operation makes privacy homomorphism vulnerable to a wide variety of attacks including elementary cryptanalytic attacks such as the ciphertext-only attack [64].

6.2.2. Okamoto-Uchiyama's cryptosystem

Okamoto et al. [68] proposed a provably secure homomorphic encryption scheme. The additive homomorphism supported by Okamoto-Uchiyama's cryptosystem makes it useful for the CDA protocols of WSNs. The cryptosystem remains semantically secure under the p-subgroup assumption. Security of Okamoto-Uchiyama's cryptosystem depends on the intractability of factoring $n = p^2q$. However, as shown by Okamoto et al. [68], the fastest algorithm for factoring $n = pq$ or $n = p^2q$ is the number field sieve method. In addition, the running time of the number field sieve algorithm is only dependent on the composite size, n. Therefore, the parameters of Okamoto-Uchiyama cryptosystem can be chosen such that the size of $n = p^2q$ remains the same as the size of $n = pq$ of the RSA cryptosystem [90] for sufficiently large n (e.g., 1024-bit [113]).

Mykletun et al. [31] comparatively evaluate the performance of various cryptosystems, including the Okamoto-Uchiyama's cryptosystem [68]. The analysis shows the viability of Okamoto-Uchiyama's cryptosystem for the CDA protocols. In scenarios where elliptic curve ElGamal cryptosystem (EC-ElGamal) [67] is not viable due to its expensive reverse mapping function required for decryption, the second best option is to use Okamoto-Uchiyama's cryptosystem. Okamoto-Uchiyama's cryptosystem remains second due to its larger ciphertext size. The ciphertext size of Okamoto-Uchiyama's cryptosystem is nearly three times larger than the ciphertext size of the EC-ElGamal cryptosystem.

6.2.3. Elliptic curve Paillier's cryptosystems

Paillier [71] introduces three probabilistic cryptosystems based on trapdooring discrete logarithms on elliptic curves over a ring, E_n. They are as follows: (1) elliptic curve Naccache-Stern's cryptosystem ($n = pq$) (2) elliptic curve Okamoto-Uchiyama's cryptosystem ($n = p^2q$) (3) elliptic curve Paillier's cryptosystem ($n = p^2q^2$). The elliptic curve Naccache-Stern's cryptosystem [71] is a variant of the Naccache-Stern's cryptosystem [69] and defined using an elliptic curve over a ring, $E(x, y) \in \mathbb{Z}_n$. Here, n is the product of two distinct primes p and q. The cryptosystem is semantically secure with respect to the intractability of the high-degree residuosity problem. The high-degree residuosity problem extends the properties of quadratic residuosity to prime degrees greater than two.

The second cryptosystem proposed by Paillier [71] is a variant of the Okamoto-Uchiyama's cryptosystem [68], and defined on an elliptic curve over a ring, $E(x, y) \in \mathbb{Z}_n$. Here, $n = p^2q$ for two distinct and large primes p and q. As shown by Paillier [71], security properties of the Okamoto-Uchiyama's cryptosystem [68] are preserved in its elliptic curve variant. The cryptosystem is secure with respect to the intractability of the high (p) degreed residuosity on E_n, where $n = p^2q$ for two distinct and large primes p and q.

The third cryptosystem proposed by Paillier [71] is an efficient embodiment of the Paillier's cryptosystem [70]. It is defined on an elliptic curve over a ring, $E(x, y) \in \mathbb{Z}_{n^2}$. Here, $n = pq$ is the prod-

Okamoto-Uchiyama's Cryptosystem [68]

Key Generation $\mathcal{K}$:

1. Select large primes p and q
2. Compute, $n = p^2 * q$
3. Choose, $g \in \mathbb{Z}_n^*$ such that $g^{p(p-1)} \equiv 1 \bmod p^2$ and $g^{p-1} \neq 1 \bmod p^2$
4. Compute, $h = g^n \bmod n$
5. Compute $\mu = (L(g^{p-1} \bmod p^2))^{-1} \bmod p$ where, $L(u) = (u-1)/p$

Encryption $\mathcal{E}$:

1. A plaintext, $m \in (0, 2^{k-1})$ and a random integer $r \in \mathbb{Z}_n$
2. A ciphertext $c = g^m \times h^r \bmod n$

Ciphertexts Aggregation $\mathcal{A}$:

1. Given $c_1 = \mathcal{E}(m_1)$ and $c_2 = \mathcal{E}(m_2)$
2. Compute an aggregated ciphertext, $c = c_1 * c_2 \bmod n^2 = \mathcal{E}(m_1 + m_2) \bmod p$

Decryption $\mathcal{D}$:

1. Decrypt the ciphertext, $\mathcal{D}(c) = L(c^{p-1} \bmod p^2) \times \mu \bmod p = m$

Elliptic Curve Naccache-Stern Cryptosystem [71]

Key Generation $\mathcal{K}$:

1. Choose two B-smooth integers u and v
2. Compute, $\sigma = u \cdot v$
3. Choose a point G on $E_n(0, b)$ of order a multiple of σ
4. Compute $\mu = lcm(p + 1, q + 1)$

Encryption $\mathcal{E}$:

1. A plaintext, $m \in \mathbb{Z}_\sigma$ and a random integer $r < n$
2. Compute a ciphertext, $c = (m + \sigma r) \cdot G$

Ciphertexts Aggregation $\mathcal{A}$:

1. Given ciphertexts c_1 and c_2
2. Compute an aggregated ciphertext, $c = c_1 + c_2 \mod n = \mathcal{E}(m_1 + m_2)$

Decryption $\mathcal{D}$:

1. Decrypt the ciphertext, $\mathcal{D}(c)$, $u = (\mu/\sigma) \cdot C = m \cdot G^{'}$
2. Discrete log of u in base $G^{'}$ gives the plaintext m

Elliptic Curve Okamoto-Uchiyama Cryptosystem [71]

Key Generation $\mathcal{K}$:

1. Select large primes p and q
2. Compute, $n = p^2 \cdot q$
3. Compute $E_n(a, b)$ from $E_{p^2}(a_p, b_p)$ and $E_q(a_q, b_q)$
4. Choose a point $G \in E_n(a, b)$ of maximal order $lcm(|E_{p^2}|, |E_q|)$
5. Compute $H = n \cdot G$

Encryption $\mathcal{E}$:

1. Choose a plaintext, m and a random integer r
2. Compute a ciphertext, $c = m \cdot G + r \cdot H$

Ciphertexts Aggregation $\mathcal{A}$:

1. Given ciphertexts c_1 and c_2
2. Compute an aggregated ciphertext, $c = c_1 + c_2 \mod n = \mathcal{E}(m_1 + m_2)$

Decryption $\mathcal{D}$:

1. Decryption of ciphertext, $\mathcal{D}(c) = \frac{\psi_p((p+2) \cdot C)}{\psi_p((p+2) \cdot G)} \mod p$

uct two distinct and large primes p and q. The semantic security supported by the cryptosystem is dependent on the indistinguishably of n-residues of E_{n^2}. It is based on the intractability of distinguishing the points of $E[\mu] = n \cdot E_{n^2}$ from other points on the curve E_{n^2}. Paillier's cryptosystem [71] is additively homomorphic, and, therefore, malleable against adaptive chosen ciphertext attacks (CCA2).

As shown by Paillier [71], all three cryptosystems are additively homomorphic, probabilistic, and semantically secure with respect to the high degree residuosity problems associated with elliptic curves, E_{pq}, E_{p^2q}, $E_{p^2q^2}$, respectively. All three elliptic curve Paillier's cryptosystems [71] are defined on an elliptic curve over a composite, $E(\mathbb{Z}_n)$, where n comprises two large primes p and q. The most powerful algorithm for integer factorization is a number field sieve method, and the complexity of a number field sieve method is dependent on the size of a number to be factored. Hence, elliptic curve Okamoto-Uchiyama's cryptosystem can use the primes p and q of size 341-bit ($\approx n = p^2q$ of size 1024-bit) to achieve the equivalent security as provided by the 1024-bit RSA cryptosystem [114, 115].

Mykletun et al. [31] and Peter et al. [47] comparatively evaluate the performance of elliptic curve Naccache-Stern's cryptosystem [71], elliptic curve Okamoto-Uchiyama's cryptosystem [71], and elliptic curve Paillier's cryptosystem [71], with respect to the well-known asymmetric-key based cryptosystems [67, 68].

These three cryptosystems incur significant message expansion as compared to other elliptic curve based cryptosystems such as the EC-ElGamal cryptosystem [67]. The message expansion increases the communication overhead and reduces the lifespan of WSNs. Despite the significant communication overhead, Paillier's cryptosystems [71] are not secure and allow the secret key to be recovered from the publicly available information [73]. Although elliptic curve Paillier's cryptosystems [71] are theoretically analyzed by Mykletun et al. [31] and Peter et al. [47] for resource constrained WSNs, the communication overhead introduced by the transmission of large ciphertexts and inherent security vulnerabilities limit their applicability for the CDA protocols of WSNs.

Elliptic Curve Paillier Cryptosystem [71]

Key Generation $\mathcal{K}$:

1. Select large primes p and q
2. Compute, $n = p \cdot q$
3. Compute $E_{n^2}(a, b)$ from $E_{p^2}(a_p, b_p)$ and $E_{q^2}(a_q, b_q)$
4. Choose a point $G \in E_{n^2}(a, b)$ of order divisible by n
5. Compute $\mu = lcm(p + 2, q + 2)$

Encryption $\mathcal{E}$:

1. Choose a plaintext, $m \in \mathbb{Z}_n$ and a random integer, $r < n$
2. Compute a ciphertext, $c = (m + nr) \cdot G$

Ciphertexts Aggregation $\mathcal{A}$:

1. Given ciphertexts c_1 and c_2
2. Compute an aggregated ciphertext, $c = c_1 + c_2 \mod n = \mathcal{E}(m_1 + m_2)$

Decryption $\mathcal{D}$:

1. Decryption of ciphertext, $\mathcal{D}(c) = \frac{\psi_n(\mu \cdot C)}{\psi_n(\mu \cdot G)} \mod n$

Elliptic Curve ElGamal's Cryptosystem [67]

Key Generation $\mathcal{K}$:

1. Select a large prime p
2. Choose an elliptic curve E over $\mathbb{F}_p$
3. Choose a point P on $E(\mathbb{F}_p)$
4. Randomly choose a secret s_k and compute, $p_k = s_k \cdot P$ on $E(\mathbb{F}_p)$

Encryption $\mathcal{E}$:

1. A plaintext, $m \in E(\mathbb{F}_p)$ and a random integer r
2. Compute ciphertexts $c_1 = r \cdot P$ and $c_2 = m + r \cdot p_k$

Ciphertexts Aggregation $\mathcal{A}$:

1. Given an encryption $\mathcal{E}(m_1)$ as c_{11} and c_{12}
2. Given an encryption $\mathcal{E}(m_2)$ as c_{21} and c_{22}
3. Compute aggregated ciphertexts, $c_1 = c_{11} + c_{21}$ and $c_2 = c_{12} + c_{22}$
4. Decryption of c_1 and c_2 gives an aggregated plaintext $m_1 + m_2$ on $E(\mathbb{F}_p)$

Decryption $\mathcal{D}$:

1. Decrypt the ciphertexts, $\mathcal{D}(c) = c_2 - s_k \cdot c_1 = m$

6.2.4. Elliptic curve ElGamal cryptosystem

Koblitz introduced the use of elliptic curves for cryptographic constructions [67]. Author proposed the first elliptic curve based public-key cryptosystem that supports additive homomorphism. The additive homomorphic cryptosystem is an analogue of the ElGamal cryptosystem [91]. The ElGamal cryptosystem [91] is based on an intractability of solving the discrete logarithm problem (DLP) while the elliptic curve variant of ElGamal cryptosystem [67] is based on an intractability of solving the elliptic curve discrete logarithm problem (ECDLP). Unlike Paillier's cryptosystems [71] that are defined on an elliptic curve over a ring, EC-ElGamal cryptosystem is defined on an elliptic curve over a finite field $\mathbb{F}$. Therefore, the EC-ElGamal cryptosystem [67] requires only 160-bit key-size to achieve the same level of security as provided by the 1024-bit RSA cryptosystem [113]. The smaller key size improves bandwidth requirements, energy utilization, and storage capabilities in WSNs.

Elliptic curve cryptosystems (based on finite fields) provide the same level of security as provided by the asymmetric-key based cryptosystems, however, with smaller parameter sizes. Nevertheless, there exist some practical difficulties to use elliptic curve based cryptosystems such as the EC-ElGamal cryptosystem. They are as follows:

- The ElGamal cryptosystem [91] has a 2-to-1 message expansion ratio. However, the EC-ElGamal cryptosystem [67] has at least a 4-to-1 message expansion ratio. The reason behind this is due to the fact that each elliptic curve point is represented by two or more coordinate values. Each point in elliptic curve comprises of two coordinate values, x and y, in the affine coordinate system and three coordinate values, x, y, and z, in the projective and Jacobian coordinate system [116]. Therefore, the message expansion ratio of the EC-ElGamal cryptosystem is at least $1 : 4$, where a plaintext is converted to two ciphertexts and each ciphertext has at least two coordinate values. Such increased overhead can be efficiently reduced by a point compression technique as

mentioned by Hoffstein et al. [117]. By using a point compression technique [117], we can efficiently compute a value of y-coordinate from the x-coordinate value and with the help of an additional sign bit. Hence, the EC-ElGamal cryptosystem requires only two extra bits as compared to the ElGamal cryptosystem.

- There is no efficient way to map plaintext values to elliptic curve points. In addition, the mapping function needs to be deterministic such that it can uniquely associate each plaintext value to an elliptic curve point, and vice versa. Moreover, the mapping function needs to be homomorphic such that aggregated plaintext values can be uniquely mapped to the corresponding elliptic curve points representing aggregated ciphertexts. The deterministic and homomorphic mapping function ensures that the aggregation of elliptic curve points always yields an elliptic curve point in such a way that the resultant point can be mapped back to the corresponding aggregated plaintext value. The mapping function that transforms the plaintext values to corresponding elliptic curve points needs to be independent from the encryption and decryption operations of the EC-ElGamal cryptosystem.

The mapping function [31] that transforms the plaintext values to corresponding elliptic curve points, and vice versa, has to meet the following requirement.

$$map(m_1 + m_2) = map(m_1) + map(m_2) \quad \forall m_1, m_2 \in \mathbb{F}_p$$

The mapping function map can be defined as follows:

$map : m \rightarrow m \cdot G$ Here, $m \in \mathbb{F}_p$ and $G \in E(\mathbb{F}_p)$

The mapping function adopted by Ugus et al. [118], Lin et al. [119], and Mykletun et al. [31] supports concealed data aggregation in WSNs. The mapping function ensures the additive privacy homomorphism supported by the EC-ElGamal cryptosystem.

$rmap : m \cdot G \rightarrow m$ Here, $m \in \mathbb{F}_p$ and $G \in E(\mathbb{F}_p)$

The reverse mapping function can be constructed by Pollard ρ or Pollard λ method [119]. The reverse mapping function is based on brute-force techniques [31]. The EC-ElGamal cryptosystem performs repeated point additions to retrieve a plaintext value from the corresponding elliptic curve point.

As shown by Mykletun et al. [31], the smaller parameter sizes can significantly improve the bandwidth and performance of the EC-ElGamal cryptosystem. The major limitation of the EC-ElGamal cryptosystem is that the reverse mapping function needs to solve the elliptic curve discrete logarithm problem (ECDLP). Although algorithms, such as the big-step little-step, can help to speed up the brute-force process, they require a large storage space (2^{17}-bit, or 16-Kbyte). Such a large storage can exceed the storage capacities of popular sensor nodes. Nevertheless, the decryption in CDA is performed at the base station due to the privacy requirements at intermediate nodes. Moreover, the base station in WSNs is assumed to be a resource-rich device, and it can perform the resource-intensive reverse mapping operations required by the decryption of the EC-ElGamal cryptosystem.

Girao et al. [33] explore the requirement to store encrypted and aggregated data in WSNs. They proposed a tiny persistent encrypted data storage (tinyPEDS) using the CMT cryptosystem [30] and the EC-ElGamal cryptosystem [67]. Due to the resource-constrained nature of WSNs, they used different security primitives for data storage and data transmission. Elliptic curve based ElGamal cryptosystem does not store any private key(s) at sensor nodes while CMT cryptosystem requires to store the secret key(s) at each sensor nodes. Hence, if data are encrypted using CMT cryptosystem and stored at the same node, it can be decrypted using the same key(s). Such a key storage can be a major weakness for physically vulnerable sensor nodes. Nevertheless, if data are encrypted and stored using the EC-ElGamal cryptosystem, they cannot be decrypted without having the private key(s). In addition, the private key of the EC-ElGamal cryptosystem is only available at the base station. Hence, data stored using the EC-ElGamal cryptosystem remains secure at sensor nodes. For data transmission, tinyPEDS employs a bandwidth efficient CMT cryptosystem.

Ugus et al. [118] analyzed the performance of the EC-ElGamal cryptosystem [67] using the MICAz mote [8] for tinyPEDS [33]. They described the software architecture of the EC-ElGamal cryptosystem in three layers. They are as follows: (1) Finite field arithmetic - comprises operations re-

lated to the finite fields such as modular addition, modular subtraction, and modular multiplication (2) Elliptic curve arithmetic - contains elliptic curve arithmetic operations such as point addition, point doubling, and point multiplication (3) Application level - the actual logic of the EC-ElGamal cryptosystem. They made several design decisions for efficient implementation of the EC-ElGamal cryptosystem. Authors analyze the performance of EC-ElGamal cryptosystem under a prime field, $\mathbb{F}_p$, and a binary field, $\mathbb{F}_{2^n}$. The use of a binary field arithmetic increases the code size, and it requires more memory accesses as compared to the prime field arithmetic. In addition, the scalar multiplication in a binary field is not adequately supported by standard microprocessors used by sensor nodes [8, 9, 87]. Hence, the choice of a prime field, $\mathbb{F}_p$, improves the performance as compared to the binary field, $\mathbb{F}_{2^n}$. In addition, Ugus et al. evaluated the impact of different coordinate systems (e.g., Affine, Projective, Jacobian, Chudnovsky-Jacobian, modified Jacobian, and mixed coordinate system [34]) on the performance. As shown in Gura et al. [106], 85% of the total execution time is spent on the multi-precision multiplication when performed on the MICAZ mote [8]. Therefore, Authors [118] analyzed different techniques for multi-precision multiplication and suggested a hybrid multiplication method [106]. The hybrid multiplication method requires a very few registers and memory access operations. In addition, Montgomery reduction, Barrett reduction, and the pseudo-Mersenne prime reduction are analyzed to select the modular reduction technique for improving the performance on resource-constrained devices. The analysis shows the viability of pseudo-Mersenne prime reduction for improving the performance in WSNs. One of the crucial operations in elliptic curve cryptosystem is the scalar point multiplication. Ugus et al. [34] evaluated the left-to-right and right-to-left binary methods [120] used for scalar point multiplication and suggested that the left-to-right method is superior due to its lower storage requirements.

Albath et al. [45] adopted the EC-ElGamal cryptosystem for privacy protection and a variant of elliptic curve digital signature algorithm for integrity preservation in the CDA protocols. In addition, Sun et al. [40, 54] used the EC-ElGamal cryptosystem [67] and Boneh et al.'s digital signature algorithm [121] for privacy protection and integrity preservation in WSNs. The algorithms proposed for privacy protection and integrity preservation support homomorphic operations over encrypted data and digital signatures respectively. The aggregation of data, as well as signatures, ensure that the communication overhead at each cluster head remains constant. One of the limitations of additive aggregation is that the original data cannot be verified at the base station. However, Sun et al. suggested a technique based on the concatenation of encrypted data and the aggregation of digital signatures for integrity verification at the base station. As shown in Sun et al. [40, 54], the base station can securely recover the original sensed information rather than an aggregated result. However, due to excessive communication cost involved with transmitting unaggregated data, the same recoverability property can become a weakness for resource-constrained WSNs.

Although privacy homomorphism has been frequently used to provide additive aggregation of ciphertexts, it is scarcely used to provide the support for various other operations such as median, minimum, and maximum. Lin et al. [119] proposed a novel sorting scheme using the EC-ElGamal cryptosystem. The proposed concealed data sorting scheme performs the comparison operations over encrypted data. In addition, it supports the operations, such as medium, minimum, and maximum, over encrypted data.

6.2.5. Elliptic curve Boneh's cryptosystem

Boneh et al. [122] defined an additive homomorphic cryptosystem over an elliptic curve group, $\mathbb{G}$. The cryptosystem is based on finite groups of composite order with support for a bilinear map. Boneh et al.'s cryptosystem can support arbitrary addition operations and a single multiplication operation over encrypted data. Security of Boneh et al.'s cryptosystem is based on an intractability of the subgroup decision problem. The cryptosystem is semantically secure if given a group element x of composite order $n = pq$ for distinct odd primes p and q, it is infeasible to decide whether a group element $x \in n$ belongs to a subgroup of order p or not.

Bahi et al. [48] proposed an end-to-end secure data aggregation protocol for privacy preservation in WSNs. Authors [48, 49] used Boneh et al.'s cryptosystem to support arbitrary addition operations and one multiplication operation over encrypted data.

The integrity protecting hierarchical CDA protocol [51] employs Boneh et al.'s cryptosystem for privacy preservation at intermediate nodes. The

Elliptic Curve Boneh's Cryptosystem [122]

Key Generation $\mathcal{K}$:

1. Given a security parameter $\tau \in \mathbb{Z}^+$
2. Choose two random τ-bit primes p and q
3. Compute $n = p * q \in \mathbb{Z}$
4. Generate two cyclic groups $\mathbb{G}$ and $\mathbb{G}_1$ of finite order n
5. $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ is a bilinear map
6. Randomly choose two generators, $g, u \xleftarrow{R} \mathbb{G}$
7. Set $h = u^q$

Encryption $\mathcal{E}$:

1. A plaintext, $m < q$ and a random integer $r \xleftarrow{R} \mathbb{Z}_n$
2. A ciphertext, $c = g^m \cdot h^r \in \mathbb{G}$

Ciphertexts Aggregation $\mathcal{A}$:

1. Given $c_1 = \mathcal{E}(m_1)$ and $c_2 = \mathcal{E}(m_2)$
2. Compute an aggregated ciphertext, $c = c_1 * c_2 * h^r$. Choose r randomly from $\mathbb{Z}_n$. Here, $c = \mathcal{E}(m_1 + m_2)$

Decryption $\mathcal{D}$:

1. Decrypt the ciphertext, $\mathcal{D}(c), c^p = (g^m \cdot h^r)^p = (g^p)^m$
2. Let $\widehat{g} = g^p$. Compute the discrete log of c^p `base` $\widehat{g}$ to recover a plaintext m

protocol partitions the network into multiple regions and encrypts each region's data with a public-key unique to that region. In addition, the protocol achieves integrity assurance using the aggregate MAC algorithm [23, 123]. Aggregate MAC aggregates (X-OR) the MAC tags and produces a MAC tag that is used for verifying the integrity of packets on which the MACs are generated. The essential difference between the aggregate MAC algorithm and the homomorphic MAC algorithm [76] is that an aggregate MAC tag needs the original data packets on which corresponding MACs are generated. However, a homomorphic MAC tag can verify the integrity of an aggregated data packet without the need for original data packets.

Lin et al. [56] proposed a secure data aggregation protocol for multi-application environments. A single network deployment for multiple applications can significantly improve network utilization [124, 125]. Moreover, the state-of-the-art sensor nodes [8, 9] are capable of sensing various phenomena such as humidity, temperature, pressure, acceleration, magnetization, etc. Lin et al.'s protocol allows the base station to extract application specific data from the aggregated ciphertexts. In addition, to avoid an unauthorized aggregation, Lin et al. provide a secure technique for counting the exact number of ciphertexts used to produce the aggregated results.

Zhou et al. [61] adopted Boneh et al.'s cryptosystem for secure and enhanced data aggregation in WSNs. They adopted an aggregation tree disjoint method for dividing the tree into a number of sub-trees and applying different public keys for encrypting the data of each sub-tree. The data collected from different sub-trees ensure the integrity preservation while achieving the privacy protection of sensor readings. Nevertheless, the deployment of redundant sub-trees for integrity verification increases the overall deployment cost.

One of the inherent limitations associated with Boneh et al.'s cryptosystem is that the use of bilinear pairing increases the computation cost compared to the conventional elliptic curve based cryptosystems such the EC-ElGamal cryptosystem [67], elliptic curve Paillier cryptosystems [71], etc.

6.2.6. Summary of asymmetric-key based cryptosystems

In Table 2, we compare asymmetric-key based cryptosystems including those based on elliptic curve cryptography. Table 2 provides the information about the underlying mathematical assumptions, homomorphic operations, and message expansion ratio of various asymmetric-key based cryptosystems.

As shown in Table 2, we evaluate cryptosystems that support additive and multiplicative privacy homomorphism. The RSA cryptosystem [90] and the ElGamal cryptosystem [91] has a least message expansion as compared to other asymmetric-key based cryptosystems. However, due to the need for additive data aggregation, they are not viable for WSNs applications. Although elliptic curve based cryptosystems achieve the same level of security with reduced parameter sizes, the fact only applies to the cryptosystems that are based on the prime field $\mathbb{F}_p$. If the cryptosystems are defined over elliptic curve rings $\mathbb{Z}_n$ for two large and distinct primes p and q, they require the parameters to be equivalent to the RSA cryptosystem for an equivalent security

Table 2. Comparison of Asymmetric-key Based Homomorphic Cryptosystems

Cryptosystem	**Security Assumption(s)**	**Homomorphic Operation(s)**	**Message Expansion**
RSA [90]	Integer Factorization & RSA Problem	$\otimes$	1
Goldwasser Micali [92]	Quadratic Residuosity Problem	X-OR	n
Okamoto Uchiyama [68]	Integer Factorization and p-subgroup	$\oplus$ $\ominus$ $\otimes_c$	3
Paillier [70]	Composite Residuosity Problem	$\oplus$ $\ominus$ $\otimes_c$	n
Naccache Stern [69]	Higher Residuosity Problem	$\oplus$ $\ominus$ $\otimes_c$	≥ 4
ElGamal [91]	Discrete Logarithms and Diffie-Hellman	$\otimes$	2
EC Naccache Stern [71]	ECDLP & High-Degree Residuosity	$\oplus$ $\ominus$ $\otimes_c$	$\frac{n}{\sigma}$
EC Okamoto Uchiyama [71]	ECDLP & p-residuosity over the Ring $\mathbb{Z}_{p^2q}$	$\oplus$ $\ominus$ $\otimes_c$	$\frac{n}{2^{k-1}}$
EC-Paillier [71]	ECDLP & Residuosity Classes over E_{n^2}	$\oplus$ $\ominus$ $\otimes_c$	n
EC-ElGamal [67]	Elliptic Curve Discrete Log Problem	$\oplus$ $\ominus$ $\otimes_c$	2 (+ 2-bit)
EC-Boneh [122]	Subgroup Decision Problem	$\oplus$ $\ominus$ $\otimes_c$ $\otimes$ (*once*)	$\frac{n}{r}$

n - The size of ciphertext space such that the factorization of n is hard.

$\otimes$ - Homomorphic multiplication of ciphertexts

$\oplus$ - Homomorphic addition of ciphertexts

$\ominus$ - Homomorphic subtraction of ciphertexts

$\otimes_c$ - Homomorphic multiplication with a known constant

r - A bound on message size for efficient discrete logarithm computations.

r - A bound on message size for efficient discrete logarithm computations.

σ - A product of the chosen B-smooth integers u and v.

level. In Table 2, the EC-ElGamal cryptosystem [67] is the only cryptosystem that is defined over a finite field $\mathbb{F}_p$ and require only 160-bit parameter sizes to achieve the equivalent security as compared to the 1024-bit RSA cryptosystem.

7. Integrity protection with in-network data aggregation

Hop-by-hop secure data aggregation protocols [15, 16] provide the integrity verification in a hop by hop manner. However, in data aggregation scenarios, the representation of original sensor readings changes due to en route aggregation of sensor readings. In addition, privacy homomorphism used to protect against passive adversaries makes sensor readings more vulnerable to active adversaries. The privacy homomorphism not only allows genuine aggregator nodes but also allows malicious adversaries to manipulate encrypted data. Hence, hop-by-hop integrity verification is insufficient for end-to-end secure data aggregation protocols. The malicious intermediate nodes, as well as their ability to perform en route aggregation of data packets, necessitate integrity verification in end-to-end secure data aggregation. End-to-end secure data aggregation protocols require the integrity verification at intermediate nodes as well as at the base station. An

end-to-end integrity verification enables the base station to verify the correctness of the aggregated sensor readings.

The problem of an end-to-end integrity verification, while supporting en route encrypted data processing requires the fulfillment of the following conditions.

- Integrity verification of original sensor readings at intermediate nodes.
- Integrity verification of previously aggregated sensor readings at intermediate nodes.
- Integrity verification of aggregated sensor readings at the base station.
- Verifying the correctness of aggregated sensor readings at the base station. (It ensures that the aggregated data is a correct representation of the original sensor readings.)

The fulfillment of the above-mentioned conditions ensures the detection of malicious data packets nearer to their sources. In addition, it improves the energy utilization and security in WSNs. In this section, we discuss the mechanisms used for integrity preservation in end-to-end secure data aggregation scenarios. Due to space constraints, we omit the discussion of conventional integrity preserving mechanisms such as hash functions, digital signatures, and MACs, and their applications in WSNs. However, interested readers are referred to the article of Simplicio Jr [126] for more discussion on the applications of conventional integrity preservation mechanisms in WSNs.

7.1. Identity-based aggregate signature

An identity-based aggregate signature [127] is a special class of digital signature that aggregates multiple signatures to produce a compact signature. The aggregate signature scheme can combine the signatures produced by different signers over different messages. An identity-based aggregate signature reduces the total information required for verifying the signed message. In an identity-based aggregate signature, a verifier does not need to obtain/store the public keys of the signers; instead, a verifier needs a short description of who signed what and two constant-length tags. The aggregate signature scheme is efficient and requires only 4 scalar multiplications and 2 point additions over elliptic curves to generate a signature, and only 2 point addition operations over elliptic curves to aggregate signatures. In CDA scenarios, signature generation and aggregation operation are to be performed on the sensor nodes. For signature verification, 3 pairing computations, 1 point multiplication, $2n-1$ point additions, and n scalar multiplication over elliptic curves are required. Here, n is the total number of signatures required to be aggregated. In CDA scenarios, the verification is performed by the base station, and it is assumed to be a resource-rich device capable enough to execute the above-mentioned operations.

Identity-Based Aggregate Signature [127]

Setup:

- Given groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q and an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$:
- Randomly select $P \in \mathbb{G}_1$, $s \in \mathbb{Z}/q\mathbb{Z}$ and compute $Q = sP$
- Let hash functions H_1, $H_2 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}/q\mathbb{Z}$
- A node ID_i receives from the base station the values of $sP_{i,j}$ for $j \in \{0,1\}$, where $P_{i,j} = H_1(ID_{i,j}) \in \mathbb{G}_1$.

Generation: Each node with identity, ID_i, signs a message, m_i, as follows:

1. Computes $P_w = H_2(w) \in \mathbb{G}_1$, here w is a unique string.
2. Computes $c_i = H_3(m_i, ID_i, w) \in \mathbb{Z}/q\mathbb{Z}$
3. Generates a random number $r_i \in \mathbb{Z}/q\mathbb{Z}$
4. Computes a signature, (w, S'_i, T'_i). Here, $S'_i = r_i P_w + sP_{i,0} + c_i sP_{i,1}$ and $T'_i = r_i P$.

Aggregation: Given signatures, (w, s'_i, T'_i) for $1 \leq i \leq n$, do:

- Compute $S_n = \sum_{i=1}^{n} S'_i$
- Compute $T_n = \sum_{i=1}^{n} T'_i$
- Here, aggregated signature is (w, S_n, T_n)

Verification: Given the identity-based aggregate signature, verify:

1. $\hat{e}(S_n, P) = \hat{e}(T_n, P_w)\hat{e}(Q, \sum_{i=1}^{n} P_{i,0} + \sum_{i=1}^{n} c_i P_{i,1})$. Here, $P_{i,j} = H_1(ID_i, j)$, $P_w = H_2(w)$ and $c_i = H_3(m_i, ID_i, w)$

Sun et al. [40, 54] adopted the EC-ElGamal cryptosystem [31, 67] and Boneh et al.'s aggregate signature scheme [121] for privacy protection and in-

tegrity preservation in WSNs. Their recoverable CDA protocols [40, 54] concatenate the encrypted data at aggregator nodes, instead of performing the lossy data aggregation like other CDA protocols [29, 31, 42]. At aggregator nodes, data, as well as their corresponding signatures, are aggregated before forwarding them toward the base station. Although, the signature size in Boneh et al.'s signature scheme [121] is compact, the total information needed to verify the signature is not necessarily compact. The objective of Gentry et al.'s aggregate signature [127] is to reduce the total information required for signature verification.

Li et al. [46] introduce a way for preserving integrity using the combination of homomorphic hashing [74] and identity-based aggregate signature [127]. The identity-based aggregate signature scheme enables all intermediate nodes to verify the integrity of the raw hash values, as well as the integrity of aggregated messages. The similar approach using homomorphic hashing [74] and identity-based aggregate signature [127] is proposed by Niu et al. [128] for integrity preservation in a lossy data aggregation scenario of WSNs. Authors used an identity-based aggregate signature scheme for producing a single signature that verifies the authenticity of different hash tags produced by different sensor nodes.

7.2. Homomorphic hash functions

Krohn et al. [74] describe a collision-resistant homomorphic hash function. The hash function is provably secure under the discrete-log assumption. In addition, it satisfies the following two conditions:

- Collision Resistance - Given vectors m_1, m_2, m_3 for which $H(m_3) = H(m_1)^{w_1} H(m_2)^{w_2}$, then there must be $m_3 = w_1 m_1 + w_2 m_2$.
- Privacy Homomorphism: Given messages m_1, m_2, and scalars w_1, w_2, the hash function can compute, $H(w_1 m_1 + w_2 m_2) = H(m_1)^{w_1} H(m_2)^{w_2}$. [1]

Li et al. [46] proposed three secure data aggregation protocols that ensure integrity using different homomorphic primitives such as homomorphic hash function [74], homomorphic digital signature [127], and homomorphic MAC [76]. As the hash function alone cannot ensure integrity preservation in the presence of malicious adversaries, authors combined the homomorphic hashing with an aggregate MAC algorithm [123]. In the proposed approach, every node shares a unique key with the base station for integrity verification at the base station.

Homomorphic Hash Function [74]

Setup:

- Let $\mathbb{G}$ be a cyclic group of order p and the public parameters include the description of $\mathbb{G}$ and generators $g_1, g_2, \cdots g_n \in \mathbb{G}$.

Generation:

- A hash function H on message $m = (m_1, m_2, \cdots m_n) \in Z_p^n$ is defined as follows:

$$H(m) = \prod_{i=1}^{n} g_i^{m_i}$$

Aggregation:

- Given $H(m_1)$ and $H(m_2)$, compute, $H(m_1 + m_2) = H(m_1)H(m_2)$.

Verification:

- Given an aggregated message $m = \sum_{i=1}^{j}(w_j m_i)$ and j-pairs of (h_i, w_i), verify:

$$\prod_{i=1}^{j} h_i^{w_i} \stackrel{?}{=} H(m)$$

Niu et al. [128] proposed a secure identity-based data aggregation using a homomorphic hash function [74] and an identity based aggregate signature [127]. The proposed approach enables every node in the network to share a unique key with the base station. The distinct keys improve the security of the aggregated data. A hash function is used to generate a hash tag over the raw data while an aggregate signature is used to sign the hash values. A homomorphic hash tag, as well as its aggregate signature, are appended to the data before forwarding the packet towards intermediate nodes.

7.3. Homomorphic message authentication codes

Although homomorphic digital signatures can verify the integrity while allowing en route aggregation, they are too slow for per packet integrity verification [76]. In addition, the overhead (computation and communication) associated with digital signatures is enormous for per-packet integrity

[1] The homomorphic equation is equivalent to $H(w_1 m_1 + w_2 m_2) = w_1 H(m_1) + w_2 H(m_2)$.

verification [106]. Therefore, Peter et al. [36] discuss the need for additive homomorphic MACs such that, $MAC(a+b) = MAC(b)+MAC(b)$. Although malleability is an undesirable property for conventional MAC algorithms, encrypted data processing at intermediate nodes and the need for verifying the encrypted packets before processing them, make a controlled malleability a necessary requirement for the CDA protocols. Although authors [36] discuss the need for homomorphic MAC, the design and development of homomorphic MAC remains an open research issue until the first homomorphic MAC construction proposed by Agrawal et al. [76].

Agrawal et al. [76] proposed a homomorphic MAC algorithm for verifying the integrity of network coded systems [129]. In network coded systems, data are processed en route in the same way as it is being processed in in-network processing. In the homomorphic MAC algorithm, given pairs of the vector and tag, (v_1, t_1) and (v_2, t_2), the aggregated tag t is generated for verifying integrity of a vector $y = \alpha_1 v_1 + \alpha_2 v_2$ for any $\alpha_1, \alpha_2 \in \mathbb{F}_q$. Homomorphic MAC comprises three probabilistic, polynomial time algorithms. They are as follows: (1) A $\mathcal{G}eneration$ algorithm is used to generate a tag $\mathcal{T}$ for each vector $v_i \in \mathbb{F}_q^{n+m}$, $\forall i \in \{1, 2, \cdots m\}$. Here, values of n, m, and q are fixed and remain the same for all nodes. (2) An $\mathcal{A}ggregation$ algorithm is used to generate a homomorphic MAC tag $\mathcal{T}$. (3) A $\mathcal{V}erification$ algorithm is used to verify the integrity of the aggregated vectors using the aggregated MAC tag $\mathcal{T}$. The details of relevant correctness proofs and security proofs of the homomorphic MAC algorithm can be found in Agrawal et al. [76].

The CDA protocols utilize the malleability property of different cryptosystems for processing encrypted data. However, the same malleability property is exploited by the adversaries for falsifying the aggregated sensor readings. Li et al. [46] adopted the homomorphic MAC algorithm [76] for integrity preservation in network coded WSNs. However, the symmetric-key based homomorphic MAC algorithm [76] shares a secret key between leaf nodes and the base station. Hence, if leaf nodes are not tamper-proof, compromising a single node may reveal the stored secret key and affects the overall security.

Westhoff et al. [57] combine a homomorphic MAC algorithm [76] with a homomorphic encryption algorithm [67] to provide the malleability resilient (premium) concealed data aggregation (MR-P-CDA). As shown by Westhoff et al. [57], the difference between a homomorphic MAC algorithm [76] and an aggregate authentication scheme [42] is in the key management. The secret key, k $= (k_1, k_2)$, in a homomorphic MAC algorithm, is shared between leaf nodes and the base station. However, in aggregate authentication [42], the key k_1 is shared across all nodes and the base station. The second key $k_2 = f(i)$, $\forall i \in (1, 2, \cdots n)$, is unique to the node i and shared only with the base station. In addition, aggregate authentication uses the key k_1 to generate valid authentication tags for the messages. Therefore, the aggregate authentication approach is only secure against external adversaries to whom the key k_1 is unknown. Westhoff et al.'s MR-P-CDA protocol [57] can only be secure against only outsider adversaries. In addition, the

Homomorphic MAC [76]

$\mathcal{S}etup$:

- Given a pseudo random generator $G : \mathcal{K}_G \rightarrow \mathbb{F}_q^{n+m}$ and a pseudo random function $F : \mathcal{K}_F \times (\mathcal{I} \times [m]) \rightarrow \mathbb{F}_q$.
- Let $k_1 \in \mathcal{K}_G$ and $k_2 \in \mathcal{K}_F$ are the keys used for the MAC construction.

$\mathcal{G}eneration$:

- Given i^{th} basis vector $v \in \mathbb{F}_q^{n+m}$ and a key pair $k = (k_1, k_2)$ do:
  1. $u \leftarrow G(k_1) \in \mathbb{F}_q^{n+m}$
  2. $b \leftarrow F(k_2, (id, i)) \in \mathbb{F}_q$
  3. $\mathcal{T} \leftarrow (u \cdot v) + b \in \mathbb{F}_q$

  Here, $\mathcal{T} \in \mathbb{F}_q$ is a MAC tag.

$\mathcal{A}ggregation$:

- Given (v_1, t_1, α_1), ..., (v_m, t_m, α_m), compute,
$$\mathcal{T} \leftarrow \sum_{j=1}^{m} \alpha_j \mathcal{T}_j \in \mathbb{F}_q$$

$\mathcal{V}erification$:

- Given a secret key $k = (k_1, k_2)$ and $y = (y_1, \cdots, y_{n+m}) \in \mathbb{F}_q^{n+m}$, verify a tag $\mathcal{T}$ as follows.
  - $u \leftarrow G(k_1) \in \mathbb{F}_q^{n+m}$ and $a \leftarrow (u \cdot y) \in \mathbb{F}_q$
  - $b \leftarrow \sum_{i=1}^{m} [y_{n+i} \cdot F(k_2, (id, i))] \in \mathbb{F}_q$
  - If $a + b = \mathcal{T}$ then output 1; otherwise output 0

MR-P-CDA protocol remains vulnerable to unauthorized aggregation by active insider adversaries.

Zhou et al. [60] proposed a secure data aggregation protocol for ensuring privacy and integrity of sensor readings. Their protocol adopts a symmetric-key based homomorphic cryptosystem [43] and a homomorphic MAC algorithm [76] for protecting the privacy and integrity of sensor readings. However, any symmetric-key based cryptosystem either requires a key to be shared across all nodes, such as Domingo-Ferrer's cryptosystem [72], Peter et al.'s cryptosystem [36], and Aldar C-F. Chan's cryptosystem [43], or requires a unique key for each sensor node such as Castelluccia et al.'s cryptosystem [30, 42]. As Zhou et al.'s protocol [60] adopts Aldar C-F. Chan's cryptosystem [43], a single malicious node can decrypt the data encrypted by any other node in the network. In addition, the same key can be used to generate malicious data packets.

Parmar et al. [59] proposed a malleability resilient concealed data aggregation (MR-CDA) protocol for ensuring privacy and integrity of sensor readings against insider and outsider adversaries. The protocol ensures the privacy and integrity of sensor readings using homomorphic primitives, namely, a homomorphic encryption proposed by Koblitz et al. [67] and a homomorphic MAC proposed by Agrawal et al. [76]. Authors use a non-malleable symmetric-key based cryptosystem (AES, RC5, etc.) for layer-wise integrity protection. Parmar et al. [62] extended their protocol to incorporate replay protection against insider and outsider adversaries. The use of homomorphic primitives and a pair-wise keying mechanism ensure the protection against active and passive adversaries.

Apavatjrut et al. [130] and Izawa et al. [77] provided integrity protection using the universal hash functions [131]. They considered the universal hash functions having support for X-OR privacy homomorphism. As the hash function cannot ensure integrity preservation in the presence of malicious adversaries, its output needs to be processed before using it for message authentication.

8. Comparison of secure data aggregation protocols

In this section, we compare the secure data aggregation protocols for measuring their security strengths. As shown in Table 3, the comparison is based on the well-known security requirements of WSNs' applications. In addition, we consider in-network data aggregation for the comparison due to its significant impact on the security attributes of different protocols.

As shown in Table 3, data aggregation has a significant impact on the security attributes such as privacy, integrity, and freshness of sensor readings. Although the state-of-the-art concealed data aggregation protocols ensure the confidentiality and privacy of sensor readings, integrity, and freshness preserving solutions are considered as a formidable challenge. Active insider and outsider adversaries and the lack of physical security make encrypted data processing vulnerable to a wide variety of attacks towards data integrity and data freshness. Table 3 highlights the fact that although there exist solutions for hop-by-hop message authentication and end-to-end message authentication, very few protocols target both these objectives together. In addition, the conflicting requirements of in-network data aggregation and freshness preserving solutions make it formidable to achieve them together. As shown in Table 3, the comparison of secure data aggregation protocols suggests a need for alternative solutions that achieve the essential security attributes together in resource-constrained WSNs.

9. Open research issues and future research directions

In this article, we discuss the state-of-the-art concealed data aggregation protocols in wireless sensor networks. Although we discuss the impact of in-network data aggregation on security features and present their corresponding solutions for mitigating the security vulnerabilities, there are still open research issues that need to be considered for ensuring security in concealed data aggregation protocols.

Although privacy homomorphism ensures the privacy and confidentiality of sensor readings, it negatively affects other security attributes such as data integrity and data freshness. The encrypted data processing at intermediate nodes makes data integrity verification and data freshness verification challenging. The verification of data integrity and data freshness requires the raw sensor readings for verification while the privacy preservation requires the encrypted data at intermediate nodes. Although the conflicting objectives such as privacy preservation and integrity verification or freshness verification have been considered in concealed data

Table 3. Comparison of Secure Data Aggregation Protocols

Protocol	Agg.	Conf.	Privacy	HH-MA	EE-MA	Replay
Perrig et al. [80]	×	✓	×	✓	×	✓
Girao et al. [29]	✓	✓	✓	×	×	×
Castelluccia et al. [30]	✓	✓	✓	×	×	×
Westhoff et al. [32]	✓	✓	✓	×	×	×
Mykletun et al. [31]	✓	✓	✓	×	×	×
Luk et al. [132]	×	✓	×	✓	×	✓
Ugus [34]	✓	✓	✓	×	×	×
Ozdemir [35]	✓	✓	✓	×	×	×
Peter et al. [36]	✓	✓	✓	×	×	×
Girao et al. [33]	✓	✓	✓	×	×	×
Mlaih et al. [41]	✓	✓	✓	✓	×	×
Armknecht et al. [39]	✓	✓	✓	×	×	×
Sun et al. [40]	✓	✓	✓	×	✓	×
Di Pietro al. [44]	✓	✓	✓	×	×	×
Castelluccia et al. [42]	✓	✓	✓	✓	×	×
Apavatjrut et al. [130]	✓	×	×	×	✓	×
Wang et al. [52]	✓	✓	✓	×	×	×
Ozdemir et al. [51]	✓	✓	✓	×	✓	×
Sicari et al. [55]	✓	✓	✓	✓	×	×
Izawa et al. [77]	✓	×	×	×	✓	×
Lin et al. [56]	✓	✓	✓	×	×	×
Westhoff et al. [57]	✓	✓	✓	×	✓	×
Parmar et al. [59]	✓	✓	✓	✓	✓	×
Zhou et al. [60]	✓	✓	✓	×	✓	×
Parmar et al. [62]	✓	✓	✓	✓	✓	✓

Agg. - En Route (Data) Aggregation
Conf. - Confidentiality
Privacy - Privacy at Intermediate Nodes
HH-MA - Hop-by-Hop Message Authentication
EE-MA - End-to-End Message Authentication
Replay - Replay Protection

aggregation protocols, the corresponding solutions provide either hop-by-hop integrity and freshness verification or introduce heavy energy consumptions. In addition, the conventional mechanisms used for integrity verification either provide hop-by-hop integrity verification or provide end-to-end integrity verification. However, data-centric networks such as WSNs require the integrity verification at intermediate nodes as well as at the base station. Hence, the development of a mechanism that simultaneously provides integrity verification at intermediate nodes as well as at the base station is an interesting research issue.

The need for verifying the freshness of encrypted sensor readings as well as aggregated sensor readings, in the presence of insider and outsider adversaries, also poses unique challenges for concealed data aggregation protocols. The conventional mechanisms used for ensuring data freshness are not viable in concealed data aggregation scenario. The threat of insider adversaries and their ability to process the encrypted data make freshness verification a formidable research issue. As shown in Table 3, a limited number of concealed data aggregation protocols ensure these conflicting security objectives together. The development of concealed data protocols that simultaneously realize the conflicting security objectives such as privacy, integrity,

and freshness is still an open research area.

Along with the desired security objectives, the key management also provides ample research opportunities. The hop-by-hop secure data aggregation protocols only consider outsider adversaries, while the concealed data aggregation protocols consider insider and outsider adversaries together. Therefore, the conventional key management solutions used to provide hop-by-hop secure data aggregation are not viable for concealed data aggregation scenarios. The distribution and storage of secret keys considering the presence of active insider adversaries pose newer challenges.

In addition, as the concealed data aggregation protocols rely on the privacy homomorphism for encrypted data processing, there is a need to develop fully homomorphic algorithms (encryption algorithms, MACs, digital signatures) that support full arithmetic operations over encrypted data. Although concealed data aggregation protocols consider additive homomorphism, support for other homomorphic operations increases the viability of CDA protocols in real-world application scenarios.

10. Conclusion

The comprehensive survey of the state-of-the-art concealed data aggregation protocols provides a framework for understanding the existing literature. The survey analyzes the impact of in-network data aggregation on vital security objectives such as privacy, integrity, and freshness of sensor readings. The survey explores the range of privacy preservation techniques with different keying mechanisms (symmetric or asymmetric) to analyze the impact of key size on resource-constrained devices. One of the major ingredients of all the techniques used for privacy preservation in concealed data aggregation is privacy homomorphism. We outline the techniques that provide integrity preservation and replay protection while performing encrypted data processing. Furthermore, techniques that provide concatenation and classification of encrypted sensor readings and encrypted data searching have been explored to analyze their impact on the domain of concealed data aggregation.

We comparatively evaluate the performance of concealed data aggregation protocols using different metrics such as keying mechanisms, security attributes, and well-known cryptographic attacks. The comparison of concealed data aggregation protocols, having different keying mechanisms, helps in identifying the algorithms that consume fewer computation and communication resources. The comparison based on different security attributes, such as privacy, integrity, and freshness help in identifying the alternative protocols that satisfy the demand of real-world applications with high-end security requirements. In addition, the extensive analysis of the state-of-the-art concealed data aggregation protocols ensures a trade-off between security and resource overhead in WSNs. Although the privacy issue has been widely explored and evaluated, the lack of integrity and freshness protecting mechanisms can provide abundant research opportunities. In addition, the security solutions proposed in the area of concealed data aggregation may further help the research in closely related areas such as network coding and cloud computing. The possible solutions to the highlighted open research issues can narrow the gap between theoretical research and real-world application scenarios.

Acknowledgement

This research was a part of the project "A Secure Data Aggregation System and An Intrusion Detection System for Wireless Sensor Networks". It was supported by the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India.

References

[1] G. J. Pottie, Wireless sensor networks, in: Proceedings of the Information Theory Workshop, IEEE, Killarney, Ireland, 1998, pp. 139–140. doi:10.1109/ITW.1998.706478.

[2] G. J. Pottie, W. J. Kaiser, Wireless integrated network sensors, Communications of the ACM 43 (5) (2000) 51–58. doi:10.1145/332833.332838.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: A survey, Computer Networks: The International Journal of Computer and Telecommunications Networking 38 (4) (2002) 393–422. doi:10.1016/S1389-1286(01)00302-4.

[4] D. Culler, D. Estrin, M. Srivastava, Guest editors' introduction: Overview of sensor networks, Computer 37 (8) (2004) 41–49. doi:10.1109/MC.2004.93.

[5] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Computer Networks 52 (12) (2008) 2292–2330. doi:10.1016/j.comnet.2008.04.002.

[6] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Communications of the ACM 47 (6) (2004) 53–57. doi:10.1145/990680.990707.

[7] H. Karl, A. Willig, Protocols and Architectures for Wireless Sensor Networks, John Wiley & Sons, 2005. doi:10.1002/0470095121.

[8] MEMSIC, MICAz mote platform, Datasheet, http://www.memsic.com/userfiles/files/Datasheets/WSN/6020-0060-04-B_MICAz.pdf, Accessed - September 9, 2015.

[9] MEMSIC, TelosB mote platform, http://www.memsic.com/userfiles/files/Datasheets/WSN/6020-0094-02_B_TELOSB.pdf, Accessed - September 9, 2015.

[10] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, System architecture directions for networked sensors, ACM SIGPLAN Notices 35 (11) (2000) 93–104. doi:10.1145/356989.356998.

[11] B. Krishnamachari, D. Estrin, S. B. Wicker, The impact of data aggregation in wireless sensor networks, in: Proceedings of the 22nd International Conference on Distributed Computing Systems, ICDCSW'02, IEEE, Vienna, Austria, 2002, pp. 575–578. doi:10.1109/ICDCSW.2002.1030829.

[12] A. Boulis, S. Ganeriwal, M. B. Srivastava, Aggregation in sensor networks: An energy-accuracy trade-off, Ad Hoc Networks 1 (23) (2003) 317–331. doi:10.1016/S1570-8705(03)00009-X.

[13] R. Rajagopalan, P. Varshney, Data-aggregation techniques in sensor networks: A survey, IEEE Communications Surveys Tutorials 8 (4) (2006) 48–63. doi:10.1109/COMST.2006.283821.

[14] E. Fasolo, M. Rossi, J. Widmer, M. Zorzi, In-network aggregation techniques for wireless sensor networks: A survey, Wireless Communications 14 (2) (2007) 70–87. doi:10.1109/MWC.2007.358967.

[15] L. Hu, D. Evans, Secure aggregation for wireless networks, in: Proceedings of the Symposium on Applications and the Internet Workshops, SAINT'03, IEEE, Washington, D.C., USA, 2003, pp. 384–391. doi:10.1109/SAINTW.2003.1210191.

[16] B. Przydatek, D. Song, A. Perrig, SIA: Secure information aggregation in sensor networks, in: Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, SenSys'03, ACM, Los Angeles, USA, 2003, pp. 255–265. doi:10.1145/958491.958521.

[17] H. Chan, A. Perrig, Security and privacy in sensor networks, Computer 36 (10) (2003) 103–105. doi:10.1109/MC.2003.1236475.

[18] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, Ad Hoc Networks 1 (2-3) (2003) 293–315. doi:10.1016/S1570-8705(03)00008-8.

[19] Y. Wang, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks, IEEE Communications Surveys & Tutorials 8 (2) (2006) 2–23. doi:10.1109/COMST.2006.315852.

[20] A. Becher, Z. Benenson, M. Dornseif, Tampering with motes: Real-world physical attacks on wireless sensor networks, in: Proceedings of the 3rd International Conference on Security in Pervasive Computing, SPC'06, Vol. 3934 of Lecture Notes in Computer Science, Springer-Verlag, York, UK, 2006, pp. 104–118. doi:10.1007/11734666_9.

[21] X. Chen, K. Makki, K. Yen, N. Pissinou, Sensor network security: A survey, IEEE Communications : Surveys & Tutorials 11 (2) (2009) 52–73. doi:10.1109/SURV.2009.090205.

[22] D. Wagner, Resilient aggregation in sensor networks, in: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN'04, ACM, Washington D.C., USA, 2004, pp. 78–87. doi:10.1145/1029102.1029116.

[23] H. Chan, A. Perrig, D. Song, Secure hierarchical in-network aggregation in sensor networks, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS'06, ACM, Alexandria, USA, 2006, pp. 278–287. doi:10.1145/1180405.1180440.

[24] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan, N. Xiong, Secure data aggregation in wireless sensor networks: A survey, in: Proceedings of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT'06, IEEE, Taipei, Taiwan, 2006, pp. 315–320. doi:10.1109/PDCAT.2006.96.

[25] Y. Yang, X. Wang, S. Zhu, G. Cao, SDAP: A secure hop-by-hop data aggregation protocol for sensor networks, in: Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc'06, ACM, Florence, Italy, 2006, pp. 356–367. doi:10.1145/1132905.1132944.

[26] H. Alzaid, E. Foo, J. G. Nieto, Secure data aggregation in wireless sensor network: A survey, in: Proceedings of the 6th Australasian Conference on Information Security - Volume 81, AISC'08, Australian Computer Society, Wollongong, Australia, 2008, pp. 93–105.

[27] S. Ozdemir, Y. Xiao, Secure data aggregation in wireless sensor networks: A comprehensive overview, Computer Networks: The International Journal of Computer and Telecommunications Networking 53 (12) (2009) 2022–2037. doi:10.1016/j.comnet.2009.02.023.

[28] J. Girao, M. Schneider, D. Westhoff, CDA: Concealed data aggregation in wireless sensor networks, in: Proceedings of the ACM Workshop on Wireless Security, WiSe'04, ACM, Philadelphia, USA, 2004, pp. 1–2, poster presentation.

[29] J. Girao, D. Westhoff, M. Schneider, CDA: Concealed data aggregation for reverse multicast traffic in wireless sensor networks, in: Proceedings of the 40th International Conference on Communications, ICC'05, IEEE, Seoul, Korea, 2005, pp. 3044–3049. doi:10.1109/ICC.2005.1494953.

[30] C. Castelluccia, E. Mykletun, G. Tsudik, Efficient aggregation of encrypted data in wireless sensor networks, in: Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MOBIQUITOUS'05, IEEE, Washington, D.C., USA, 2005, pp. 109–117. doi:10.1109/MOBIQUITOUS.2005.25.

[31] E. Mykletun, J. Girao, D. Westhoff, Public key based cryptoschemes for data concealment in wireless sensor networks, in: Proceedings of the IEEE International Conference on Communications, ICC'06, IEEE, Istanbul, Turkey, 2006, pp. 2288–2295. doi:10.1109/ICC.2006.255111.

[32] D. Westhoff, J. Girao, M. Acharya, Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation, IEEE Transactions on Mobile Computing 5 (10) (2006) 1417–1431. doi:10.1109/TMC.2006.144.

[33] J. Girao, D. Westhoff, E. Mykletun, T. Araki, TinyPEDS: Tiny persistent encrypted data storage in asynchronous wireless sensor networks, Ad Hoc Net-

works 5 (7) (2007) 1073–1089. doi:10.1016/j.adhoc.2006.05.004.

[34] O. Ugus, Asymmetric homomorphic encryption transformation for securing distributed data storage in wireless sensor networks, Master's thesis, Technische Universität Darmstadt, Germany, http://www.ist-ubisecsens.org/publications/diplarb_ugus.pdf, Accessed 31 July 2015 (April 2007).

[35] S. Ozdemir, Concealed data aggregation in heterogeneous sensor networks using privacy homomorphism, in: Proceedings of the IEEE International Conference on Pervasive Services, IEEE, Istanbul, 2007, pp. 165–168. doi:10.1109/PERSER.2007.4283909.

[36] S. Peter, K. Piotrowski, P. Langendoerfer, On concealed data aggregation for WSNs, in: Proceedings of the 4th IEEE Consumer Communications Networking Conference, CCNC'07, IEEE, Las Vegas, USA, 2007, pp. 192–196. doi:10.1109/CCNC.2007.45.

[37] S. Q. Ren, D. S. Kim, J. S. Park, A secure data aggregation scheme for wireless sensor networks, in: Proceedings of the Frontiers of High Performance Computing and Networking Workshops, ISPA'07, Vol. 4743 of Lecture Notes in Computer Science, Springer-Verlag, Niagara Falls, Canada, 2007, pp. 32–40. doi:10.1007/978-3-540-74767-3_4.

[38] L. Ertaul, V. Kedlaya, Computing aggregation function minimum/maximum using homomorphic encryption schemes in wireless sensor networks (WSNs), in: Proceedings of the International Conference on Wireless Networks, ICWN'07, CSREA Press, Las Vegas, Nevada, 2007, pp. 186–192.

[39] F. Armknecht, D. Westhoff, J. Girao, A. Hessler, A lifetime-optimized end-to-end encryption scheme for sensor networks allowing in-network processing, Computer Communications 31 (4) (2008) 734–749. doi:10.1016/j.comcom.2007.10.019.

[40] H.-M. Sun, Y.-C. Hsiao, Y.-H. Lin, C.-M. Chen, An efficient and verifiable concealed data aggregation scheme in wireless sensor networks, in: Proceedings of the International Conference on Embedded Software and Systems, ICESS'08, IEEE, Sichuan, China, 2008, pp. 19–26. doi:10.1109/ICESS.2008.9.

[41] E. Mlaih, S. A. Aly, Secure hop-by-hop aggregation of end-to-end concealed data in wireless sensor networks, in: Proceedings of the 2nd IEEE Workshop on Mission Critical Networking, in Conjunction with Infocom'08, MCN'08, IEEE, Phoenix, USA, 2008, pp. 1–6. doi:10.1109/INFOCOM.2008.4544601.

[42] C. Castelluccia, A. C.-F. Chan, E. Mykletun, G. Tsudik, Efficient and provably secure aggregation of encrypted data in wireless sensor networks, ACM Transactions on Sensor Networks (TOSN) 5 (3) (2009) 20:1–20:36. doi:10.1145/1525856.1525858.

[43] A. C.-F. Chan, Symmetric-key homomorphic encryption for encrypted data processing, in: Proceedings of the IEEE International Conference on Communications, ICC'09, IEEE, Dresden, Germany, 2009, pp. 774–778. doi:10.1109/ICC.2009.5199505.

[44] R. Di Pietro, P. Michiardi, R. Molva, Confidentiality and integrity for data aggregation in WSN using peer monitoring, Security and Communication Networks 2 (2) (2009) 181–194. doi:10.1002/sec.93.

[45] J. Albath, S. K. Madria, Secure hierarchical data aggregation in wireless sensor networks, in: Proceedings of the Wireless Communications and Networking Conference, WCNC'09, IEEE, Budapest, Hungary, 2009, pp. 1–6. doi:10.1109/WCNC.2009.4917960.

[46] Z. Li, G. Gong, Data aggregation integrity based on homomorphic primitives in sensor networks, in: Proceedings of the 9th International Conference on Ad-hoc, Mobile and Wireless Networks, ADHOC-NOW'10, Vol. 6288 of Lecture Notes in Computer Science, Springer-Verlag, Edmonton, Canada, 2010, pp. 149–162. doi:10.1007/978-3-642-14785-2_12.

[47] S. Peter, D. Westhoff, C. Castelluccia, A survey on the encryption of convergecast traffic with in-network processing, IEEE Transactions on Dependable and Secure Computing 7 (1) (2010) 20–34. doi:10.1109/TDSC.2008.23.

[48] J. M. Bahi, C. Guyeux, A. Makhoul, Secure data aggregation in wireless sensor networks: Homomorphism versus watermarking approach, in: Proceedings of the 2nd International Conference on Ad Hoc Networks, ADHOCNETS'10, Vol. 49 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer-Verlag, Victoria, Canada, 2010, pp. 344–358. doi:10.1007/978-3-642-17994-5_23.

[49] J. M. Bahi, C. Guyeux, A. Makhoul, Efficient and robust secure aggregation of encrypted data in sensor networks, in: Proceedings of the 4th International Conference on Sensor Technologies and Applications, SENSORCOMM'10, IEEE, Venice, Italy, 2010, pp. 472–477. doi:10.1109/SENSORCOMM.2010.76.

[50] A. C.-F. Chan, C. Castelluccia, A security framework for privacy-preserving data aggregation in wireless sensor networks, ACM Transactions on Sensor Networks (TOSN) 7 (4) (2011) 29:1–29:45. doi:10.1145/1921621.1921623.

[51] S. Ozdemir, Y. Xiao, Integrity protecting hierarchical concealed data aggregation for wireless sensor networks, Computer Networks: The International Journal of Computer and Telecommunications Networking 55 (8) (2011) 1735–1746. doi:10.1016/j.comnet.2011.01.006.

[52] L. Wang, L. Wang, Y. Pan, Z. Zhang, Y. Yang, Discrete logarithm based additively homomorphic encryption and secure data aggregation, Information Sciences 181 (16) (2011) 3308–3322. doi:10.1016/j.ins.2011.04.002.

[53] S. Papadopoulos, A. Kiayias, D. Papadias, Secure and efficient in-network processing of exact SUM queries, in: Proceedings of the 27th International Conference on Data Engineering, ICDE'11, IEEE, Hannover, Germany, 2011, pp. 517–528. doi:10.1109/ICDE.2011.5767886.

[54] C.-M. Chen, Y.-H. Lin, Y.-C. Lin, H.-M. Sun, RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 23 (4) (2012) 727–734. doi:10.1109/TPDS.2011.219.

[55] S. Sicari, L. A. Grieco, G. Boggia, A. Coen-Porisini, DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks, Journal of Systems and Software 85 (1) (2012) 152–166. doi:10.1016/j.jss.2011.07.043.

[56] Y.-H. Lin, S.-Y. Chang, H.-M. Sun, CDAMA: Concealed data aggregation scheme for multiple applications in wireless sensor networks, IEEE Transactions

on Knowledge and Data Engineering 25 (7) (2013) 1471–1483. doi:10.1109/TKDE.2012.94.

[57] D. Westhoff, O. Ugus, Malleability resilient (premium) concealed data aggregation, in: Proceedings of the 4th IEEE International Workshop on Data Security and Privacy in Wireless Networks, D-SPAN'13, IEEE, Madrid, Spain, 2013, pp. 1–6. doi:10.1109/WoWMoM.2013.6583470.

[58] M. B. O. Rafik, F. Mohammed, SA-SPKC: Secure and efficient aggregation scheme for wireless sensor networks using stateful public key cryptography, in: Proceedings of the 11th International Symposium on Programming and Systems, ISPS'13, IEEE, Algiers, Algeria, 2013, pp. 96–102. doi:10.1109/ISPS.2013.6581500.

[59] K. Parmar, D. C. Jinwala, Malleability resilient concealed data aggregation, in: Proceedings of the 20th EUNICE/IFIP WG 6.2, 6.6 Workshop on Advances in Communication Networking, EUNICE'14, Vol. 8846 of Lecture Notes in Computer Science, Springer-Verlag, Rennes, France, 2014, pp. 160–172. doi:10.1007/978-3-319-13488-8_15.

[60] Q. Zhou, G. Yang, H. Liwen, An efficient secure data aggregation based on homomorphic primitives in wireless sensor networks, International Journal of Distributed Sensor Networks 2014 (962925) (2014) 1–11. doi:10.1155/2014/962925.

[61] Q. Zhou, G. Yang, L. He, A secure-enhanced data aggregation based on ECC in wireless sensor networks, Sensors 14 (4) (2014) 6701–6721. doi:10.3390/s140406701.

[62] K. Parmar, D. C. Jinwala, Malleability resilient concealed data aggregation in wireless sensor networks, Wireless Personal Communications 85 (*) (2015) 1–23. doi:10.1007/s11277-015-2633-6.

[63] A. Viejo, Q. Wu, J. Domingo-Ferrer, Asymmetric homomorphisms for secure aggregation in heterogeneous scenarios, Information Fusion 13 (4) (2012) 285–295. doi:10.1016/j.inffus.2011.03.002.

[64] R. L. Rivest, L. Adleman, M. L. Dertouzos, On data banks and privacy homomorphisms, Foundations of Secure Computation 4 (11) (1978) 169–180.

[65] D. Dolev, C. Dwork, M. Naor, Non-malleable cryptography, in: Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, STOC'91, ACM, New Orleans, USA, 1991, pp. 542–552. doi:10.1145/103418.103474.

[66] C. Fontaine, F. Galand, A survey of homomorphic encryption for nonspecialists, EURASIP Journal on Information Security 2007 (15) (2007) 1–15. doi:10.1155/2007/13801.

[67] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48 (177) (1987) 203–209. doi:10.1090/S0025-5718-1987-0866109-5.

[68] T. Okamoto, S. Uchiyama, A new public-key cryptosystem as secure as factoring, in: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology, EUROCRYPT'98, Vol. 1403 of Lecture Notes in Computer Science, Springer-Verlag, Espoo, Finland, 1998, pp. 303–318. doi:10.1007/BFb0054135.

[69] D. Naccache, J. Stern, A new public key cryptosystem based on higher residues, in: Proceedings of the 5th ACM Conference on Computer and Communications Security, CCS'98, ACM, San Francisco, USA, 1998, pp. 59–66. doi:10.1145/288090.288106.

[70] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in: Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT'99, Vol. 1592 of Lecture Notes in Computer Science, Springer-Verlag, Prague, Czech Republic, 1999, pp. 223–238. doi:10.1007/3-540-48910-X_16.

[71] P. Paillier, Trapdooring discrete logarithms on elliptic curves over rings, in: Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT'00, Vol. 1976 of Lecture Notes in Computer Science, Springer-Verlag, Kyoto, Japan, 2000, pp. 573–584. doi:10.1007/3-540-44448-3_44.

[72] J. Domingo-Ferrer, A provably secure additive and multiplicative privacy homomorphism, in: Proceedings of the 5th International Conference on Information Security, ISC'02, Vol. 2433 of Lecture Notes in Computer Science, Springer-Verlag, Sao Paulo, Brazil, 2002, pp. 471–483. doi:10.1007/3-540-45811-5_37.

[73] S. D. Galbraith, Elliptic curve paillier schemes, Journal of Cryptology 15 (2) (2002) 129–138.

[74] M. N. Krohn, M. J. Freedman, D. Mazières, On-the-fly verification of rateless erasure codes for efficient content distribution, in: Proceedings of the IEEE Symposium on Security and Privacy, IEEE, California, USA, 2004, pp. 226–240. doi:10.1109/SECPRI.2004.1301326.

[75] R. Gennaro, J. Katz, H. Krawczyk, T. Rabin, Secure network coding over the integers, in: Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography, PKC'10, Vol. 6056 of Lecture Notes in Computer Science, Springer-Verlag, Paris, France, 2010, pp. 142–160. doi:10.1007/978-3-642-13013-7_9.

[76] S. Agrawal, D. Boneh, Homomorphic MACs: MAC-based integrity for network coding, in: Proceedings of the 7th International Conference on Applied Cryptography and Network Security, ACNS'09, Vol. 5536 of Lecture Notes in Computer Science, Springer-Verlag, Paris-Rocquencourt, France, 2009, pp. 292–305. doi:10.1007/978-3-642-01957-9_18.

[77] K. Izawa, A. Miyaji, K. Omote, Lightweight integrity for XOR network coding in wireless sensor networks, in: Proceedings of the 8th International Conference on Information Security Practice and Experience, ISPEC'12, Vol. 7232 of Lecture Notes in Computer Science, Springer-Verlag, Hangzhou, China, 2012, pp. 245–258. doi:10.1007/978-3-642-29101-2_17.

[78] R. Johnson, D. Molnar, D. X. Song, D. Wagner, Homomorphic signature schemes, in: Proceedings of the Cryptographer's Track at the RSA Conference on Topics in Cryptology, CT-RSA'02, Vol. 2271 of Lecture Notes in Computer Science, Springer-Verlag, London, UK, 2002, pp. 244–262. doi:10.1007/3-540-45760-7_17.

[79] D. Boneh, D. Freeman, J. Katz, B. Waters, Signing a linear subspace: Signature schemes for network coding, in: Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography, PKC'09, Vol. 5443 of Lecture Notes in Computer Science, Springer-Verlag, Irvine, USA, 2009, pp. 68–87. doi:10.1007/978-3-642-00468-1_5.

[80] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler, SPINS: Security protocols for sensor networks, Wireless Networks 8 (5) (2002) 521–534. doi:10.1145/990680.990707.

[81] S. Madden, M. J. Franklin, J. M. Hellerstein, W. Hong, TAG: A tiny aggregation service for ad-hoc sensor networks, ACM SIGOPS Operating Systems Review 36 (SI) (2002) 131–146. doi:10.1145/844128.844142.

[82] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva, Directed diffusion for wireless sensor networking, IEEE/ACM Transactions on Networking (TON) 11 (1) (2003) 2–16. doi:10.1109/TNET.2002.808417.

[83] W. B. Heinzelman, A. P. Chandrakasan, H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670. doi:10.1109/TWC.2002.804190.

[84] O. Younis, S. Fahmy, HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks, IEEE Transactions on Mobile Computing 3 (4) (2004) 366–379. doi:10.1109/TMC.2004.41.

[85] A. Manjhi, S. Nath, P. B. Gibbons, Tributaries and deltas: Efficient and robust aggregation in sensor network streams, in: Proceedings of the International Conference on Management of Data, ACM SIGMOD'05, ACM, Baltimore, Maryland, 2005, pp. 287–298. doi:10.1145/1066157.1066191.

[86] K. Akkaya, M. Demirbas, R. S. Aygun, The impact of data aggregation on the performance of wireless sensor networks, Wireless Communications & Mobile Computing 8 (2) (2008) 171–193. doi:10.1002/wcm.454.

[87] CrossBow, MICA2 mote platform, Datasheet, http://www.eol.ucar.edu/isf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf, Accessed - September 9, 2015.

[88] E. Çayirci, C. Rong, Security in Wireless Ad Hoc and Sensor Networks, John Wiley & Sons, Inc., New York, USA, 2008.

[89] Y. Wu, D. Ma, T. Li, R. Deng, Classify encrypted data in wireless sensor networks, in: Proceedings of the 60th IEEE Vehicular Technology Conference, Vol. 5 of VTC Fall'04, Los Angeles, USA, 2004, pp. 3236–3239. doi:10.1109/VETECF.2004.1404660.

[90] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126. doi:10.1145/359340.359342.

[91] T. El Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in: Proceedings of the Advances in Cryptology, CRYPTO'84, Vol. 196 of Lecture Notes in Computer Science, Springer-Verlag, California, USA, 1985, pp. 10–18. doi:10.1007/3-540-39568-7_2.

[92] S. Goldwasser, S. Micali, Probabilistic encryption, Journal of Computer and System Sciences 28 (2) (1984) 270–299. doi:10.1016/0022-0000(84)90070-9.

[93] C. Rackoff, D. R. Simon, Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, in: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO'91, Vol. 576 of Lecture Notes in Computer Science, Springer-Verlag, Santa Barbara, USA, 1992, pp. 433–444. doi:10.1007/3-540-46766-1_35.

[94] P. Kamat, Y. Zhang, W. Trappe, C. Ozturk, Enhancing source-location privacy in sensor network routing, in: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, ICDCS'05, IEEE, Columbus, USA, 2005, pp. 599–608. doi:10.1109/ICDCS.2005.31.

[95] N. Li, N. Zhang, S. K. Das, B. Thuraisingham, Privacy preservation in wireless sensor networks: A state-of-the-art survey, Ad Hoc Networks 7 (8) (2009) 1501–1514. doi:10.1016/j.adhoc.2009.04.009.

[96] R. L. Rivest, The RC5 encryption algorithm, in: Proceedings of the Fast Software Encryption: 2nd International Workshop, Vol. 1008 of Lecture Notes in Computer Science, Springer-Verlag, Leuven, Belgium, 1994, pp. 86–96. doi:10.1007/3-540-60590-8_7.

[97] K. Sohrabi, J. Gao, V. Ailawadhi, G. Pottie, Protocols for self-organization of a wireless sensor network, IEEE Personal Communications 7 (5) (2000) 16–27. doi:10.1109/98.878532.

[98] D. Wagner, Cryptanalysis of an algebraic privacy homomorphism, in: Proceedings of the 6th International Conference on Information Security, ISC'03, Vol. 2851 of Lecture Notes in Computer Science, Springer-Verlag, Bristol, UK, 2003, pp. 234–239. doi:10.1007/10958513_18.

[99] J. H. Cheon, W.-H. Kim, H. S. Nam, Known-plaintext cryptanalysis of the domingo-ferrer algebraic privacy homomorphism scheme, Information Processing Letters 97 (3) (2006) 118–123. doi:10.1016/j.ipl.2005.09.016.

[100] C. Karlof, N. Sastry, D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, in: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, SenSys'04, ACM, Baltimore, USA, 2004, pp. 162–175. doi:10.1145/1031495.1031515.

[101] G. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications, Transactions of the American Institute of Electrical Engineers XLV (-) (1926) 295–301. doi:10.1109/T-AIEE.1926.5061224.

[102] O. Goldreich, S. Goldwasser, S. Micali, How to construct random functions, Journal of the ACM (JACM) 33 (4) (1986) 792–807. doi:10.1145/6490.6503.

[103] M. Önen, R. Molva, Secure data aggregation with multiple encryption, in: Proceedings of the 4th European Conference on Wireless Sensor Networks, EWSN'07, Vol. 4373 of Lecture Notes in Computer Science, Springer-Verlag, Delft, The Netherlands, 2007, pp. 117–132. doi:10.1007/978-3-540-69830-2_8.

[104] M. Bellare, A. Desai, E. Jokipii, P. Rogaway, A concrete security treatment of symmetric encryption, in: Proceedings of the 38th Annual Symposium on Foundations of Computer Science, FOCS'97, IEEE, Miami Beach, USA, 1997, pp. 394–403. doi:10.1109/SFCS.1997.646128.

[105] M. Bellare, T. Kohno, V. Shoup, Stateful public-key cryptosystems: How to encrypt with one 160-bit exponentiation, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS'06, ACM, Alexandria, USA, 2006, pp. 380–389. doi:10.1145/1180405.1180452.

[106] N. Gura, A. Pate, A. Wander, H. Eberle, S. C. Shantz, Comparing elliptic curve cryptography and RSA on 8-bit CPUs, in: Proceedings of the 6th International

Workshop on Cryptographic Hardware and Embedded Systems, CHES'04, Vol. 3156 of Lecture Notes in Computer Science, Springer-Verlag, Cambridge, USA, 2004, pp. 119–132. doi:10.1007/978-3-540-28632-5_9.

[107] A. S. Wander, N. Gura, H. Eberle, V. Gupta, S. C. Shantz, Energy analysis of public-key cryptography for wireless sensor networks, in: Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications, PerCom'05, IEEE, Kauai, Hawaii, 2005, pp. 324–328. doi:10.1109/PERCOM.2005.18.

[108] D. J. Malan, M. Welsh, M. D. Smith, Implementing public-key infrastructure for sensor networks, ACM Transactions on Sensor Networks (TOSN) 4 (4) (2008) 22:1–22:23. doi:10.1145/1387663.1387668.

[109] B. K. Samanthula, W. Jiang, S. Madria, A probabilistic encryption based MIN/MAX computation in wireless sensor networks, in: Proceedings of the 14th International Conference on Mobile Data Management, MDM'13, IEEE, Milan, Italy, 2013, pp. 77–86. doi:10.1109/MDM.2013.18.

[110] T. Sander, A. Young, M. Yung, Non-interactive cryptocomputing for NC^1, in: Proceedings of the 40th Annual Symposium on Foundations of Computer Science, FOCS'99, IEEE, New York, USA, 1999, pp. 554–566. doi:10.1109/SFFCS.1999.814630.

[111] M. Acharya, J. Girao, D. Westhoff, Secure comparison of encrypted data in wireless sensor networks, in: Proceedings of the 3rd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, WIOPT'05, IEEE, Washington, D.C., USA, 2005, pp. 47–53. doi:10.1109/WIOPT.2005.44.

[112] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, Order preserving encryption for numeric data, in: Proceedings of the ACM SIGMOD International Conference on Management of Data, SIGMOD'04, ACM, Paris, France, 2004, pp. 563–574. doi:10.1145/1007568.1007632.

[113] D. Hankerson, A. J. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, 1st Edition, Springer, Secaucus, USA, 2003. doi:10.1007/b97644.

[114] A. K. Lenstra, Unbelievable security matching AES security using public key systems, in: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT'01, Vol. 2248 of Lecture Notes in Computer Science, Springer-Verlag, Gold Coast, Australia, 2001, pp. 67–86. doi:10.1007/3-540-45682-1_5.

[115] P. Ebinger, E. Teske, Factoring $n = pq^2$ with the elliptic curve method, in: Proceedings of the 5th International Symposium, Algorithmic Number Theory, ANTS-V, Vol. 2369 of Lecture Notes in Computer Science, Springer-Verlag, Sydney, Australia, 2002, pp. 475–490. doi:10.1007/3-540-45455-1_37.

[116] H. Cohen, A. Miyaji, T. Ono, Efficient elliptic curve exponentiation using mixed coordinates, in: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT'98, Vol. 1514 of Lecture Notes in Computer Science, Springer-Verlag, Beijing, China, 1998, pp. 51–65. doi:10.1007/3-540-49649-1_6.

[117] J. Hoffstein, J. Pipher, J. Silverman, An Introduction to Mathematical Cryptography, 1st Edition, Springer-Verlag, 2008. doi:10.1007/978-1-4939-1711-2.

[118] O. Ugus, A. Hessler, D. Westhof, Performance of additive homomorphic EC-Elgamal encryption for TinyPEDS, 6. fachgespräch "drahtlose sensornetze", RWTH Aachen University, http://www.ist-ubisecsens.org/publications/EcElgamal-UgHesWest.pdf, Accessed 31 July 2015 (July 2007).

[119] Y.-H. Lin, B.-Z. He, H.-M. Sun, Y.-H. Chen, CDS: Concealed data sorting scheme in wireless sensor networks, in: Proceedings of the International Computer Symposium, ICS'10, IEEE, Tainan, Taiwan, 2010, pp. 370–375. doi:10.1109/COMPSYM.2010.5685484.

[120] A. J. Menezes, S. A. Vanstone, P. C. V. Oorschot, Handbook of Applied Cryptography, 1st Edition, CRC Press, Inc., Boca Raton, USA, 1996.

[121] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, in: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology, EUROCRYPT'03, Vol. 2656 of Lecture Notes in Computer Science, Springer-Verlag, Warsaw, Poland, 2003, pp. 416–432. doi:10.1007/3-540-39200-9_26.

[122] D. Boneh, E.-J. Goh, K. Nissim, Evaluating 2-DNF formulas on ciphertexts, in: Proceedings of the 2nd International Conference on Theory of Cryptography, TCC'05, Vol. 3378 of Lecture Notes in Computer Science, Springer-Verlag, Cambridge, MA, 2005, pp. 325–341. doi:10.1007/978-3-540-30576-7_18.

[123] J. Katz, A. Y. Lindell, Aggregate message authentication codes, in: Proceedings of the Cryptopgraphers' Track at the RSA Conference on Topics in Cryptology, CT-RSA'08, Vol. 4964 of Lecture Notes in Computer Science, Springer-Verlag, 2008, pp. 155–169. doi:10.1007/978-3-540-79263-5_10.

[124] N. Trigoni, Y. Yao, A. Demers, J. Gehrke, R. Rajaraman, Multi-query optimization for sensor networks, in: Proceedings of the 1st IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS'05, Vol. 3560 of Lecture Notes in Computer Science, Springer-Verlag, Marina del Rey, USA, 2005, pp. 307–321. doi:10.1007/11502593_24.

[125] H. Gao, X. Fang, J. Li, Y. Li, Data collection in multi-application sharing wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 26 (2) (2015) 403–412. doi:10.1109/TPDS.2013.289.

[126] M. A. Simplicio, Jr, B. T. De Oliveira, C. B. Margi, P. S. L. M. Barreto, T. C. M. B. Carvalho, M. NäSlund, Survey and comparison of message authentication solutions on wireless sensor networks, Ad Hoc Networks 11 (3) (2013) 1221–1236. doi:10.1016/j.adhoc.2012.08.011.

[127] C. Gentry, Z. Ramzan, Identity-based aggregate signatures, in: Proceedings of the 9th International Conference on Theory and Practice in Public-Key Cryptography, PKC'06, Vol. 3958 of Lecture Notes in Computer Science, Springer-Verlag, New York, USA, 2006, pp. 257–273. doi:10.1007/11745853_17.

[128] S. Niu, C. Wang, Z. Yu, S. Cao, Lossy data aggregation integrity scheme in wireless sensor networks, Computers & Electrical Engineering 39 (6) (2013) 1726–1735, special Issue on Wireless Systems: Modeling, Monitoring, Transmission, Performance Evaluation and Opti-

mization. doi:10.1016/j.compeleceng.2012.11.022.

[129] R. Koetter, M. Medard, An algebraic approach to network coding, IEEE/ACM Transactions on Networking 11 (5) (2003) 782–795. doi:10.1109/TNET.2003.818197.

[130] A. Apavatjrut, W. Znaidi, A. Fraboulet, C. Goursaud, C. Lauradoux, M. Minier, Energy friendly integrity for network coding in wireless sensor networks, in: Proceedings of the 4th International Conference on Network and System Security, NSS'10, IEEE, Melbourne, Australia, 2010, pp. 223–230. doi:10.1109/NSS.2010.32.

[131] J. Carter, M. N. Wegman, Universal classes of hash functions, Journal of Computer and System Sciences 18 (2) (1979) 143–154. doi:10.1016/0022-0000(79)90044-8.

[132] M. Luk, G. Mezzour, A. Perrig, V. Gligor, MiniSec: A secure sensor network communication architecture, in: Proceedings of the 6th International Conference on Information Processing in Sensor Networks, IPSN'07, ACM, Cambridge, USA, 2007, pp. 479–488. doi:10.1145/1236360.1236421.