A SECURE DATA AGGREGATION APPROACH IN WSN USING ANN

Nishant Jakhar*

Rainu Nandal**

ABSTRACT

Security is one of the major Concern 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.*

*U.I.E.T, M.D.U., Rohtak.

**Assistant Professor, U.I.E.T, M.D.U., Rohtak.

I INTRODUCTION

WIRELESS sensor networks are vulnerable to many types of security attacks, including false data injection, data forgery, and eaves dropping. Sensor nodes can be compromised by intruders, and the compromised nodes can distort data integrity by injecting false data. The transmission of false data depletes the constrained battery power and degrades the band-width utilization. False data can be injected by compromised sensor nodes in various ways, including data aggregation and relaying. Because data aggregation is essential to reduce data redundancy and/or to improve data accuracy, false data detection is critical to the provision of data integrity and efficient utilization of battery power and bandwidth. In addition to false data detection, data confidentiality is required by many sensor network applications to provide safeguard against eavesdropping.

This proposed work integrates the detection of false data with data aggregation and confidentiality. Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. However, data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation. The existing false data detection algorithms address neither data aggregation nor confidentiality. Although they could be modified easily to support data confidentiality, it is a challenge for them to support the data aggregation that alters data. For instance, the basic idea behind the false data detection algorithm in is to form pairs of sensor nodes such that one pairmate computes a message authentication code (MAC) of forwarded data and the other pairmate later verifies the data using the MAC. Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy. Data aggregation results in better bandwidth and battery utilization which enhances the network lifetime because communication constitutes 70% of the total energy consumption of the network. Although data aggregation is very useful, it could cause some security problems because a compromised data aggregator may inject false data during data aggregation. When data aggregation is allowed, the false data detection technique should determine correctly whether any data alteration is due to data aggregation or false data injection. A joint data aggregation and false data detection technique has to ensure that data are altered by data aggregation only.

Wireless Sensor Networks have emerged as an important area in wireless technology. In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive nodes, each having sensing capability with limited computational power which enables us to deploy a large-scale sensor network.

A wireless network consists of tiny devices which monitor physical or environmental conditions such as temperature, pressure, motion or pollutants at different areas. Such sensor networks are expected to be widely deployed in a vast variety of environments for commercial, civil, and military applications such as surveillance, vehicle tracking, climate and habitat monitoring, intelligence, medical, and acoustic data gathering.

This proposed work presents a dynamic model of wireless sensor networks (WSNs) and its application to sensor node fault detection. Recurrent neural networks (NNs) are used to model a sensor node. Use of NN give high accuracy and data aggregation reduce memory overhead. The model is based on a new structure of a back propagation-type NN.It increases the life time of the sensor nodes.

Data aggregation techniques explore how the data is to be routed in the network as well as the processing method that are applied on the packets received by a node. They have a great impact on the energy consumption of nodes and thus on network efficiency by reducing number of transmission or length of packet. Elena Fosolo et al in [3] defines the in-network aggregation process as follows: “In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime.”

We would like to present an algorithm that performs data aggregation within a cluster and thus reducing the load of aggregation at cluster-head to provide energy efficiency for maximizing network lifetime.

II LITERATURE SURVEY

Algorithm developed in artificial neural network can be easily developed to wireless sensor network platforms and can satisfy the requirement for sensor networks kike: simple parallel distributed computation distributed storage, data robustness & auto classification of sensor readings, fault tolerance & low computation. Neural networks can help through dimensionality reduction obtain from the outputs of the neural networks clustering algorithms, leads to lower communication cost & energy saving. The other reason to use neural network based methods in WSNs is the analogy between WSNs & ANNs. As authors strongly believe that ANNs exhibit exactly the same architecture WSNs since neural networks compared to sensor nodes & communications corresponds to radio links classification techniques.

Cluster based routing are most frequently used energy efficient routing protocols in WSNs which avoid single gateway architecture through developing of network into several clusters, while cluster head of each cluster play the role of a local base station.

The main concern in Wireless Sensor Networks is how to handle with their limited energy resources. The performance of Wireless Sensor Networks strongly depends on their lifetime. As a result, Dynamic Power Management approaches with the purpose of reduction of energy consumption in sensor nodes, after deployment and designing of the network, have drawn attentions of many research studies. Recently, there have been a strong interest to use intelligent tools especially Neural Networks in energy efficient approaches of Wireless Sensor Networks, due to their simple parallel distributed computation, distributed storage, data robustness, auto-classification of sensor nodes and sensor reading. Dimensionality reduction and prediction of sensor data obtained simply from the outputs of the neural-networks algorithms can lead to lower communication costs and energy conservation. All these characteristics show great analogy and compatibility between wireless sensor networks and neural networks.

Energy conservation is the most important concern in Wireless Sensor Networks applications which should be considered in all aspects of these networks. Neural Networks as intelligent tools show great compatibility with WSN's characteristics and can be applied in different energy conservation schemes of them.

The most important application of neural networks in WSNs can be summarized to sensor data prediction, sensor fusion, path discovery, sensor data classification and nodes clustering which all lead to less communication cost and energy conservation in WSNs. Another classification for neural network based methods can be according to neural network topologies that applied such as Self Organizing Maps, Back propagation neural networks, recurrent neural networks, Radial Basis Functions etc. However, Self Organizing Map neural networks show more applications in WSN platforms.As future work, more studies are required on different types of neural network topologies and training algorithms which would be more compatible with WSNs platforms in the terms of lower computation time. A primary constraint in wireless sensor networks (WSNs) is obtaining reliable and prolonged network operation with power-limited sensor nodes. There is an exciting new wave in sensor applications-wireless sensor networking- which enables sensors and actuators to be deployed independent of costs and physical constraints of wiring[31]. For a wireless sensor network to deliver real world benefits, it must support the following requirements in deployment: scalability, reliability, responsiveness, power efficiency and mobility.

In this new approach an intelligent analysis is used to process the structure of a wireless sensor network (WSN) and produce some information which can be used to improve the performance of WSNs' management application[16]. Wireless sensor networks need to be managed in different ways; e.g. power consumption of each sensor, efficient data routing without redundancy, sensing and data sending interval control, etc. The random distribution of wireless sensors, numerous variables which affect WSN's operation and the uncertainty of different algorithms (such as sensors' self-localization) give a fuzzy nature to WSNs [3, 4]. Considering this fuzzy nature and numerous details, a neural network is an ideal tool to be used to cover these details which are so hard to be explicitly discovered and modeled

Even if their resources in terms of energy, memory, computational power and bandwidth are strictly limited, sensor networks have proved their huge viability in the real world, being just a matter of time until this kind of networks will be standardized and used broadly in the field. One of the important problems that are related to the use of wireless sensor networks in harsh environments is the gap in their security.

The paper by Curiac, Daniel, Volosencu, Constantin, Doboli, Alex, Dranga, Octavian, and Bednarz, Tomasz (2007) provides a solution to discover malicious nodes in wireless sensor networks using an on-line neural network predictor based on past and present values obtained from neighboring nodes. This solution can also be a way to discover the malfunctioning nodes that were not a subject of an attack. Being localized on the base station level, our algorithm is suitable even for large-scale sensor networks.

Preserving energy or battery power of wireless sensor network is of major concern. As such type of network, the sensors are deployed in an ad hoc manner, without any deterministic way. The standard routing protocols can be applied into wireless sensor network by using topology modified by neural network which proves to be energy efficient as compared with unmodified topology.

Neural network has been proved to be a powerful tool in the distributed environment. Here, to capture the true distributed nature of the Wireless Sensor Network (WSN), neural network's Self-Organizing Feature Map (SOFM) is used[5].

III RESEARCH DESIGN

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 injections during data forwarding only and do not allow any change on the data by data aggregation. However, this proposed work 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 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 neighbouring 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 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

The proposed system will follow the following Steps :

1. At first build the network by specifying the network parameters such a number of nodes, protocol specification, representation of Base Station etc.
2. Once the network is established the next work is to specify the communication parameters such as data transmission rate, packet size etc.
3. Performing the SHA to implement the security respective to the signature matching. Now the data will be transferred in an encrypted form.
4. Perform the Data Aggregation on each node as the data is transferred from each node.
5. Train the network data over the neural approach on the receiver side to find the false data within network.

IV CONCLUSION

Attackers have a higher chance of gaining access to the forwarding group when the number of multicast senders is small and/or the number of multicast receivers is large. Get Higher success rate of successful data transmission

REFERENCES

1. A. Boulis, S. Ganeriwal, and M. Srivastava. Aggregation in sensor networks: An energy accuracy trade-off. In Proc. 1st IEEE Intl. Workshop on Sensor Network Protocols and Applications (SNPA), Anchorage, AK, May 2003.
2. A.Dimitrievski, V.Pejosvska and D. Davcev; Security Issues and Approaches in WSN; Department of computer science, Faculty of Electrical Engineering and Information Technology; Skopje, Republic of Macedonia.
3. Akyildiz F., et al," Wireless Sensor Networks : A survey Computer Networks" 2002, 38
4. Anastasi G & Francesco M.D. " How to prolong the lifetime of wireless sensor Networks", In: Mobile Ad Hoc & Pervasive Communications
5. Ahmad Hosseingholizadeh, Dr. Abdolreza Abhari, "A neural network approach for Wireless sensor network power management".
6. Azzam I. Moustapha, and Rastko R. Selmic," Wireless Sensor Network Modeling Using Modified Recurrent Neural Networks:Application to Fault Detection"IEEE transaction on instrumentation and measurement, vol:57 no:5 may2008.
7. B. Chen, K. Jamieson, H. Balakrishnan, R. Morris, SPAN: an energyefficient coordination algorithm for topology maintenance in ad hoc wireless networks, Wireless Networks, Vol. 8, No. 5, pp. 481-494, 2002.
8. B. Krishnamachari, D. Estrin, and S. Wicker, Impact of data aggregation in wireless sensor networks, International Workshop on Distributed Event-Based Systems, Vienna, Austria, July 2002.
9. Bryan Parno, Marl Luk, Evan Gaustad, Adrian Perrig, "Secure Sensor Network Routing: A CleanSlate Approach"
10. C. Buragohain, D. Agrawal and S. Suri, "Power Aware Routing for Sensor Databases", in Proceedings of IEEE Infocom 2005.
11. C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," Proc. of ACM MobiCom '00, Boston, MA, 2000, pp. 56-67.

12. C.Han, R.K. Rengaswamy, R. Shea, E. Kohler, and M. Srivastava. SOS: A dynamic operating system for sensor networks. In MobiSys '05,2005.
13. D. E. Goldberg, Genetic algorithms in search, optimization, and machine l earning, Addison Wesley.
14. Demirkol I, Ersoy C, Alagoz F, (2006) "MAC Protocols for Wireless Sensor Networks: aSurvey", IEEE Communications Magazine.
15. Estrin D., Govindan R., J. Hsseidemann S. & Kumar S." Next Centuary challenges, scalable coordination in sensor network. In: Mobile Computing and Networking 199: 263-270.
16. Frank Oldewurtel and Petri M¨ah¨onen," Neural Wireless Sensor Networks".