A New Approach in WSN for Secure Data Aggregation Using ANN

Gayatri Dagar, Amanpreet Kaur
1,2ITM University Gurgaon, Haryana, India

Abstract
Security is one of the major Concerns to achieve the secure communication. When the data is over the network there are more chances of some Active or passive attack. The proposed approach is about to detect the Active attack in the network. It means if some user add some extra information with data packet or destroy some information, the proposed approach can detect such kind of false data packets. We are presenting a neural network based approach to detect the fault in data packets. The proposed approach is non-linear sensor model, in which nodes are placed dynamically. This approach will combine the concept of data verification and user authentication along with data aggregation. The approach is driven to both the integrity as well as the security to transfer data.

Keywords
Security, False Data, Aggregation, Neural, Sensor Network

I. Introduction
Data aggregation is a widely used technique in wireless sensor networks. The security issues, data confidentiality and integrity, in data aggregation become vital when the sensor network is deployed in a hostile environment. There has been many related work proposed to address these security issues. In-network aggregation is a well known technique to achieve energy efficiency when propagating data from information sources (sensor nodes) to multiple sinks. The main idea behind in-network aggregation is that, rather than sending individual data items from sensors to sinks, multiple data items are aggregated as they are forwarded by the sensor network. Data aggregation is application dependent, i.e., depending on the target application, the appropriate data aggregation operator (or aggregator) will be employed [7]. However since various sensor nodes often detect common phenomena, there is likely to be some redundancy in the data the various sources communicate to a particular sink. In-network filtering and processing techniques can help to conserve the scarce energy resources [3]. Fig. 1 shows the basic principle of the in-network data aggregation technique.

![Fig. 1: Principle of In – Network Data Aggregation Technique](image)

In addition to the data aggregation, there are many other forms of in-network processing that can help reduce the size of data to be transmitted and hence help save energy. These in-network processing techniques include data fusion, data compression, data filtering, and data elimination [5].

A. Data Aggregation in Wireless Sensor Network
In-network data aggregation reduces energy consumption in WSN. Specifically, the main problems to consider are how to create the converge cast tree, how to select the routes, and where to do the aggregation in this tree. There are number of different data aggregation processes in in-network data aggregation. For example:

- Tree based in – network data. Aggregation
- Application specific data aggregation.
- Structure free in – network data aggregation. But the most important one is
- Cluster based in – network data aggregation [5].

In cluster based in - network data aggregation partitioning the network into clusters and deploying cluster-heads to perform data aggregation. The job of these cluster-heads is specifically aggregating the data received from the sensors and transmitting them to the BS. In most scenarios, they do not perform any sensing. Low-Energy Adaptive Clustering Hierarchy (LEACH), Energy-Efficient and Secure Pattern-based data aggregation (ESPDA) and Power-Efficient Gathering in Sensor Information Systems (PEGASIS) are some of the example of Cluster based in – network data aggregation. They select a cluster-head among the sensor nodes that performs the data aggregation. Although LEACH considers clusters where each sensor can reach the cluster-head within one hop, PEGASIS creates chains of sensor nodes in which a leader is designated as the aggregator. ESPDA, on the other hand, considers clusters with multi-hop routes. In all of these approaches, sensor nodes take turns to be elected as the cluster-head so that the load of being cluster-head is distributed evenly among the sensor nodes in the network [5].

II. ANN in WSN
Wireless sensor network is highly data centric. Data communication in WSN must be efficient one and must consume minimum power. Every sensor node consists of multiple sensors embedded in the same node. Thus every sensor node is a source of data. These raw data streams cannot be straightforwardly communicated further to the neighboring node or the base station. These sensor data streams need to be classified. A group of sensor nodes forms a cluster. Each node transfer data to a cluster head and then cluster head aggregates the data and sends to base station/sink node. Hence clustering and classification techniques are important and can give new dimension to the WSN paradigm. Hence efficient data clustering techniques must be used to reduce the data redundancy and in turn reduce overhead on communication. This can be very well accomplished by using some of the algorithms developed within the artificial neural networks paradigm, which can be easily adapted to WSN. In fig. 2, we can see the multihop communication in Wireless Sensor network.
In wireless sensor networks, compromised sensor nodes can inject false data during both data aggregation and data forwarding. The existing false data detection techniques consider false data during both data aggregation and data forwarding. In wireless sensor networks, compromised sensor nodes can inject false data during data forwarding only and do not allow any change on the data by data aggregation. However, this paper presents a data aggregation and authentication protocol, called DAA, to integrate false data detection with data aggregation and confidentiality. To support data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pairmates. To support confidential data transmission, the sensor nodes between two consecutive data aggregators verify the data integrity on the encrypted data rather than the plain data. Performance analysis shows that DAA detects any false data injected by up to compromised nodes, and that the detected false data are not forwarded beyond the next data aggregator on the path. Despite that false data detection and data confidentiality increase the communication overhead, simulation results show that DAA can still reduce the amount of transmitted data by up to 60% with the help of data aggregation and early detection of false data.

In Wireless Sensor Networks (WSNs) and its application to sensor node fault detection, Recurrent Neural Networks (NNs) are used to model a sensor node, the node’s dynamics, and interconnections with other sensor network nodes. An NN modeling approach is used for sensor node identification and fault detection in WSNs. The input to the NN is chosen to include previous output samples of the modeling sensor node and the current and previous output samples of neighboring sensors. The model is based on a new structure of a back propagation-type NN. The input to the NN and the topology of the network are based on a general nonlinear sensor model. To support data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pairmates. To support confidential data transmission, the sensor nodes between two consecutive data aggregators verify the data integrity on the encrypted data rather than the plain data. Use of NN give high accuracy and data aggregation reduce memory overhead SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design. The original specification of the algorithm was published in 1993 as the Secure Hash Standard, FIPS PUB 180, by US government standards agency NIST (National Institute of Standards and Technology). This version is now often referred to as SHA-0. It was withdrawn by NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly referred to as SHA-1. SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function; this was done, according to NSA, to correct a flaw in the original algorithm which reduced its cryptographic security. However, NSA did not provide any further explanation or identify the flaw that was corrected. Weaknesses have subsequently been reported in both SHA and SHA-1. SHA-1 appears to provide greater resistance to attacks, supporting the NSA’s assertion that the change increased the security. The proposed system will follow the following Steps:

- At first build the network by specifying the network parameters such a number of nodes, protocol specification, representation of Base Station etc.
- Once the network is established the next work is to specify the communication parameters such as data transmission rate, packet size etc.
- Performing the SHA to implement the security respective to...
the signature matching. Now the data will be transferred in 
an encrypted form.

- Perform the Data Aggregation on each node as the data is 
  transferred from each node.
- Train the network data over the neural approach on the 
  receiver side to find the false data within network.

IV. Results

MATLAB is a high-level language and interactive environment 
that enables you to perform computationally intensive tasks faster 
than with traditional programming languages such as C, C++, 
and Fortran. For our experimental work we have used MatLab 
(R2009a).

![Graph showing False Data Detection Using Neural Network](image)

**Fig. 4: False Data Detection Using Neural Network**

The above shown graph thus obtained on traing the ANN-WSN. 
The graph plots Total Transmission with SNR(Speed to Noise 
Ratio). The red coloured line in the graph indicate the DAA(Data 
Aggregation and Authentication) protocol performance whereas 
the blue coloured line indicate the performance of neural network 
based network. It can be concluded from the plot that Neural 
network reduce the false data detection better in comparison to 
the DAA algorithm.

V. Conclusion

In wireless sensor networks, compromised sensor nodes can is 
assumed to be not compromised. It follows that the lemma distort 
the integrity of data by injecting false data. Previously holds. 
known techniques on false data detection do not support data 
confidentiality and aggregation, even though they are usually 
essential to wireless sensor networks.

References

  Intl. Workshop on Sensor Network Protocols and Applications 
  (SNPA), Anchorage, AK, May 2003.

  and Approaches in WSN”, Department of computer 
  science, Faculty of Electrical Engineering and Information 
  Technology; Skopje, Republic of Macedonia.

  Computer Networks”, 2002.

  wireless sensor Networks”, In: Mobile Ad Hoc & Pervasive 
  Communications

  network approach for Wireless sensor network power 
  management”.

  Network Modeling Using Modified Recurrent Neural 
  Networks: Application to Fault Detection”, IEEE transaction 
  on instrumentation and measurement, Vol. 57, No. 5, May 
  2008.

  An energyefficient coordination algorithm for topology 
  maintenance in Ad-Hoc wireless networks”, Wireless 

  aggregation in wireless sensor networks”, International 
  Workshop on Distributed Event-Based Systems, Vienna, 
  Austria, July 2002.

  Sensor Network Routing: A Clean Slate Approach”.


  diffusion: A scalable and robust communication paradigm 
  for sensor networks”, Proc. of ACM MobiCom ’00, Boston, 

  “SOS: A dynamic operating system for sensor networks”, In 
  MobiSys’05, 2005.

[13] E. Goldberg, “Genetic algorithms in search, optimization, 
  and machine learning”, Addison Wesley.

  Sensor Networks: aSurvey”, IEEE Communications 

  Century challenges, scalable coordination in sensor 
  263-270.

  Networks”.

  sensor networks: A survey”, Computer Networks, Vol. 38, 
  No. 4, pp. 393-422, 2002.

[18] Padmavathi, D. Shanmugapriya, “A Survey of Attacks, 
  Security Mechanisms and Challenges in Wireless Sensor 
  Networks”, International Journal of Computer Science and 
  Information Security (IJCSIS), Vol. 4, No. 1& 2, Department 
  of Computer Science, Avinashilingam University for Women, 
  Coimbatore, India, 2009.

  of Correlated Data in Sensor Networks”, in Proceedings of 
  ACM MobiHoc’05, pp. 402–413.

  networks”, In : Iiyas M & Mahgoub. I (Eds.) Handbook 
  of sensor Networks : Compact Wireless and Wired sensing 

  network approach for Wireless sensor network power 
  management”, 2009.

  “A survey m sensor Network”, IEEE Communications 
  magazine, August 2002.

  network using MatLab6.0”.


Gayatri Dagar received her B.Tech degree in Electronics and communication from SBMN, Rohtak 2010, the M.Tech degree in Electronics and communication from ITM University, Gurgaon, in 2012. Her research interests include Wireless Sensor Network and digital signal processing techniques. She had already presented a paper on WSN at Eternal University in Himachal Pardesh.