Abstract— MANET is a well-known network in which wireless nodes are connected. The infrastructure-less nature of the Node [1] causes several issues including secure routing, energy consumption and node authentication. This paper ensures an Energy Efficient Administrator [2] and Watch node based Secured Routing (EEAWSR) protocol that ensures energy efficient secure routing in MANET. Thus this attempts to reduce the computational overhead to offer an energy efficient scheme. In MANET there is no fixed scenario, which provides help to setup or perform the required network activity. Thus the nodes are the routers transferring the data packets themselves. So a robust routing protocol that will perform all the functions but with an optimized network activity to decrease the network traffic as well as make the transmission fast is essential. While building the routing protocol, it is kept in mind these three factors: making the transmission fast, decreasing the network traffic and properly utilizing the energy consumed by each router. To ensure security, this paper classifies the nodes in the network into several categories such as administrator nodes, associative nodes, watch nodes and common nodes based on the range and the position of the nodes in the network. Basically watch nodes have been used to promote security in the network. This protocol hopes that, if it is able to implement security in the admin and the associative nodes, it can guarantee that the total network is secured from any attacks since the common nodes do not have any role to play in transmission of data apart from sending or receiving of data packets. So our proposed work selects an energy efficient watch nodes to monitor the admin/ associative nodes effectively. The proposed EEEAWSR outperforms the existing solutions and leads to a decent solution as it sends data at an optimal speed while taking care of the computational overhead.

Keywords— Admin Node, Associative Node, Common Node, Watch Node.

I. OBJECTIVES

- To propose a novel protocol called Energy Efficient Administrator and Watch node based Secured Routing (EEAWSR) to ensure energy efficient secure routing of data packets in MANET with reduced computational overhead than existing schemes.
- To select energy efficient watch nodes to monitor the activities of the admin and associative nodes.

- To reduce the amount of network activity for each node required to route a data packet to achieve high security with reduced energy consumption.
- To detect and prevent various routing attacks that may jeopardize any wireless network.

II. EXISTING AODV SYSTEM

In AODV, a source node initiates route discovery when it needs to communicate with a destination for which it does not have a route. Then the Route discovery is initiated by the source node broadcasting a route request message (RREQ) that contains a request ID. If a node receives a RREQ that it received previously, it drops the request. Otherwise, it stores the address of node from which it received the request. In this manner, a reverse route to the source is maintained or established. If the RREQ reaches the destination node or a node that has a route to destination, the node sends a route reply message (RREP) to the source node. Intermediate nodes that do not have a path to the destination re-broadcast the request when they receive it for the first time. As the RREP is sent back to the source node, each node stores the address of node that sent the reply [3]. The forward path determined from the source to the destination is used for sending packets to the destination. AODV uses sequence numbers maintained for the different destinations so as to guarantee freshness of routing information. AODV nodes offer connectivity information by broadcasting local Hello messages[4]. If a node does not broadcast within a specified time period, it broadcasts a Hello message. Thus, a node may have a local table that contains all of its correspondence neighbors.

III. DRAWBACKS

AODV has involved in a lot of network activity associated with it since there are routing packets transmitted all over the network to know the desired route with more wastage of energy. Moreover, AODV does not ensure secured routing and is susceptible to many attacks. In the proposed protocol the admin nodes take the duty of network transmission and so the overall load on the network decreases many folds.
The network traffic depends on the dynamic nature of the network, lower the amount of changes in network, lower will be network traffic.

IV. PROPOSED SYSTEM

This work proposes a novel energy efficient and administrator based secure routing protocol for MANETs. This protocol ensures security to the MANET by using various types of nodes such as associative nodes, common nodes, administrator nodes, associative nodes and watch nodes [5]. The watch nodes play an important role in ensuring the security. Initially this protocol involves in the selection of the admin or administrator nodes. A list having the names of all the nodes and their corresponding neighbors is prepared and sorted according to the highest number of neighbors each node has and all the possible nodes are selected in a top-down sequential manner. If the list of nodes is the subset of neighbor of that node, then that node will be considered as an admin node. If it does not cover the entire nodes in the network, union of any other nodes can be considered till it satisfies the subset criteria. The admin nodes communicate with the associative nodes and if necessary they communicate through associative pairs. Any two neighbors of each admin nodes are considered as watch dogs. All other nodes apart from these three categories fall under common nodes. This protocol works under the principle that if security principle is applied on the admin nodes and associative nodes, it is able to ensure complete security to the entire network [6]. Watch nodes implements the security principle. Watch nodes monitors the traffic patterns of each admin and Associative node in which, it checks after every time interval if any data packet entering into an Admin or Associative node goes out of the node within a stipulated period of time, failing which it issues a warning to its previous admin that the node may be a malicious node then The detected node is not used further for data transmission through the network.

V. ADVANTAGES

- The proposed existing EEAWSR protocol ensures energy efficient and secured data transmission in MANET using the watch nodes and admin nodes.
- Through using the admin node, this protocol reduces the amount of network activity for each node that is required for data transmission that leads to less energy consumption.
- The proposed protocol ensures security with reduced energy consumption.

VI. CONTRIBUTION

It is known that watch dogs are used to ensure security in this proposed approach. The proposed work hopes that if security system is implemented in the admin and the associative nodes, it can guarantee that the entire network system is secured from any attacks. Activities of the common nodes are not to be concentrated as they do not have any other role in data transmission apart from sending or receiving of data packets. Instead of selecting any two neighbors of admin and associative node as watch nodes, this paper proposes to select energy efficient watch node selection process. The admin or associative node may have two or more neighbors. In that case, two nodes with high energy can be selected as the watch nodes. As the watch nodes have to perform additional works, they should have sufficient energy.

VII. ENERGY EFFICIENT WATCH NODE SELECTION

If the admin or associative nodes have only two neighbors, those two neighbors are selected as the watch nodes. In case, if the admin or associative nodes have more than two neighbors, then the list of energy levels of neighbor nodes of admin and associative nodes are prepared. Then Sort the energy level list in the decreasing order. Select the first two nodes as the watch nodes.

VIII. INTRODUCTION

A major role to globally reduce energy consumption will be played by Ad hoc routing technologies. The communication in case of Mobile Adhoc network, MANET, is mainly based on the radio signals transmitted by the node. Again MANET, being a wireless network, is quite different from the common Mobile communication. In Mobile communication bridge networks within its own range are used by the nodes to communicate with another nodes. The bridge networks act as base stations which the source node needs to contact while sending a data packet to its destination. In MANET, there is no base station or any other scenario help to setup or perform required the network activity. Hence in this case the nodes are the routers transferring the data packets it selves. Hence a robust and good routing protocol that will perform all the necessary functions but with an optimized network activity to decrease the network traffic as well as make the transmission fast is very essential.
International Journal of Emerging Technology and Advanced Engineering

The insecurity of the wireless links, energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes have been identified in literature as such challenges. So, the single most important feature that differentiates MANET is the absence of a fixed infrastructure. In the absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a line of defense, separate nodes into trusted and non-trusted. Such a distinction would have been based on a security policy, the possession of the required credentials and the ability for nodes to validate them. In the MANET context, there may be no ground for an a priori classification, thus all the nodes are required to cooperate in supporting the network operation, meanwhile no prior security association can be assumed for all the network nodes.

Additionally, in MANET freely roaming nodes form transient associations with their neighbors, join and leave MANET sub-domains independently and without any notice. In such environment, there is no guarantee that a path between two nodes would be free from malicious nodes, which may not comply with the currently existing protocol and attempt to harm the network operation, currently The mechanisms incorporated in MANET routing protocols cannot cope with disruptions due to malicious behavior of node. For example, any node can claim that is one hop away from the destination, causes all routes to destination to pass through itself. unfortunately a malicious node might corrupt any in-transit route request (reply) packet and cause data to be misrouted [7]. The presence of even a small number of adversarial nodes could result in repeatedly compromised routes, as a resultant, the network nodes would have to rely on cycles of time-out and new route discoveries to communicate.

This paper proposes a novel protocol that mitigates the network activity ensuring energy efficient and secured routing protocol in MANET. Moreover, the proposed protocol detects the malicious activity by using the watch nodes in the network. The network set-up or organization of nodes in this paper is different from the existing works.

IX. OVERALL DESCRIPTIONS

- **Highly secure**: Provides transmission of data in a secured manner and detects the attacks that may jeopardize the network operation.
- **Communication**: Communication occurs and data was sent in a data forwarding path.
- **User friendly**: The Architecture is simple and allows users to access the project easily.

- **Energy efficiency**: The node’s operation involved in this proposal consumes less energy.

X. QUALITY ATTRIBUTES

- **User-friendliness**: The proposed system will be user-friendly, designed to be easy to use through simple interface. The software could be used by anyone with necessary computer knowledge. The software is created by an easy look and feel concept.

- **Reliability**: The system will never crash and fail. But in case of system failure, the recovery could be done by using advance backup features.

- **Maintainability**: All code shall be fully documented. Each function shall be commented with pre- and post-conditions. All program files will include comments concerning date of last modification. The code should be modular, to allow future modifications. Here for defects the system maintains its solution database.

XI. SIMULATION MODEL

An extensive simulation model having scenario of n (user defined) Mobile nodes and n UDP/TCP connections is used to study inter-layer interactions and their performance implications. The other parameters are used in this model are as under:

**MODULES**
1. Friend’s list preparation
2. Admin nodes selection
3. Associative, common and watch nodes selection
4. Battery Life, Admin Reselection and Backtracking
5. Misbehavior activity detection
6. Performance evaluation

**MODULE 1**

**Friend’s List Preparation:**

Every node in a MANET has a range of itself i.e. no node is capable of transmitting a data packet to an infinite distance. The nodes which fall in the range of a particular node are called its Neighboring nodes. In our algorithm we have alternatively used friend nodes for neighbor nodes, both being the same. In the network, four types of nodes have been used:
1. Common nodes
2. Associative nodes
3. Administrator nodes
4. Watch Nodes

The classification is based on the range and the position of the nodes in existing network. But to understand the classification, it is required to understand how the entire network sets up [8]. After a stipulated time period each node checks for its neighbors nodes, i.e. which nodes are within its range. From this friend list, a list is prepared which contains all the neighboring nodes for all the nodes in network. Next, the node compares its present and previous list to check for network change and reports any difference to its administrator. The administrator node always lies in the range of the node in question. The selection of admin node will be discussed in the following section. If there is no change in the topology of the network, there is no need to choose an administrator node. For the clear explanation, let us consider the following network:

For the above network in figure, the friend’s list has to be prepared first and only then can selection of admin nodes can be done. The neighbor list is as follows (table 1):

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Friends</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A,B,M</td>
</tr>
<tr>
<td>B</td>
<td>A,B,C,D,H</td>
</tr>
<tr>
<td>C</td>
<td>B,C</td>
</tr>
<tr>
<td>D</td>
<td>B,D,F</td>
</tr>
<tr>
<td>E</td>
<td>E,F,I</td>
</tr>
<tr>
<td>F</td>
<td>D,E,F,G,I</td>
</tr>
<tr>
<td>G</td>
<td>F,G</td>
</tr>
<tr>
<td>H</td>
<td>B,H</td>
</tr>
<tr>
<td>I</td>
<td>E,F,I</td>
</tr>
<tr>
<td>J</td>
<td>J,L</td>
</tr>
<tr>
<td>K</td>
<td>K,L</td>
</tr>
<tr>
<td>L</td>
<td>J,K,L,M</td>
</tr>
<tr>
<td>M</td>
<td>A,L,M</td>
</tr>
</tbody>
</table>

**MODULE 2**

**Admin nodes selection:**

A list with the names of all the nodes and their corresponding neighbors written beside them is prepared and sorted according to the highest number of neighbors each node has and all the possible nodes are selected in a top-down sequence. If the list of names of all the nodes is a subset of the neighbor list of that node we will designate it as the Admin node else consider any two nodes from the comprehensive sorted list in a top-down sequence. Next the union of the neighbors of the two selected nodes is considered, if the entire list results as a subset of the union those two nodes are considered as the Admin nodes. However for a negative result, consider any three nodes from the sorted comprehensive list in a top-down sequence and continue the process. This process is continued by increasing the number of nodes until the subset criteria is satisfied after which the Admin’s are selected as those nodes whose friend list covers the complete network. The sorted friend’s list is shown in table 2.
TABLE 2: SOR TED FRIEND’S LIST

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Friends</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>A, B, C, D, H</td>
</tr>
<tr>
<td>F</td>
<td>D, E, F, G, I</td>
</tr>
<tr>
<td>L</td>
<td>J, K, L, M</td>
</tr>
<tr>
<td>A</td>
<td>A, B, M</td>
</tr>
<tr>
<td>D</td>
<td>B, D, F</td>
</tr>
<tr>
<td>E</td>
<td>E, F, I</td>
</tr>
<tr>
<td>I</td>
<td>E, F, I</td>
</tr>
<tr>
<td>M</td>
<td>A, L, M</td>
</tr>
<tr>
<td>C</td>
<td>B, C</td>
</tr>
<tr>
<td>G</td>
<td>F, G</td>
</tr>
<tr>
<td>H</td>
<td>B, H</td>
</tr>
<tr>
<td>J</td>
<td>I, L</td>
</tr>
<tr>
<td>K</td>
<td>K, L</td>
</tr>
</tbody>
</table>

It is clearly visible that node B alone does not cover the whole network, its neighbor nodes A, B, C, D, H are not all the nodes of the network. Hence, choose a pair of nodes and their union is considered. Hence F along with B is chosen and the resultant union gives us the nodes A, B, C, D, E, F, G, H and I. Now still some nodes are missing, it is necessary to take a third node for union. Let us take L and get all the nodes.

Admin nodes: B, F, L

MODULE 3

Associative, common and energy efficient watch nodes selection:

The Associative nodes are nodes lying in the region common to multiple Admin nodes. If any Admin node does not have an Admin node or an associative node attached to it, then an associative node pair is selected. It is the pair of nodes through which Admin can communicate with the next Admin node. All the nodes in the network excepting the Admin nodes and the associative nodes are the common nodes.

A list of energy levels of neighbor nodes of admin and associative nodes are prepared. Sort the energy level list in the descending order, choose the first two nodes as the watch nodes. From the figure, node D is neighbor of both admin nodes B and F. Hence D acts as the associative node for admin nodes B and F. It is clear that there is no associative node attached to admin node L. So, it is liable to choose A, M pair by which admin L can communicate with admin node B. So A, M pair is called the special associative node pair.

Associative node: D
Associative node pair: A, M

MODULE 4

Battery Life, Admin Reselection and Backtracking:

- **Battery Life**

  The nodes in an Ad-hoc network are constantly in motion and hence will run out of battery power sooner or later. However for the proposed protocol, the battery life is particularly important for the Admin nodes since they perform the maximum amount of work. Hence when the power of a certain admin decreases below a certain level, it is necessary to get that battery to recharge before it can take part in any re-transmission. The proposed protocol have been developed such a way that for every admin, there is a special field for the battery life and if the threshold value of the battery of an admin node is reached, it immediately withdraws itself from the network and recharges and admin reselection takes place. After recharging it can be again reconsidered in the network.

- **Admin reselection**

  There may be a few cases when admin reselection is required. If an admin node is found to be malicious it is blocked from the network immediately and the network chooses a new admin again in the same way as described above. Again if the battery power of an admin gets drained off completely then it is suspended temporarily from the network for recharging and admin reselection takes place.

- **Back tracking**

  In many cases it may so happen that when a data packet reaches an admin, it has multiple paths to move to. The data packet may choose one path, but the destination may very well be on the other path. In such cases a back tracking is required. The proposed protocol have added two bits along with the data packet which records the last traversed admin and then forwards the data packet, if data packet does not find its destination on the traversed path then it backtracks to the admin where it finds a multiple path and then moves to the other alternative path. In this way, re-transmit the data from an admin with multiple paths to reach the destination.

MODULE 5

Misbehavior activity detection:

Watch nodes have been used basically to promote security in the network.
As is the case with our protocol, if we are able to implement security in the admin and the associative nodes, we can guarantee that the total network is secured from any attacks since the common nodes do not have any role to play in transmission of data apart from sending or receiving of data packets. Hence we have added two watch nodes to each admin and Associative node which checks after every time interval if any data packet entering into an Admin or Associative node goes out of the node within a stipulated time period failing which it issues a warning to its previous admin that the node maybe a malicious node and the node is not used for transmission of data through the network.

The proposed protocol used the two neighboring nodes of each admin as the watch nodes in our protocol. In the network in figure if a data packet is sent from node A to node I then the path followed will be A-B-D-F-I When the data packet is in admin B, any two nodes from A, C, D and H will be selected as watch nodes and will keep an eye on the admin node B for any aberrant behavior.

The watch nodes monitor the activities of the admin/associative nodes. If they detect any misbehaving activity of a node for more than 3 times, the corresponding admin/associative node is eliminated from the network. The admin reselection is performed as discussed in the module 2.

MODULE 6

**Performance Metrics:**

**Delay:**

Delay is the time taken for a packet to reach the destination from the source node.

\[
\text{End to End delay} = \frac{\sum (\text{Delay of each entities data Packet})}{\text{Total number of delivered data packets}} \text{ (ms)}
\]

**Number of Packets dropped:**

It is the number of packets dropped by the admin/associative nodes in case of attack or energy exhaustion.

Number of Packets dropped = (number of packets received – number of packets transmitted).

**Average consumed power:**

It is the amount of power consumed by nodes for each communication.

The performance of the proposed protocol, EEAWSR is compared with the AODV [8] protocol. In EEAWSR protocol, packets will be dropped only when the admin battery gets exhausted below a threshold. In the meantime a new admin will be selected & the previous admin will be recharged.

It performs consistently well. In AODV, it is observed that overhearing consumed most of the energy, overhearing effects, Idle power and dominate the energy consumption in the simulation of a dense network. In EEAWSR, the network traffic is mostly restricted in between the admin and hence the all overhead is reduced, since reduce the overall energy consumption.

**XII. Conclusion**

The main aim of developing EEAWSR is to reduce network overhead and computations and also to ensure a complete security of the data packet transmitting through the network and it performs very effectively. This protocol will be more optimal compared to the existing protocol AODV unless a small network is considered and tolerate the rate of topology change. The existing protocols too transmit the data packets very fast, but they introduce high overhead. In the proposed EEAWSR, the network traffic is almost restricted to the admin node, and hence, reduces the overhead considerably. The proposed work selects only the energy efficient nodes as the watch nodes to monitor the admin/associative node’s activities effectively. The proposed protocol prevents the network from a set of routing attacks including the hello flooding, black hole attack, cooperative black hole attack, gray-hole attack, and sleep deprivation attack. This proposal also considers the node’s energy exhaustion condition and provides solution. The proposed EEAWSR outperforms the existing AODV protocol and ensures energy efficient and secured routing with less computational overhead and energy consumption.

**REFERENCES**


