INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Survey paper on data aggregation in MANET with advance security protocol using NS2

Yudhvir Kumar
guliayuvi12@gmail.com
CBS Group of Institution, Jhajjar, Haryana

Tarun Dalal
tarundalal88@gmail.com
CBS Group Of Institution, Jhajjar, Haryana

ABSTRACT

Wireless sensor networks (WSNs) consist of sensor nodes and these nodes can vary from a few numbers to a highly dense number. Data aggregation is a very important technique in wireless sensor networks through which diverse parameters performance can be increased effectively. Energy consumption by nodes can be decreased using data aggregation technique by eliminating redundancy because these parameters play a vital role in MANET. Wireless sensor nodes are very tiny in size and have limited processing capability very low battery power. This diminution of low battery power makes the sensor network vulnerable to failure. Sensor networks consist of several sensor nodes which co-operatively send sensed data to base station. One of the critical constraints of sensor nodes is the power consumption requirement. As sensor nodes are battery driven, an efficient utilization of power is essential to reduce data traffic inside sensor networks thus reduce the amount of data that need to send to base station thereby enhancing the network lifetime. In this survey paper, our main focus is to know data aggregation, data aggregation strategies, private key, public key, and security concept how to data can be a guard from hackers or malicious nodes. Networks have huge application in habitat monitoring, disaster management, security, and military, etc.

Keywords— *Data aggregation, Hop, Cluster, WSN, Strategies, Protocol*

1. INTRODUCTION

In data aggregation, Confidentiality and integrity are the key security issues. Data confidentiality is to protect the sensitive transmitted data from passive attacks. It is particularly vital in a hostile environment, where the wireless channels are vulnerable to eavesdropping. The complicated encryption and decryption operations can use the sensor power quickly. Another security issue is data integrity which avoids the compromised source nodes or aggregator nodes from significantly changing the final aggregation value [1-2]. Sensor nodes are easy to be compromised due to lack of expensive tampering- resistant hardware and even that hardware might not always be reliable. A compromised node can alter, forge or discard messages. The system architecture for the proposed multi-level data aggregation model is shown in figure 1.

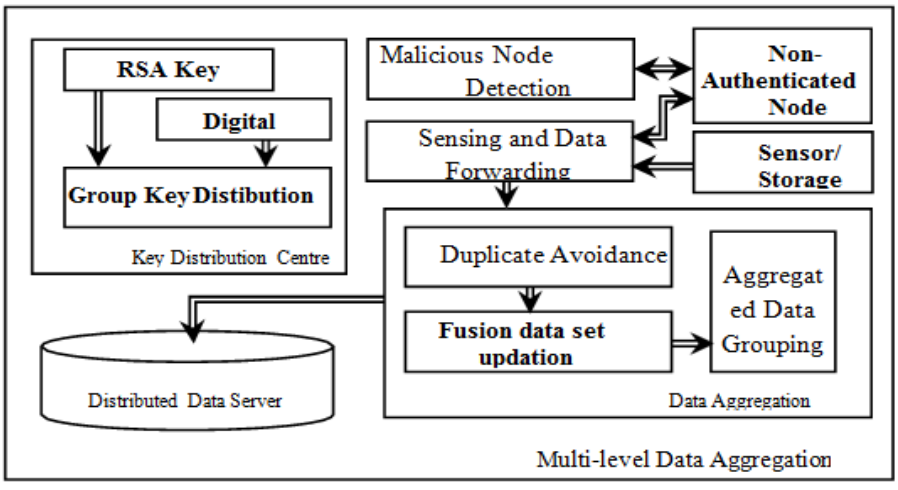

Fig. 1: System architecture for multi-level data aggregation

In the proposed multi-level data aggregation model for reliable data transmission, the distributed data server is used to store and process the data. The key distribution center is used to generate session keys and a digital signature which is then used to distribute the signature to all the authenticated nodes [3]. Data aggregation avoids the duplication and removes the similar data set

while updating the final group of data based on the region along with the session. The sensors sense the data and forward it to the base station for computation. The malicious node detection process is used to evaluate the nodes based on its behavior [5]. Two different methods can be used for secure data aggregation in WSN, first one is hop-by-hop encrypted data aggregation and the second one is end-to-end encrypted data aggregation. There are two main practical issues involved in implementing data encryption at the sensors (Duarte & Liu 2003), namely, the size of the encrypted message and next execution time for encryption at the sensor nodes. Another main aspect of security in sensor networks is the secret key establishment between the sensor and the base station. Girao et al (2005) proposed a security protocol for sensor networks which address the key establishment problem. Here, all nodes trust the base station at the network creation time and each node is given a master key which is shared with the base station. A message authentication code is used, and the keys for encrypting the data and computing the code are derived from the master key using a pseudo-random function. When a key is compromised, a new key is derived without transmitting confidential information [4].

2. RELATED WORK

Abdul Suchithra, Sumitha Thankachan: In this paper, we concentrate on the security of Wireless Sensor Networks, since the set of challenges in the sensor networks are much diverse in nature. We have made a depth threat analysis of Wireless Sensor Network and also propose some of the countermeasures against these threats. We also propose some of the security goals for the Wireless Sensor Network. In further, security is more important for the acceptance and the usage of the sensor networks for as many applications [6]. Nanthini.D and R.A.Roseline [2014]: In this paper, we provide a review of existing approaches, techniques and protocols for aggregation in wireless sensor networks. Throughout this paper, we discuss some of the various types of aggregation in Wireless Sensor Networking field. Various protocols have been proposed for routing packets for facilitating data aggregation. Generally, the users require only efficient aggregate functions. A sensor network may consist of hundreds or thousands of low-cost sensors. Each acts as an information source, sensing and collecting data from the environment for a given task [7]. V. Umarani, K. Soma Sundaram: The major challenge faced by wireless sensor networks is security. Because of the dynamic and collaborative nature of sensor networks the connected sensor devices make the network unusable. To solve this issue, a trust model is required to identify malicious, selfish and compromised nodes. It supports the decision making processes in wireless sensor networks such as pre-key-distribution, data aggregation, sink node selection and self-reconfiguration of sensor nodes. This paper discussed the general structure, design issues, trust metrics and the corresponding attacks and defense mechanisms of trust model. It also discusses the various trust models used in the decision-making process of Wireless Sensor Networks [9]. Sushruta Mishra and Hiren Thakkar: The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. In this paper, we present some important aspects of wireless sensor networks related to data aggregation and various techniques of data aggregation. Our aim is to provide a good understanding of data aggregation in WSN and its related issues [10].

3. DATA AGGREGATION

There are several proposed mechanisms with the main goal to reduce the power consumption of wireless sensor networks. Mechanisms such as radio scheduling, control packet elimination, topology control, and most importantly data aggregation [12]. Data aggregation is defined as the process of summarizing and combining sensor data in order to reduce the amount of data transmission in the network. With the aim of reducing power consumption, data aggregation is the global process of gathering and routing information through a multi-hop network and processing data at intermediate nodes. It attempts to collect the most critical and important data from the sensors nodes and make it available to the Base Station in an energy efficient manner with minimum data latency and minimum possible bandwidth.

3.1 Key Points in data aggregation are as follows:

- Nodes sense attributes over the entire network and route to nearby nodes.
- A node can receive different versions of the same message from several neighboring nodes.
- Communication is usually performed in the aggregate.
- Neighboring nodes report similar data.
- Combine data coming from different sources and routes to remove redundancy.

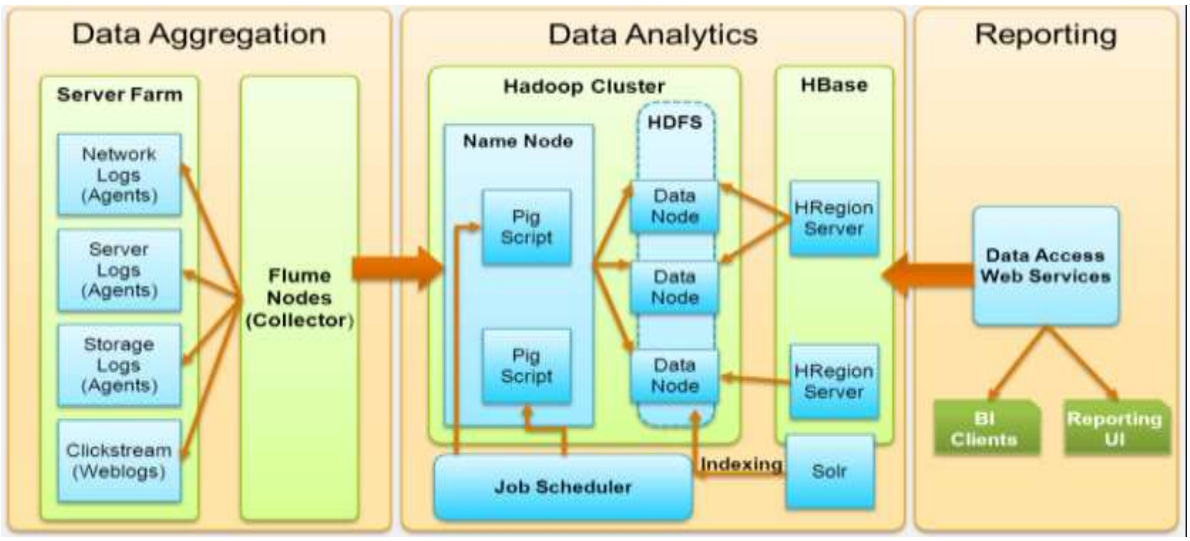

Fig. 2: Data aggregation process with data analytics

3.2 Advantages

Data Aggregation uses the parameters of nodes joining the cluster so that the data attributes are selected and stored in an aggregated format for further evaluation and usage. For data collected from sensor nodes, data aggregation can reduce the existing redundant data by data fusion processing, whereby it reduces the traffic load and conserve energy of the sensors.
Another advantage is that with data aggregation the robustness and accuracy of information obtained by the entire network are enhanced.

3.3 Disadvantages

Data aggregation works with different clusters and sensor nodes send data to Cluster Heads and send fuse data to the base station. A problem can occur that the Cluster Head may be affected by malicious attacks. If a cluster head is compromised, then the base station cannot ensure the correctness of the fusion data that has been sending to it. Several copies of the fusion result may be sent to the Base Station and this can be another problem since it increases the traffic and the power consumed by the sensor nodes [13]. Nowadays there are different techniques, algorithms, etc. aimed to achieve an energy efficient data aggregation protocol explained in detail in the next paragraphs.

4. DATA AGGREGATION STRATEGIES

There are so many data aggregation strategies which are listed as: Centralized Approach, In-Network Aggregation, Tree-Based Approach and cluster-Based Approach are some of the existing strategies related used for data aggregation [9].

4.1 Centralized Approach

In this strategy, the node sends data to a central node via the shortest possible route. These data are aggregated by the central node (header node) to reduce the redundancy.

4.2 In Network Aggregation

There are two approaches to in-network aggregation:

- With size reduction: each node combines and compresses the data packets received from its neighbors in order to reduce the packet length which will be transmitted towards Base Station.
- Without size reduction: is defined as the process of merging data packets received from different neighbors into a single data packet. The process merging data packets received from different neighbors into a single data packet but unlike with size reduction process, it is without processing the value of data.

Tree-Based Approach: This strategy [15] is held by constructing an aggregation tree, in which Base Station is considered as roots and sensor nodes are the leaves. Each node has a parent node whose data are forwarded. The flow of data starts from sensor nodes (leaves) up to the Base Station (roots) and the aggregation is done by parent nodes.

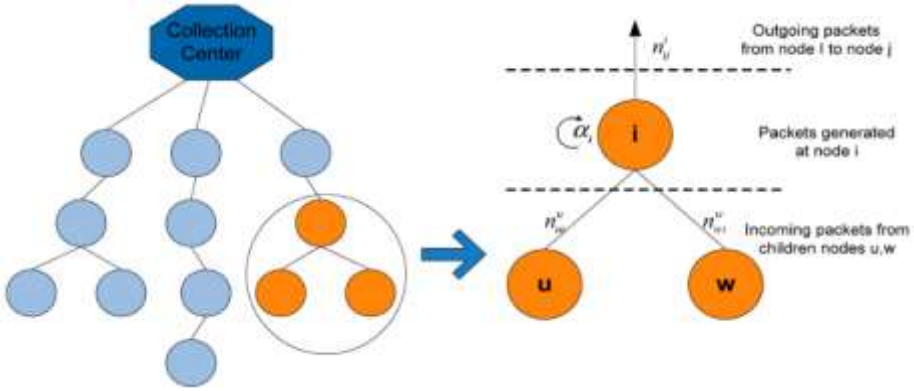

Fig. 3: Data aggregation Tree-based approach

Cluster-Based Approach: With this approach [14] the whole network is divided into different clusters. A Cluster Head is selected in each cluster among different sensor nodes or cluster members. The nodes selected as a Cluster Heads are responsible for the aggregation process of data received from cluster members and then transmit the result to the Base Station.

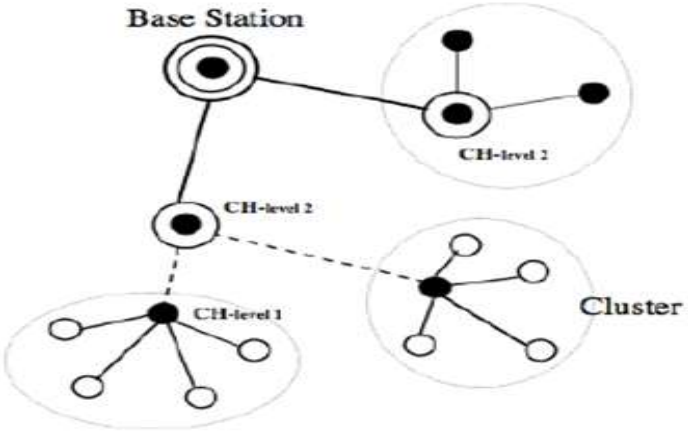

Fig. 4: Data aggregation Tree-based approach

To carry out research work we will use NS-2 (2.35), a network simulation tool to simulate a wireless communication network. NS2 is a discrete event simulator developed. It provides a good platform for wsn simulation. The random waypoint model is selected as a mobility model.

5. CONCLUSION

After studying various research papers in this survey paper we came to know about data aggregation and how to secure our data from a malicious node or unauthorized person. There are two main domains on which we have to carry out work successfully. First one is data aggregation, in data aggregation technique all the node send their information to the cluster head node not to base station. Now cluster head node aggregate the data and transmit only useful information to the base station therefore by doing this phenomenon energy consumption is saved up to large extent. In our research work, we will execute two level aggregations because energy is a very crucial parameter as every node has limited energy. Another domain in MANET is security due to the continuous changing behavior of the network. There must be a proper security process so that an unauthorized person unable to fetch information. We studied various encryptions, decryption algorithm and also gather information about the private key, public key, and secret key. Our research work will be based on the RSA algorithm which has a concept of public-key encryption and private- key decryption. Besides this, we also studied data aggregation strategies like tree-based, cluster-based and centric aggregation strategies.

6. REFERENCES

[1] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Member, "An Efficient Distributed Trust Model for Wireless Sensor Networks" IEEE, and Mohsen Guizani, Fellow, IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 5, May 2015.

[2] Mr.Rakesh, Kr.RanjanMrs., S.P.Karmore, "Survey on Secured Data Aggregation in Wireless Sensor Network" IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems 2015.

[3] Sumedha Sirsikar, Samarath Anavatti, "Issues of Data Aggregation Methods in Wireless Sensor Network: A Survey" in Proceedings of 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15) Science direct 2015.

[4] V.Vineel Kumar, K.Ananda Brahmi, "Data Aggregation Using Synopsis Diffusion Approach In Wireless Sensor Networks" International Journal of Innovative Engineering Research (E-ISSN: 2349-882X) Vol 2, Issue 1, September 2014.

[5] Nanthini.D and R.A.Roseline, "Aggregation Protocols in Wireless Sensor Network- A Survey" by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 7, July 2014.

[6] Mousam Dagar and Shilpa Mahajan, "Data Aggregation in Wireless Sensor Network: A Survey", International Journal of Information and Computation Technology, Volume 3, Number 3, 2013. ISSN 0974-2239.

[7] V.Umarani, K.Soma Sundaram, "Survey of Various Trust Models and Their Behavior in Wireless Sensor Networks", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 10, pp. 180-188, October 2013.

[8] Sushruta Mishra and Hiren Thakkar, "Features of WSN and Data Aggregation techniques in WSN: A Survey" International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[9] Nandini. S. Patil, Prof. P. R. Patil, "Data Aggregation in Wireless Sensor Network" in IEEE International Conference on Computational Intelligence and Computing Research, 2010.

[10] Kasirajan, Priya, Et Al. "Demonstration of a Multi-Interface Multi-Channel Routing Protocol (Mmcr) For Wsns Using Missouri S&T Motes." Lcn Demo (2010).

[11] Suat Ozdemir, Yang Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview" Science direct Volume 53, Issue 12, August 2009.

[12] R. Anguswamy, M. Zawodniok and S. Jagannathan, "A Multi-Interface Multichannel Routing (Mmcr) Protocol For Wireless Ad Hoc Networks" Proc. Of The IEEE Wireless Communications And Networking Conference, Pp. 1-6, Apr 2009.

[13] S. Misra Et Al. (Eds.), Guide To Wireless Sensor Networks, Computer Communications, And Networks, Doi: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.

[14] Suman Nathy; Phillip B. Gibbons, Srinivasan Seshan, Zachary R. Anderson, "Synopsis Diffusion for Robust Aggregation in Sensor Networks" ACM Transactions on Sensor Networks, Vol. V, No. N, September 2007.

[15] Wei Zhang, Sajal K. Das, and Yonghe Liu "A Trust-Based Framework for Secure Data Aggregation in Wireless Sensor Networks", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006.

