International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 6(D); June 2018; Page No. 13327-13330
DOI: http://dx.doi.org/10.24327/ijcar.2018.13330.2371

Research Article

CONSTRUCTION OF INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORKS BY SYNTHESIZING ANOMALY AND MISUSE TECHNIQUES

Umarani C[1] and Kannan S[2]

[1]Research and Development Centre, Bharathiar University, Coimbatore, India, Jain University, Bangalore-69
[2]Madurai Kamaraj University Madurai Madurai, India

A R T I C L E I N F O

Article History:

Received 11th March, 2018
Received in revised form 6th April, 2018 Accepted 26th May, 2018
Published online 28th June, 2018

Key words:

Anomaly, Misuse, cluster, intruder

A B S T R A C T

Wireless sensor network (WSN) refers to a group of low cost, mini sensor nodes geographically deployed for monitoring and recording the physical conditions of the environment and aggregating the gathered data at a base location. Sensor nodes have self organizing ability, dynamic topology but they possess limited bandwidth, computing ability, limited battery power and storage space. Inspite of the above, sensor networks are being used widely and considered to be a boon where human interaction and wiring is impossible. As they are subject to various security attacks, Ensuring security is an important task in WSNs. In this research work, presented a tissue growing procedures inherited from human immune Biology which does security enhancement by concentrating on effective node aggregation wherein malicious nodes are eliminated and then clustering is initiated in the Anomaly detection procedure, misuse identification procedure detects the multiple attacks. When both the procedures are combined together, it provides a effective Intrusion detection system against attacks which combines both anomaly and misuse detection techniques together.

INTRODUCTION

Anomaly Detection: In WSN, there are many IDS mechanisms that use anomaly detection techniques. These types of systems usually rely on analyzing whether the behavior of sensor nodes can be measured as normal or abnormal according to certain assumptions and metrics. Most researchers have taken this approach as a main method to detect intrusions, as they consider it is easier to apply than misuse or specification based detections.

Misuse Detection: The relevance of rule-based or misuse detection techniques in the perspective of a WSN is a intricate task. In practice, it is difficult to think exactly as an attacker or to know the intention of the attack. So it is necessary to model attack patterns according to attacks that might occur in future. Moreover, the severe memory constraints of WSNs make misuse-detection based IDSs that need to store attack signatures relatively difficult to utilize and less likely to be efficient.

This work is a combination of both Anomaly and Misuse detection techniques. Cross breed of two techniques are designed to provide High levels of security in the wireless sensor networks.

Corresponding author:* **Umarani C
Bharathiar University, Coimbatore, Madurai, India

The First level effectively cluster the cells in the network by enhancing grouping scheme, routing discovery and scheduling calculations for anomaly detection. After predicting the malicious cell, update the abnormal cell in the routing table. The second level identify the intruder cell in the network.

Related study

Clustering Algorithm Based Approach: Loo *et al*. developed an intrusion detection scheme for routing attacks that uses a fixed-width clustering algorithm to build a model of normal behavior. Note that here we refer to clustering algorithm as unsupervised learning algorithms, not cluster-based network structure (although this approach can be used in clustered networks). They use this model to detect anomalous traffic patterns. The IDS module is implemented on each sensor node and twelve network traffic patterns are identified.

These features are used in the training and testing stages. In the training stage, a fixed-width clustering algorithm is used to build a set of clusters in the feature space. Clusters that contain less training traffic samples than a specific threshold are identified as anomalous. During the testing stage, each traffic sample is compared to the cluster set to determine whether it is anomalous or not too much computation on sensor node. The authors claim that since the proposed IDS do not require communication between sensor nodes, it significantly reduces the power consumption. However, a statistical analysis of the actual reduction in power consumption compared to other existing IDSs is not provided.

Wang and Zhang proposed an anomaly detection system based on the arrival order of different packets. The system is based on certain assumptions: all sensor nodes can become cluster heads, only communicate with a limited number of nodes, and should follow corresponding protocol specifications. The IDS has two stages: profile learning and anomaly detection. In the profile learning stage, a node traffic profile is created by extracting data from the information flow such as the source and destination addresses and the packet types. In the anomaly detection phase, a pattern matching technique is used to detect any unknown subsequences of packet events. Drawbacks: The limitation of this work is that the algorithm was not evaluated and performance results were not provided.

Artificial Immune System: In a departure from traditional anomaly detection techniques, the necessity of artificial immune systems (AIS) was discussed. Shaust *et al*. address these biologically inspired algorithms as a possible solution to detect misbehavior in WSNs.

Anomaly Detection Procedure in WSN

Tissue comprises of a series of linked cells, each cell "grown" according to its interaction with tissue environment. There are some significant issues to be tacked to make the proposed procedure truly effective.

1. Cells should grow and be supported by homogeneous data. Where data does not exist to support a cell, the cell dies. Where too diverse data exist for a cell, the cell divides.
2. Given a data stream of temporally homogenous data items, the tissue will quickly grow to form a specific shape, structure and size. If the data changes, the tissue will change in response.
3. The tissue should have the ability to dynamically cluster cells and be sensitive to cellular damage.

The anomaly detection procedure is clearly observed that the tissue cells are grouped to maintain the cells in a dynamic system. The progression of the combination of cells in a closely organized an enormous measure of tissue is recognized as the networked tissue growing. Thus the cluster head selection process is initiated as the IDS cell and pointing towards the corresponding neighbor cells as the cluster members. The anomaly detection framework is performed based on this technique for explicit attack patterns and it verified in terms of normal or malicious behavior of the cell. The procedure to perform the networked tissue growing is listed as follows:

Anomaly Detection Procedure

1. Gather the nodes with similarity in their resources based on their log Information.
2. Compute the Packet dropping Rate of the individual nodes and the Maximum dropping rate.
3. Include cluster member based on the position and low failure rate.
4. Ensure the maximum number of nodes does not exceed 15 for a single cluster Head.
5. Confirm cluster members are located in the identical location with Cluster head to enable single hop communication.
6. Preliminary Data communication starts with the nodes having identical resources.
7. Packet drop rate is considered as a parameter and if it is more than 60%, then the node is identified as danger and alarmed
8. Remove the node in the cluster if it satisfied the above condition to evade miss detection by the neighbor node for future routing.
9. Recombine all the nodes that have sufficient resources to form successful hierarchical routing to base station.
10. Calculate the life time of each node based on the parameters like Tx, Rx, Idle and sleep time for a particular time slot and decide if they are relay node to others.
11. Node is not chosen as relay node if it has energy less than 20% on comparison with other cluster members.

Then derive the communication network tissue based on the specific cells. The tissue is made up of multiple number of cells. This cells are employed for transmitting the data packets without loss packet information. In this procedure, clustered the group of cells to communication between the sources to destination cell based on the route discovery. The efficient data transmission path is discovered based on the route discovery helps to predict the path, in case of failure in one path it will take another path to reach the destination. Next, evaluate the cell based on the RREQ, the source cell will select the neighboring cell to transmit the message. If sense the signal of the cell due to the route request code. Otherwise, drop the request. If presence of malicious cell in the communication tissue, then re-evaluate the RREQ and cell scalability. Or else, update the normal cell information in the routing table for using communication tissue.

After that, initiating the data aggregation scheme which is a process of aggregating and summarizing the sensor data packets of several cells using the network aggregation approach. It is the global process of routing and gathering data over a multi-hop system. The reduction of resource consumption and increase the network lifetime are the major scenarios. The number of transmission reduces and improve the WSN utilized bandwidth and energy. Finally, evaluate the forward path to transmit the data packets.

Misuse Detection Procedure in WSN

The work inherits the danger theory and the dendritic cell (DC) procedure. Inspired by Human Immune system .Sensor nodes identify intrusion by monitoring the environment and collaborating with others. In this framework, sensor nodes have two roles, DC sensor and organization sensor. Monitoring module, intrusion detection module, environment module, parameter library module, and rule module are deployed on DC sensor; decision module and operation module are deployed on organization sensor. Tests were carried out in simulated environment, and the framework has better detection efficiency and lower energy consumption compared with the existing model.

Inspired by the dendritic cell differentiation theory of the congenital immune mechanism in biological immune system, this work proposes a wireless sensor network intrusion detection framework. The main contributions of this framework are as follows: abstracts the information fusion process of DCs; In this work, performances of the model are analyzed, including the scalability, robustness, and complexity, and experimental results show that the model has better

detection performance and reduces the system energy consumption.

Danger signals are released when cells die. Danger signals are also index of anomaly, showing that the possibility of anomaly is larger. Safety signals are released when cells perform apoptosis normally. When DC receives security signals, it produces semi-mature DC cytokines signals, which shows that the antigen is collected in the normal environment. If there are cell apoptosis and necrosis in the organization at the same time, safety signals can inhibit mature DC cytokine signal. Safety signals are index of normal behavior. When it is applied to intrusion detection, it also can be derived from the frequency of sending/receiving network packets per second, and lower value means that the system behaves normally.

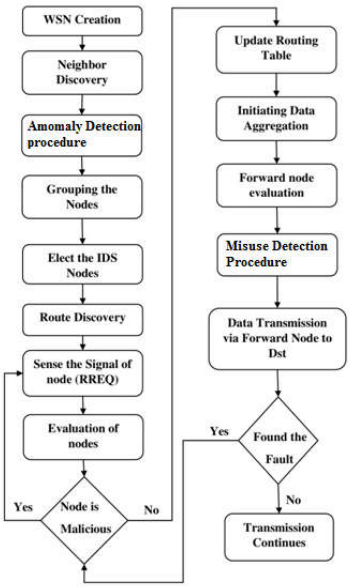
Misuse Detection Procedure

1. Load the nodes which are IDS nodes to detect live attacks.
2. Hello Packets are broadcasted by normal and malicious nodes at fixed intervals, the IDS nodes update their neighbor's lists by overhearing these Hello Packets.
3. Calculate all failure types in the cluster nodes.
4. Find out if round failure value is greater than the cumulative value.
5. If step 4 is true then, report about the attacker as an error to the source.
6. If step 4 is true then, update cumulative value by combining it with round-failure value.
7. Repeat steps 3-6 for all the neighbors in cluster.

Deals with finding out the malicious cell by taking into consideration the clustered cells grown into normaltissue. Dendritic cells are antigen presenting cells.Dendritic differentiation theory is applied to differtiate the dendritic cells into Semimature or mature cells.if the concentration of semi mature cytokine is greater than the mature cytokine,it is set as semi-mature otherwise as mature.Antigens are computed for mature or semimature status in the dendritic framework.And if tested semimature most of the time,it is set as normal else malicious.

Synthesis of Anomaly and Misuse Detection Procedure In WSN

The propose Procedure is mainly utilized for the task of detecting the anomaly presence in the sensor cells that tissue (communication network) is made up of the multiple number of cells. The tissue is designed with the help of Artificial Immune Systems (AIS) which includes a sequences of connected cells, for each node "developed" in reaction to a detailed information in a data stream being participation of the network. There are multiple ways in which communication tissue can be created. But, at this time double processes are performed such as networked, and a Misuse detection procedure. If any anomalies presence in the input stream, then using danger signals as approximate alerts because both tissue growing commendably acts as a dynamic clusters. Then the characteristics of the two procedure states that the computational time be subject to the scope of the opening on the information-size of any dataset are independent, and the bitrate of the information stream.



Synthesis of Anomaly and Misuse Detection Procedure

1. Gather the nodes with similarity in their resources based on their log Information.
2. Compute the Packet dropping Rate of the individual nodes and the Maximum dropping rate.
3. Include cluster member based on the position and low failure rate.
4. Ensure the maximum number of nodes does not exceed 15 for a single cluster Head.
5. Confirm cluster members are located in the identical location with Cluster head to enable single hop communication.
6. Preliminary Data communication starts with the nodes having identical resources.
7. Packet drop rate is considered as a parameter and if it is more than 60%, then the node is identified as danger and alarmed
8. Remove the node in the cluster if it satisfied the above condition to evade miss detection by the neighbor node for future routing.
9. Recombine all the nodes that have sufficient resources to form successful hierarchical routing to base station.
10. Calculate the life time of each node based on the parameters like Tx, Rx, Idle and sleep time for a particular time slot and decide if they are relay node to others.
11. Node is not chosen as relay node if it has energy less than 20% on comparison with other cluster members.
12. Load the nodes which are IDS nodes to detect live attacks.
13. Hello Packets are broadcasted by normal and malicious nodes at fixed intervals, the IDS nodes update their neighbor's lists by overhearing these Hello Packets.
14. Calculate all failure types in the cluster nodes.
15. Find out if round_failure value is greater than the cumulative value.
16. If step 4 is true then, report about the attacker as an error to the source.
17. If step 4 is true then, update cumulative value by combining it with round-failure value.
18. Repeat steps 3-6 for all the neighbors in cluster.

Implementation Process Using NS2

Simulation Model: In the simulation model, the proposed framework is evaluated with the help of NS2 tool. The 1000m × 1000m square area of the simulation field is evaluated and applied with the random clustered management of sensor cells.

RESULTS AND EVALUATION

This section use the NS2 modeler to construct the WSN topology and analyze the communication phase and shows the effectiveness of the proposed system by comparing with the existing frameworks in terms of end to end delay, throughput, routing overhead, packet delivery fraction, and the remaining energy. The results shows that this synthesized procedure produces good results.

CONCLUSION

In this work, Anomaly detection is implemented by effective clustering of the cells in the network. After predicting the malicious cell, update the abnormal cell in the routing table. The misuse detection procedure identify the intruder cell in the network. The simulation results of the proposed procedure is compared to the existing methods .The computed performance metrics such as energy consumption, packet delivery fraction, routing overhead, throughput, and end to end delay assured the effectiveness of the proposed technique recommendation.

References

1. N. Assad, B. Elbhiri, M. A. Faqihi, M. Ouadou, and D. Aboutajdine, "Efficient deployment quality analysis for intrusion detection in wireless sensor networks," *Wireless Networks,* vol. 22, pp. 991-1006, 2016.
2. M. Wazid and A. K. Das, "An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks," *Wireless Personal Communications,* vol. 90, pp. 1971-2000, 2016.
3. G. Rajeshkumar and K. Valluvan, "An energy aware trust based Intrusion Detection System with adaptive acknowledgement for Wireless Sensor Network," *Wireless Personal Communications,* pp. 1-15, 2017.
4. A. Puri and N. Sharma, "A Survey On Intrusion Detection System," 2017.
5. N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks,* vol. 9, p. 167575, 2013.
6. T. Eswari and V. Vanitha, "A novel rule based intrusion detection framework for Wireless Sensor Networks," in Information Communication and Embedded Systems (ICICES), 2013 International Conference on, 2013, pp. 1019-1022.
7. C.Umarani, Dr.S.Kannan, "Bio Inspired Dynamic Routing protocol", *International Journal of Pharma and Biosciences*, ISSN 0975-6299
8. N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energyefficient routing protocols in wireless sensor networks: A survey," IEEE Communications surveys & tutorials, vol. 15, pp. 551-591, 2013.
9. C.Umarani and Dr.S.Kannan, "Malicious nodes Expulsion and clustering in WSN based on Network Tissue growing Procedure Galvanized by Immunobiology" in the *International Journal for Research and Development in technology ISSN 2321-9939April 2018.*
10. C.Umarani and Dr.S.Kannan, "Human Immune based Intrusion detection in WSN using Swarm Tissue growing Algorithm " in the *International Journal of advanced Research in computer and communication Engineering ISSN 2278-1021 April 2018.*
11. I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE communications surveys & tutorials, vol. 16, pp. 266-282, 2014.

How to cite this article:

Umarani C and Kannan S (2018) 'Construction of Intrusion Detection System for Wireless Sensor Networks by Synthesizing anomaly and Misuse Techniques', *International Journal of Current Advanced Research,* 07(6), pp. 13327-13330.
DOI: http://dx.doi.org/10.24327/ijcar.2018.13330.2371

****