Asian Journal of Information Technology 17 (2): 167-176, 2018
ISSN: 1682-3915

Improved Secure and Efficient Distance Effect Routing Algorithm Against DDOS Attack in MANET

[1]H.J. Shanthi and [2]E.A. Mary Anita
[1]AMET University, Chennai, India
[2]S.A. Engineering College, Chennai, India

Abstract: In mobile ad hoc network, the mobile nodes are susceptible to distributed denial of service attack where more than one node will turn out to be compromised and mislead the other mobile nodes on the MANET. To provide the solution for this problem in MANET, we have already proposed Secure and Efficient Distance Effect Routing Algorithm (SE_DREAM) protocol which is robust against flood attack in MANET. SE_DREAM uses traffic analysis method to discover the flood attack in MANET. In this study, we concentrate on other distributed denial of service attack such as Blackhole, Grayhole and Sybil attack for which we, propose a novel approach "O bliging Entice Discovery Approach (OEDA)". The OEDA scheme differentiates the attacker nodes from the legitimate nodes by analyzing the address list in the Route Reply (RREP) Packets. OEDA is embedded with existing SE_DREAM protocol to make the path to destination much more robust gainst DDoS attack. The new proposed secure routing protocol is named as improved secure and efficient distance effect routing algorithm. OEDA approach detects numerous malicious nodes concurrently present in MANETs. Simulation results show that our improved SE_DREAM outperform the SE_DREAM in the presence of malicious nodes in MANET.

Key words: Distributed Denial of Service attack (DDoS), Mobile Adhoc Network (MANET), Secure and Efficient Distance Effect Routing Algorithm for Mobility (SE_DREAM), cooperative bait detection approach, legitimate, destination

INTRODUCTION

Nowadays the mobile devices are widely used for the communication. Hence, the mobile ad hoc network is widely used in many sophisticated application such as tactical networks, military battlefield and disaster recovery. This is mainly because of the infrastructure less property of the MANET. In MANET, each node can act as router to assist the communication of other nodes. The cooperation of other nodes is very important in MANET to ensure the reliable communication among the nodes. These great characteristics of MANET emphasize its application in various fields but in the security standpoint this is the major weakness of MANET (Corson and Macker, 1999). The occurrences of malicious node in the MANET leads to malfunctioning in the network by agitating the routing process (Marti *et al.*, 2000). Security in MANETs has focused by many research works but all the security scheme contracts with the individual misbehaving nodes. The efficiency of these security schemes turn weak when many malicious nodes are join together to initiate the distributed denial of service attack. In this study, we dissolve these problem by propose a security scheme against distributed denial if the service attack in the MANET.

Due to the dynamic nature of mobile nodes, the link between the nodes changes dynamically and making availability of providing reliable path among the mobile nodes as a critical task in MANET. Geographic routing protocols are best one to provide the reliable path in MANET with less overhead by restricting the forwarding area with minimum angle. We have chosen distance effect routing algorithm for mobility to provide the security against attacker nodes in the forwarding path. The proposed security scheme is applied to the geographic routing protocol DREAM to provide the secure path with less overhead and minimum energy consumption. Initially the traffic analysis method was embedded with DREAM protocol to provide the solution against flooding attack. That new protocol is called as Secure and Efficient Distance Effect Routing Algorithm for Mobility (SE_DREAM) (Shanthi and Anita, 2016).

The presence of Black Hole/Grayhole attacker in the network will decline the overall performance of the network by discarding the data packets instead of forwarding towards the intended destination.

Corresponding Author: H.J. Shanthi, AMET University, Chennai, India

A Sybil attacker can also harm the ad hoc networks. For instance, Sybil attacker can upset location based or multipath routing by take part in the communication, giving the bogus impression of being particular nodes on various areas or node disjoint paths. In reputation and trust-based bad conduct discovery plots a Sybil node can disturb the precision by expanding its notoriety or trust and exploiting, so as to diminish other's notoriety or trust its virtual identities.

The proposed scheme will make the DREAM protocol robust against flood attack, Blackhole and Grayhole attack. The traffic analysis method will provide the solution against flood attack and the proposed OEDA approach (Chang *et al*., 2015) will make the SE_DREAM robust against Blackhole/Grayhole attack and Sybil attack. This security approaches are applied only to the nodes in the forwarding area. Hence, the resource consumption for security scheme is low and this can provide high throughput with the presence of multiple malicious nodes in the network.

Literature review: Numerous research works have examined the problem of security in MANET. But those mainly deal with single malicious node performed attack or necessitate more resources in-terms of time and cost to detect the distributed attack in MANET. In this study, we survey the research work related to our proposed technique.

Shanthi and Antita (2016) provided the security for geographic routing by using RC4 algorithm. In addition to that the researchers have proposed Adaptive Position Update (APU) scheme for geographic routing. This scheme dynamically set the regularity in position updates based on the mobility patterns of the nodes in the network. They have proved that APU scheme reduce the update cost and amend the performance of geographic routing in MANET. To make the intermediate nodes unable to view the data, the researchers have used the encryption algorithm RC4.

Lyu *et al.* (2013) proposed secure geographic routing protocol for Wireless Sensor Networks (WSN). They have examined effect of the wide variety of attacks in WSN and proposed the Efficient and Secure Geographic Routing protocol (ESGR). ESGR is robust against Sybil attack and wormhole attack by using geographic constraints and TESLA scheme. They have made use of trust model to prevent the Blackhole and Grayhole attacks.

Yasinsac and Carter (2002) to protect the position information in MANET routing protocols, the researchers have proposed Secure Position Aided Adhoc Routing (SPAAR). This routing protocol uses the position information of nodes to take the forwarding decision to reduce the routing overhead in MANET. The position information is broad casted within its range including the malicious node in the network. To avoid this problem, the proposed SPAAR uses the signature based cryptography and authentication technique.

Sharon Ranjini to check whether the forwarder node in the geographic routing is secured or not the researchers have proposed security efficient routing in MANET. In this routing scheme, the node which is having the highest trust value id the best forwarder. The trust value is computed by using RREQ algorithm.

Priyanka Malgi *et al.* have proposed SC_LARDAR (Security Certificate Location Aided Routing Protocol with Dynamic Adaptation of Request Zone) protocol which is a new location based ad hoc routing protocol. SC-LARDAR concentrates on Blackhole attack in MANETs. It is a reactive routing protocol. It discovers the route between the nodes only as needed. This protocol is used to discover the secure route in the request zone constructed based on minimum angle.

The main advantages of this protocol are reduction in flooding RREQ packets and reduction of power consumption. But certificate based security scheme consumes extra memory to store keys.

Pyati and Rekha (2014) proposed high secured location based efficient routing protocol in MANET named as Anonymous Location based Efficient Routing protocol (ALERT). This protocol provides high anonymity protection with low cost. ALERT dynamically partitioned the network into zones and select the forwarder node from the zone to form the non traceable route in MANET.

Tsou *et al.* (2011) have provided the security solution against malicious nodes disturb the routing process in MANET. This proposed scheme is called as collaborative bait detection approach. The researches have applied this technique in the dynamic source routing in which this integrates both proactive and reactive defense architecture. The researches have proved that this CBDS approach effectively detects the Blackhole/Grayhole attack present in the MANET. The CBDS scheme can detect the multiple malicious nodes present in the network concurrently.

Priyanka Malgi *et al.* (Shanthini and Kumar, 2014) have proposed SC_LARDAR (Security Certificate Location Aided Routing Protocol with Dynamic Adaptation of Request Zone) protocol which is a new location based ad hoc routing protocol. SC-LARDAR deliberates on black hole attack in MANETs. It is a reactive routing protocol. It detects the route between the nodes only on demand. This protocol is used to detect the secure route in the request zone constructed based on minimum angle.

MATERIALS AND METHODS

Mobile ad hoc network is more vulnerable to DDOS attack such as flood attack, Blackhole attack, Grayhole attack, Sybil attack, etc., the nodes should cooperate with each other to establish the communication among the mobile nodes. The presence of malicious nodes in the network causes serious impact on the reliable communication between the nodes in MANET. To ensure reliable communication, we need to avoid the participation of misbehaving nodes in routing the information to the destination (Vishnu and Paul, 2010). Dynamic nature of the mobile nodes leads to high overhead and high bandwidth consumption for route discovery. The geographic routing in MANET render the solution for this problem. So, we have chosen best geographic standard routing protocol the DREAM (Shanthi and Anita, 2014) to provide the security against DDOS attack.

DREAM discovers the route by using location information of each node in the network. Each node knows its position by any positioning system. The node should know the position of its immediate neighbor and the destination node to relay the data packet to the destination. In DREAM, each node maintains the location table to discover the location of other nodes in the network. The location table gets updated by exchanging the location packet among the nodes. The location packet consists of coordinates of the source node, source node's speed and the time in which location packet has transmitted. After receiving the location packet each node updates its location table. In DREAM, the route discovery area is restricted to reduce the overhead for discovering the route. The restricted area is called as request zone. In this study, we apply the security scheme for only those nodes present in the request zone. Already, we have embedded traffic analyses method with DREAM protocol to provide the solution against flooding attack in MANET which is called as Secure and Efficient Distance Effect Routing algorithm (SE_DREAM) (Shanthi and Anita, 2016). In addition to this, we propose OEDA approach to vanquish the Black hole/Gray hole and Sybil attacker inside the request zone. Hence, we have named our proposed scheme as improved SE_DREAM (ISE_DREAM). Our proposed secure routing scheme consists of 4 Phases. They are:

- Zone discovery
- Traffic analysis
- OEDA approach
- Routing data packets

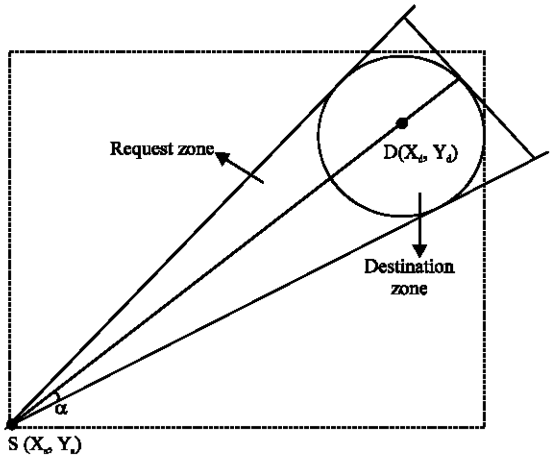

Fig. 1: Limitation of route discovery area to reduce the overhead in the mobile environment

Zone discovery: In DREAM, two zones are discovered such as expected zone and request zone. The circular area within which the destination node is expected to be present during the communication is called as expected zone or destination zone as shown in Fig. 1. The source node restricts the area where the route request packets will be broadcasted to discover the route to reach the destination. The area enclosed by angle α apex is at the source and whose sides are tangent to the circle around destination (Expected zone) is called as request zone as shown in Fig. 1. The destination zone is calculated by the source node. The source node takes the recent location of destination and the last known speed as the input to calculate the circle around the destination. The following equation gives the radius of circle around the destination:

$$R = V_{max}\times(t_1-t_0)_{\text{Centered at}}\ X_d,\ Y_d \quad (1)$$

Subsequently the source estimates the request zone by calculating the angle α in the following way:

$$\text{Angle } \alpha = \arcsin\,(R \div d_{SD}) \quad (2)$$

Where, d_{SD} is the distance between source and the destination.

The source calculates the distance by using the location value in the location table. The area enclosed by an angle from the source towards the destination is called as restricted forwarding or request zone. After zone discovery, the traffic analysis method is used to filter out the flooding attacker in the network.

Traffic analysis: The traffic flow between the each pair of nodes in the request zone is calculated to form the traffic matrix. In mobile ad hoc network, the link between the nodes changes dynamically. But definitely the link exists between the nodes for some time duration. Consider that we are having N number of mobile nodes in our network such as n_1, n_2, ..., n_N. Now, we will take any two mobile nodes n_i and n_j to calculate the traffic flow between those nodes. The traffic flow between two mobile nodes is given by Eq. 3:

$$TF_{ij} = P^s_{ji} \times T_{ij} \times B_{ij} \tag{3}$$

Where:

Tf_{ij} = The traffic flow between node n_i and n_i
P^s_{ji} = The probability of containing node n_i in the neighbor list of node n_j
T_{ji} = The data transfer rate from node n_j to n_i
B_{ij} = The throughput achieved between node n_i and n_i

The neighbor list of node n_j means that the list of nodes presents inside the communication range of node n_j . To calculate the value of P^s_{ji}, the probability of not getting n_i inside the communication range of n_j is calculated by using Eq. 4:

$$\bar{P}^s_{ji} = L_j/N \tag{4}$$

Where:

L_j = The list of nodes present inside the communication rage of node n_i
N = The denotes the total number of mobile nodes in the network

By subtracting this probability value from total probability 1, we can get the probability of containing node n_i in the neighbor list of node n_j through Eq. 5:

$$P^s_{ji} = 1-\bar{P}^s_{ji} \tag{5}$$

The data transfer rate from n_j to n_i is T_{ji} is given by:

$$T_{ji} = \text{Amount of data transferred/Time} \tag{6}$$

Throughput is the rate at which the data can be transmitted. The flow the throughput B_{ij} is given by:

$$B_{ij} = \text{Amount of data/Transmission time} \tag{8}$$

By substituting these values in Eq. 3, we can get the traffic flow value between nodes n_i and n_j . Likewise, the traffic flow between each pair of nodes in the request zone has been estimated and traffic matrix has been created.

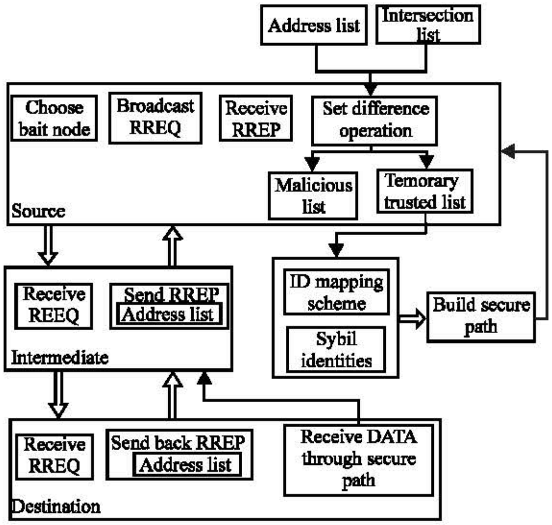

Fig. 2: Architecture diagram of proactive defense phase of OEDA approach

In our scheme, the maximum traffic out flow of source node is taken as the threshold value. The traffic values in the traffic matrix are analyzed by using this threshold value. If the traffic value is lesser than the threshold value, there are no malicious nodes in the network. If the traffic value of node n_i and n_j value is greater than threshold value in the sense, the node n_j send the revocation message against node n_i to all the nodes present inside its communication range at that time. The revocation message is transmitted with the signature in the way specified in to reduce false positive and false negative rate. If the signature is valid, the particular node n_i is revoked from request zone list. Now the request zone is free from flooding attacker. Still to filter out the Blackhole and Grayhole attacker in the request zone we are using proactive defense phase of OEDA approach.

Obliging entice discovery approach: The OEDA approach is mainly used to the detect the Blackhole/Grayhole attacker in the cooperative environment of adhoc networks. These two types of attacks cause serious impact on the route discovery by directing the data packets through the false path (Wang *et al*., 2009). The attacker voluntarily sends the route reply messages for the false route.

The OEDA approach uses the bait node to tempt the malicious node for sending a RREP message to the source

Table 1: Parameter description

Parameters	Description
L_{RREP}	List of nodes send the RREP packets to the source node
A_L	Address list attached with the RREP
T_L	List of trusted nodes
S_L	List of suspected nodes
K_K	Divided address list by node k
R_{REP}	List of nodes in reply route

upon receiving RREQ having bait node as the destination address. The malicious node publicizes itself as having shortest path to the node holds the data packet to transmit. The Bait node is chosen randomly from the nodes those are present inside the communication range of source node. We will explain the process of OEDA approach by using Fig. 2.

The source node is waiting for RREP (Route Reply) from the nodes having path to reach the bait node. In Fig. 2, the source node 'S ' broadcast the RREQ' packets to the nodes in the request zone. The source node is waiting for RREP (Route Reply) from the nodes having path to reach the bait node. In Fig. 2, the source node 'S' broadcast the RREQ' packets to the bait node and the nodes n2-n4. In this network, the node n4 is assumed as the malicious node. After receiving RREQ' packets the bait node and the node n4 send the RREP packets along with the address list to the source node. If the source receives the RREP from only the bait node, there is no malicious node in the network. So, the source node stars its transmission of data packets towards the destination through forwardingor request zone. The source node receives the RREP from other nodes indicate that the malicious nodes are exists in the reply routing. Then the source node will execute the algorithm 1.

Algorithm 1:

```
Input: $L_{RREP}$, $A_L$, $R_{REP}$, Bait
Output: $T_L$
$S_L \rightarrow \varnothing$
While $n_1 \in L_{RREP}$ do
Foreach node $n_2 \in R_{REP}$
$K_k$ = Separate $A_L$ by destination address $n_2$
End Foreach
$S_L = K_1 \cap K_2 \cap ,..., K_n$
$T_L = A_L - S_L$
Return $T_L$
End while
```

The description of all parameters used in Algorithm 1 is listed in Table 1. In the OEDA approach, the reverse tracing technique is used to find the blackhole and grayhole attack in MANET. The address list has been attached with the RREP, by splitting out and finds the intersection of that address list only we find out temporary trusted identities and the malicious list. So, identity of a node is the very much important in the reverse of tracing technique.

But in Sybil attack more than one identity can correspond to a single entity. To detect the Sybil identity present in the network, we map the id with the entity or node in the network. For that, we propose a scheme called as ID mapping scheme.

Consider the example network in Fig. 2 for the explanation of Algorithm1. In the example, the source node receive the RREP from bait node and the malevolent node n_4. In the OEDA approach, the RREP packets holds the address list A_L. When the node receives the RREP with address list, it separated the address list by the destination address as its own address. In our example, the node n_3 receives the RREP from node n_4 with the address list A_L = {S, n2, n3, n4, n5, D}. The node n_3 divides the address list by the destination address n_3 of the RREP and obtains the address Kn_3 = {S, n2, n3} and Kn_3' = {n4, n5, D} list and. Then the node n_3 forward the RREP along with address list to the next node n_2. The node n_2 is also divide the address list in the same way and get the address list K_{n2} = {S, n2} and K_{n2}' = {n3, n4, n5, D}. Finally, the RREP reaches the source node "S" where the address lis t is separated and get the result as K_s = {S, n2} and K_s' = {n3, n4, n5, D}. Then the source node finds the list of suspected nodes by calculating the intersection of the separated address list of each node in the reply route:

$$S_L = K_{n3}' \cap K_{n\,2}' \cap K_s'$$

$$SL = \{n4, n5, D\} \cap \{n3, n4, n5, D\} \cap \{n2, n3, n4, n5, D\} = \{n4, n5, D\}$$

Finally, the source obtain the intersection set {n4, n5, D}. This is unsure path information replied by malicious node n4. The set difference operation of A_L and S_L is carry out to obtain the temporary trusted list T_L by using Eq. 9:

$$T_L = A_L - S_L \qquad (9)$$

To check that the nodes present in the list S_L is a malicious node, the source node send the test packets through this reply route and send the recheck message to the last node in the list S_L toward the other nodes in the list. The source node enter in to the licentious mode to listen the transmission taken by the nodes in the list S_L. If the nodes dropped the data packets instead of redirecting them, the source node store that node id in the malicious list (Table 2).

Table 2: ID_Table

ID	X Pos	Y Pos	No. of replies
1	401	399	1
2	502	425	2
3	590	410	1
4	510	425	1
5	620	425	1
6	720	400	1

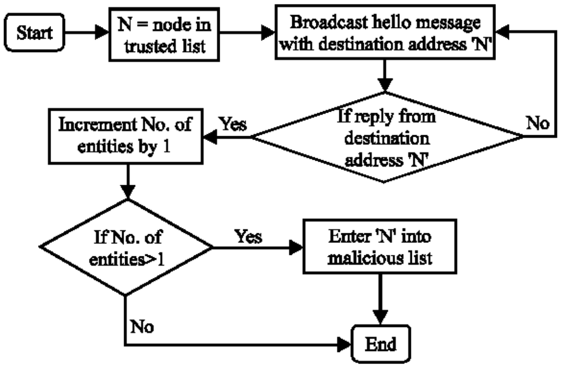
Start
N = node in trusted list
Broadcast hello message with destination address 'N'
If reply from destination address 'N'
No
Yes
Increment No. of entities by 1
If No. of entities>1
Yes
Enter 'N' into malicious list
No
End

Fig. 3: Flow diagram of ID mapping scheme

After detecting the temporary trusted list the source node check for Sybil identity in the network by executing Algorithm 2. The Sybil node is having more than one identity to act as multiple nodes in the network simultaneously. The source node runs the following algorithm to detect the Sybil identities in the network. Before that, the source node maintains a table in the following format.

This table has been constructed by considering the example in Fig. 2. The source node maintains this table for only the nodes in the temporary trusted node list. Source node broadcasts the Hello message to all the nodes in its forwarding zones. The node which receives the Hello message sends the reply to the source node along with its position information includes latitude and longitude. After receiving reply the source node will update the ID-Table. This process flow is diagrammatically represented in Fig. 3 and Table 2 consists of four values such as identity of each mobile node, X-coordinate, Y-coordinate and the no. of replies from the corresponding node. If a node receives more than one reply from a same geographical location with different identities then that node is a Sybil node.

Algorithm 2:

```
For each node 'n' in trusted list {
    Nid = n
    While (Not reach all the nodes) {
            Source node broad cast hello message
            If (source receives reply with source address n) {
                    Increment no. of entities by 1
            }
    }
    If (no. of entities>1) {
            Insert node with id "n" to the mali cious List
    }
}
```

The Sybil nodes are also put into the malicious list and revoke that node from the request zone. The main advantage of using ID mapping scheme with the OEDA approach is as follows:

- Requires low cost
- Does not require extra hardware
- Detection of Sybil identity reduces the resource consumption

Routing data packets: Subsequent to traffic analysis and OEDA approach, the request zone contains no malicious nodes. Then, the source node forwards the data packet towards the destination through the nodes in request zone. When the destination receives the DATA packet it sends back the ACK packets to the source node. If the source node did not receive ACK packet within certain time period then source remedies to the revival procedure.

RESULTS AND DISCUSSION

We conduct a series of experiments by varying data transmission interval. The nodes are distributed in the simulation area of 1500×1000 m sec. The UDP/CBR (Constant Bit Rate) traffic is generated between the source and destination. The data packets are scheduled after 0.05 m sec. The detailed simulation parameters are listed in Table 3.

The NS2 Simulator is mainly used in the research field of networks and communication. The NS2 is a discrete event time driven simulator which is used to evaluate the performance of the network. Two languages such as C++, OTCL (Object Oriented Tool Command Language) are used in NS2. The C++ is act as back end and OTCL is used as front end. The X-graph is used to plot the graph. The performance evaluated by using the network parameter packet delivery ratio, packet loss ratio, end to end delay, routing overhead and throughput.

The packet delivery ratio is the ratio of the data packets delivered to the destination successfully. The packet delivery ratio is one of the important parameter to evaluate the quality of the network. The equation used to find the packet delivery ratio is as follows:

Table 3: Simulation parameters

Parameter types	Parameter values
Simulation time	60 m sec
Simulation area	1500×1000 m
Number of nodes	10, 20, 30, …, 50
Mobility speed	10, 20, 30, 40 m/m sec
Path loss model	Two ray ground
Antenna type	Omni antenna
Mobility model	Random way point
MAC protocol	802.11
Transmission range	250 m
Traffic model	CBR

$$\text{PDR} = \frac{\text{No. of packets deliverd}}{\text{Time}}$$

Figure 3 gives the graph for packet delivery ratio. The graph shows that the proposed scheme ISE_DREAM provides high performance when compared with SE_DREAM and SC_LARDAR. But the performance slightly varies according to the node speed. Higher the packet delivery ratio indicates that the high performance of the network. The simulation results obtained prove that the proposed scheme outperforms than the existing scheme in the presence of multiple malicious nodes in the network (Fig. 4-8).

The Packet loss ratio is used to evaluate the quality of the network provided by the routing scheme. The packet loss ratio of the proposed scheme is compared with the existing approaches SE_DREAM and SC_LARDAR. The packet loss ratio of the proposed scheme is lower than the SE_DREAM and SC_LARDAR as shown in Fig. 4.

This packet loss is mainly due to the presence of malevolent nodes in the network. As the proposed scheme considers the Blackhole/Grayhole and Sybil attack, the packet loss ratio is lower than the existing schemes. Lower the packet loss ratio indicates that the high performance of the network.

The time taken by the source node to deliver the data successfully to the destination is called as End to End delay. The following formula is used to calculate the End to End delay

$$\text{End to end delay} = A_T - S_T/n$$

Where:

A_T = The arrival time
n = The number of connections
S_T = The sent time

Figure 5 shows that the end to end delay analysis of the proposed scheme. The delay increases as the mobility speed of the node increases. But the slight variation is there. The proposed scheme leads to only tolerated delay in the network even though the speed increases. Figure 5 gives the comparison analysis of end to end delay by varying packet size. The graphs shows that the proposed

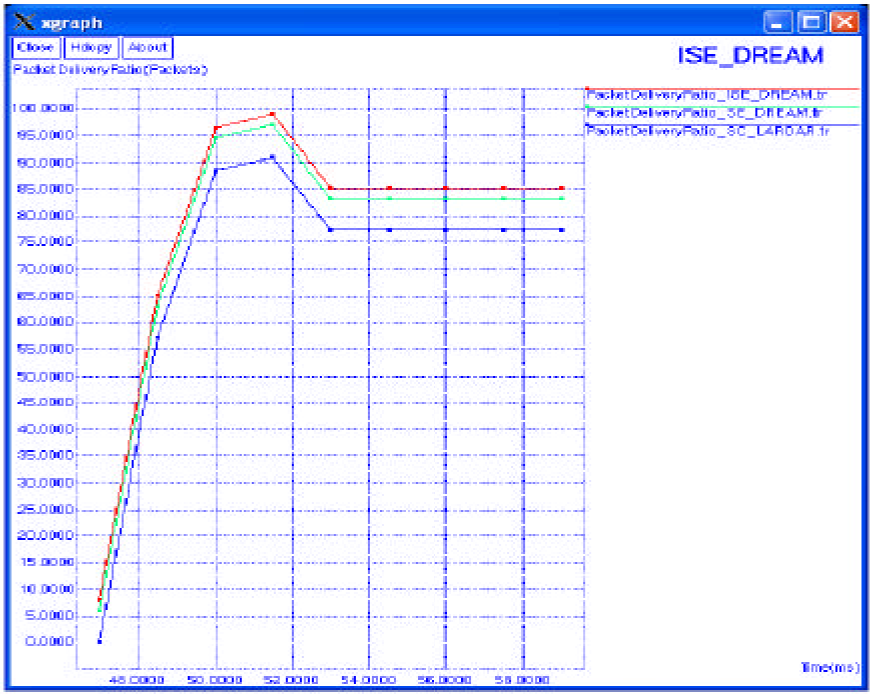

Fig. 4: Comparison analysis of packet delivery ratio with existing approaches

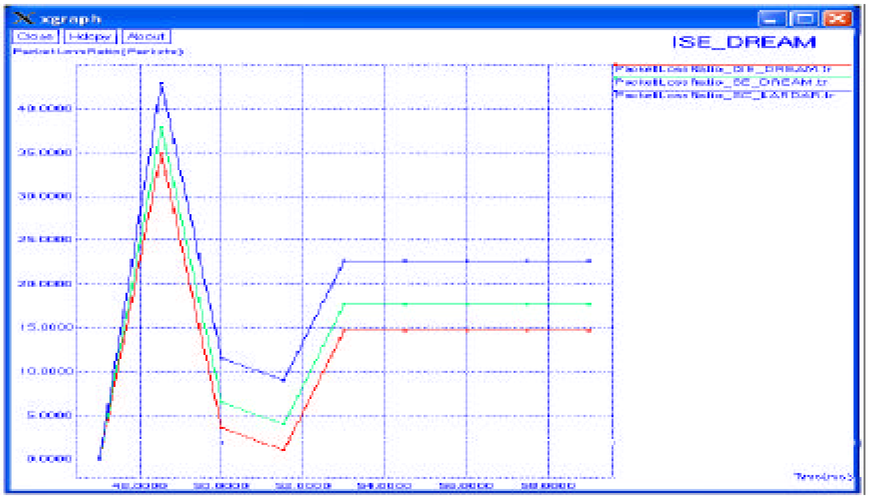

Fig. 5: Comparison analysis of packet loss ratio with existing approaches

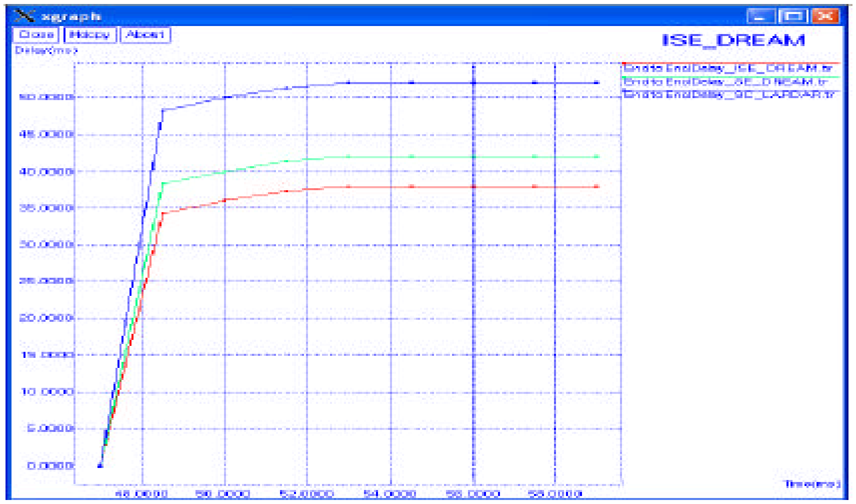

Fig. 6: Comparison analysis of end to end delay with existing approaches

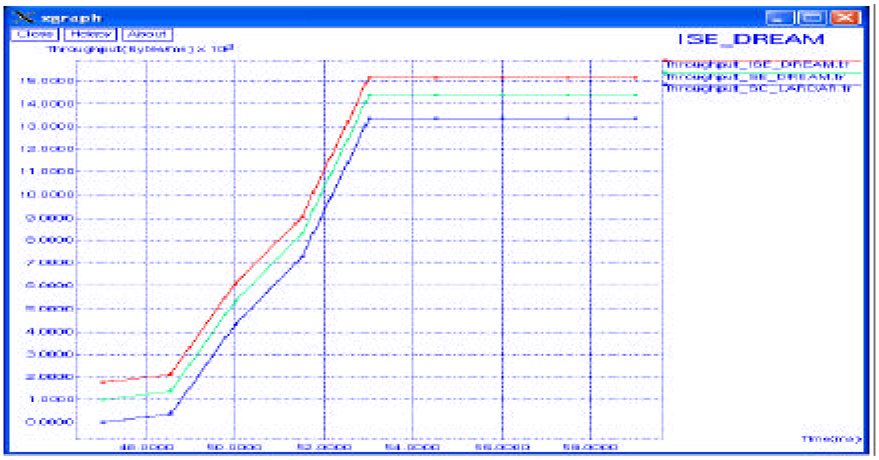

Fig. 7: Comparison analysis of throughput with existing approaches

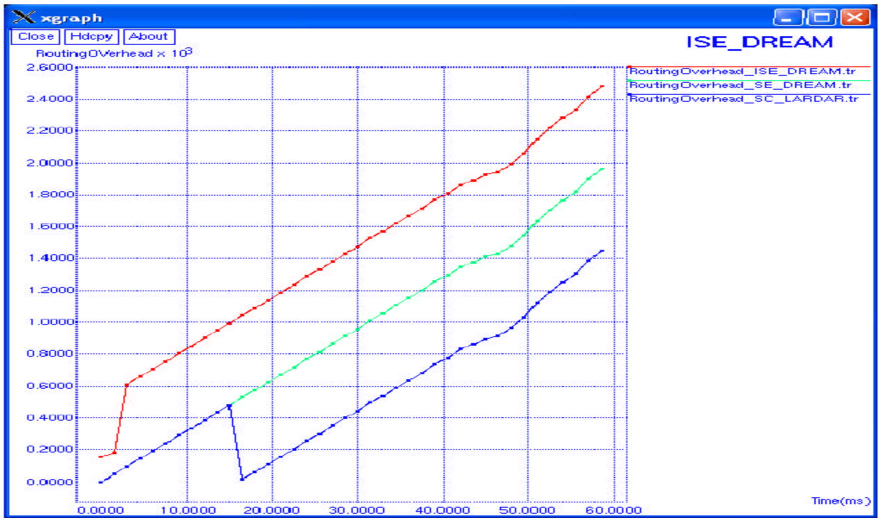

Fig. 8: Comparision analysis of routing overhead with existing approaches

scheme leads to the less delay when the compared with the existing approaches SE_DREAM and SC_LARDR.

Throughput is the amount of packets delivered to the destination per unit of time. The Throughput is calculated by using the equation.

$$\text{Throughput} = \frac{\text{No. of packets delivered}}{\text{Time period}}$$

The system provides high throughput when compared with the node with high mobility speed as shown in Fig. 6. The throughput obtained is high when compared with the existing schemes SE_DREAM and SC_LARDAR as shown in Fig. 6. As a result, the proposed secure and efficient route discovery scheme can able to guarantee QoS requirements in the Mobile Adhoc Network. The routing overhead is the summation of the number of packets has been transmitted to find out the route to reach the destination. The routing overhead is calculated by the following equation.

$$\text{Routing Overhead} = \Sigma(N_{RREQ}\text{-}N_{RREP})$$

Where:

N_{RREQ} = The number of route request packets
N_{RREP} = The number of route reply packets

The routing overhead increases after applying OEDA approach in addition to traffic analysis method in DREAM as shown in Fig. 7. The simulation result shown in Fig. 7 proves that the routing overhead in ISE_DREAM is higher than the SE_DREAM. Mean while the routing overhead in SE_DREAM is higher than the SC_LARDAR. But ISE_DREAM can ensure the reliable communication by providing the secure path even in the presence of multiple malicious nodes in the forwarding zone.

CONCLUSION

In this study, we have proposed a new secure geographic routing protocol ISE_DREAM by embedding the newly proposed OEDA approach with SE_DREAM routing protocol to make the SE_DREAM robust against DDoS attack. After discovery of the destination zone and request zone, the traffic analysis method is used in between each pair of nodes to identify the flood attack in the request zone. This scheme filters out the flood attacker from the request zone. Later the OEDA approach is used for the remaining nodes in the request zone. This scheme filtered out the Blackhole/Grayhole and Sybil attacker in the MANET. Subsequently the Data packets are forwarded through the trusted nodes in the request zone towards to the destination. ISE_DREAM can detect more than one malevolent node in the network simultaneously. Thus the proposed protocol ISE_DREAM can provide high security in the multiple collaborative attackers in the MANET.

REFERENCES

Chang, J.M., P.C. Tsou, I. Woungang, H.C. Chao and C.F. Lai, 2015. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Syst. J., 9: 65-75.

Corson, S. and J. Macker, 1999. Mobile ad hoc Networking (MANET): Routing Protocol Performance Issues and the Evaluation Considerations. RFC., USA.

Lyu, C., D. Gu, Y. Zhang, T. Lin and X. Zhang, 2013. Towards efficient and secure geographic routing protocol for hostile wireless sensor networks. Intl. J. Distrib. Sens. Netw., 2013: 1-11.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, MA., USA., pp: 255-265.

Pyati, D. and S. Rekha, 2014. High secured location-based efficient routing protocols in MANET's. Intl. J. Recent Dev. Eng. Technol., 2: 78-84.

Shanthi, H.J. and E.M. Anita, 2016. Secure and efficient distance effect routing algorithm for mobility (SE_DREAM) in MANETs. Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC'16), March 10-11, 2016, Springer, Berlin, Germany, pp: 65-80.

Shanthini, A.V. and M.M. Kumar, 2014. Security for geographic routing in mobile ad-hoc networks using RC4 algorithm. Intl. J. Innov. Res. Sci. Eng. Technol., 3: 10474-10481.

Tsou, P.C., J.M. Chang, H.C. Chao and J.L. Chen, 2011. OEDA: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture. Proceedings of the 2nd International Conference on Wireless Communication, Feburary 28-March 03, 2011, Vitae Publisher, Chenai, India, pp: 1-5.

Vishnu, K. and A.J. Paul, 2010. Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks. Int. J. Comput. Appl., 1: 38-42.

Wang, W., B. Bhargava and M. Linderman, 2009. Defending against collaborative packet drop attacks on MANETs. Proceedings of the 2nd International Workshop on Dependable Network Computing and Mobile Systems, September 27-30, 2009, Niagara Falls, New York, USA., pp: 1-6.

Yasinsac, A. and S. Carter, 2002. Secure position aided Ad-hoc routing. Master Thesis, Florida State University, Tallahassee, Florida.