A Survey on Secure Data Aggregation Scheme for Wireless Sensor Networks

G.Prabhu[1], K.A.Dhamotharan[2]

Abstract— **Wireless sensor network is a collection of large number of sensor nodes that are communicating using wireless medium. Sensor nodes are resource constrained in battery power, computational capability, communication capability, memory. Data Aggregation scheme is the most practical technique that reduces large amount of transmission of bits in wireless sensor network. Security is an important criterion to be considered because, wireless sensor nodes are deployed in a remote or hostile environment area that is prone to attacks easily. So data aggregation and security are essential for WSN. Homomorphic Encryption can be applied to conceal communication such that enciphered data can be aggregated algebraically without decryption. Many secure aggregations are proposed in wireless sensor network. But due to security and resource constrained nature, secure data aggregation also need new approaches. In this survey we are going to compare existing secure data aggregation protocol and their limitations and advantages.**

Index Terms—**Data aggregation, Encryption, Sensor nodes,Wireless Sensor Networks**

I. INTRODUCTION

Wireless sensor networks(WSN) consist of thousands of sensor nodes (SN) that gather data from deployed environments. Currently, there are plenty of rich applications proposed for WSNs, such as environment monitoring, accident reporting, and military investigation. Depending on the purpose of each application, SN are customized to read different kinds of data (e.g., temperature, light, or smoke). Typically, SN are restricted by the resources due to limited computational power and low battery supply. Thus, energy saving technologies must be considered when we design the protocols. For a better energy utilization, cluster-based WSNs have been proposed. In cluster-based WSNs, SN resident in nearby area would form a cluster and select one among them to be their cluster head (CH). The CH organizes data pieces received from SN into an aggregated result, and then forwards the result to the base station based on regular routing paths. Generally, aggregative operations are algebraic, such as the addition or multiplication of received data, or statistical operation, such as a median, a minimum, or a maximum of a data set. Although data aggregation could significantly reduce transmission, it is vulnerable to some attacks. For instance, compromising a CH will allow adversaries to forge aggregated results as similar as compromising all its cluster members. Concealed Data Aggregation utilizes the privacy homomorphism encryption (PH) to facilitate aggregation in encrypted data. By leveraging the additive and multiplicative homomorphism properties, CHs are able to execute algebraic operations on encrypted numeric data. Hence we adopted several public key-based PH encryptions to construct the systems.

II. AGGREGATION MODEL

In WSNs, SN collect information from deployed environments and forward the information back to base station (BS) via multihop transmission based on a tree or a cluster topolgy. The accumulated transmission carries large energy cost for intermediate nodes. To increase the lifetime, tree-based or cluster networks force the intermediate nodes (a subtree node or a cluster head) to perform aggregation, i.e., to be aggregators (AG). After aggregation done, AGs would forward the results to the next hop. In general, data can be aggregated via algebraic operations (e.g. ,addition or multiplication) or statistical operations (e.g., median, minimum, maximum, or mean). For example, an AG can simply forward the sum of numerical data received instead of forwarding all data to the next hop.

ISSN: 2278 – 7798

III. ATTACK MODEL

First of all, we categorize the adversary's abilities as follows:

- Adversaries can eavesdrop on transmission data in a WSN.
- Adversaries can send forged data to any entities in a WSN (e.g., SN, AG, or BS).
- Adversaries can compromise secrets in SNs or AGs through capturing them.

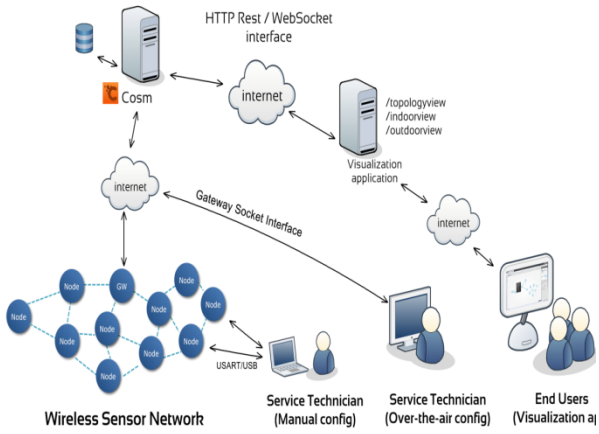

Figure1.Wireless Sensor Networks

IV. RESEARCH ISSUES IN AGGREGATION AND ATTACK MODEL

In this paper, we have analyzed some methods Secure data aggregation over Wireless Sensor Networks as follows:

A. Security in Wireless Sensor Networks

Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks. Sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects,and other properties . In case of wireless sensor network, the communication among the sensors is done using wireless transceivers.The attractive features of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus. In this paper[6], we explore the security issues and challenges for next generation wireless sensor networks and discuss the crucial parameters that require extensive investigations.

B. Secure Information Aggregation in Sensor Networks

Sensor networks promise viable solutions to many monitoring problems. However, the practical deployment of sensor networks faces many challenges imposed by real-world demands. Sensor nodes often have limited computation and communication resources and battery power. Moreover, in many applications sensors are deployed in open environments, and hence are vulnerable to physical attacks, potentially compromising the sensor's cryptographic keys. One of the basic and indispensable functionalities of sensor networks is the ability to answer queries over the data acquired by the sensors. The resource constraints and security issues make designing mechanisms for information aggregation in large sensor networks particularly challenging. A novel framework for secure information aggregation in large sensor networks[7]. In our framework certain nodes in the sensor network, called aggregators, help aggregating information requested by a query, which substantially reduces the communication overhead. By constructing efficient random sampling mechanisms and interactive proofs, we enable the user to verify that the answer given by the aggregator is a good approximation of the true value even when the aggregator and a fraction of the sensor nodes are corrupted. In particular, we present efficient protocols for secure computation of the median and the average of the measurements, for the estimation of the network size, and for finding the minimum and maximum sensor reading. Our protocols require only sublinear communication between the aggregator and the user. To the best of

ISSN: 2278 – 7798

our knowledge, this paper is the first on secure information aggregation in sensor networks that can handle a malicious aggregator and sensor nodes.

C. Energy Efficient Secure Pattern Based Data Aggregation for WSN

Data aggregation in wireless sensor networks eliminates redundancy to improve bandwidth utilization and energy-efficiency of sensor nodes. This paper[2] presents a secure energy-efficient data aggregation protocol called ESPDA (Energy-Efficient Secure Pattern based Data Aggregation). Unlike conventional data aggregation techniques, ESPDA prevents the redundant data transmission from sensor nodes to cluster-heads.If sensor nodes sense the same data, ESPDA first puts all but one of them into sleep mode and generate pattern codes to represent the characteristics of data sensed by sensor nodes. Cluster-heads implement data aggregation based on pattern codes and only distinct data in encrypted form is transmitted from sensor nodes to the base station via cluster-heads. Due to the use of pattern codes, cluster-heads do not need to know the sensor data to perform data aggregation, which allows sensor node to establish secure end-to-end communication links with base station. Therefore, there is no need for encryption/decryption key distribution between the cluster-heads and sensor nodes. Moreover, the use of NOVSF Block-Hopping technique improves the security by randomly changing the mapping of data blocks to NOVSF time slots. Performance evaluation shows that ESPDA outperforms conventional data aggregation methods up to 50% in bandwidth efficiency. Such sensor networks are expected to be widely deployed in a vast variety of environments for commercial, civil, and military applications such as surveillance, vehicle tracking, climate, medical, and acoustic data gathering. The key limitations of wireless sensor networks are the storage, power and processing. These limitations and the specific architecture of sensor nodes call for energy efficient and secure communication protocols.

D. Secure Reference Based Data Aggregation Protocol for Wireless Sensor Networks

Data aggregation in wireless sensor networks is crucial due to its enhancement of bandwidth usage and energy utilization by minimizing the transfer of redundant data. This paper[8] presents a secure data aggregation protocol, called SRDA, for wireless sensor networks. In order to reduce the number of bits transmitted, SRDA requires sensor nodes to send differential data instead of raw sensed data. Effectiveness of the SRDA is further demonstrated by applying its key mechanism to enhance existing data aggregation protocols. SRDA establishes secure connectivity among sensor nodes by taking advantage of deployment estimation and not performing any online key distribution. The incremental security requirement due to the nature of the data aggregation process is met by an aggregation specific security technique. Simulation results show that SRDA yields significant savings in the energy consumption while preserving the data security. Wireless sensor networks have emerged as a popular research area with the advances in the sensor technology and reductions in the cost of sensor hardware. Wireless sensor networks usually contain a large number of nodes and provide the global view of the phenomena observed from monitored area by combining the local measurements of individual nodes. A wireless sensor network is a collaborative network in which nodes both perform their sensing task and if necessary, function as relay for transferring the data of other nodes. The main traffic flow in a wireless sensor network is from the sensor nodes to the base station. Optionally, an interest can be flooded from the user to the sensor nodes in the region of interest. Nodes can also communicate locally with each other for sensing tasks, cluster formation and scheduling active/sleep times of nodes. These networks provide long lived and autonomous systems for environmental monitoring in military operations and life sciences, tracking vehicles or animals, airport surveillance, telemedicine and smart home applications.

E. Classify Encrypted Data in Wireless Sensor Networks

End-to-end security mechanisms like SSL, which are popular on Internet, may seriously limit the capability of In network processing that is the most critical function in sensor network. Since supporting In-network processing can significantly improve the performance of extremely resource-constraint sensor networks featuring many-to-one traffic pattern. It is an open problem of how to protect the traffics and to support In-network processing at the same time. This paper[10] tackles the problem by proposing a model of categorizing encrypted messages in wireless sensor networks. A classifier, an intermediate sensor node in our setting, is embedded with a set of searching keywords in encrypted format. Upon receiving an encrypted message, it matches the

ISSN: 2278 – 7798

message with the keywords and then processes the message based on certain policies such as forwarding the original message to the next hop, updating it and forwarding or simply dropping it on detecting duplicates. The messages are encrypted before being sent out and decrypted only at its destination. Although the intermediate classifiers can categorize the messages, they learn nothing about the encrypted messages except several encrypted keywords, even the statistic information. The presented scheme is efficient, flexible and resource saving. The performance analysis shows that the computational cost and communication cost are minimized. Furthermore, it is resilient to node capture attack and many other kinds of attacks. Wireless appliances will be dominant in the near future. Many kinds of wireless technique have been used or proposed, such as GSM, GPRS, 3G, Bluetooth and 802.11b. Of the whole wireless family, one emerging wireless standard, 802.15.4, is currently being proposed, which is foreseen as the new specification for wireless sensor network.

F. Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks

Routing in wireless sensor networks is different from that in commonsense mobile ad-hoc networks. It mainly needs to support reverse multicast traffic to one particular destination in a multihop manner. For such a communication pattern, end-to-end encryption is a challenging problem. To save the overall energy resources of the network, sensed data needs to be consolidated and aggregated on its way to the final destination. It conceals sensed data end-to-end by and still providing efficient and flexible in-network data aggregation[9]. The aggregating intermediate nodes are not required to operate on the sensed plaintext data. We apply a particular class of encryption transformations and discuss techniques for computing the aggregation functions "average" and "movement detection." We show that the approach is feasible for the class of "going down" routing protocols. The risk of corrupted sensor nodes by proposing a key redistribution algorithm that limits an attacker's gain and show how key pre distribution and a key-ID sensitive "going down" routing protocol help increase the robustness and reliability of the connected backbone. One major application scenario for a WSN is to monitor environmental data and to transmit it to a central point. Here, the data is analyzed and eventually serves to initiate some specific action. Analysis in most scenarios presumes computation of an optimum, such as the minimum or maximum, the computation of the average, or the detection of a certain movement pattern. These computations may either occur at a central point or in the network itself. The latter has the advantage of reducing the amount of data transmitted over wireless connections. Since the energy consumption increases linearly with the amount of transmitted data, an aggregation approach helps increase the WSN's overall lifetime. Another approach toward saving energy is to only maintain a connected backbone of nodes forwarding traffic, while the remaining nodes persist in sleep mode until they are reactivated

G. Secure Aggregation for Wireless Networks

Emerging class of important applications uses ad hoc wireless networks of low-power sensor devices to monitor and send information about a possibly hostile environment to a powerful base station connected to a wired network. To conserve power, intermediate network nodes should aggregate results from individual sensors. However, this opens the risk that a single compromised sensor device can render the network useless, or worse, mislead the operator into trusting a false reading. Wireless sensor networks are emerging technologies that have a wide range of potential applications such as battlefield surveillance and emergency response. Research on sensor networks generally assumes a trusted environment, but in many likely sensor network applications, the network will be deployed in situations where an adversary may be motivated to disrupt the function of the network. An adversary may be able to position several intruder nodes within the network and use them to transmit false messages. Further, an adversary may compromise a node in the network and gain access to its key material. In this paper[4], we focus on an adversary who wants to corrupt the information being produced by the sensor network. We regard confidentiality of the messages themselves to be unnecessary and focus only on the integrity of the results transmitted to the base station.

H. Public Key based Crypto Schemes for Data Concealment in WSN

Wireless sensor networks (WSNs) are becoming increasingly popular in many spheres of life. Application domains include monitoring of the environment (such as temperature, humidity, entity movement and seismic activity) as well as numerous other ecological, law enforcement and military settings. Due to the limited amount of

ISSN: 2278 – 7798

power a sensor is deployed with, the technique of data aggregation is commonly employed in an effort to minimize the amount of data that needs to be transmitted. It is a method which consists in condensing the sensed values according to a specific application and does not aim at reconstructing all the values at the receiver. By using data aggregation and in-network processing, the network can converge to a single result, such as, for example, the average, variance, minimum or maximum of the sensed values. This method can also be applied in certain points of the network, that store the values sensed over a region and time. Since applications often do not require every individual aggregated value, we can also aggregate for long-term storage, thus minimizing the amount of storage space required. In this work we consider data privacy issues between readers, aggregators and the sensors themselves. We aim at providing end-to-end encryption of sensors' measurements as they are aggregated in the network via hop-by-hop transmission[5]. We attempt to achieve the highest level of security possible, while taking power consumption and platform specific limitations as the major metric for the overall system.

I. Evaluating 2-DNF Formulas on Ciphertext

Secure computation allows several parties to compute a function of their joint inputs without revealing more than what is implied by their own inputs and the function outcome. Any polynomial time functionality can be computed by a secure protocol, requiring polynomial resources. These seminal results are obtained by a generic transformation that converts an insecure computation of a functionality to a secure version (often referred to as the 'garbled circuit' transformation). Secure protocols generated from the garbled circuit transformation typically have poor efficiency. In particular, the communication complexity of the resulting protocols is proportional to the size of a circuit evaluating the functionality, and hence precludes sub-linear communication protocols. The result is that unless circuits are very small, the garbled circuit transformation is seldom used in protocols. To avoid using the garbled circuit transformation, researchers have sought for tools that give more efficient protocols for specific functionalities. Homomorphic encryption enables "computing with encrypted data" and is hence a useful tool for secure protocols[1]. Current homomorphic public key systems have limited homomorphic properties: given two ciphertexts Encrypt(PK, x) and Encrypt(PK, y), anyone can compute either the sum Encrypt(PK, x+y), or the product Encrypt(PK, xy), but not both.1 The problem of constructing 'doubly homomorphic' encryption schemes where one may both 'add and multiply' is a long standing open question already mentioned by Rivest.

J. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack

A new public key cryptosystem that is provably secure against adaptive chosen cipher text attack . The scheme is quite practical, requiring just a few exponentiations over a group. Moreover, the proof of security relies only on a standard intractability assumption, namely, the hardness of the Hellman decision problem in the underlying group. The hardness of the Diffie-Hellman decision problem is essentially equivalent to the semantic security of the basic El Gamal encryption scheme.Thus, with just a bit more computation, we get security against adaptive chosen ciphertext attack, whereas the basic El Gamal scheme is completely insecure against adaptive chosen ciphertext attack. Actually, the basic scheme we describe also requires a universal one-way hash function.In a typical implementation, this can be efficiently constructed without extra assumptions; however, we also present a hash-free variant as well. While there are several provably secure encryption schemes in the literature, they are all quite impractical. Also, there are several practical cryptosystems that have been proposed, but none of them has been proven secure under standard intractability assumptions. The significance of our contribution [3] is that it provides a scheme that is provably secure and practical at the same time. There appears to be no other encryption scheme in the literature that enjoys both of these properties simultaneously.

ISSN: 2278 – 7798

Table 1: Comparison of Secure Data Aggregation Algorithms

Scheme	Algorithm	Description	Advantage	Disadvantage
Secure Information Aggregation	A novel framework	A novel framework for secure information aggregation in large sensor networks.	It provides security to data based on RSA scheme, High Efficiency, Reliability	It Does not any Acknowledgement scheme and without any Randomization
Security	Ensuring layered and robust security	The inclusion of wireless communication technology also incurs various types of security threats.	It provides to control their attacks and reliability	It Does not control the malicious Behavior Attacks
Aggregation	Robust Sensory Input	To conserve power, intermediate network nodes should aggregate results from individual sensors	High level security	Low level Energy Efficiency
Data aggregation	Secure Reference-Based Data Aggregation	SRDA requires sensor nodes to send differential data instead of raw sensed data.	High level of Reliability	Secured without any authentications
Wireles Sensor Networks	Encryption Algorithm	The messages are encrypted before being sent out and decrypted only at its destination.	High level of throughput and energy level	It does not provide any authentication
Multicast Traffic in Sensor Networks	Key Redistribution algorithm	Key redistribution algorithm that limits an attacker's gain and show how key pre distribution	It provides to control their attacks and reliability	It Does not control the malicious Behavior Attacks
Concealed Data Aggregation	Reverse Multicast Traffic	Applications for wireless sensor networks are envisioned to be on the biomedical sector and even on monitoring the health status of cattle stocks.	It control the energy level and Battery Power	Secured without any authentications
Data Concealment	Public Key Based Cryptography	It is a method which consists in condensing sensed values according to specific application and does not aim at reconstructing all the values at the receiver.	Secured level and authentication	It does not provide any randomization techniques

ISSN: 2278 – 7798

Converge cast Traffic	Encryption Algorithm	The sensor nodes themselves are preferably cost-cheap, tiny, and consisting application-sensors	High level of energy and battery level	Encryption is used only for tiny network

V. CONCLUSION

This paper conducts a theoretical analysis study on secure data aggregation over wireless sensor networks. A brief discussion of those techniques is summarized. The advantages and limitations of different security mechanisms are summarized with reference to various issues related to secure data aggregation over wireless sensor networks.

REFERENCES

[1] D.Boneh, E.Goh , and K.Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," Proc. Second Int'l Conf. Theory of Cryptography (TCC), vol. 3378, pp. 325-341,2005.

[2] H.Cam., S.Ozdemir., P.Nair., D.Muthuavinashiappan., and H.O.Sanli., "Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks," Computer Comm., vol. 29, no. 4, pp. 446-455,2006

[3] R.Cramer and V.Shoup, "A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack," Proc. 18th Ann. Int'l Cryptology Conf. Advances in Cryptology, pp. 13-25,1998.

[4] L.Hu and D.Evans,"Secure Aggregation for Wireless Networks," Proc. Symp. Applications and the Internet Workshops, pp. 384-391,2003.

[5] E.Mykletun, J.Girao, and D.Westhoff,(2006), "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm. (ICC '06), vol. 5.

[6] A.Perrig, J.Stankovic, and D.Wagner, "Security in Wireless Sensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57,June 2004

[7] B.Przydatek, D.Song, and A.Perrig "SIA: Secure Information Aggregation in Sensor Networks," Proc. First Int'l Conf. Embedded Networked Sensor Systems, pp. 255-265,2003

[8] H.Sanli, S.Ozdemir, and H.Cam, "SRDA: Secure Reference-based Data Aggregation Protocol for Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf. (VTC '04-Fall), vol. 7,2004

[9] D.Westhoff, J.Girao, and M.Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation," IEEE Trans. Mobile Computing, vol. 5, no. 10, pp. 1417-1431,Oct.2006.

[10] Y.Wu, D.Ma, T.Li, and R.H.Deng, "Classify Encrypted Data in Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf., pp. 3236-3239,2004.

AUTHOR's PROFILE:

1. G.PRABHU
PG Scholar,
Department of Computer Science Engineering,
Erode Sengunthar Engineering College.

2. K.A.DHAMOTHARAN
Assistant Professor (Senior Grade),
Department of Computer Science Engineering,
Erode Sengunthar Engineering College.

ISSN: 2278 – 7798