A Review on Secure Group Key Management Schemes for Data Gathering in Wireless Sensor Networks

M. B. Apsara
Information Science and Engineering Department
J.S.S Academy of Technical Education
Bangaluru, India
iseapsaramba@gmail.com

P. Dayananda
Information Science and Engineering Department
J.S.S Academy of Technical Education
Bangaluru, India
dayanandap@gmail.com

C. N. Sowmyarani
Computer Science and Engineering Department
RV College of Engineering
Bangaluru, India
sowmyaranicn@rvce.edu.in

***Abstract*—Wireless Sensor Networks (WSNs) is a fast-emerging technology which has become an integral part of the research. WSNs have various applications covering military, environment monitoring, health care, surveillance, national security, etc. Due to the inherent nature of wireless communication, such types of networks are more vulnerable to security attacks, and the authentication and confidentiality of wireless networks are much more critical. WSNs needs include efficient clustering methods, data aggregation methods, data compression methods, data encryption and authentication methods, and data gathering methods. WSNs are more vulnerable to attacks due to their ad hoc nature, so the design of a good key management scheme to provide security is necessary. In this paper, different methods of clustering, data aggregation, data compression, data encryption and authentication, and data gathering are analyzed. A survey is conducted on the key management schemes of WSNs.**

Keywords-Wireless Sensor Networks (WSNs); data compression; data aggregation; data gathering; clustering; key management

I. INTRODUCTION

Wireless sensor networks are a simple and economic approach in deploying monitoring and control devices. Such networks can be deployed easily and economically in any type of application environment where sensor nodes sense their surroundings. WSNs are typically self-healing and self-organizing in nature. They organize themselves to maintain communication between the nodes of the network. The network sensors sense environmental parameters such as temperature, humidity, pressure, acoustic vibrations, mechanical stress, and more. Due to the finite battery power and low computing capacity of the sensors, their main need is to design protocols which perform computing with less energy. A WSN consists of a number of nodes which are battery driven devices. Basically, they perform the following tasks: they sense the physical quantity from the surroundings where they are deployed, they process the acquired data, and they transfer the data through wireless communication to data collection points which are called base stations, destinations or sink nodes. Self-organizing means that the network allows newcoming nodes to automatically join the network. Some of the basic topologies they use are star, mesh, and point to point.

In WSN security, data confidentiality is the most important requirement. To achieve this, malicious nodes should not have access to the network. Due to the nodes' limited energy and resources, many secure cluster-based protocols have been developed for routing. To achieve the security requirements, an efficient scheme for group key management is needed. Energy is one important concern in WSNs. Here, wireless transfer plays a vital role in energy consumption, so data gathering techniques (tree based, cluster based, or chain based). are a significant part of the wireless communication. Aggregation methodology also reduces energy consumption in data transferring. A WSN usually consists of a sink node and many small sensor components. Aggregation methodologies reduce the traffic in the network. The main points in network security are data confidentiality and data integrity. By using the existing encryption, end to end confidentiality can be achieved. In data gathering process, a malicious node may communicate with the valid nodes which may compromise the entire network. So, it is necessary to develop an efficient key management scheme.

Key management is mainly classified into static and dynamic. In the static key management schemes all the keys are pre-distributed in the sensor nodes and then each node chooses a set of keys from a key pool. In dynamic key management schemes some keys or key seeds are redistributed, and the session keys are established on demand. Figure 1 shows an overview of the Secure Group Key Management Scheme for data gathering in WSN. Initially, the network is set up and by using an efficient clustering algorithm a cluster head is selected for each cluster. Then, the data sensed by the sensors are aggregated by existing data aggregation methods. To reduce the size of the data to be transferred, data compression is used. Data encryption is done for security purposes. Finally, by using efficient data gathering methods, the data are gathered at the base station. To perform the above operation, a secure group key management is necessary.

Corresponding author: P. Dayananda

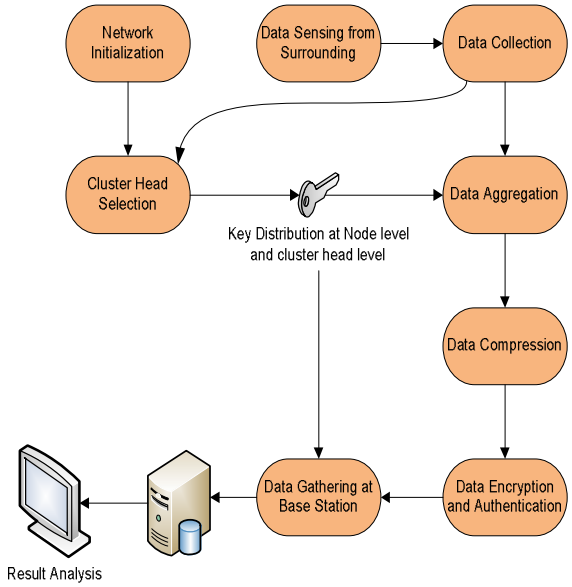

Fig. 1. Overview of the secure group key management for data gathering in WSNs

II. LITERATURE SURVEY

The main objective of the current survey is to highlight the limitations and advantages of the various existing security methods. There are different techniques for encryption, data compression, key management, clustering, and aggregation, which are presented and compared.

A. Clustering

Clustering in WSNs is a process of grouping sensor nodes. All the nodes are linked to the cluster head for maintaining communication. The cluster head is chosen randomly. After the cluster head selection, all the nodes communicate locally through the cluster head. The clustering algorithm should provide solutions on minimizing energy consumption, reducing communication, and organizing the messages among the cluster head and member nodes. Authors in [1] provide solution to the isolated nodes which are not in the range of the cluster head. To solve this, the O-LEACH (Orphan Low Energy Adaptive Clustering Hierarchy) routing algorithm was proposed which takes care of the orphan nodes. The O-LEACH maintains full coverage for the applications which requires transferring data to the entire area. O-LEACH performs better than the LEACH algorithm in terms of energy, connectivity rate, coverage and scalability [1]. The Energy Balanced Clustering algorithm based on LEACH for WSNs is an improved version of the LEACH protocol to enhance the energy of the network. Different versions of LEACH are collated to perform better than the existing protocols. The SLEEP LEACH outperforms all the existing LEACH versions in terms of residual energy, throughput, and packet delivery ratio [2]. Energy efficient clustering is very important in prolonging the lifespan of a WSN. Hence, authors in [3] provided a clustering algorithm which minimizes the intra cluster distance to optimize the usage of network energy. The clustering with PSO presented a better clustering via the uniform allocation of CH throughout the network [3]. Authors in [4] presented the FLC-PSO algorithm for WSNs which outperforms LEACH, conventional FLC, and FLC-GA in terms of the number of dead nodes, remaining energy level, number of cluster heads and surviving nodes.

A review of the surveyed literature is summarized in Table I with the advantages and improvements of clustering protocols. Most of the key features of the methods are mentioned in the Table.

TABLE I. CLUSTERING ALGORITHMS COMPARISON

Algorithm	Year	Advantages	Improvements
O-LEACH [1]	2016	Connectivity rate &coverage	Improves energy consumption
SLEEP LEACH [2]	2016	Outperforms the existing LEACH versions	Improves energy consumption
Cluster formation with PSO [3]	2017	Better network stability	Improves energy efficiency and network life span
FLC-PSO [4]	2018	Efficient energy method	Only the remaining energy and the number of dead nodes are the considered factors

B. Compression and Aggregation

Compression is the process of reducing the transmitted data. It reduces the needed memory space and increases transmission ratio. Data aggregation is the process which forms the set of data from data sets from different physical quantities. The universal LZW data compression is a lossless data compression algorithm. In this method, a dictionary is created while encoding data. Choosing a large dictionary reduces overflow but spoils compression. The algorithm in [5] performs best on images and text files. By using this method, a compression ratio of 60-70% is achieved. Authors in [6] mainly concentrated on reducing the amount of communication needed for data transmission by sensors. They proposed a routing algorithm called funneling which reduces network energy consumption. The method used for compression was coding by ordering. Combining both funneling and coding by ordering, the energy consumption is reduced by half, while the collisions in the wireless medium were also reduced. Good compression ratio can be achieved by coding by ordering, which is a lossy technique so there is a chance of losing data at the end. Authors in [7] described the data distributed wavelet transform (DWT) compression method which is based on the lifting scheme. In WSNs the energy consumption is the main issue which effects the life time of the network. The DWT method performs better than the other distributed wavelet algorithms in terms of calculation complexity and time. A novel data transmission mechanism named data selecting mechanism (DSM) was also proposed and simulated. It was concluded that this method reduces the network's redundant data and increases its lifetime by reducing energy consumption. Authors in [8] proposed a data aggregation technique using the RSA key management approach for the WSNs. The data sampled by the sensor nodes contain redundant data, so data aggregation becomes very

important to eliminate data redundancy. This reduces transmissions and saves energy. ANT colony algorithm was used to aggregate the data. Dynamic routing protocols were employed with the data aggregation to transfer the data. To make the aggregation more efficient, the authors used the RSA for implementing key based data transmission. This proposed method sends data via a secure path and performs time to time key value change in the network. Authors in [9] proposed a deterministic code allocation technique for data compression. This method obtained better compression performance with less computation complexity.

A review of the studied literature is summarized in Table II with the advantages and improvements of compression and aggregation techniques.

TABLE II. COMPARISON OF THE COMPRESSION AND AGGREGATION METHODS

Algorithm	Year	Advantages	Improvements
Funneling and coding by ordering [5]	2003	High compression ratio	More CR can be achieved
WSM with DSM [6]	2013	Less energy consumption	Compression ratio is improved
LZW [7]	2014	More compression ratio for monochrome images and text files	60-70% of compression ratio is achieved
ANT colony and RSA [8]	2014	Send data packets through secure routing	Dynamically key value changes
Deterministic code allocation algorithm [9]	2019	Better compression performance with less computational complexity	This algorithm can be embedded in the real WSN hardware

C. Key Management and Data Gathering

Authors in [10] proposed group key management using symmetric key and threshold cryptography (EGKMST) for cluster based WSNs. Key management plays a very important role in group communication and protection from attacks in sensor networks. Since limited resources are providing security in the WSNs, it has become a must for them. The proposed method uses the hierarchical cluster structure and adopts the pair-wise key and group key management based on threshold cryptography, which efficiently generates key and distribute it among the clusters, while periodically updates the key. So EGKMST, offers continuous security from attacks during data transmission. By this method low overhead, low cost, and more energy saving can be achieved, compared to existing methods. Authors in [11] described an efficient key management scheme for WSNs. Due to their inherent nature, the WSNs are more vulnerable to attacks than the traditional networks. So, providing authentication and confidentiality is more critical in such networks. The authors proposed a novel key management method called MAKM (modular arithmetic based key management), based on congruence property. Each sensor node stores the key seed, this key seed is used to generate the shared key with its cluster head and the group key is shared with the other members in the same cluster. MAKM demands less storage space. It outperforms the key pool-based methods in terms of delay and energy for large scale WSNs. The WSNs led to the development of various new data gathering protocols. Authors in [12] proposed the SELADG (secure energy efficient location aware data gathering approach for wireless sensor networks) for gathering data securely. They used the ECDHKE algorithm for key generation and key exchange between the sensor nodes to protect the data from malicious nodes and provide security. This scheme outperforms the existing EEHA and SMART methods. Authors in [13] proposed a data gathering technique in WSNs through an intelligent compressive sensing scheme for efficient data gathering. Recently emerge compressive sensing (CS) theory provides a whole new era for data gathering in wireless sensor networks. Due to the disadvantages of existing compressive sensing methods, they proposed an adaptive data gathering scheme by using compressive sensing. They introduced a concept named autoregressive (AR) model into the reconstruction of the sensed data. The reconstructed data were then evaluated by utilizing the successive reconstructions, the relation between measurements and error. Testing on real data and experimental results confirm the efficiency of this scheme.

A review of the studied methods is summarized in Table III with the advantages and improvements of each studied key management and data gathering method.

TABLE III. COMPARISON OF KEY MANAGEMENT AND GATHERING METHODS

Algorithm	Year	Advantage	Improvement
MAKM and ECDSA [11]	2011	Reduces energy consumption	Reduces delay
Intelligent compressive sensing [13]	2012	More efficient than conventional CS	Improved reconstruction quality
EGKMST [10]	2014	Low cost, low memory overhead, energy saving	100% connectivity is achieved
SELADG and ECDHKE [12]	2015	Achieves better performance than the existing EEHA and SMART	Improve the network life time

D. Encryption and Authentication

A WSN consists of low cost and small sized sensor nodes with no predetermined location as they are randomly spread in the application terrain. For such networks authentication and key agreement are important. In [14], the authors proposed an enhanced authentication and key agreement protocol, the elliptic curve-based authentication and key agreement protocol, which satisfies all security issues. There are many security mechanisms used in WSNs, the authors in [15] described RSA and biometric based authentication for WSNs which are very effective methods in securing information and message security by cryptographic mechanism and give the best authentication results in WSN. Authors in [16] proposed a secure aggregation using an efficient key management technique for WSNs. Data aggregation is an effective method in WSNs because it reduces

the number of packets to be sent to the base station. This technique uses the clustering mechanism reducing network traffic and contention in the wireless channel. So, aggregation increases network lifetime by reducing energy usage. Authors in [16] propose the key exchange management protocol which helps two users to exchange key securely while these keys can be used to encrypt the messages efficiently. Sande–Tukey Algorithm is proposed to provide the key. This technique is developed to aggregate the total computation outputs and to identify the number of failures in the environment.

TABLE IV. COMPARISON OF DATA ENCRYPTION AND AUTHENTICATION METHODS

Algorithm	Year	Advantage	Improvement
Elliptic curves [14]	2013	Low computation cost	Satisfies all necessary security requirements
Sande-Tukey [16]	2014	Security to selective discrete method in WSN	Lifetime of the system is improved. Consumes less time and eliminates traffic with less energy.
RSA [15]	2016	Cost efficient	The life time of sensor nodes is increased
EC based key management scheme [17]	2016	Better computational complexity and resist to side channel attacks	Satisfies high security requirements
CL-EKM [18]	2016	Secure communication in dynamic WSN	Effective against attacks
CL-AKM [19]	2016	Economical key revocation. Ensures backward and forward key secrecy.	Effective against several attacks

Authors in [17] presented the hardware implementation of an efficient key management scheme for WSNs in the applications which require high security. The basic functions of authentication and random number generation are performed by using elliptic curves-based algorithms instead of using AES or SHA. This method was implemented on a kintex7 FPGA board. By this method better computational complexity and resistance to side channel attacks can be achieved. Even though a lot of research is done on key management, it remains an important issue in WSNs. In [18], the authors proposed the certificate less effective key management method. It supports the economical key revocation when the node joins or exits from the network and it ensures backward and forward key secrecy. By using CL-EKM, secure communication is established. It was confirmed by simulations that the proposed protocol performs well in terms of memory, energy and communication. Authors in [19] presented the active key management in dynamic wireless sensor networks. They used the certificate less technique in key management. It supports the economical key revocation when a node joins or exits the network and it ensures backward and forward key secrecy. This proposed scheme is effective in several attacks. Simulation is done to assess its delay, threshold, and energy.

A review of the studied methods is exhibited in Table IV.

III. CONCLUSION

In this paper, a study on different clustering, data compression, aggregation, authentication, encryption, data gathering, and key management approaches has been done. Various approaches for the above mentioned tasks have been explained with their objectives and limitations. This paper is a short description and analysis of the proposed and implemented methods and techniques for key management and data gathering. Various techniques for data compression, aggregation, clustering, encryption and authentication, data gathering, and key management have been presented. These techniques provide complete security for WSNs and transfer the data efficiently. It was observed that in spite of the research conducted in this regard, there is still space for future work.

REFERENCES

[1] W. Jerbi, A. Guermazi, H. Trabelsi, "A novel clustering algorithm for coverage a large scale in Wireless Sensor Networks", International Journal on Computational Science & Applications, Vol. 6, No. 2, pp. 1-16, 2016

[2] D. Charaan, R. Ramesh, E. Uma, "Energy balanced clustering algorithm on LEACH Protocol for WSN", International Journal of Innovation and Scientific Research, Vol. 23, No. 2, pp. 293-302, 2016

[3] S. P. Singh, S. C. Sharma, "A novel energy efficient clustering algorithm for Wireless Sensor Networks", Engineering, Technology & Applied Science Research, Vol. 7, No. 4, pp. 1775-1780, 2017

[4] C. Cao, X. Zhu, "Energy management using Optimal Fuzzy Logic Control in Wireless Sensor Network", International Journal of Online and Biomedical Engineering, Vol. 14, No. 9, pp. 35-52, 2018

[5] H. N. Dheemanth, "LZW Data Compression", American Journal of Engineering Research, Vol. 3, No. 2, pp. 22-26, 2014

[6] D. Petrovic, R. C. Shah, K. Ramchandran, J. Rabaey, "Data funneling: routing with aggregation and compression for Wireless Sensor Networks", IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, USA, May 11, 2003

[7] D. Ye, C. Shen, "Data compression algorithm for Wireless Sensor Networks", available at: https://pdfs.semanticscholar.org/33dd/f5fe6f7fe396622e25dd3471637fd89d1f40.pdf, 2013

[8] G. Malathy, C. Krishnan, "Data aggregation using RSA key management technique in Wireless Sensor Networks", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, No. 1, pp. 274-277, 2014

[9] H. Anwer Basha, S. Arivalagan, P. Sudhakar, R. P. Narmadha, "A new deterministic code allocation technique for data compression in Wireless Sensor Networks", International Journal of Recent Technology and Engineering, Vol. 7, No. 5C, pp. 80-86, 2019

[10] A. Diop, Y. Qi, Q. Wang, "Efficient group key management using symmetric key and threshold cryptography for cluster based Wireless Sensor Networks", I. J. Computer Network and Information Security, Vol. 8, pp. 9-18, 2014

[11] D. Du, H. Xiong, H. Wang, "An efficient key management scheme for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Vol. 2012, Article ID 406254, 2011

[12] M. R. Juliana, S. Srinivasan "SELADG: Secure Energy Efficient Location Aware Data Gathering Approach for Wireless Sensor Networks", International Journal on Smart Sensing and Intelligent Systems, Vol. 8, No. 3, pp. 1748-1767, 2015

[13] J. Wang, S. Tang, B. Yin, X. Y. Li, "Data gathering in Wireless Sensor Networks through Intelligent Compressive Sensing", 2012 IEEE Infocom, Orlando, USA, March 25-30, 2012

[14] M. Bayat, M. Reza Aref, "A secure and efficient elliptic curve based authentication and key agreement protocol suitable for WSN", IACR Cryptology ePrint Archive 2013, Article ID 374 2013, 2013

[15] S. Katiyar, S. Rizwan, R. Gujaral, "Network security described technology based on RSA and biometrics for authenticity in WSN", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6, No. 2, pp. 328-333, 2016

[16] V. Jayaraj, M. Indhumathi, U. Durai, "Secure data aggregation using efficient key management technique in Wireless Sensor Network", International Journal of Computer Applications, Vol. 89, No. 9, pp. 6-11, 2014

[17] P. Jilna, P. P. Deepthi, U. K. Jayraj, "Hardware implementation of an efficient key management scheme for Wireless Sensor Networks", International Journal of Intelligent Computing Research, Vol. 7, No. 1, pp. 663-671, 2016

[18] D. Dhayalan, S. Nandhini, "Certificate less effective key management in dynamic Wireless Sensor Network", Imperial Journal of Interdisciplinary Research, Vol. 2, No. 4, 2016

[19] A. G. Priyanga, C. Narmadha, "A certificate less active key management in dynamic Wireless Sensor Networks", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, No. 1, pp. 119-123, 2016