International Conference on Information Engineering, Management and Security 2016 [ICIEMS]

ISBN	978-81-929866-4-7
Website	iciems.in
Received	02 – February – 2016
Article ID	ICIEMS010

VOL	01
eMail	iciems@asdf.res.in
Accepted	15 - February – 2016
eAID	ICIEMS.2016.010

A Survey on Energy Efficient and Key Based Approach for Data Aggregation in WSN

S Mohanraj [1], **N Suganya** [2], **V Priyadharshini** [3], **K Hemalatha** [4]
Angel College of Engineering and Technology, Tirupur District, Tamilnadu.

Abstract: *A Wireless Sensor Network is a multiple collection of large number of sensor nodes. These sensor nodes are used to collect the information from the surroundings and pass it to the base station. Data Aggregation is an important technique to achieve power resource effectively in the sensor network. Because sensor node has limited battery power so data aggregation techniques have been proposed for WSN. The data from the multiple sensor nodes are aggregated is usually performed by averaging method. The aggregated data are stored into header aggregator node and it is highly susceptible to attacks. To address this security issue, Iterative Filtering algorithms are used to monitor sensor nodes and provide great promise by detecting vulnerable errors. For transferring aggregator data from aggregated node to base station, this paper introduces Cryptography and Random Key Generation technique. We use encryption technique for original message and simultaneously create a key for that encrypted message. That generated key and encrypted message will be sent to the receiver through the possible paths where the hackers cannot hack the original message.*

Keywords: *Data Aggregation, Sensor Networks, Network level Security, Collision Attacks.*

I. INTRODUCTION

A Wireless Sensor Network (WSN) are widely distributed autonomous sensors to monitor physical or surrounding conditions such as temperature, noise etc., and to cooperatively pass their data through the network to a main location. WSNs are widely used in several applications, such as wild habitat observation, forest fire exposure, and military surveillance. Individual sensor nodes transmit the data to the base station continuously; therefore power consumption is increased [2]. In order to reduce the power consumption of WSNs, several approaches are proposed such as radio scheduling, control packet elimination, topology control, and data aggregation [1].

An example data aggregation scheme is presented in Fig. 1 where a collection of multiple sensor nodes gather information from a target boundary. When the base station queries the network, rather than sending each and every sensor node's data to base station, any one sensor node from the network is called as data aggregator. It will gather the information from its nearby nodes aggregates them and transmit the aggregated data to the base station through a multi hop path. WSN are influenced by many types of security attacks including false data injection and data forgery. Sensor nodes can be mutually concession by intruders and the compromised nodes can distort data integrity by injecting false data [9]. In [9] the first of its kind to integrate the detection of false data with data aggregation and confidentiality.

Cite this article as: S Mohanraj, N Suganya, V Priyadharshini, K Hemalatha. "A Survey on Energy Efficient and Key Based Approach for Data Aggregation in WSN". *International Conference on Information Engineering, Management and Security 2016*: 47-50. Print.

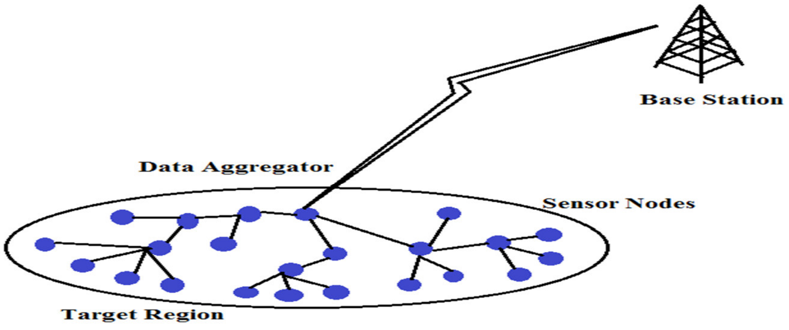

Fig. 1. Data aggregation in a wireless sensor network.

Data aggregation is implemented in WSN to eliminate data redundancy, reduce data transmission, and improve data validity. Data aggregation results in better bandwidth and battery utilization [9]. To detect false data injected by a data aggregator, some neigh boring nodes of the data aggregator also perform data aggregation and evaluate MACs for the aggregated data to activate their pair mates to verify the data later. DAA also provides data secrecy and the data are forwarded between data aggregators [9]. In this scheme, they use a ring topology in which a node may have multiple parents in the aggregation hierarchy and every sensed value or sub aggregate is denoted by a duplicate-insensitive bitmap called synopsis [10]. Reputation and trust play an essential role in such applications by enabling multiple parties to establish relationships that achieve mutual profit. Reputation allows parties to build trust, or the degree to which one party has confidence in another within the framework of a given purpose or decision [4]. Trust management systems for WSN could be very useful for detecting malicious nodes and for assisting the decision-making process [5].

The rest of this paper is organized as follows. The associated work is presented in Section II, Section III describes the problem statement and the assumptions, Section IV starts with a brief summary of security requirements of wireless sensor networks and show how they narrate with data aggregation process, Section V describes a Message Digest (MD5) algorithm and Section VI concludes this paper.

II. Related Work

Several researchers have studied problems related to data aggregation in WSNs. Header aggregator nodes can be easily compromised by attackers. The hackers may inject false data into the node and it is highly vulnerable. To address this problem they used Iterative Filtering algorithm [1]. For example, In the Page Rank algorithm, they accept that a random walk over the network is a good model of real navigation for web surfer. In trust propagation over networks, we accept the transitivity of trust if node A trusts node B and B trusts node C, then A will trust C [7]. Compromised nodes might attempt to frustrate the aggregate computation process in multiple ways; they are violating data privacy, Falsifying the local value and Falsifying the sub aggregate.

Several key establishment protocols are developed for sensor networks which propose “direct key establishment” for neighboring nodes and “path key establishment” for sensor nodes [9]. Our work is also closely related to provide security for transmitting the data from aggregator node to base station.

III. Problem Statement and Assumption

Our goal is to transfer the encrypted message and its key to the base station through the multi hop path. In [10] technique, the mutually concession node can inject a large amount of error in the final estimate of BS (inflation attack). Although sensor nodes are considered to have limited computational capabilities, there are in fact different types of nodes with different levels of constraints are Weak nodes, Normal nodes and Heavy-Duty nodes. Weak nodes are extremely constrained, Heavy-Duty nodes have PDA-like capabilities and Normal nodes are the most common type of sensor node device with enough resources to create a fully functional sensor network [5].

We assume that the sensor nodes for a multi hop network with BS as the central point of control. A compromised node can corrupt the aggregate estimate of the base station, keeping their focus on the ring-based hierarchical aggregation algorithms. To address this issue, they presented a lightweight verification algorithm which would activate the base station to verify whether the computed aggregate was valid [10].

Cite this article as: S Mohanraj, N Suganya, V Priyadharshini, K Hemalatha. “A Survey on Energy Efficient and Key Based Approach for Data Aggregation in WSN”. *International Conference on Information Engineering, Management and Security 2016*: 47-50. Print.

IV. Security Requirement

Due to unfriendly environments and unique properties of w, it is a challenging task to defend sensitive information transmitted by WSN [2]. Therefore, security is a main concern for WSN and there are many security esteems that should be investigated. In this section, we present the necessary security requirements that are raised in a WSN atmosphere and make clear how these requirements narrate with data aggregation and transmission process. Trust and Reputation Systems (TRS) represent a significant class of decision support tools that can help to reduce risk when engaging in transactions and interactions on the Internet [3].

Data aggregation protocols must decrypt the sensor data to carry out data aggregation and encrypt the aggregated data behind transmitting it. Data aggregation protocols can be classified into two parts: tree-based data aggregation and cluster-based data aggregation protocols [2]. The protocol called EADAT (Energy- Aware Distributed Aggregation Tree) is based on an energy-aware distributed heuristic. Security requirements of WSN can be satisfied using any symmetric key or asymmetric key cryptography. Due to resource limitations of sensor nodes, symmetric key cryptography is preferable more than asymmetric key cryptography. Secure DAV protocol is very similar except that elliptic curve cryptography is used for encryption purposes and provides data confidentiality, data security and source authentication [2].

V. Message Digest (MD5) Algorithm

This section presents about Message Digest (MD5) algorithm and its operations. A MD5 algorithm is also known as cryptographic hash function. It receives a message as input and creates a fixed-length output, which is generally lower than the length of the input message. The output is known as hash value, a fingerprint or a message digest. In [9] elaborate the protocol DAA and its algorithms, namely MNS and SDFC. The limitations of DAA due to the value depends strictly on several circumstances such as geographical area situation, modes of deployment, transmission range of sensor nodes and power management. The Bipartite method has two major drawbacks are the statistical ranking methods are very hard to be used to detect the users who give random rating scores and some important rating scores given by some users can be possibly removed by the statistical methods applied [8]. The properties of MD5 includes: one-way, collision-resistant and satisfy pseudo-randomness.

When the above properties are satisfied, we describe the algorithm a collision-resistant message-digest algorithm. Message-digest algorithms are mainly used in implementing digital signature. On account of its property of pseudo-randomness, MDA is also used to be an element of the mechanism for random number generation. There are three kinds of operations in MD5 are Bitwise Boolean Operation, Modular Addition, Cyclic Shift Operation. All these three operations are very rapid on a 32-bit machine. So MD5 is quite fast. The mechanism of MD5 as well as MD2 and MD4, follows a design principle planned by Merkle and Damagard. Its basic idea in block-wise mode to do hash. In a word, MD5 consists of two phases: padding phase and compression phase. In the padding stage, some extra bits (1 to 512bits) are appended to the input message. In the compression stage, a compression function is used on each 512-bit block and generates a 128-bit output. The output is always involved in the calculation of next round.

VI. Conclusion

This paper provides a detailed review of secure data aggregation and security concept in wireless sensor networks. We discussed how to prevent the encrypted message from the hackers while transmitting to the base station. To address this problem, we used Message Digest (MD5) algorithm that provides security by compressing the data. This algorithm would guarantee the successful protection of the encrypted data even in the presence of an attack. As for the future work, we will investigate that our approach can protect against compromised attackers.

References

1. Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, Sanjay Jha “Secure data aggregation technique for wireless sensor network in presence of collision attack” IEEE transactions on dependable and secure computing, vol. 12, no. 1, Jan/Feb 2015.
2. S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless sensor networks: A comprehensive overview,” Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.
3. A. Jøsang and J. Golbeck, “Challenges for robust trust and reputation systems,” in Proc. 5th Int. Workshop Security Trust Manage., Saint Malo, France, 2009, pp. 253–262.
4. K. Hoffman, D. Zage, and C. Nita-Rotaru, “A survey of attack and defense techniques for reputation systems,” ACM Comput. Surveys, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.
5. R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, “Trust and reputation systems for wireless sensor networks,” in Security and Privacy in Mobile and Wireless Networking, S. Gritzalis, T. Karygiannis, and C. Skianis, eds.,Leicester, U.K.: Troubador Publishing Ltd, 2009 pp. 105–128,.

Cite this article as: S Mohanraj, N Suganya, V Priyadharshini, K Hemalatha. “A Survey on Energy Efficient and Key Based Approach for Data Aggregation in WSN”. *International Conference on Information Engineering, Management and Security 2016*: 47-50. Print.

6. H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenance-based trustworthiness assessment in sensor networks,” in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.
7. C. de Kerchove and P. Van Dooren, “Iterative filtering in reputation systems,” SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.
8. R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, “Robust reputation based ranking on bipartite rating networks,” in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.
9. S. Ozdemir and H. C¸ am, “Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks,” IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 736–749, Jun. 2010.
10. S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1040–1052, Jun. 2012.

Cite this article as: S Mohanraj, N Suganya, V Priyadharshini, K Hemalatha. “A Survey on Energy Efficient and Key Based Approach for Data Aggregation in WSN”. *International Conference on Information Engineering, Management and Security 2016*: 47-50. Print.