Fuzzy Logic in Secure WSN: A Review

D. Hevin Rajesh

Department of IT, St. Xavier's Catholic College of Engineering, Nagercoil, Tamil Nadu, India

Abstract Wireless Sensor Networks (WSN) are deploy in the hostile environment to collect data. WSN undergo various attacks during deployment and data collection. The security is very essential during the time of data collection and aggregation. Various soft computing methods are used along with secure WSN. In this paper, fuzzy logic based secure WSN are discussed and surveyed. The strength and weaknesses of different methods are studied. The different methods are compared in terms of various parameters.

Keywords Wireless sensor networks, Security, Fuzzy logic, Sensor node, Cluster.

I. EXISTING WORKS

Fuzzy based LEAP in WSN (ELEAP) [1], This is the cluster oriented fuzzy based protocol. This protocol has the ability to detect and eliminate sinkhole attack effectively. In sinkhole attack the compromised node will disguise as base station and receive all the information in the network, pass to adversaries. Here the node selection for forwarding the sensed data packet is decided by the fuzzy rule based system. The fuzzy logic system considered four input parameters namely energy level of the node wanted the packet to be forwarded, distance between nodes to base station, key input for detecting the sinkhole attack area and the pair wise key need for secure authentication. The output of the fuzzy system is two output variable namely, 'select' and 'reject'. If the fuzzy system output gives 'select', then the data packet forwarded to next node. Otherwise it searches another node for forwarding the data packet.

Strength:

This protocol identifies the attack area effectively and forwarded the data packet in the alternate path to reach the base station. It blocks the false messages generated by the compromised node. The heavy traffic is diverted to the nearby nodes. The nodes which have low traffic are considered for more traffic.

Weakness:

In the worst case scenario it consumes much energy for forwarding the data packet from the node to base station.

Fuzzy based Countering Endorsement attacks in WSNs (FBFEIA) [2], False Endorsement Insertion attack is one of the security threats in WSNs. The aim of this attack is to block the detection of real events from sensor fields and insert wrong endorsements in to the true sensing reports. The Fuzzy Based Endorsement Insertion Attack (FBFEIA) has two phase fuzzy based systems. The first fuzzy based system is responsible for the detection of attack on the report collected by the base station from the sensor field. The collected report is stored temporarily by the base station for the short period of time. The second fuzzy system is responsible for the elimination of the threat by sending proper control messages to the affected node for its deactivation.

Strength:

In this scheme the detection and countermeasures against the attack is very accurate. The fuzzy based approach performs the above tasks like detection and elimination, as the outcome of an analysis. The analysis is based on the collected reports by the base station.

Weakness:

The computational overhead cause by the two fuzzy based system and genetic algorithm is too high. The second fuzzy based system is working along with genetic algorithm.

Cooperative fuzzy system in WSNs (CO-FAIS) [3], Cooperative based Fuzzy Artificial Immune System (CO-FAIS) is for to detect and eliminate Distributed Denial of Service (DDoS) attack in WSNs. This protocol is organized as six phases. The first phase examines and analyzes the incoming data packet to base station. In the second phase the suspicious behavior of the network is evaluated. The third phase recognizes the attacks in the system by analyze the deviations from the normal behavior of the system. In the fourth phase the continuous inputs are converted to four fuzzy inputs. If any abnormalities in the network, it will be controlled by the actions directed by the fuzzy outputs. Fifth phase is responsible for taking the final decision for the elimination of the specific attack. Sixth phase act as the prevention system in network for the possible future DDoS attack.

Strength:

This protocol is act as the artificial immune system for the WSNs. It can speedily detect and eliminate the attack as well as prevent the future possible DDoS attack on the nodes of WSNs.

Weakness:

In case of heavy traffic from nodes in the sensor field to base station, the data packet needs to be sniffs in offline (store it and process). It results high time complexity.

Anomaly detection in WSNs (TBAD) [4], Trust Based Anomaly Detection (TBAD) protocol has five phases. The first phase monitors the node in which needs to assess. In

the second phase characteristics of the node is represented as fuzzy system inputs, the fuzzy system produce suitable output based on the inputs. Third phase synthesis the evidence theory rules and determine the possible invasion to the system, the Direct Trust Value (DTV) is calculated. Fourth phase Indirect Trust Value (IDTV) is calculated by the evolution node from the evaluated node parameters. Fifth phase calculate the final trust value by considering the DTV and IDTV. Then the evaluated node is declared as malicious or normal node.

Strength:

The detection percentage of this model is high. By means of using fuzzy theory the trust value is generated. So that it reflect the possibility of the attack in the WSN more accurately.

Weakness:

In this approach the evolution node can able to collect packets from its one-hop node neighbor only. It reduces the possibility of getting more information regarding about the evaluated node.

Distributed anomaly detection for WSNs (DAD) [5], this protocol is proposed for the detection of anomalies in the large scale WSNs. It identifies both local and global anomalies in the WSNs. The local anomalies are one in which it cause in the node level of WSNs. The global anomalies are the one in which cause in the group of node in the cluster level of WSNs. In the local anomaly the particular node will be identified as threat. But in the group anomaly the particular cluster will be identified as the threat. The sensed data are partitioning by the fuzzy-C means clustering. The outlying data are identified by means of comparing with the threshold. This identification is extending to all clusters in the WSNs. The final anomaly computation is carried out by the gateway node.

Strength:

The experimental results show that the protocol is low communication overhead. This protocol is suitable for large scale WSNs. It is accurate and effective identification of anomaly throughout the sensors.

Weakness:

This protocol shows that high computational and communicational costs. The reported sensitivity value is marginal only.

Fuzzy Based Data Aggregation in WSNs (FBSDA) [6], FBSDA is a secure data aggregation protocol for WSNs. It organized as three phases. In the first phase sensor nodes are arranged as clusters. Each cluster a cluster head is selected based on the strongest signal strength of the node. Second phase is responsible for the calculation of the distance and trust value. The trust value is calculated by considering the communication factor and battery factor. The nodes for the data aggregation are selected by using fuzzy logic in the third phase. The fuzzy system considers the distance, power and trust value of the node to identify the legitimate node for the data aggregation from the group of nodes available in the cluster. So the malicious nodes were not allowed for the aggregation.

Strength:

This protocol is classifying the nodes in the cluster in to best node, normal node and worst node. The best nodes are only allowed for the data aggregation. That is why the malicious node and faulty node were eliminated from the aggregation. This protocol is consuming less energy.

Weakness:

Before start the data aggregation, every time the fuzzy decision has to be made. It will lead computation overhead whenever data aggregation is needed in the cluster level for more often.

Fuzzy Based Trust Prediction in WSNs (FTPR) [7], The FTPR protocol is design to counter black hole, on-off, bad mouthing and conflicting behavior attacks in WSNs. This protocol provides three inputs to the fuzzy system, such as trust value, number of fluctuations and recommendation inconsistency. The trust value is based on the direct and indirect trust values generated by nodes, considering the historical behavior and recommendation obtained from the neighbor nodes. The fluctuations are obtained by monitoring the change in the trust level of the neighbor nodes. The good node has almost constant thrust value. By considering the conflict behavior of the node, consistency value is calculated. The fuzzy system provides the future behavior of the node based on the above said three historical data inputs.

Strength:

This protocol is consuming less energy. It detects and eliminates various attacks such as black hole, on-off, bad mouthing and conflicting behavior. This protocol shows good packet delivery ratio.

Weakness:

The historical behavior of the nodes needs to analyze for to find out the future behavior of the node. Historical data includes the past transaction like failure and success rate of data forwarding of the particular node. So this protocol is incurring very high computational costs.

Fuzzy Based Anomaly Detection for WSNs (FBAIDS) [8], FBAIDS is an anomaly detection protocol in WSN. This protocol take various parameters as inputs such as energy of anode, honest of a node, unselfishness of a node and prediction variance of the node in a cluster. Honest of a node is calculated based on the past suspicious experience. Energy of a node is based on the residual energy. Unselfishness is based on the direct observation of a node in the cluster. Prediction variance enables the detection of an anomaly.

Based on the fuzzy output the particular node is selected or rejected as the member of the cluster.

Strength:

Each node involve in the data forwarding are undergo detailed observation based on its various parameters. This technique reduces the false positive rate in the WSNs.

Weakness:

In order to select various metrics such as honest, unselfishness, energy and the prediction variance of each node are by comparing the threshold values. The selected threshold value should be optimum always otherwise it won't give good results.

Fuzzy based Multi-hop Authentication in WSNs (FIMA) [9], FIMA protocol is a fuzzy based false negative attack detection scheme. The next node involve to en-route data packet to base station is decided by the fuzzy system in this protocol. Fuzzy system takes three inputs to produce verification interval. The inputs such as energy, hop count and false count generated by the cluster. Energy represents the balance energy available in the en-route node. Hop count represents the number of nodes between source and base station. When the false report is intimated by node, the false count will be incremented. Based on the fuzzy rule the suitable verification interval is report by the fuzzy system. When the fuzzy system reports high interval, then the skipping nodes will be more in the path of en-route to base station.

Strength:

This protocol is suitable for very large scale sensor networks. The cluster head is change often among the nodes to prevent the energy drain of the particular node as cluster head. Cluster head aggregates and compressed the sensed data before to the base station.

Weakness:

The sensor nodes are needs to maintain a large memory to store large amount of key values such as individual key and association keys. The verification node needs to perform various function such as receiving, transmit report and verification. The node act as verification node for long time, easily run out of energy.

II. CONCLUSION

The different fuzzy logic based secure WSN methods are compared in terms of node organization, type of attacks, authentication between node and base station communication, detection of the attack in the protocol, elimination of the attack and type of node considered in WSN.

TABLE: I

Protocol	**Node organization**	**Type of attack considered**	**Is Authenticate between node and base station communication**	**Detection of the attack**	**Elimination of the attack**	**Type of node considered**
ELEAP [1]	Cluster	Sinkhole	yes	yes	yes	Heterogeneous
FBFEIA [2]	Flat	False endorsement insertion	yes	yes	yes	Homogenous
CO-FAIS [3]	Cluster	Distributed Denial of Service	No	yes	yes	-do-
TBAD [4]	Flat	Anomaly Detection	No	Yes	No	-do-
DAD [5]	Cluster	Anomaly Detection	No	Yes	No	-do-
FBSDA [6]	Cluster	Detection of malicious nodes	No	Yes	Yes	-do-
FTPR [7]	Cluster	Black hole, on-off, bad mouth and conflicting behavior	Yes	Yes	Yes	-do-
FBAIDS [8]	Cluster	Anomaly detection	No	Yes	No	-do-
FIMA [9]	Cluster	False Negative attack	Yes	Yes	Yes	-do-

REFERENCES

[1]. Su Man Nam and Tae Ho Cho (2015) A fuzzy rule-based path configuration method for LEAP in sensor networks, Ad Hoc Networks 31:63–79

[2]. Hae Young Lee (2015) Fuzzy-Based Adaptive Countering Method against False Endorsement Insertion Attacks in Wireless Sensor Networks, International Journal of Distributed Sensor Networks,Volume, 11 pages

[3]. Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha Mat Kiaha, Vala Ali Rohani, Dalibor Petković, Sanjay Misra and Abdul Nasir Khan (2014) Co-FAIS:Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks, Journal of Network and Computer Applications, 42:102–117

[4]. Renyong Wu, Xue Deng, Rongxing Lu and Xuemin (Sherman) Shen (1015) Trust-Based Anomaly Detection in Emerging Sensor Networks, International Journal of Distributed Sensor Networks, 14 pages

[5]. Heshan Kumarage, Ibrahim Khalil , Zahir Tari and Albert Zomaya (2013) Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modeling, J. Parallel Distrib. Comput. 73: 790–806

[6]. Hevin Rajesh, D. and B. Paramasivan (2012) Fuzzy Based Secure Data Aggregation Technique in Wireless Sensor Networks, Journal of Computer Science 8:899-907

[7]. X. Anita, M. A. Bhagyaveni and J.Martin LeoManickam (2014) Fuzzy-Based Trust Prediction Model for Routing in WSNs, The Scientific World Journal, Volume 2014, 11 pages

[8]. Sumathy Murugan and M. Sundara Rajan (2015) Fuzzy Based Anomaly Intrusion Detection System for Clustered WSN, Research Journal of Applied Sciences, Engineering and Technology 9: 760-769

[9]. Thao P. Nghiem and Tae Ho Cho (2009) A fuzzy-based interleaved multi-hop authentication scheme in wireless sensor networks, J. Parallel Distrib. Comput. 69 : 441-450