Abstract: Data aggregation in wireless sensor networks (WSN) is a rapidly emerging research area. It can greatly help conserve the scarce energy resources by eliminating redundant data thus achieving a longer network lifetime. However, securing data aggregation in WSN is made even more challenging by the fact that the sensor nodes and aggregators deployed in hostile environments are exposed to various security threats. In this paper we survey the current research related to security in data aggregation in wireless sensor networks. We have classified the security schemes studied in two main categories: cryptographic based scheme and trust based scheme. We provide an overview and a comparative study of these schemes and highlight the future research directions to address the flaws in existing schemes.

Author Address: tzia@csu.edu.au

Data Aggregation Security Challenges in Wireless Sensor Networks

Nabila Labraoui [1], Mourad Guerroui [2], Tanveer Zia [3]
[1] University of Tlemcen, Algeria
[2] PRISM university of Versailles, France
[3] Charles Sturt University, Australia

Abstract

Data aggregation in wireless sensor networks (WSN) is a rapidly emerging research area. It can greatly help conserve the scarce energy resources by eliminating redundant data thus achieving a longer network lifetime. However, securing data aggregation in WSN is made even more challenging by the fact that the sensor nodes and aggregators deployed in hostile environments are exposed to various security threats. In this paper we survey the current research related to security in data aggregation in wireless sensor networks. We have classified the security schemes studied in two main categories: cryptographic based scheme and trust based scheme. We provide an overview and a comparative study of these schemes and highlight the future research directions to address the flaws in existing schemes.

1. Introduction

Advancements in micro electro mechanical systems (MEMS) [9] and wireless networks have made possible the advent of tiny sensor nodes called "smart dust" which are low cost small tiny devices with limited coverage, low power, smaller memory sizes and low bandwidth [2]. A wireless sensor network (WSN) [5] is an ad-hoc network consisting of a large number of sensor nodes deployed to sense their surrounding environment. Sensor nodes are usually used to collect and report application-specific data to the monitoring node, known as a "sink node" [1]. WSNs are expected to be solutions to many applications [12,13], such as providing health care for the elderly, surveillance, emergency, and battlefield intelligence data gathering.

Along with the attractive features and increasingly important roles, sensor networks however have their inherent limitations: resource constraints, which is determined by the design goal of small-size and low-cost; security vulnerability, due to the open nature of wireless communication channels and the lack of physical protection of individual sensor nodes which makes it easy for the adversaries to eavesdrop the communication and compromise sensor nodes [3]. Security solutions require high computation, memory, storage and energy resources which creates an additional challenge when working with tiny sensor nodes [2]. Extensive research has been conducted to address these limitations by developing schemes that can improve resource efficiency and enhance security.

In the resource constrained WSN environment, forwarding of large amounts of data becomes the major focus of energy and bandwidth optimization efforts. Data aggregation has thus been put forward as an essential technique to achieve power and bandwidth efficiency in WSN. Based on the principle that the sink does not necessarily need all raw pieces of data collected by each sensor but only a summary or aggregated data thereof, data aggregation is done by aggregators which are comparatively powerful sensor nodes having the ability to aggregate and process data forwarded by source nodes at each intermediate node enroute to the sink. The Data communication constitutes an important share of the total energy consumption of the sensor network; sending one bit requires almost the same amount of energy as executing 50 to 150 instructions [38]. Thus, data aggregation can greatly help conserve the scarce energy resources by eliminating redundant data [6], and achieving a longer network lifetime. Typical aggregation functions include SUM, AVERAGE, MAX/MIN, and so on [4, 11]. However, data aggregation in sensor networks is even more challenging by the fact that the sensor nodes and aggregators deployed in hostile environments are exposed to various threats such as node compromise, injection of bogus aggregators, disclosure of sensed data and aggregate values to intruders or tampering with nodes and data transmitted over wireless links. Therefore, the processing and aggregation mechanisms need to be resilient against attacks where the aggregator and a fraction of the sensor nodes may be compromised.

The rest of the paper is organized as follows. Section II introduces the problem statement of secure data aggregation in WSN. While Section III presents the classification of secure aggregation schemes with description of existing works and Section IV discusses the performance comparison of the cited schemes. Concluding remarks are given in Section V.

2. Problem statement

2.1 Security Requirement in WSN aggregation

In-network data processing, such as data fusion and aggregation [40], has emerged in the recent years as an active research area in WSN. One of the important issues related to data aggregation is to find a realistic balance between computational overhead, delay, data resolution and trustworthiness [7]. This section describes the required security primitives to strengthen the security in aggregation schemes.

Data Integrity: This property ensures that the content of a message has not been altered, during transmission process. An adversary near the aggregator point will be able to change the aggregated result sent to the sink by adding some fragments or manipulating the packet's content without detection. Moreover, even without the existence of an adversary, data might be damaged or lost due to the wireless environment.

Data confidentiality: It is also essential to prevent leakage of sensitive data. If, for example, a network was responsible for monitoring a military target for the purpose of planning a surprise attack, then it would be necessary to ensure that the privacy of the information is preserved so that the target does not become aware of the ensuing plans. For this reason, a sensor network that uses data aggregation is also required to protect the confidentiality of the aggregated data just as it was required to protect the confidentiality of the non-aggregated data.

Data Authentication: guarantees that the reported data is the same as the original one and it has come from reliable source "identification". In secure data aggregation, both identification and authentication are important to ensure the legitimate data transfer between sensors. For instance, electing an aggregator point or reporting invalid aggregated results are authenticated using their identity while data authentication ensures that raw data are received at the aggregators at the same time as they are being sensed.

Data Freshness and Availability: Given that sensor networks are used to monitor time-sensitive events, it is important to ensure that the data provided by the network is current and available at all times. This means that an adversary can not replay old messages in the future. Moreover, data aggregation security requirements should be carefully implemented to avoid extra energy consumption. If no more energy is left, the data will no longer be available.

Non-repudiation: ensures that a transferred packet has been sent and received by a node claiming to have sent and received the packet. In secure aggregation schemes, once the aggregator sends the aggregation results, it should not be able to deny sending it. This gives the sink the opportunity to determine what causes the changes in the aggregation results.

2.2 Attacks against WSN aggregation

WSNs are vulnerable to different types of attacks [16] due to the nature of the transmission medium (broadcast), remote and hostile deployment location, and the lack of physical security in each node. However, the damage caused by these attacks varies in applications depending on the assumed threat model. Therefore, data aggregation must be done securely so as to prevent a deceptive reading of the state of the environment being monitored. In this section, we discuss about the attacks that might affect the aggregation in the WSN.

Node compromise: Current sensor hardware does not provide any resistance to physical tampering. If an adversary captures a node, they can easily extract the cryptographic primitives as well as exploit the shortcomings of the software implementation. This allows the adversary to launch attacks from within the system as an insider, bypassing encryption and password security systems. Considering the data aggregation scenario, the compromised nodes can successfully authenticate bogus reports to their neighbours, which have no way to distinguish bogus data from legitimate ones [8].

Denial of Service Attack: is a standard attack on the WSN by transmitting radio signals that interfere with the radio frequencies used by the WSN and is sometimes called jamming. As the adversary capability increases, it can affect larger portions of the network. In the aggregation context, an example of the DoS can be an aggregator that refuses to aggregate and prevents data from travelling into the higher levels.

Sybil attacks: refers to the scenario when a malicious node pretends to have multiple identities. For example, the malicious node can claim false identities, or impersonate other legitimate nodes in the network [16]. It affects aggregation schemes in different ways [15]. Firstly, an adversary may create multiple identities to generate additional votes in the aggregator election phase and select a malicious node to be the aggregator. Secondly, the aggregated result may be affected if the adversary is able to generate multiple entries with different readings. Thirdly, some schemes use witnesses to validate the aggregated data and data is only valid if n out of m witnesses agreed on the aggregation results. However, an adversary can launch a Sybil attack and generate n or more witness identities to make the base station accept the aggregation results.

Selective Forwarding Attack: In selective forwarding, a malicious node acts like a black hole and refuses to forward every packet. Adversary uses the compromised node to forward the selected messages. In the aggregation context, any compromised intermediate nodes have the ability to launch the selective forwarding attack and this subsequently affects the aggregation results.

Replay Attack: In this case an attacker records some traffic from the network without even understanding its content and replays them later on to mislead the aggregator and consequently the aggregation results will be affected.

Stealthy Attack: the adversary's goal is to make the user accept false aggregation results, which are significantly different from the true results determined by the measured values, while not being detected by the user.

2.3 Security challenges in Data Aggregation

Consequently, it is believed that a secure data aggregation is very challenging issue, and requires more attention during design process. According to the properties required by the application and according to the type of attack and the type of adversary, a secure data aggregation scheme should have as well as possible following properties:

Low communication overhead: the purpose of conducting aggregation is to reduce communication overhead. Thus a secure scheme should maintain this purpose.

Scalability: Secure aggregation techniques should provide high-security features for small networks, but also maintain these characteristics when applied to larger ones.

Flexibility: secure aggregation techniques should be able to function well in any kind of environments and support dynamic deployment of nodes.

Effectiveness: it is important to ensure the accuracy of the final aggregation result.

Generality: the secure aggregation scheme should apply to various aggregation function, such as MAX/MIN, MEAN, SUM, COUNT, and so forth.

Graceful Degradation: the designed mechanisms should be resilient to node compromise, and the performance of the networks degrades gracefully when aggregator and a small portion of the nodes are compromised.

3. Classification of secure aggregation schemes

Many innovative and intuitive secure aggregation schemes for WSNs have been proposed for solving the problem of security in sensor networks. In this section we survey these schmes and classify them into two classes: cryptographic-based secure data aggregation and trust-based secure data aggregation schemes. See figure 1.

3.1 Cryptographic-based secure aggregation

The security issues, such as data confidentiality and integrity in data aggregation become vital when the sensor network is deployed in a hostile environment. Most current research in securing data aggregation in WSNs, have been achieved through cryptographic scheme. We distingue two techniques: techniques based on concealed data (End-to-End privacy) and techniques based on revealed data (Hop-By-Hop privacy).

A. Techniques based on Concealed Data

Concealed data aggregation (CDA) is an improved version of the in-network aggregation, which in contrast to the classic Hop-by-Hop ensures the End-to-End privacy, i.e. encrypted values do not need to be decrypted for the aggregation. Instead, the aggregation is performed with encrypted values and only the sink can decrypt the result. The fundamental basis for CDA are cryptographic methods that provide the privacy homomorphism (PH) property. An encryption algorithm E() is homomorphic, if for given E(x) and E(y) one can obtain E(x*y) without decrypting x,y for some operation *. The concept was introduced by Rivest et al. [17] in 1978. The two most common variations of PHs are the additive PH and the multiplicative PH. The latter provides the property $E(x\times y)=E(x)\otimes E(y)$.

Girao et al. [18] propose a CDA scheme (CDAM) that is based on the PH proposed in [20]. They claimed that, for the WSN data aggregation scenario, the security level is still adequate and the proposed PH method can be employed for encryption.

Castelluccia et al. proposed a simple and provable secure additively homomorphic stream cipher (HSC) that allows for the efficient aggregation of encrypted data [19]. The new cipher replace the xor (Exclusive-OR) operation with modular addition and is therefore very well suited for CPU-constrained devices such as those in WSNs. The aggregation based on this cipher can be used to efficiently compute statistical values such as the mean, variance, and standard deviation of sensed data while achieving significant bandwidth gain. One limitation of this proposal is the important overhead and scalability problem that generates if the network is unreliable.

Recently, Önen et al. [21] and Castellucia [22] propose a new scheme that combines a PH and multiple encryptions, (PHM1 and PHM2). Theses two works are quite similar but were developed in parallel and independently. The homomorphic of the underlying encryption technique allows sensors to aggregate their cleartext measurements with the encrypted aggregate values whereas the multiple encryption scheme assure that aggregates values and individual measurements results remain oblivious to all intermediate nodes enroute to the sink. The joint use of the homomorphism and multiple encryption assures that a secret channel is established between every sensor node and the sink without having to establish pairewise security association or a public-key infrastructure. The proposed scheme assures the end-to-end confidentiality and scales efficiency. It improves the bandwidth performance of secure aggregation scheme described in [19] and allows resisting against *n* compromised nodes.

B. Techniques based on revealed data

Many protocols based on revealed data (hop-by-hop privacy) provide more efficient aggregation operation and highly consider data integrity.

Hu and Evans proposed the first secure data aggregation (SDA) protocol for WSNs that is resilient to both intruder devices and single device key compromises [23]. However, the protocol may be vulnerable if a parent and a child node in the hierarchy are compromised.

Przydatek et al. proposed a secure information aggregation (SIA) framework for sensor networks [24]. This framework provides resistance against stealthy attacks. It consists of three node categories: a home server, a base station, and sensor nodes. A base station is a resource enhanced node which is used as intermediary between the home server and the sensor nodes, and is also the candidate to perform the aggregation task. SIA assumes that each sensor has a unique identifier and shares a separate secret cryptographic key with both the home server and the aggregator. The keys enable message authentication and encryption if data confidentiality is required. Moreover, it assumes that the home server and base station can use a mechanism, such as μTESLA, to broadcast authentic messages. SIA consist of three parts: collecting data from sensors and locally computing the aggregation result, committing to the collected data, and reporting the aggregation result while providing the correctness of the result.

Çam et al. proposed an energy-efficient secure pattern based data aggregation (ESPDA) protocol for wireless sensor networks in [25,26]. ESPDA is applicable for hierarchy-based sensor networks. In ESPDA, a cluster head first requests sensor nodes to send the corresponding pattern code for the sensed data. If multiple sensor nodes send the same pattern code to the cluster head, only one of them is permitted to send the data to the cluster head. ESPDA is secure because it does not require encrypted data

to be decrypted by cluster heads in order to perform data aggregation.

Du et al. proposed a witness-based data aggregation (WDA) scheme for WSNs to assure the validation of the data sent from data fusion nodes to the base station [27]. In order to prove the validity of the fusion result, the fusion node has to provide proofs from several witnesses. A witness is one who also conducts data fusion like a data fusion node, but does not forward its result to the base station. Instead, each witness computes the message authentication code (MAC) of the result and then provides it to the data fusion node who must forward the proofs to the base station.

Discussion

The field of cryptography within in-network data processing is a very promising research field, and introduces many interesting challenges [7]. However, selecting the appropriate cryptography method for sensor nodes is fundamental to providing security services in WSNs. Symmetric key cryptography is commonly used in WSN, and is superior to public key cryptography in terms of speed and low energy cost.

In spite of the diversity and the proved efficiency of these solutions, many of them assume that the sensor nodes are trustworthy and reporting data truthfully. In practice though, sensors are usually deployed in open unattended environments, and hence are susceptible to physical tampering. When a node is compromised, the adversary can inject bogus data into the network. However, we argue that the conventional view of security based on cryptography alone is not sufficient for the unique characteristics and novel misbehaviours encountered in open networks. Even though cryptography can provide integrity, confidentiality, and authentication, it fails in the face of insider attacks. This necessitates a system that can cope with such internal attacks.

3.2 Trust-based secure data aggregation

As we cite above, WSNs are often deployed in unattended territories that can often be hostile, they are subject to physical capture by adversaries. A simple tamper-proofing is not a viable solution [10]. Hence, sensors can be modified to misbehave and disrupt the entire network. This allows the adversary to access the cryptographic material held by the captured node and allow the adversary to launch attacks from within the system as an insider, bypassing encryption and password security systems. The compromised nodes can successfully authenticate bogus reports to their neighbors, which have no way to distinguish false data from legitimate ones [8]. Trust and reputation systems have been proposed as an attractive complement to cryptography in securing WSNs. They provide the ability to detect and isolate both faulty and malicious nodes that are behaving inappropriately in the context of the specific WSN.

Recently, attention has been given to the concept of trust to increase security and reliability in Ad Hoc [32, 33] and sensor networks [35, 34]. The notion of trust to be used throughout this paper is briefly defined as: *trust is the degree of belief about the future behavior of other entities, which is based on the ones the past experience with and observation of the others actions*. Reputation is another complex notion that spans across multiple disciplines. It is quite different from but easily confused with trust.

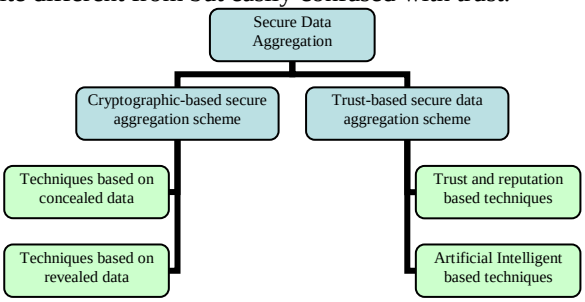

Figure 1: Classification of secure aggregation schemes

The mathematical foundation for reputation management is rooted in statistics and probability [39]. Furthermore, reputation is based on collection of evidence of good and bad behaviour undertaken by other entities. It is based on past experience with a given entity, whereas trust is not restricted to this. In this section, we study the proposed schemes based on trust and reputation for secure data aggregation in networks. We classify them into two categories: trust and reputation-based framework, and artificial intelligent- based framework.

A. Trust and reputation-based framework

In [28], the authors propose a trust based framework for secure data aggregation in WSN based on Bayesian model and beta distribution probability (TKL). They first evaluate trust in individual sensor nodes based on Kullback-Leibler (KL) distance or relative entropy. The idea is to calculate the distance between an ideal node behaviour and the actual node behaviour. The authors assign a confidence value to aggregated sensor data. Based on sensor data confidence, the framework computes an opinion which encompasses belief and uncertainty on the aggregation of sensor data by means of the consensus operator [37]. Nevertheless, this approach is still time-consuming for establishing a stable reputation on sensor nodes. The reputation on a node, based the inverse square of its KL distance, suffers from severe oscillation for the first reputation evaluation.

Hur et al. propose in [29] a trust-based aggregation scheme for WSN based on local trust evaluation (LTE). This local trust evaluation mechanism is suitable for resource-limited sensor networks. The trustworthiness of a node is computed based upon several trust evaluation factors, such as battery lifetime, sensing communication ratio, sensing result and consistency level. Each sensor node computes only their neighbour node's trust accumulatively. Prior to a data aggregation, sensor nodes elect an aggregator node in their own grid, which has the highest trust value among all the nodes in an identical grid by the majority of vote. A trust agreement process is necessary, because the trust value of a node is evaluated by its neighbour nodes, that is any node never know it's own trust value. Sensing data from multiple nodes are

aggregated in consideration of agreed trust values of member nodes per each grid. Deceitful data from malicious or compromised nodes whose trust value are lower than those of the other legal nodes can be excluded. One drawback of this scheme is that it considers that the trust evaluation is computed by only trustworthiness nodes.

Rabinovich et al. [30] propose a mechanism to detect and mitigate stealthy attacks against sensor networks by using distributed localized constraint validation and randomized routing (RTM). More specifically, they consider those applications of sensor networks where measurements are spatially correlated. This correlation is expressed in the form of measurement constraint. Sensors observe their neighbors during transmission and file "complaints" if their neighbours' data violate the constraint when compared with their own. Protection against compromised aggregators is achieved via construction of randomized delivery trees. Every time the SN sends data to the server it includes both current and small number of recent measurements. This allows the server to detect an attack when a fairly small fraction of sensors have been compromised. Based on complaints, the server uses a beta reputation system [36] to identify compromised sensors. In order to test the effectiveness of the scheme, authors

		CRYPTOGRAPHIC BASED SCHEMES								TRUST BASED SCHEMES			
		Concealed Data Techniques				Revealed Data Techniques				Trust and Reputation			IA
		CDAM [18]	HCS [19]	PHM1 [21]	PHM2 [22]	SDA [23]	SIA [24]	ESPDA [25,26]	WDA [27]	TKL [28]	LTE [29]	RTM [30]	IAF [31]
Security services	Confidentiality	*	*	*	*		*	*					
	Integrity					*	*		*				
	Authentication					*	*						*
	Freshness					*	*			*	*	*	*
	Availability			*						*	*	*	*
Attacks existence	Node compromise	*	*	*	*	*	*	*	*				
	DoS	*	*	*	*	*	*	*	*	*	*	*	*
	Selective forwarding			*	*	*	*		*				
	Sybil							*	*	*	*	*	*
	Stealthy					*			*				
Goal Design	Scalability			*	*			*			*		
	Overhead	high	high	high	high	low	low	low	low	low	low	high	high
	Flexibility	*		*	*								
	Effectiveness		*				*		*	*	*	*	
	Generality		*	*	*	*		*	*	*	*	*	*
	Graceful Degradation		*				*		*	*	*	*	*

Table1: a summary of comparison between secure data aggregation schemes.

developed a custom simulator to analyse the time to detect a compromised sensors, the fraction of compromised sensors successfully detected by the system, and the communication overhead introduced by the security protocol.

B. Artificial intelligent-based framework

Interest on applying Artificial Intelligence techniques on securing sensor network environments is rising. [11] Use offline neural network based learning technique to model spatial patterns in sensed data. [13] applies reinforcement learning techniques for intrusion detection. [14] and [12] base their detection systems on multi-agent systems. The critical issue of aggregation, however, is not taken into consideration by any of these researches.

In [31] the authors propose the first mechanism (IAF) that combines statistics and artificial intelligence techniques for robust detection of malicious nodes in a sensor network environment without unnecessarily eliminating honest nodes, e.g., the descendants of a malicious node. In particular, hypothesis testing mechanisms are used by a child node to estimate the probability of error reporting by a child node over one data reporting epoch, while reinforcement learning schemes are used to update such reputation over successive epochs. The use of straightforward statistical techniques is not sufficient for error monitoring in sensor networks. Due to variations in the environment and intrinsic sensing error characteristics, there can be significant short-range deviations between data reported by one node and its siblings. Hence significant tests may observe deviations between individual reported values and aggregates reported by parent nodes for a given epoch. To create a more robust system, reputations must be accumulated over successive epochs, and only if consistent deviations are observed should a parent node be labelled to be malicious. One drawback of this scheme is that it cannot detect unbiased errors introduced by the aggregator node. A very high learning rate can increase detection but also introduce unacceptable false positives.

Discussion

Building a robust trust and reputation system presents several important challenges on its own [10]. The most pressing is the possibility that a malicious node that participates in the reputation system can prevent it from functioning by lying. A compromised node can falsely accuse well-behaving nodes of malicious actions or falsely praise bad-behaving nodes (pollution reputation). To maintain its integrity the reputation system must be able to

prevent these kinds of attacks. Another important issue when building reputation is determining when a node has performed a malicious action and being able to distinguish it from natural failures. Due to the uncertain nature of WSN environment, such as collisions on the wireless channel, it is not always possible to distinguish these two kinds of erroneous behaviours.

4. Performance Comparison

This section, attempts to compare the secure data aggregation schemes that were reviewed in the last section. Comparison of security schemes can be difficult since the designers solve secure aggregation from different angles. Therefore, these schemes are compared in a number of different ways: security services provided (confidentiality, integrity, authentication, freshness and availability), goal design (scalability, generality), and resilience against attacks described in section 2.2. We summarise this comparison in table 1.

Since the assumed adversary varies from one scheme to other, each proposed scheme has different requirements. In cryptographic based scheme, the data confidentiality represents the minimum security requirements. As we see in table, the techniques based on revealed data provide more efficient aggregation operation in term of overhead and highly consider data integrity. However, they represent weaker model of data confidentiality perspective than techniques based on concealed data. However, in trust based scheme, the availability and the network lifetime are the principle concern and should be provided as well as possible.

We notice that all the proposed schemes based on cryptography are vulnerable to DoS and physical attacks, while all the trust based schemes are vulnerable to DoS and Sybil attacks.

As for the design goal, there is no scheme which is perfect. Each proposal has its advantages and its limitations. A tradeoff between security level and performance must be carefully balanced.

5. Conclusion

Sensor networks are vulnerable to insider and outsider attacks much more than other wireless networks for the reasons discussed in section 2. When designing a security protocol it is important to understand the dangerous and damaging effects these attacks can have so that the protocol can guard against them. Secure data aggregation in wireless sensor networks is a critical issue that has been addressed through many proposed schemes. These proposals are classified into two categories: cryptographic based scheme and trust based scheme.

Some promising results have been recently achieved in secure data aggregation. They are based on advanced cryptographic concepts, such as privacy homomorphism. Despite of the diversity and the proved efficiency of these solutions, many of them assume that the sensor nodes are trustworthy and reporting data truthfully. Even though cryptography can provide integrity, confidentiality, and authentication, it fails in the face of insider attacks. Another important issue is related to assessment of trustworthiness and reliability of the data provided by WSNs. However, this issue is still in its infancy, and there are not clear trust evaluation models which can be applied to sensor networks properly.

This paper provides an overview of theses techniques, each of which offers different advantages and disadvantages. A balance between the requirements and resources of a WSN determines which technique should be employed. We notice that no secure aggregation technique is ideal to all the scenarios where sensor networks are used; therefore the techniques employed must depend upon the requirements of target application and resources of each individual sensor network.

Despite of potentially great importance and very interesting theoretical and practical challenges, the topic of secure data aggregation in wireless sensor networks have received until recently much less attention than, e.g., secure routing or key management. Therefore, despite of many interesting initial results, the security questions related to data aggregation in WSN remain largely open, and in our opinion constitute an interesting area for further research.

Reference

[1] O. Moussaoui, A. Ksentin, M. Naimi and M. Gueroui, " a novel clustering algorithm for efficient energy saving in wireless sensor networks" in the 7th IEEE International Symposium on Computer networks (ISCN'06), Istanbul, Turkey, June 2006.

[2] T.A Zia and A.Y Zomaya, "A security framework for wireless sensor networks". In Proceedings of the IEEE Sensor Applications Symposium (SAS) , Houston, Texas, February 7-9, 2006.

[3] H. Wenbo, L. Xue, N. Hoang, K. Nahrstedt And T. Abdelzaher, "PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks", In 26th IEEE International Conference on Computer Communications, (INFOCOM), Anchorage, AK, May 2007, pp. 2045-2053

[4] N. Xu, S. Rangwala, K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A Wireless Sensor Network for Structural Monitoring,", In Proceedings of the ACM Conference on Embedded Networked Sensor Systems, Baltimore, MD, November 2004.

[5] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, "SPINS: Security protocols for sensor network", Wireless Networks, 2002, vol. 8, no. 5, pp. 521-534.

[6] R. Rajagopalan and P. K. Varshney, "Data aggregation techniques in sensor networks: A survey", In Communications Surveys & Tutorials, IEEE, Fourth Quarter 2006, Vol. 8, Issue 4, pp 48-63.

[7] A.Sorniotti, L.Gomez, K.Wrona and L.Odorico "Secure and trusted in-network data processing in wireless sensor networks: a survey", JIAS, Journal of Information Assurance and Security, September 2007, Vol. 2, Issue 3.

[8] A. Perrig, J. Stankovic, D.Wagner, "Security in Wireless Sensor Networks", Communication of the ACM, June 2004.

[9] B. Warneke, K.S.J. Pister, "MEMS for Distributed Wireless Sensor Networks," 9th Int'l Conf on Electronics, Circuits and Systems, Dubrovnik, Croatia, September 2002.

[10] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN), October 2004 , pp. 66-77.

[11] P.Mukherjee and S.Sen, “Detecting malicious sensor nodes from learned data patterns”, In Proceedings of the Workshop on Agent Technology for Networks, 2007, pp. 11-17.

[12] R. M. Ruairi and M. T. Keane, “An energy-efficient, multi-agent sensor network for detecting diffuse events”, In IJCAI, 2007, pp. 1390–1395.

[13] A. L. Servin and D. Kudenko, “Multi-agent reinforcement learning for intrusion detection”, In Adaptive Learning Agents and Multi Agent Systems, 2007, pp. 158–170.

[14] J. Wu, C. jun Wang, J. Wang, and S. fu Chen, “Dynamic hierarchical distributed intrusion detection system based on multi-agent system”, In Proceedings of the 2006 IEEE/WIC/ACM international conference on Web Intelligence and Intelligent Agent Technology, Washington, DC, USA, 2006, pp. 89–93.

[15] H. Alzaid, E. Foo And J.M Gonzalez. “secure data aggregation in wireless sensor networks: a survey” In L. Brankovic and M.Miller, editors, Sixth Australasian Information Security Conference (AISC) Wollongong, NSW, Australia, 2008, vol. 81 of CRPIT, pp. 93-105.

[16] T. Roosta, S. Shieh, And S. Sastry, “Taxonomy of security attacks in sensor networks”, In ‘The First IEEE International Conference on System Integration and Reliability Improvements’, IEEE International, Washington, DC, USA, 2006.

[17] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On Data Banks and Privacy Homomorphisms,”, In Foundations of Secure Computation, New York: Academic, 1978, pp. 169–79.

[18] J. Girao, D. Westhoff, and M. Schneider, “CDA: Concealed Data Aggregation for Reverse Multicast Traffic wireless Sensor Networks,” In Proceeding IEEE Int’l. Conf. Commun. , Seoul, Korea, May 2005.

[19] C. Castelluccia, E. Mykletun, and G. Tsudik, “Efficient Aggregation of Encrypted Data Wireless Sensor Network,” In Proceeding .ACM/IEEE Mobiquitous, San Diego, CA, July 2005.

[20] J. Domingo-Ferrer, “A Provably Secure Additive and Multiplicative Privacy Homomorphism,” Lecture Notes Comp. Sci., vol. 2433, 2002, pp. 471–83.

[21] M. Onen and R. Molva, “Secure data aggregation with multiple encryption” 4th European conference on Wireless Sensor Networks, Delft, The Netherlands, January 29-31, 2007, Also published as LNCS Vol. 4373 , pp 117-132.

[22] C.Castellucia, “Securing very dynamic groups and data aggregation in wireless sensor networks”, IEEE International Conference on Mobile Adhoc and Sensor Systems, (MASS), Pisa, Italy, October 2007, pp. 1-9.

[23] L. Hu and D. Evans, “Secure aggregation for wireless networks”, In Proceeding Of Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 2003.

[24] B. Przydatek, D. Song, and A. Perrig, “SIA : Secure information aggregation in sensor networks”, In Proceeding Of SenSys’03, Los Angeles, CA, Nov 5-7, 2003.

[25] H. Çam, D. Muthuavinashiappan, and P. Nair, “ESPDA: Energy Efficient and Secure Pattern-Based Data Aggregation for Wireless Sensor Networks,” In Proceding IEEE Sensors, Toronto, Canada, Oct. 2003, pp. 732–36.

[26] H. Çam, D. Muthuavinashiappan, and P. Nair, “Energy-Efficient Security Protocol for Wireless Sensor Networks,”, In Proc.IEEE VTC Conf., Orlando, FL, Oct. 2003, pp. 2981–84.

[27] Du, W., Deng, J., Han, Y. S. & Varshney, P. A witness-based approach for data fusion assurance in wireless sensor networks, In ‘IEEE Global Communications Conference (GLOBEC*OM)*, 2003, Vol. 3, pp. 1435– 1439.

[28] W. Zhang, S. Das and Y. Liu, A trust based framework for secure data aggregation on wireless sensor networks. In Proceedings of th 3rd Annual IEEE Communications Society and Networks (SECON), 2006, pp. 60-69.

[29] J. H. Junbeom , L. Yoonho, H. Seongmin, Y. Hyunsoo, “Trust-based aggregation in wireless sensor networks”, *International Conference on Computing, Communications and Control Technologies*, July 2005.

[30] P. Rabinovich, R. Simon, “Secure aggregation in sensor networks using neighbourhood watch” , In IEEE International Conference, Glasgow, June 2007, pp. 1484-1491.

[31] A. Gursel, O. Mistry, S. Sandip, “ Robust Trust Mechanisms for Monitoring Aggregator Nodes in Sensor Networks”, Int. Workshop on Agent Technology for Sensor Networks (ATSN-08), Estoril, Portugal, May 2008.

[32] S. Buchegger and J. L. Boudec, “Performance analysis of the CONFIDANT protocol,” In Proceeding in 3rd ACM int. symp. Mobile ad hoc networking & computing, 2002.

[33] P. Michiardi and R. Molva, “CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks,” 2001.

[34] A. Srinivasan, J. Teitelbaum, and J. Wu, “DRBTS: Distributed Reputation-based Beacon Trust System,” In 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC’06), 2006.

[35] S. Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN ’04), October 2004, pp. 66-77.

[36] A. Jsang and R. Ismail, “The Beta Reputation System”, In Proceedings of the 15th Bled Electronic CommerceConference, June 2002.

[37] Audun Joang, A logic for uncertain probabilities. Int. J. Uncertain. Fusiness Knowl-based system, 9(3):279-311, 2001

[38] S. Peter, K.Piotrowski, and P. Langndoerfer. “On concealed data aggregation for aggregation for wireless sensor networks”, In Proceedings of the IEEE Consumer Communications and Networking Conference, January 2007.

[39] P. Robinson and M. Beigl, “Trust context spaces: An infrastructure for pervasive security”, In Proceedings of the first International Conference on Security in Pervasive Computing, 2003.

[40] R.Rajagopalan and P.K Varshney “data aggregation techniques in sensor networks: a survey”, communications surveys and tutorials IEEE, 2006.