International Journal of Engineering & Technology, 7 (2.31) (2018) 212-218

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Efficient multi stage security model based on cross layer mechanism for identifying and preventing black hole attack in wireless ad-hoc networks

S. Jagadeesan[1*], V. Parthasarathy[2]

[1]Department of Computer Science and Engineering, Anjalai Ammal-MahalingamEngineeringCollege, Thiruvarur, Tamil Nadu, India..
[2]Department of ECE, VelTech Multi Tech Dr.RangarajanDr.Sakunthala Engineering College, Chennai, Tamil Nadu, India.
**Corresponding author E-mail:jagavasan@gmail.com*

Abstract

Mobile Adhoc Network (MANET) is one of the popular and highly demanded networks functioning under wireless adhoc network. It has high demand by various emerging applications in the entire world. MANET and its necessities are increasing day by day. MANET and its various components like node, route and etc., are too dynamic regarding creating, deployment, mobility, speed, join and disconnect from the network. MANET does not require any existing infrastructure whereas it starts functions in any place at any time. Due these reasons various malicious activities are created dynamically and it degrades the performance of the network. This paper focused on detecting and identifying malicious activities one who affects the data directly. Such kind of malicious activity is blackhole attack where it destroys the data during transmission in a route. In order to detect and eliminated blackhole attack this paper focused on monitoring and investigating various functionalities of the network using a Multi Stage Security Model (MSSM). The MSSM is used for detecting and preventing blackhole attacks in MANET which involves investigating cross layer functionalities during data transmission. And it also investigates and analyzes the entire information that is available in the network. This proposed MSSM is simulated in Network Simulation-2 software and the results are verified and the performance is evaluated.

Keywords: *Mobile adhoc network, cross layer, malicious attacks, blackhole attack, security in wireless adhoc networks.*

1. Introduction

A wireless adhoc id a network without any base stations, infrastructure less or multihop network. More number of devices well-appointed with wireless communications and networking capability is in WANET. It supports any kind of computing at anywhere. WANET comprises of two different topologies such as heterogeneous and homogeneous devices. The nodes in the heterogeneous topologies have different capabilities, whereas the nodes in homogeneous topologies have identical capabilities and responsibilities. WANET follows a one-hop neighbor based broadcasting. In broadcasting the data is propagated from source nodes to all the nearest neighbor nodes within the communication range [1]. Data transmission loss and power are the major concern affecting the entire functionalities of WANET. The incapability to preserve a balanced transmission power, thus, worsens the transmission range and strength of the signal, and hence the reliability of WANET are doubtful [2-3].

One of the decentralized wireless adhoc networks is MANET. It is classified as an adhoc network due to MANET never rely on the existing infrastructure like wired networks, routers or access points in the wireless networks. MANET is self-configuring, highly dynamic and the nodes in the networks are moving from anywhere in the network. It lacks the impediments of infrastructure set and administration. Also, any devices can create and join in the network at anytime, anywhere. Nodes in MANET are moving in nature, with different speed, direction, and uniformity in moving behaviour. MANET is a collection of mobile nodes which can transfer any kind of data without any support from infrastructure. MANET is used in various emerging applications like defence, business, academia, natural disaster and medical industry. Nodes in MANET also act as routers. Also security threats are increasing day by day in adhoc networks do not limit within their own region. It may come as threats to the security of the WLAN and wired networks [8]. If a fraud node can make an adhoc network with a legitimate WLAN station, then it easily compromises that station and then it used the station for backdoor operations on the network. It was solved using a cross layer IDS method. Various critical issues which degrade the network performances are solved mostly by cross layer design methods. This teaches a lesson for the readers, as cross layer design can solve most of the problems including controlling malicious activities. Hence this paper also aimed to design and implement a MSSM model based on cross layer investigation.

2. Related work

Several earlier research works are discussed here to understand the problem statement and helps in designing the proposed approach. The author in [4] presented the protocols more related with different layers through which the current information on the network is shared. Also, it can able to maintain the layers individually using the protocol design. In [5], the authors proposed a new protocol called as Adaptive Link Weight (ALW) which chooses an optimized route regarding long delay, long time for routing and available bandwidth. ALW adapts a cross layer integrates the application into the physical layer. Using this design any application conveys inclinations to the protocol regarding overriding the path selection. In order to solve power related problems, the authors in [6] proposed a cross-layer design method for saving the power by controlling the power consumption during data transmissions. Power and throughput related problems, mostly influenced by various malicious activities. Some of the malicious activities affect data transmission on the network layers such as physical, network and MAC which degrades the performance in terms of delay, packet loss and throughput. Generally ad-hoc networks used a common technique called as cooperative routing [9] because of no-infrastructure and there is no centralized node for routing. The author in [10] stated that designing a secured routing protocol is an open challenge in adhoc networks. So, in this paper, it is aimed to design and develop a secured routing protocol to detect and eliminate blackhole attacks in MANET. To do that and provide a complete security mechanism a multi stage security mechanism is deployed in the existing routing protocol and modified it. The author in [11] discussed about various IDS and classification methods. A cross layer based adaptive real time routing attack detection system for MANET is proposed in [12, 14-15]. The data pattern and the network environment patterns are verified using SVM method. The authors in [13] proposed a dynamic method for learning, verifying and comparing the network data to detect and eliminate malicious activities.

Problem statement and motivation

Various earlier research works are discussed in the above section. From the above discussion it comes to know that security is one of the major concerns degrades the network performance due its dynamic nature. In any network customer satisfaction is increased only by providing better throughput within a less delay. More customers increased the profit of the network, which gives better financial improvement in the Government. Hence this paper considers detecting and eliminating malicious activities which affects directly on data transmission. Blackhole attack is one of the malicious activities affects directly the data on the network. This problem is taken into account, and this paper motivated to propose and develop a novel cross layer mechanism referred as Multi Stage Security Model (MSSM) to detect and eliminate the blackhole attach in MANET. This MSSM approach is suitable for any applications under WANET.

Existing system

Though several approaches are proposed in the earlier research works, the author in [7] proposed JDCT-C algorithm for controlling flooding attach by adopting cross layer design is considered as the reference for comparison with the challenge presented here. The proposed cross layer design in [7] verifies the signal strength, neighbor information and REQ-RES generation occurs in the physical layer, network layer and MAC layer respectively. The author verified the retransmission of messages, control messages, back-off, defer in a MAC and packet delay based on the corresponding layers in the network. The performance of the MSSM approach proposed in this paper is evaluated by comparing the obtained results with results given in [7]. The author in [8] proposed QoS architecture for increasing the efficiency using a cross layer communication and real time scheduler method. It can be done by RMA (Rate Monotonic Algorithm) and EDF (Earliest Deadline First) scheduling that professionally schedules numerous real time applications without missing any of their deadlines. These methods are considered as the existing systems will be compared with the proposed approach.

Proposed MSSM approach

To overcome the various issues faced from earlier research works, this paper proposed a cross layer based Multi Stage Security Model for detecting and eliminating/preventing a blackhole attack in MANET. The MSSM comprises of various stages of implementation to identify, detect and prevent blackhole attacks in MANET.

The proposed network $\boldsymbol{G}$ is considered as an adhoc network represented as$\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$**,** where $\boldsymbol{V}$ is the set of nodes connected by the set of edges $\boldsymbol{E}$ (logically). $\boldsymbol{E}$ is possible only if their geographical distance is present within a determined transmission range $\boldsymbol{R}$.$\boldsymbol{G}(\boldsymbol{t})$ is a time function calculates the delay. It is assumed that all the nodes in $\boldsymbol{G}$shares a single common channel. The global information about the network topology and unidirectional links are not available to all the nodes. Hence all the nodes in the network can communicate each other by broadcasting method. Let A denotes the source node which broadcasts the $\boldsymbol{msg}$to neighbors. The following definitions can give better understanding on the proposed work.

Definition -1:$\boldsymbol{dist_{AN}}$ represents the distance among $\boldsymbol{A}$ and $\boldsymbol{N}$ within the $\boldsymbol{R}$, $\boldsymbol{dist_{AN}} \leq \boldsymbol{R}$. **N(x)** is the set of all neighbor nodes for $\boldsymbol{x}$.

Definition -2: $\boldsymbol{nbmsg_x}$says the number of messages received by $\boldsymbol{x}$ while broadcasting.

Definition-3:$\boldsymbol{Th_{dist}}$ represents the distance threshold where**,** $\boldsymbol{0 \leq Th_{dist} \leq R}$. $\boldsymbol{PrTh_{dist}}$ represents the present threshold value of the distance.

Definition-4:$(x), \boldsymbol{E}(x) \subseteq$ **N**$(\mathbf{x})$ **, where N(x)=** $\boldsymbol{E}(x) \cup \boldsymbol{I}(x)$**,**

$$\boldsymbol{I}(x) = \{\boldsymbol{x_i} | \boldsymbol{x_i} \in \boldsymbol{N}(x), \boldsymbol{dist_{AN_i}} \leq \boldsymbol{Th_{dist}}\},$$

$$\boldsymbol{E}(x) = \{\boldsymbol{x_i} | \boldsymbol{x_i} \in \boldsymbol{N}(x),\ \boldsymbol{Th_{dist}} < \boldsymbol{dist_{AN}} < R\}. \quad \textbf{(1)}$$

Definition-5:$\boldsymbol{ReT}(\boldsymbol{s})$ denotes the nodes go for retransmission, at the time of broadcasting.

$$\boldsymbol{ReT}(\boldsymbol{s}) = \left\{\boldsymbol{x_i} | \boldsymbol{x_i} \in \left\{\left\{\cap_{j=1}^{k} \boldsymbol{E}(\boldsymbol{x_j})\right\} \cup \left\{\cap_{j=1}^{k} \boldsymbol{E}(\boldsymbol{x_j}), \boldsymbol{nbmsg_{x_j}} < pTh\right\}\right\}, \boldsymbol{x_i} \in \boldsymbol{V} \quad \textbf{(2)}$$

Cross layer design

The proposed algorithm is a distributed algorithm since it needs to investigate the association among the layers in the network. The algorithm verifies the neighbors, distance of the neighbors, the messages ($\boldsymbol{msg}$) received and the neighbor nodes who participating in message transmission and re-transmission. Let assume, a node $\boldsymbol{A}$ broadcast a$\boldsymbol{msg}$**,** number of neighbors received the $\boldsymbol{msg}$ based on the distance ($\boldsymbol{dist_{AN}}$) the signal strength is verified. In order to verify the performance and non-malicious activities occur in the network, a threshold value is assigned for all the performance parameters such as

$$\boldsymbol{Th_{dist}} : threshold\ value\ for\ distance$$

$$\boldsymbol{Th_{delay}} : threshold\ value\ for\ distance$$

Each time the distance of the neighbor nodes and the delay to receive the $\boldsymbol{msg}$are compared with the threshold values. It helps to decide the distance is shorter and the delay is short. If they are shorter than the nodes are decided as normal and non-malicious nodes.

The delay is considered based on the number of $\boldsymbol{msgs}$and the distance.

The MSSM algorithm verifies the information about all the possible neighbor nodes in a distributed manner. In general the protocol layers are communicating among them in a restricted manner and they are not flexible. Thus, these routing protocols are designed in such a manner to function under vilest conditions, relatively acclimating to different conditions.

This makes use of bungling energy and spectrum. The energy and spectrum can be used efficiently by cross layer design and it is adapted to increasing the ability of WANET and MANET applications. Cross layer design can be used for observing the channel variations.

The architecture of the MSSM is illustrated in Figure-1.

NP and PN represent the data/information acquired from the physical layer. Based on the signal strength obtained from PHY layer and neighbor node’s information from network layer, MSSM determines the node will do retransmission or not.

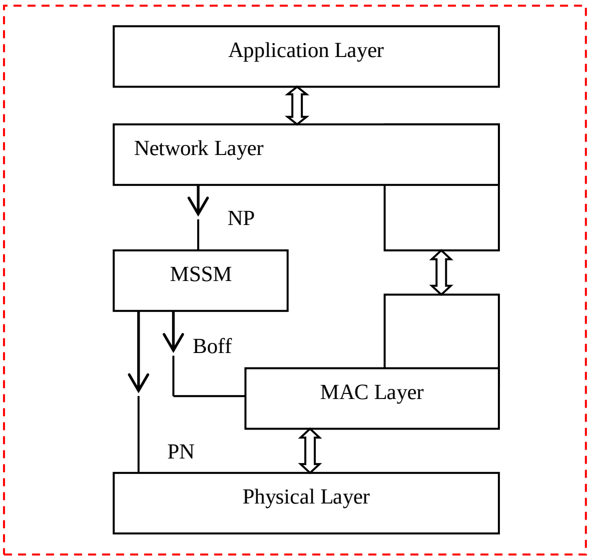

Figure 1: Architecture of MSSM cross layer model

It doesn't need any assistance from any other global information or control messages and the back-off variation in the MAC layer.

$$T^{i}_{boff} = \begin{cases} \alpha\frac{1}{dist_{ix}}, i \in E_s(x), E_s(x) = \{x|x \in \cap_{j=1}^{k} E(x_j), x \in V\} \\ \beta c_i + \alpha\frac{1}{dist_{ix}}, i \in I_{RT}(x), I_{RT}(x) = \left\{x|x \in \left\{\overline{\cap_{j=1}^{k} E(x_j)}\ , C_{xj} < C_{Th}\right\}, x \in V\right\} \end{cases} \quad (3)$$

α and **β** are constants. The MSSM algorithm starts with initializing the threshold values for all the performance metrics. The number of nodes, distance of broadcasting and the msg at first time. If the msg is retransmitted, then update the distance and compare with the threshold values. Similarly the back-off variation is calculated using equation-(3). Assign msg for transmission and wait until the original transmission happens. The msg is going to reach the neighbor node and stop the procedure. Increase the C and check if $cy < CTh$, resume the interruption. In each time of broadcasting the delay, distance and retransmission are verified.

Route analysis

Most of the malicious activities are mainly focusing on the route when and where the data is transmitted. To detect, eliminate the malicious activities on the route, there are two times the investigation is applied. One is during the route discovery and the other is data routing. Each time the nodes available from source node to a destination node, the number of possible paths and the time taken for communication, ACK between the REQ and RES shared by neighbor nodes in the route are verified. During the route discovery a node-route information table is created and managed. The node location, distance from the previous node, path-id and time taken for responses are stored in the table. Before going to do update in the table, all the information is validated to find the node and the route is good or malicious. If any misbehaviour find with the data, then the particular node is rejected from the function. After a shortest path discovery, the source node broadcasts a Hello message to the neighbors and gets ACK from them. From the ACK, time and response format, the next neighbor or next hop is selected and the neighbor information is stored in the table. This process is repeated until a route found from source to destination. A number of possible paths are discovered and stored the path information in the table with a unique path ID. Once the route discovery is completed, then the same table information is verified during data transmission.

Any malicious node can compromise the normal nodes in the route after route discovery and it influences the data. To avoid this, during the data transmission in the determined route the node information, path information is compared with the table information. The nodes in the network may move from one location to another location due to its mobility behaviour. Hence, in this paper a route analysis mechanism is designed and it is integrated with MAODV protocol. The usage of MAODV protocol is that it reduces the overheads and end-2-end delay and security analysis. The entire process of the route analysis is given in the form of pseudo code.

```
$\boldsymbol{Fucntion\ Route\_Analysis}(\,)\{$
$for\ i = 1\ to\ N$
  $for\ j = 1to\ N$
      $Node - table(i,j) = node - id, path$
                              $- id, REQT, REST, location, ACK$
                              $- comment$
                                  $end\ j$
$end\ i$
$for\ i = 1\ to\ N$
    $if\ (Table.(Node - table(i,j)$
                              $= node - id, path$
                              $- id, REQT, REST, location, ACK$
                              $- comment) =$
                              $= Current.Node.(Node - table(i,j)$
                              $= node - id, path$
                              $- id, REQT, REST, location, ACK$
                              $- commen)then$
                   $next - hop = current.node$
                              $else$
                   $move\ to\ next\ node\ in\ the\ rotue$
                      $current.node\ is\ malicious$
$end\ i$
$\}$
```

Node location analysis

Blackhole nodes are created dynamically or move into the network from outside and it focuses on data route. The location of the malicious node is changed during the compromising time. At this point of view, the node location can be used for detecting and identifying the black hole nodes in the network. It is well-known that the information about all the normal nodes in the networks is updated in the node-table in a periodic manner. Hence, in this paper, the node's location information is monitored and investigated to detect malicious activities at any time it required. By calculating the False Positive Rate in location information from the nodes is used to obtain the malicious nodes in the network base on location.

```
$\boldsymbol{Fucntion\ Node - Lcoation\_Analysis}(\,)\{$
$for\ i = 1\ to\ N$
                 $node - location(i) \leftarrow rand(x_i, y_i)$
$end\ i$
$for\ i = 1\ to\ N$
       $if\ (node - location(i) == location\ (node(i))\ then$
                     $node\ location\ is\ right$
                              $else$
                     $node\ location\ is\ wrong$
                   $and\ the\ node\ is\ malicious$
$end\ i$
$\}$
```

Time analysis

The other factor which influences the node behaviour is time. The time taken for travelling in a path depends on the number of nodes as intermediate hops. If the number of intermediate hops increases, then the time increases. One round of operation is starting from source node to destination node a hello message is travelling and from destination to source node a hello-reply message is travelling. For this one round of operations, for normal nodes the time required for travelling is less and it is same for all round of operation in the same route. If any malicious node is available in the route then the time gets varied. Also the number of hops is increased due to the malicious node compromising and the original route will be changed by diverse in the route. Hence, in this paper time analysis is applied to investigate is there any malicious activity exists in the route. Also time information is stored in the node table and it can be verified all the time whenever it requires. If any malicious node is available in the route then it will be eliminated from the network functionality.

```
$\boldsymbol{Fucntion\ Node - Time\_Analysis}()\{$
$for\ i = 1\ to\ N$
        $node - time(i) \leftarrow time(REQ) + time(RES)$
$end\ i$
$for\ i = 1\ to\ N$
        $if\ (node - time(i)\ \leq Th_{time})\ then$
            $time\ is\ perfect$
        $else$
            $time\ is\ not\ perfect$
            $and\ the\ node\ is\ malicious$
$end\ i$
}
```

Hop count analysis

A Blackhole node basically creates packet drops in the route. It is a denial of service attack which presents in the route by compromising the other nodes in the route and holds the packet and drops it. If the route is the shortest route then the number of hops is less and time taken for data transmission in the route is also less. The number of hops in all the routes discovered are stored in the node-table, and it will be verified when data transmission. If the node-ID, number of nodes and location of the node changes, then that node is considered as a blackhole node and eliminated from the network operation. If the number of hops increases or decreases it is identified that a malicious activity occurs.

```
$\boldsymbol{Fucntion\ Hop\_Analysis}()\{$
$for\ i = 1\ to\ N$
        $hop_{count(i)} \leftarrow next(hop) + 1$
$end\ i$
$for\ i = 1\ to\ N$
        $if\ (hop_{count} == numHops(S, D))\ then$
            $hops\ are\ perfect$
        $else$
            $hops\ are\ not\ perfect$
            $and\ the\ node\ is\ malicious$
$end\ i$
}
```

Neighborhood

It is assumed that the source and destination nodes are normal and good nodes in the network.

Other than that, the nodes that are going to participate in routing process should be verified. To do that, while route discovery the next nearest neighbor nodes are verified based on the data packets forwarding style.

The malicious activity is identified by a node that is dropping data packets in the route.

In this scenario, it is also called as packet dropping attack. Due to this a heavy loss of data, energy consumption and memory wastage are happening on the network. The verification function of the neighbor node involves node-location analysis, time-analysis and hop-count analysis.

Data Packets

Malicious activity can be identified and detected by comparing the data packets sent from source and received at the destination. The number of packets is investigated by the packet-ID or sequence ID, with path ID and node-ID. In case of any mismatch in the data packets within the route it is identified that there is a malicious activity. Analyzing the data packets are applied and more effective in large size networks.

Simulation Settings

The above given Pseudo code MSSM is implemented in the TCL scripting language and executed in Network Simulator software and the results are verified. To do the simulation properly and get the results accurately some of the parameters used in the NS2 software are assigned. Some of the sample parameters are given in Table-1. The network layer, Physical layer and MAC layer are configured to check the broadcast message, distance between nodes, delay taken for REQ-RES message transmission and back-off. It is noted that the network follows the IEEE 802.11 standard and the traffic pattern in defining using CBR and TCP traffic models. The number of nodes and their mobility, speed is also defined.

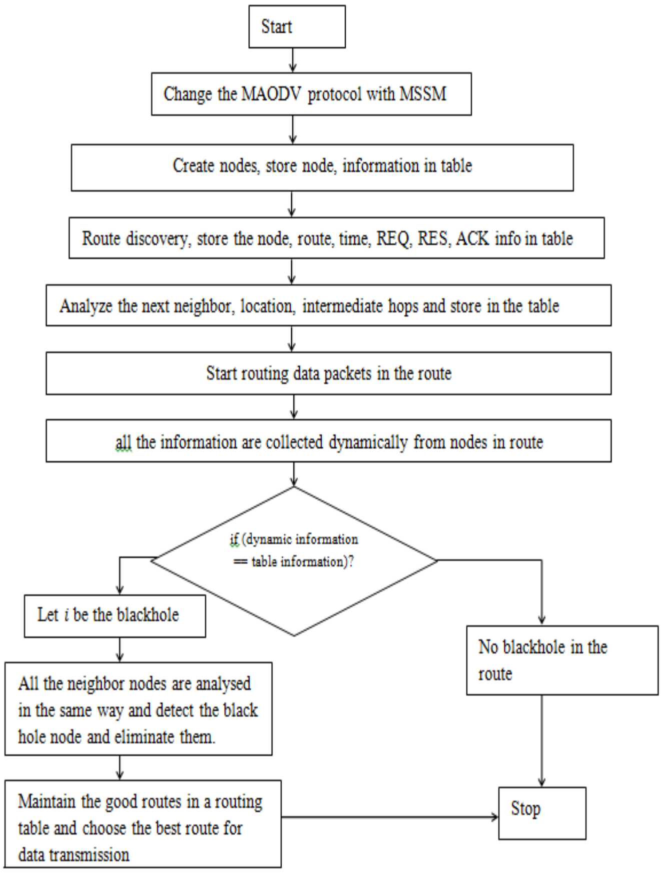
Start
Change the MAODV protocol with MSSM
Create nodes, store node, information in table
Route discovery, store the node, route, time, REQ, RES, ACK info in table
Analyze the next neighbor, location, intermediate hops and store in the table
Start routing data packets in the route
all the information are collected dynamically from nodes in route
if (dynamic information == table information)?
Let i be the blackhole
All the neighbor nodes are analysed in the same way and detect the black hole node and eliminate them.
Maintain the good routes in a routing table and choose the best route for data transmission
No blackhole in the route
Stop

Figure 2: Route analysis based blackhole detection

The entire functionalities of the proposed MSSM approach are given in the form of pseudo code and it can be implemented in any computer programming language and the performance can be verified.

```
Pseudocode_MSSM ( )
{
Initialization
        Network G, comprises of N number of nodes and the logical edges; Sensing range R, $\boldsymbol{dist_{AN}}$, msg, Source node A.
N(x), $\boldsymbol{dist_{AN}} \leq \boldsymbol{R}$is the set of all neighbor nodes for x.$\boldsymbol{Th_{dist}}$, $\boldsymbol{PrTh_{dist}}$, $\boldsymbol{Th_{delay}}$.
Routing Procedure
        $\boldsymbol{A}$broadcasts to its N(x)
        $\boldsymbol{nbmsg_x}$says the number of messages received by $\boldsymbol{x}$ while broadcasting
        divide the nodes N(x) into I(x) and E(x)
        Compare the distance with threshold values$\boldsymbol{dist_{AN_i}} \leq \boldsymbol{Th_{dist}}$
        Compare the delay threshold values$\boldsymbol{Th_{dist}} < \boldsymbol{dist_{AN}} < R$
        Check for retransmission $\boldsymbol{ReT(s)}$
        Check for back-off
        if (neighbor nodes satisfied the constraints with distance, delay, retransmission
            and back-off) then
            nodes are selected as good-node
            else
            nodes are detected as malicious nodes
            end if
Termination Condition
            If ( routing operation is completed ) and ( is any
interruption )then
                        exit
            end if
}
```

Table 1: Simulation Parameter Settings

Parameter	Value
X, Y	1500, 1500
Routing Protocol	MAODV
PROB	Radio Propagation
NN	100 to 500 Nodes
MAC	MAC/802.11
Energy Model	Energy-model=true
Mobility	Random
Moving Speed	2 m/s
Traffic	CBR
Bandwidth Link	2 Mbps
Propagation path loss model	Two-Ray ground Model
Propagation channel frequency	600KHz
Propagation speed	1500 meter/sec
Propagation limit	111 dbm
Propagation path loss model	Free-space
Transmit power	33 dbm
Receive sensitivity	98 dbm
Receive threshold	88 dbm
Data rate	100 kbps
Channel bandwidth	100 kHz
Antenna model	Omni-directional
Maximum transmission range	100 meters

3. Results and Discussion

Based on the network control parameters the network performance is calculated and verified. Throughput, E-2-E delay, packet delivery ratio and energy are some of the main metrics used to measure the performance. These parameters determine the performance of MSSM approach. From the simulation results the performance is calculated by varying the quantity of nodes, the size of the network, the distance among the nodes and mobility speed. The number of bytes of the data successfully received by the destination nodes is called as throughput. The time taken to traverse the routing path is called as E2E delay. The amount of packets effectively obtained at the destination node is referred to as a Packet Delivery Ratio (PDR). PDR mainly controls the packet overhead, routing overhead and congestion on the route. In the existing system [7], the author used JDCT-C approach for controlling wormhole attack, whereas in this paper MSSM is proposed to control blackhole attack and increase the MANET performance. Various parameters determining the quality of service used for determining the blackhole attack are computed from the simulation for MSSM and compare it with the JDCT-C.

In round of operation the number of nodes organizes in the network is altered from 100 to 500 (enlarged by 100 in each round). The number of nodes deployed in the network denotes the network density. Many existing approaches proved that if number of node increases, then the throughput increases, when there is no malicious activities. Hence, in this paper, the malicious activities are controlled before routing the data, and the throughput is increased. The throughput obtained using MSSM and JDCT-C is compared in Figure-3.

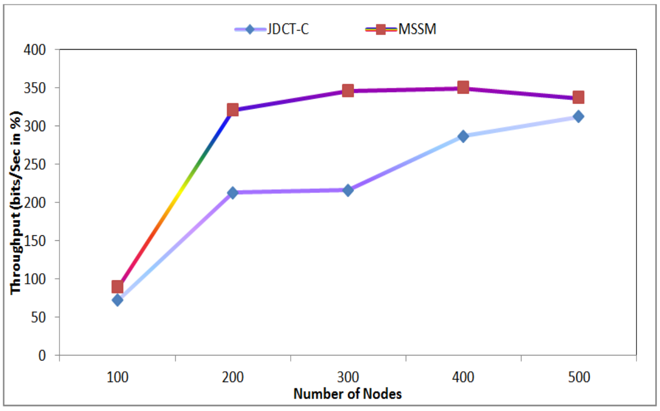

Figure 3: Number of nodes versus throughput

From the results contrast, it is observed that the throughput achieved using MSSM is higher than JDCT-C in all the rounds. Hence, MSSM is decided as better than JDCT-C in terms of throughput. One of the parameters which influence the QoS of the network is throughput.

Table 2: JDCT-C versus MSSM using different parameters

S. NO	Parameter	Existing System (JDCT-C)						Proposed System (MSSM)					
	No of Nodes	Through Put	Blackhole Detection	Energy	End to End Delay (sec)	Packet Loss	PDR	Through Put	Blackhole Detection	Energy	End to End Delay (sec)	Packet Loss	PDR
1	50	27	38.73	89	9	1	25	54	21.37	100	5	0	50
2	100	55	59.92	87	16	6	50	87	48.932	97	8	2	82
3	150	83	61.11	85	23	7	57	120	54.44	94	11	2	86
4	200	111	63.3	83	30	8	59	153	55.06	93	14	3	89
5	250	139	67.49	81	37	8	59	186	59.18	93	17	3	93
6	300	167	73.68	79	44	10	63	219	75.18	92	20	4	94
7	350	195	75.87	77	51	9	67	252	78.74	91	23	5	95
8	400	223	80.06	75	58	12	70	285	79.63	90	9	5	96
9	450	251	82.25	74	65	13	73	318	80.16	89	29	5	96
10	500	300	84.24	75	78	14	77	**347**	**81.99**	**88**	**30**	**6**	**97**

Here throughput is calculated during the simulation by changing the number of nodes from 100 to 500 and verify the throughput. To simulate the proposed approach it is assumed that 5% of the nodes are created as blackhole nodes and the performance is verified. In the simulation, MSSM is verified that out of 5%, how many percentage of blackhole is detected by it and the throughput is obtained. The obtained throughput using MSSM and the existing approach JDCT-C are plotted in Figure-3. The efficiency of the proposed MSSM approach is calculated by the number of malicious activities detected in the simulation. The time taken for detecting the blackhole attack is also calculated. The time taken by MSSM approach is given in Figure-4. From the results it is noted that MSSM taken less time than the existing JDCT-C approach. From the time analysis, it is concluded that MSSM is decided as a better approach than JDCT-C.

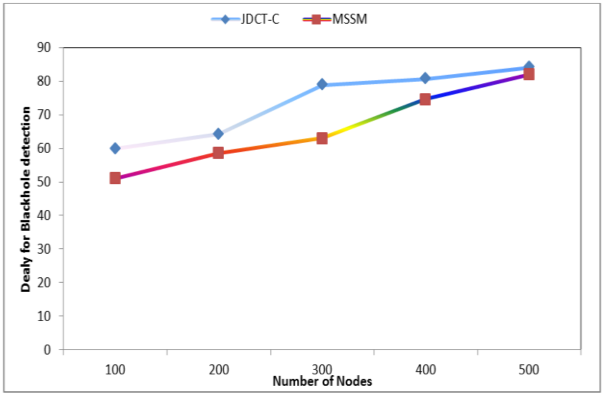

Figure 4: Number of nodes versus delay taken for blackhole detection

Energy is another factor which influences the QoS of the network. In any network, for all kinds of network activities a determined amount of energy requires to complete the activities. The amount of energy consumption varies for different network activities. Comparing with all the activities a node doesn't take more energy in its sleep mode, whereas it requires a high level energy only for transmitting and receiving a data. Each node has a full level of energy initially like 100 Jules. At each activity, a determined total of energy is enthusiastic from the whole energy of the node. . The remaining energy of the network is calculated for various numbers of nodes at various rounds is given in Figure-5. The energy consumption is increased when the number of nodes increases. The remaining energy is decreased when the number of nodes increased and it is exposed in Figure-5. From the end result, it is recognized that the proposed MSSM saves more energy than the existing JDCT-C approach.

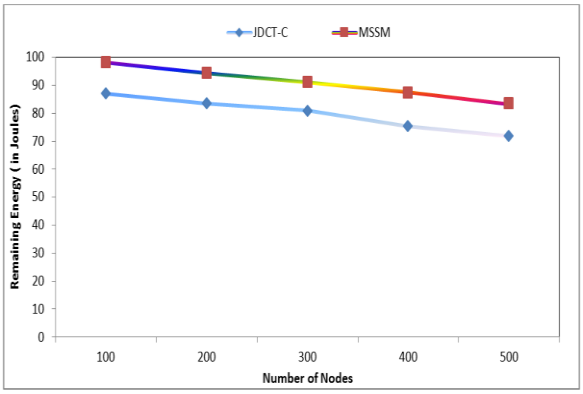

Figure 5: Number of nodes versus remaining energy

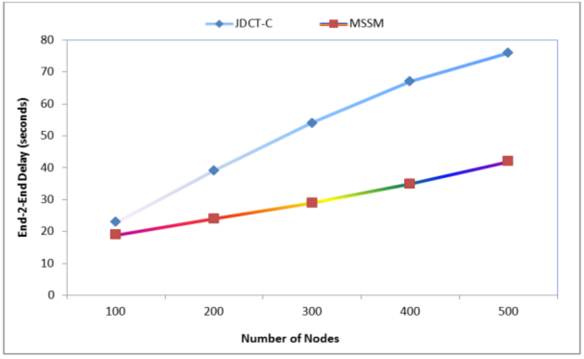

Figure 6: Number of nodes versus end-2-end delay

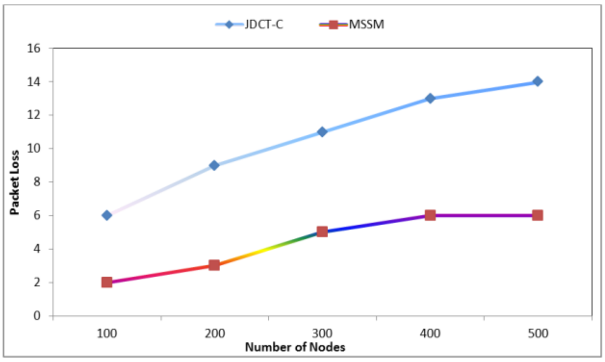

Figure 7: Number of nodes versus packet loss

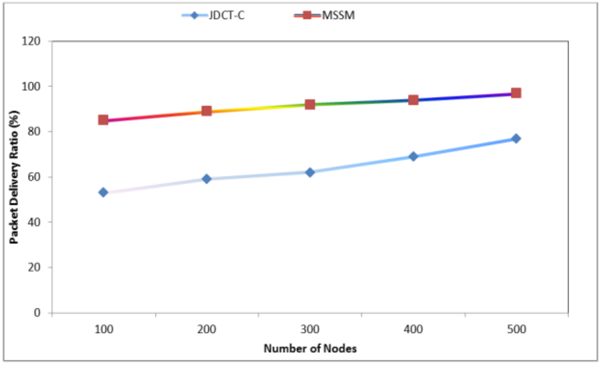

Figure 8: Number of nodes versus packet delivery ratio

The time taken for one round of operation for a fixed number of nodes in the network is referred as delay. From source to destination the required delay is called as End-to-End delay. The End- to-End delay is calculated at all the five rounds of operation and the result is given in Figure-6. From the results it is identified that MSSM is proved as a better approach than the existing JDCT-C approach. During data transmission the packet loss is also calculated since it affects the QoS. In case of a blackhole attack, it forward the data packets in the illegal route. It says that the data packets are transmitted not in the original discovered route. The data packets transmitted in an illegal route are decided as packet loss. Hence the packet loss is calculated and the obtained result is shown in Figure-7. In Table 2 from the results it is determined that the proposed MSSM is concluded as a better approach than the existing approaches.

4. Conclusion

This paper designed to detect and eliminate the blackhole attacks creation in MANET. The main objective of this paper is to design and develop a Multi Stage Security Model (MSSM). The MSSM is used for detecting and preventing blackhole attacks in MANET. The proposed algorithm comprises of various levels of investigations like node analysis, time analysis, node location analysis, hop count analysis and packet analysis. By analyzing each component of the entire network the malicious activities are identified accurately. To ensure the performance of MSSM it is simulated in NS2 software and the results are verified. Compared with the results obtained using proposed approach it is concluded that this approach is better and suitable for secured routing in MANET.

References

[1] Seungjin P & Seong MY, "An efficient reliable one-hop broadcast in mobile ad hoc networks", *Ad Hoc Netw.*, Vol.11, No.1, (2013), pp.19-28.

[2] Goldsmith J & Wicker SB, "Design challenges for energy constrained ad-hoc wireless networks", *IEEE Wireless Commun.*, Vol.9, (2002), pp.8-27.

[3] Kawadia V & Kumar PR, "Principles and protocols for power control in wireless ad-hoc networks", *IEEE J Selected Areas Commun, Part I*, Vol.23, No.1, (2005), pp.78-88.

[4] Conti M, Maselli G & Turi G, “Cross-layering in mobile ad-hoc network design”, *IEEE Comput Soc.,* (2004), pp.48-51.

[5] Alkhwildi N, Khan S, Loo KK & Al-Raweshidy HS, “Adaptive link with routing protocols using cross-layer communication for MANET”, *Wseas transactions on communications*, Vol.6, No.11, (2007).

[6] Ramachandran SS, “Received signal strength based cross-layer designs in mobile ad-hoc networks”, *IETE Tech Rev.,* Vol.25, No.4, (2009), pp.192-200.

[7] Mamata R, Bibudhendu P & Binod KP, “Cross layer based QoS platform for multimedia transmission in MANET”, *International Conference on Intelligent Systems and Control,* (2017), pp.402-407.

[8] Sun Q, Li L, Chen N & Sadia A, “A Cross-layer Design for Broadcast Algorithm in MANETs”, *Networking and Mobile Computing*, (2006), pp.1-4.

[9] Yu L, Yang L & Hong M, “A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks”, *Security and Privacy for Emerging Areas in Communications Networks*, (2005).

[10] Min HS, Ji BL & Yi PL, “Cluster-based Cooperative Back Proppagation Network Approach for Intrusion Detection in MANET”, *IEEE10th International Conference on Computer and Information Technology (CIT),* (2010), pp.1627-1632.

[11] Thamilarasu G, Mishra S & Sridhar R, “A cross-layer approach to detect jamming attacks in wireless ad hoc net-works”, *Military Communications Conference*, (2006), pp.1–7

[12] Kotov V & Vasilev V, “A survey of Modern Advances in Network Intrusion Detection,” *13th International Workshop on Computer Scince and Information Technology CSIT,* (2011), pp.18–21.

[13] John FCJ, Amitabha DB, Bu SL & Boon CS , “CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS”, *Elsevier Computer Networks,* (2010).

[14] Santoshi K, Hidehisa N, Nei K, Abbas J & Yoshiaki N, “A Self-Adaptive Intrusion Detection Method for AODV-based Mobile Ad Hoc Networks,” *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference,* (2005), pp.773-780.

[15] Rakesh S, Kyong HH, Dong YC & Seung JH, “A Novel Cross Layer Intrusion Detection System in MANET”, *IEEE 14th International Conference on Advanced Information Networking and Applications*, (2010), pp.647-654.

[16] Arjun PA & Patrick T, “Towards Secure Multi-path Routing for Wireless Mobile Ad-Hoc Networks: A Cross-layer Strategy”, *8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON),*(2011), pp.146–148.