© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A RDA Framework against False Data Aggregates in CWSN

Pavithra. M*, Ganesh Kumar. G, Anand Kumar. N

Department of Computer Science and Engineering, Park College of Engineering & Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

Sensor networks generate enormous amounts of redundant sensing data. Data aggregation techniques are required to gather and aggregate these sensor data, by which the aggregator nodes forward to the base station only the aggregate results. When a Cluster-based Wireless Sensor Network (CWSN) is deployed in an unattended environment, the sensor nodes and aggregators become highly vulnerable to various security attacks. Security violation at aggregators may lead to the routing of false data aggregates to the base station. To ensure secure aggregation and data integrity, a Robust Data Aggregation (RDA) framework is proposed in this paper. The idea is to aggregate data by varying the aggregator roles and to support integrity using a Signature-based Validation (SV) scheme. The proposed framework would enable data to be aggregated and authenticated in a robust and secure manner.

Keywords: Wireless Sensor Networks, Cluster Head, Robust Aggregation, Data Aggregates, Network Security

I. INTRODUCTION

The advancement in wireless communication and technologies have led to the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered over short ranges of distance. The wireless sensor network comprises of a large number of ***sensor nodes (source)***, spatially deployed in physical or environmental conditions for measuring parameters such as sound, pressure, humidity and temperature. These sensor nodes collaborate to form an ad-hoc network capable of monitoring and collecting information from their environment, and thus report the sensed data to a ***base station (sink)*** for further analysis.

The communication in wireless sensor networks takes place in the form of wireless multi-hop transmissions. Wireless sensor network have various applications like temperature sensing, building monitoring, health monitoring, military surveillance and target tracking [5]. Some of the challenges in wireless sensor networks include power processing, energy efficiency, robustness and network security. These are the most important factors which need to be considered for providing continuous service to the users.

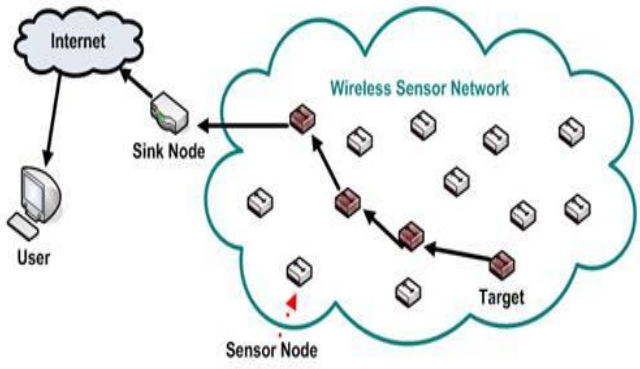

Figure 1: Architecture of a Wireless Sensor Network

A. Data Aggregation in Sensor Networks

Due to the energy constraints in sensor networks, it is inefficient for all the sensor nodes to transmit the sensed data directly to the base station. Therefore, it is essential to perform data aggregation at intermediate nodes to reduce the communication overhead for the sensor network significantly [7]. ***Data aggregation*** is an energy-efficient technique that enables information flow by combining the sensed data coming from multiple sensor nodes using suitable aggregation functions (sum,

average, MIN, MAX, count). The node where aggregation is being performed is called the ***aggregator node***. Aggregation reduces the amount of network traffic, which helps to reduce energy consumption on sensor nodes. In most applications, users require only certain aggregates of the distributed data. Examples include the average temperature in a network of temperature sensors. Fig. 2 illustrates the simple aggregation of data at intermediate nodes using multi-hop transmission.

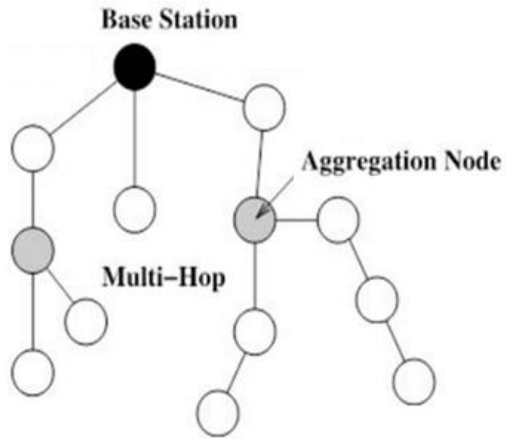

Figure 2: Data Aggregation

Since WSNs are usually unattended, they are highly susceptible to malicious attacks. Security is an important issue in data aggregation applications. The adversary may distort the actual data during both data aggregation and data forwarding by injecting false data [8]. It is necessary to provide WSN with basic security mechanisms and protocols that can guarantee a minimal protection to the services and the information flow. This means the hardware layer needs to be protected against node compromise, the network communication channels should meet certain security goals (like confidentiality, integrity and authentication), and the protocols and services of the network must be robust against any possible interferences.

B. Clustering of WSN

In order to achieve high energy efficiency and extend the network lifetime, sensors are often hierarchically organized [2]. Hierarchical data aggregation involves data fusion at special nodes, which reduces the number of messages transmitted to the sink. Cluster-based networks are one such efficient hierarchical network type more preferable for data aggregation. Clustering is a process that divides the network into interconnected substructures, called ***clusters*** [10]. In CWSNs, a sensor network is organised into a set of clusters so that the energy consumption can be evenly distributed among all the sensor nodes. A cluster is typically made up of one ***cluster head (CH)*** or ***aggregator node*** and all nodes that are controlled by it are referred to as ***cluster nodes*** or ***members***. The clusters are formed in the network as shown in Fig. 3. Clustering allows transmission to be limited to cluster heads. The cluster heads aggregate the received data, thereby reducing the total energy required for transmitting data back to the sink. Clustering approach guarantees many advantages when compared with the traditional networks.

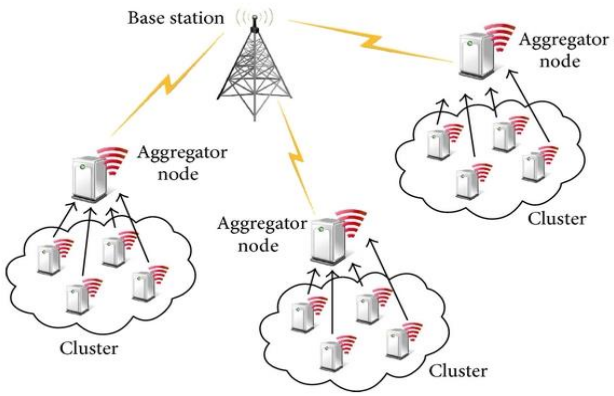

Figure 3: Clustered organization in a WSN

Clustering is one of the basic approaches for designing energy-efficient, robust and highly scalable distributed sensor networks. In many applications, cluster organization is a natural way to group spatially close sensor nodes, in order to exploit the correlation and eliminate redundancy that often exists among the sensor readings [13].

II. METHODS AND MATERIAL

A. Background Studies

The widespread use of wireless devices presents new challenges for network operators, who need to provide service to large number of end users, while ensuring security and QoS guarantees. Secure aggregation of data is a significant area of research in WSNs. Several data aggregation techniques have been proposed to enhance data integrity and availability. [6] focuses on modelling and analysing the performance of data aggregation in

networks with resource-constrained distributed event-based system. Data aggregation has been put forward as an essential paradigm for wireless routing in sensor networks. The factors affecting performance of aggregation, such as the number of placement of sources, and the communication network topology was identified and investigated. [14] highlights that it is necessary to protect the accuracy of the gathered information. A *Trust-Based and Fault-Tolerant Data Aggregation Algorithm* was thus introduced with the notion to compute self-data trust opinion, peer node trust opinion, and peer data trust opinion. This framework can evaluate both discrete data and continuous media streams and can significantly improve the quality of multimedia information as well as evaluate the trustworthiness of collected information. There is a lack of more perfect fault-tolerant and intrusion-tolerant mechanism against more complex data intrusion models. *S. Ozdemir, et.al* has presented a novel security protocol in [8], called *DAA*, to integrate data aggregation, confidentiality, and false data detection. This methodology introduces an *algorithm SDFC* to provide false data detection, secure data aggregation and data confidentiality for the DAA. The false data detection and data confidentiality relatively increase the communication overhead. It must be considered to enable every sensor node to be capable of both aggregating and forwarding data in order to improve network security and efficiency. This methodology considers only attacks such as false data injection and eaves-dropping attacks. *Secure and Efficient data Transmission (SET) protocols* for CWSNs [15] called *SET-IBS and SET-IBOOS*, by using the *Identity-Based digital Signature (IBS) scheme* and the *Identity- Based Online/Offline digital Signature (IBOOS) scheme*, respectively was presented for secure data transmission. The ID-based crypto-system was found to achieve security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. By keeping vulnerabilities to security attacks in mind, [4] an energy-efficient aggregation algorithm that is secure and robust against malicious insider attack launched by compromised or faulty node(s) in WSNs was developed. The broadcasting of sensor estimate to all neighbouring nodes makes the protocol more fault-tolerant and increases the information availability in the network. In [7], a survey on efficient techniques, working principles and security issues and challenges have been discussed. However, the authors have focussed their attention into the problem of providing security at sensor level and these schemes are inefficient over the compromised aggregators with complex security issues. [2] Clustering provides an effective way for extending the lifetime of WSNs. Experiments have proved that the networks based on cluster hierarchy structure protocol are 7~8 times more efficient than traditional dispersed flat nodes protocol in measuring the lifetime of nodes. So, more efficient hierarchical network algorithms based on cluster architecture are designed to extend the network lifetime. In [10], the authors have provided the classification for *Cluster Head Selection Algorithms* like *Identifier based, Connectivity based, Mobility based, Cost based, Power based* for wireless sensor networks. Also the main objectives, procedures and important issues were put forward. The review of literature synthesizes the current state-of-the-art in wireless sensor networks and security; looks at the techniques, various methodologies, and their effects in the research, and ends with implications and conclusions for our work.

B. System Model

The major contribution of this paper includes a ***RDA (Robust Data Aggregation)*** framework, in which an idea is proposed to address the security challenges faced by environmental monitoring systems that use WSN. All aggregation locations in a network must be secured. Authentication, integrity, and confidentiality of data must be provided for a network to be secure.

i. Overview of Framework

The proposed scheme emphasises yielding of false data aggregates as a security violation problem in sensor networks. The idea comprises the integration of effective procedures like cluster-head rotation and signature-based authentication to enable efficient and secure data aggregation for wireless sensor networks.

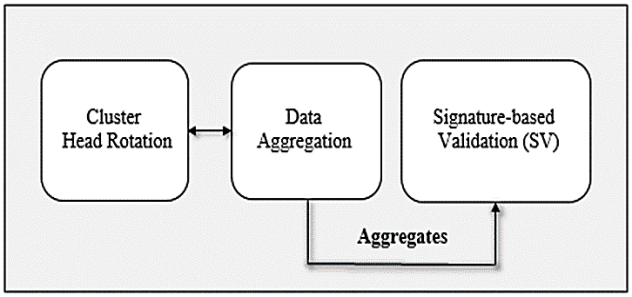

Figure 4: The proposed RDA Framework for CWSN

The framework shown in Fig. 4 may be put forward to counter malicious behaviour and so as to support the prevention of false data aggregates in CWSNs, thereby preserving the integrity of data. For a given set of clusters with sensor nodes and a cluster head (CH) for each cluster, the CH aggregates the sensor data. Base station relies only upon the aggregate results from CHs. In order to increase the security, CH roles are changed periodically and signature based validation is applied to authenticate the data aggregates at the base station. In this proposed idea, security can be enhanced by involving the roles of all sensor nodes in the environment where all individual sensor nodes compute their own signature on the data blocks.

ii. Adversary Model

In this paper, the considered attack models that could provoke malicious activities in the network are described as follows:

1) *Byzantine Attack Model:* The adversary can compromise a set of sensor nodes and inject any false data through the compromised nodes. A compromised node works alone, or a set of compromised nodes works together to carry out the attacks, which results in disruption or degradation of the services.

2) *Stealthy Attack:* A stealthy attack is defined as one in which the attacker's goal is to make the base station accept false aggregation results that are quite different from the correct results.

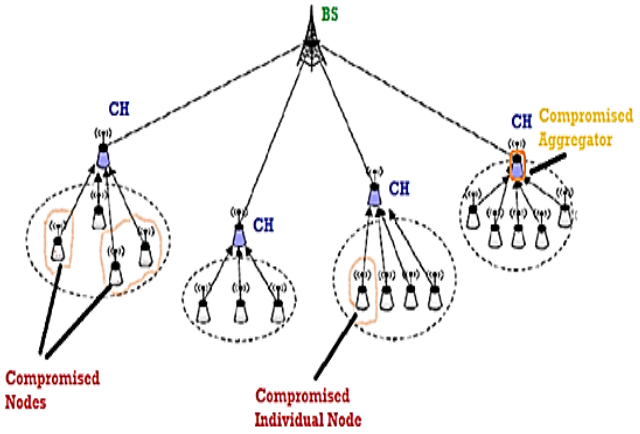

Figure 5: A model of CWSN with malicious sensor nodes and compromised data aggregators

We therefore propose this framework as a robust mechanism against such attacks and also to facilitate the routing of actual data aggregates. The details of the framework are introduced in the following section.

III. RESULTS AND DISCUSSION

The focus on adversarial environments in a CWSN with compromised aggregators is important. The proposed idea can be carried out in three phases namely: *Cluster setup phase*, *Data aggregation phase* and *Authentication phase*. The procedures are described as follows:

In *cluster setup phase*, each sensor node is configured with one or more symmetric keys selected from the key pool of the base station before deployment. After deployment, all sensor nodes in the sensing area set up the clusters. After the cluster formation, it requires the appropriate cluster head for each cluster, for that, either node select the appropriate cluster head within the cluster or base station determines the cluster head for each cluster [3]. The role of the cluster head or aggregator in each of the clusters must be rotated regularly amongst the sensor nodes for efficient integrity preservation. This would also prolong the life time of sensor network by balancing the energy consumption among all the sensor nodes.

In *data aggregation phase*, the sensor nodes within each of the clusters sense events and transmit the data to their CH over a relatively short distance. The CH computes the aggregation value based on the values it has received

from its cluster nodes and encrypts the final aggregation value using a cluster key. The final value is broadcasted to all the cluster nodes to check if the aggregate value is close to the data that they have transmitted earlier. If the aggregate matches, then the digital signature will be computed on those data blocks by each of the cluster nodes using the secret key which was shared with the base station during the first phase. After every sensor nodes compute their own signature, it will be aggregated together and forwarded to the base station.

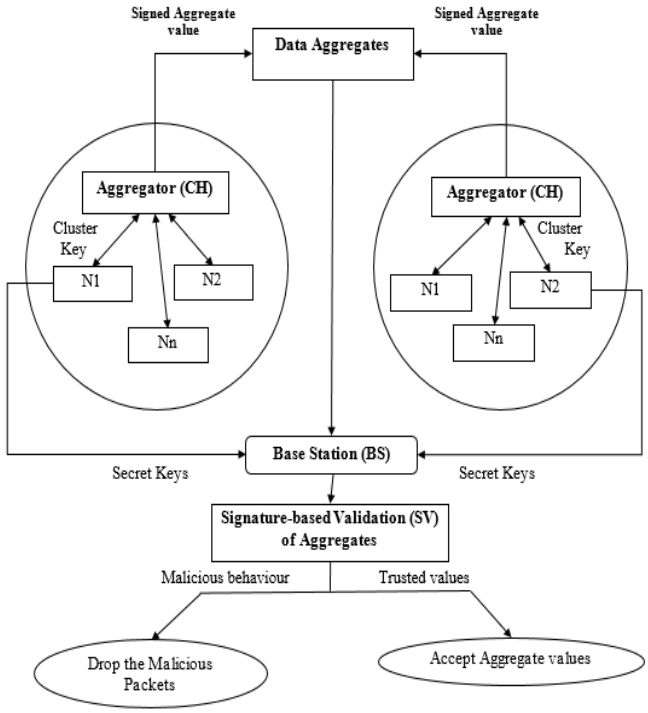

Figure 6: Illustrative diagram for the workflow in RDA

In *authentication phase*, the base station can decrypt the aggregated content by using the keys shared with all the nodes in the network. If the base station is unable to find consistent signatures, then it indicates that either the aggregator and/or the sensor nodes are compromised.

Fig. 6 illustrates the stages of the Robust Data Aggregation framework and their interconnections. Based on the proposed idea, the characteristics features and roles of the procedures to be used are listed as below:

TABLE I
PROCEDURES USED FOR THE RDA FRAMEWORK

Methodology	**Characteristics**	**Use**
Cluster head rotation	Frequent change of cluster head roles	Improved security against node compromising attacks
Data Aggregation	Operates on consecutive set of sensor readings	Reduces communication overhead by computing data aggregates
Signature-based Validation (SV)	Authentication for preventing the false data aggregates	Assessing the integrity of data aggregates with digital signatures (security)

IV. CONCLUSION

Data aggregation is a serious concern in WSN applications. Providing secure aggregation results for sensor networks is very essential. In this paper, an idea is proposed for extended security against compromised data aggregators in CWSNs. The formulated idea attempts to detect false data aggregates and adversaries at both sensor level and aggregator level in the network. This allows validation of aggregates at sensor level and BS to provide an increased level of authentication. The algorithm implementation and results are to be analysed in comparison with the other existing methodologies.

V. REFERENCES

[1] S. Bhargavi and Vishnu Prasad Goranthala, "The Impact of Collusion Attacks in WSN with Secure Data Aggregation System", *International Journal of Research, Volume 2, Issue 08, (August 2015), e-ISSN: 2348-6848.*

[2] Guoxi Ma and Zhengsu Tao, "A Hybrid Energy- and Time-Driven Cluster Head Rotation Strategy for Distributed Wireless Sensor Networks", *International Journal of Distributed Sensor Networks, (Jan 2013), ID 109307.*

[3] Jaideep Lakhotia and Rajeev Kumar, "Cluster Based Routing Protocols for Mobile Wireless Sensor Network: A Review", *International Journal of Advanced Research in Computer Engg.*

& Technology, Vol 3, Issue 7, (July 2014), ISSN: 2278– 1323.

[4] Jaydip Sen, "A Robust and Secure Aggregation Protocol for Wireless Sensor Networks", *Sixth IEEE International Symposium on Electronic Design, Test and Application (DELTA), (Jan 2011), pp. 222-227.*

[5] Kiran Maraiya, Kamal Kant and Nitin Gupta, "Wireless Sensor Network: A Review on Data Aggregation", *International Journal of Scientific & Engineering Research, Volume 2, Issue 4, (April 2011), ISSN 2229-5518.*

[6] B. Krishnamachari, D. Estrin and S. B. Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks," *in ICDCSW '02: Proceedings of the 22nd International Conference on Distributed Computing Systems. Washington, DC, USA: IEEE Computer Society, (2002), pp. 575–578.*

[7] Mousam Dagar and Shilpa Mahajan, "Data Aggregation in Wireless Sensor Network: A Survey", *International Journal of Information and Computation Technology, ISSN 0974-2239, Volume 3, Number 3 (2013), pp. 167-174.*

[8] S. Ozdemir and H. Çam, 'Integration of False Data Detection with Data Aggregation and Confidential Transmission in Wireless Sensor Networks', *IEEE/ACM Trans. Netw., Vol. 18, No. 3, (June 2010), pp.736–749.*

[9] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", *International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, (2009), ISSN 1947 5500.*

[10] V. Preetha and K. Chitra, "Clustering & Cluster Head Selection Techniques in Mobile Adhoc Networks", *International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 7, (July 2014), ISSN: 2320-9801*.

[11] 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).*

[12] P. Santhi, Md. Shakeel Ahmed, Sk. Mehertaj and T. Bharath Manohar, 'An Efficient Security Way of Authentication and Pairwise Key Distribution with Mobile Sinks in Wireless Sensor Networks', *International Journal of Modern Engineering Research, Vol. 3, Issue 4, (Jul - Aug. 2013), pp.2553-2562, ISSN: 2249-6645.*

[13] Stanislava Soro and Wendi B. Heinzelman, "Cluster Head Election Techniques for Coverage Preservation in Wireless Sensor Networks*", (2009), Journal of Ad Hoc Networks 7, pp. 955–972.*

[14] Y. Sun, H. Luo and S. K. Das, 'A Trust-Based Framework for Fault-Tolerant Data Aggregation in Wireless Multimedia Sensor Networks', *IEEE Trans. Dependable Secure Comput., Vol. 9, No. 6, (Dec. 2012), pp.785–797.*

[15] G. Vijayalakshmi, M. Sheriff and S. Mohamed Sulaiman, "Secure Environmental Data Aggregation & Query with Feedback Solution in Wireless Sensor Networks using Enhanced Leach Protocol", *Proc. of Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC, (2014), DOI: 02.ITC.2014.5.550.*