Survey on Clustering Techniques and Intrusion Detection System in Wireless Networks

[1]Dheeraj Pandey, [2]Meet Poladia, [3]Neha Sarade

[1, 2, 3] PG Students
[1]Department of Electronics and Telecommunication Engineering,
[1]Sardar Patel Institute of Technology, Mumbai, India

***Abstract* - In the wireless communication there are multiple ways in which the cluster can be made and the security can also be enhanced. In this paper we are going to review multiple clustering and Intrusion detection system. From the methods reviewed we will be conclude the best amongst them. The advantages and disadvantages would be kept in mind.**

***Index Terms* – IDS,Clustering,WSN**

I. CLUSTERING ALGORITHM

There are variety of protocols proposed for enhancing the life of the wireless sensor nodes (WSN) and for routing the correct data to its correct base station. Many of them as not suitable as the battery power is the major resource of any of the nodes so the first priority is saving the battery power. There are many greedy algorithms used for saving the battery power and to choose cluster heads in ad hoc network and wireless network. Few criteria are as follows:

1. Lowest-Id clustering algorithm.
2. Highest-connectivity clustering algorithm.
3. Least clustering change algorithm.
4. Weighted clustering algorithm

LOWEST ID CLUSTERING (LID) ALGORITHM

Basically LID is a 2-hop clustering algorithm. When the algorithm executes the, a node periodically broadcasts the list of nodes that it can hear including itself. When any nodes hears the list of nodes with higher ID than itself from the 1-hop neighborhood are termed as cluster heads. It then broadcasts its ID and cluster ID. When a nodes which has the ability to hear two or more cluster heads and that lies between the transmission ranges of the cluster heads is called as gateway nodes else is any other ordinary node. The LID uses a greedy based algorithm where a unique ID is assigned to each node and chooses the cluster head with the smallest ID value. LID is efficient in those networks where the network topology changes frequent over the time. The major disadvantage is the fast battery drainage of the cluster heads and the gateway nodes.

HIGHEST-CONNECTIVITY (HCN) CLUSTERING ALGORITHM

In HCN unlike LID the nodes here are termed as cluster heads if have the highest connectivity (or degree). The degree or the connectivity is the number of links to its 1-hop neighbors. HCN is purely based on the Link Cluster Algorithm. The HCN incurs a higher message overhead because the information about the degree or the connectivity is exchanges. Thus the throughput is comparatively low in the HCN algorithm.

LIST CLUSTER CHANGE (LCC) ALGORITHM

The list cluster change algorithm is used to minimize the frequency of the cluster heads. Since cluster stability is a major concern for the network to work so LCC is applied under such circumstances. Since the topology of the network changes often this system provides robustness to the system at large. The major advantage of using the LCC algorithm is that it has low latency and low routing overhead. In this algorithm the major disadvantage is of its load distribution amongst the nodes which is very unfair.

WEIGHTED CLUSTERING ALGORITHM (WCA)

The base of the WCA is the combined weight metric. It includes one or more parameters like the node degree, node speed, distance with respect to a node neighbor, battery of the node and the time spent as cluster head in the system. Here the nodes broadcast the weight value and the cluster head is the one with the highest weight among the neighbors. The advantage of this algorithm is its load balancing as it restricts the number of nodes in the cluster. The major disadvantage of this algorithm is the overhead as here the decision is based on the neighbor.

All the above methods are heuristic approach but are more application specific than can be used for generic Wireless mobile networks. The solution provided is not optimal that is the clustering should enhance network manageability, channel efficiency, and lastly economic energy. The more popular algorithms are as follows.

LINKED CLUSTER ALGORITHM (LCA)

In this algorithm all the nodes are organized into a set of cluster nodes. And every node should be inside any of the cluster. Here the cluster heads are linked with the gateway nodes providing the global network as the neighbors can access them. A node can be cluster head if it has the highest ID value or its neighbor has the highest ID value in the cluster. Here if the cluster nodes are arranged numerically according to the IDs then the performance of the system will degrade. One more hybrid come here of the LCA system as LCA2 which uses LID mechanism but both the algorithm has a disadvantage that is the load is not evenly distributed and also it has relatively high control message overhead since there is broadcast at the starting. The LCA also does not consider the node mobility, adaptive transmission range and power efficiency issues.

LOW-ENERGY ADAPTIVE CLUSTERING HIERARCHY (LEACH)

It is a popular energy-efficient adaptive clustering algorithm, here the cluster head nodes are created on the basis of the energy and the cluster heads act as the router for that cluster. LEACH is application specific data dimension algorithm which uses the highest energy node as cluster and increase the system time of operation. In this protocol the cluster heads are randomly (Based on energy) shuffled so that the life prolongs and the load of the nods are also evenly distributed. That is all the disadvantages of the old protocol which were used are overcome in LEACH.

LEACH uses three techniques namely

1. Randomized rotation of the cluster heads and corresponding clusters.
2. Localized coordination and control for cluster set-up and operation.
3. Local compression to reduce global communication.

In the LEACH the clustering terminates within the finite iterations as it shuffles the nodes and there can be finite number of nodes present in the cluster. It does not guarantee good cluster head distribution and also it assumes uniform energy consumption of nodes.

II. INTRUSION DETECTION ALGORITHM

Many intrusion detection system has been proposed in the wired network but similar is very difficult when we are in an Ad hoc wireless network. Since in the wireless network we have both legitimate and malicious user therefore it is difficult to identify them. Here there is no difference between the usual and malicious activity therefore the traditional detection system of wired network is not applicable here. The Intrusion detection system of the wireless network are as follows:

WATCHDOG

The main aim of the watch dog technique is to improve the output within the presence of the malicious nodes. The watchdog is divided into two types namely watchdog and the path rater. Where the work of watchdog is to serve as intrusion detector in the wireless system.

Here the watchdog will listen to its next hop's transmission and will detect the presence of malicious node accordingly. Watchdog hears that if the next node is not sending the data with the time stamp specified then it increments the failure counter of that node and if the failure counter exceeds the predefined limit then watch dog notifies that the node is misbehaving. Watch dog maintains a buffer too which contains the recently sent packets and checks if the node is forwarding the same packet or not if in case the packet is in buffer for too long the watch dog reports it as misbehaving. The drawback of watchdog are 1) ambiguous collisions, 2) receiver collisions 3) limited transmission power, 4) false misbehavior report, 5) collision, and 6) partial dropping.

END-TO-END ACKNOWLEDGEMENT SERVICE (ACK)

There are many system using ACK to detect routing misbehavior or the malicious node in the system. Here the receiver sends an acknowledgement message to the sender saying that the package has reached successfully. To detect the malicious nodes easy here as the malicious node attracts the traffic towards itself but fails to forward it a protocol named trace route was proposed which allows the sender to set the Time To Live (TTL) of the packet. It waits for a warning message from the router calculating the time when TTL expires. The trace route then disguise the packet and send over the routers. To efficiently find the malicious nodes the binary search is performed on the routes. The ACK works only in the static environment. When the malicious link is found then its weight is increased so that it cannot be used for future transmissions.

TWOACK

In TWOACK the packets are sent by the receiver for every data packet received from the sender. Acknowledging a fraction of received data packets gives the TWOACK scheme better performance with respect to routing overhead. The TWOACK scheme has an authentication mechanism to make sure that the TWOACK packets are genuine. Whereas the selective TWOACK (S-TWOACK) mainly acknowledges the receipt of a number of data packets.

ADAPTIVE ACKNOWLEDGEMENT (AACK)

The AACK is based on the TWOACK and ACK. The AACK considerably reduces the network overhead without affecting the output of the system. Here when the sender sends the data packet let say P1 to the receiver all the nodes in between just forwards to packet to the destination once the receiver receives the packet it will send an ACK to the sender if the sender receives the ACK within the specifies time stamp then only it will state it as successful else will change to TACK.

The hybrid of schemes has enhanced the network performance as the overhead in the network is greatly reduced. Since the protocols are very effective TWOACK and AACK fails to detect malicious node with the presence of false misbehavior report and forged acknowledgement packet.

ENHANCED ADAPTIVE ACKNOWLEDGEMENT (EAACK)

To overcome the drawbacks of the AACK the EAACK comes into the picture which is hardware efficient that is it requires very less amount of hardware. EAACK is an acknowledgement based IDS that is acknowledgement and time stamp are its tools for threat detection. Here Digital Signature can also be used for preventing the attacker for faking the acknowledgement packet. The EAACK is divided into three sections namely:

1. ACK
2. S-ACK
3. MRA

The major aim of the EAACK is always reducing the network overhead and removing the malicious node. EAACK uses the ACK as the transaction is based on the acknowledgement which the receiver provides to the sender. In ACK mode, when the sender sends the message to the receiver, a time stamp is started and if the acknowledge packet is not received within the predefined time limit the ACK assumes that there is some malicious present in the network and it hand over the power to S-ACK to detect the threat. In S-ACK part, now for every three consecutive nodes the third node will send an S-ACK acknowledgement packet to the first node. If the source node found something malicious in the S-ACK packet it would initiate the MRA mode that is the destination path will be changed. To start the MRA mode, the source nodes should first search its local table to find if a new route is possible or not if the new route is possible then the source should check that route and take that route to the destination node. If there is no other route possible, the source node should starts a routing request to find a new route to destination.

III. CONCLUSION

By studying the above algorithms we can review that LEACH is the best suited algorithm for the project as it enhances the network life and the load is equally divided on all the nodes leading to more stability. Here a constant energy is deducted when the node is acting as the head. For intrusion detection we have reviewed EAACK as the best method as it is hardware efficient and can easily find the malicious nodes

IV. .ACKNOWLEDGMENT

The authors of this paper take this opportunity to thank all the concerned who helped us in our research. We would like to acknowledge our Institute, Department of Electronics and Telecommunication Engineering for their constant motivation and support and helping us all to frame the issues and giving us proper guidance.

At last, we also thank all our colleagues who assisted and backed us during our research.

REFERENCES

[1] Sweta M.,Mamta A., ``Survey on Intrusion Detection Mechanisms for MANETS",IJCSIT, 2014.

[2] Pratibha Wage, Channveer Patil, ``INTRUSION-DETECTION SYSTEM FOR MANETS: A SECURE EAACK", IJRET, 2014.

[3] S. Sujatha, 2, B. Lakshmi Radhika, ``A Study On Enhanced Adaptive Acknowledge (EAACK) Scheme in Receiver Collisions – An IDS in Wireless Mobile Ad-Hoc Networks",IJES, 2013.

[4] Shio Kumar Singh 1, M P Singh 2, and D K Singh, ``Energy Efficient Homogeneous Clustering Algorithm for Wireless Sensor Networks", IJWMN, 2010.