Enhanced dynamic source routing protocol for detection and prevention of sinkhole attack in mobile ad hoc networks

Immanuel John Raja Jebadurai*,
Elijah Blessing Rajsingh and
Getzi Jeba Leelipushpam Paulraj

School of Computer Science and Technology,
Karunya University,
Coimbatore, India
Email: singhiman@gmail.com
Email: elijahblessing@gmail.com
Email: getz23@gmail.com
*Corresponding author

Abstract: Sinkhole attack is an active routing disruption attack in the routing layer of the mobile ad hoc networks. A sinkhole node attempts to entice all the network traffic towards it by broadcasting bogus routing information to other nodes in the network. On demand routing protocols such as dynamic source routing protocol and ad hoc on demand distance vector protocol are vulnerable to this attack. Sinkhole attack makes use of the route discovery and the route maintenance phases of these protocols. Sinkhole attack often facilitates other attacks such as blackhole attack, greyhole attack, wormhole attack and Sybil attack on MANETs. In this paper, we present a secondary cache based approach to prevent the sinkhole attack in DSR MANETs. The simulation results show that the proposed approach improves the performance of DSR even in the presence of multiple sinkhole attacks.

Keywords: sinkhole attack; mobile ad hoc networks; MANET; dynamic source routing; DSR; route cache; routing; adjacency table; route discovery; route maintenance; security; network.

Reference to this paper should be made as follows: Jebadurai, I.J.R., Rajsingh, E.B. and Paulraj, G.J.L. (2016) 'Enhanced dynamic source routing protocol for detection and prevention of sinkhole attack in mobile ad hoc networks', *Int. J. Network Science*, Vol. 1, No. 1, pp.63–79.

Biographical notes: Immanuel John Raja Jebadurai is with the Department of Computer Science and Engineering at Karunya University in Coimbatore, India. He received his Bachelor of Engineering in Computer Science and Engineering from M.S. University in India in 2003. He received his Master of Engineering from Karunya Institute of Technology, Anna University in India in 2005. Currently, he is pursuing his PhD in Karunya University in Coimbatore, India. His research interests lie in the area of mobile ad hoc network security and routing.

Elijah Blessing Rajsingh is Professor and Director for the School of Computer Science and Technology at Karunya University in India. He received his Master of Engineering in distinction from the College of Engineering at Anna University in India, where he also received his PhD in Information and

Communication Engineering in 2005. He has very strong research background in the areas of network security, mobile computing, wireless and ad hoc networks and image processing. He is an Associate Editor for *International Journal of Computers and Applications* in Acta Press in Canada.

Getzi Jeba Leelipushpam Paulraj is an Assistant Professor in the Department of Information Technology at Karunya University in Coimbatore, India. She received her Bachelor of Engineering with distinction in Electronics and Communication Engineering from M.S. University, India in 2004. She received her Master of Engineering with distinction from Karunya University in India in 2009. Her research interests lie in the area of mobile computing, grid and cloud computing.

1 Introduction

Mobile ad hoc networks (MANET) do not have fixed infrastructure such as base stations, access points and wired networks. The nodes in the MANET are the mobile devices which communicate each other through radio links. Nodes within the transmission range of others communicate directly and cooperation among intermediate nodes is required for nodes to communicate other nodes outside of their transmission range. As the nodes are free to move arbitrarily, the network topology may change over time resulting in the links having either bidirectional or unidirectional capabilities. Moreover, the bandwidth of the wireless links is lower than that of the wired links. These links suffer because of fading and interference conditions. The nodes in MANET rely on the batteries for their energy requirement. Hence, energy conservation is important.

These properties support the MANET to be suitable for the infrastructure-less communication systems such as military battlefield, emergency rescue operations and personal area networks. However, these make the MANET prone to various network attacks (Boudriga, 2010) including malicious traffic generation attack, route poisoning attack and malicious traffic relaying attack. The sinkhole attack is an active routing disruption attack in MANET (Shim et al., 2010). A sinkhole node attempts to lure the traffic in the network. Later it alters or drops the traffic causing disorder in the network (Kim et al., 2010).

The reactive routing protocols attempt to find the routes on demand. Compared to proactive routing protocols, reactive routing protocols are more vulnerable to route disruption attack (Ozleyis et al., 2004). Dynamic source routing (DSR) is a reactive routing protocol. During the route discovery process, the sinkhole node propagates the bogus messages advertising the fake shortest or the best route to the destination node. Upon receiving these routing messages, other normal nodes update their route cache or use the newly learned bogus shortest route. The normal nodes are unaware that the bogus route ensnares their traffic towards the sinkhole node. These lured data traffic may be altered, dropped or selectively forwarded by the sinkhole node. Usually the attacker does not perform any further malicious activity lest it be detected (Shim et al., 2010).

This paper proposes a secure routing protocol based on DSR protocol to defend against the sinkhole attack. This enhanced DSR protocol updates the route cache only after the legitimacy of the route is confirmed. This makes use of the ‘non-propagating’ route request option of DSR. Further, a secondary route cache is employed to reduce the time taken in the route discovery process. This improves the latency of the data traffic.

The remainder of this paper is organised as follows. Section 2 describes DSR protocol and sinkhole attack. Section 3 provides a brief review on the related works against the sinkhole attack. Section 4 explains the proposed enhanced DSR protocol to defend against the sinkhole attack. Section 5 offers the experimental setup and the results. Conclusions are given in Section 6.

2 DSR protocol and sinkhole attack

DSR protocol is a reactive routing protocol that uses route discovery and route maintenance mechanisms for source routing. Each data packet sent carries in its header the complete source route. When a node has data packets in its *sendbuffer*, it looks for the source route in its *route cache*. If the route is not found, it initiates the route discovery by placing the *initiator* IP address, the *target* IP address and the *sequence* number. The value of the new sequence number is higher than that were used for other route requests recently initiated in the route request (RREQ) packet. This RREQ is sent out with the destination IP as the limited broadcast IP address (i.e. 255.255.255.255).

The notations used in this paper are given in Table 1.

Table 1 Notations

IP_{Dst}	Identity of the node whose route is requested
IP_{Src}	Identity of the node which initiates RREQ
IP_{Home}	Identity of the node processing RREQ
TR_x	Route cache available in node x
$RREQ$	Route request message
$RREP$	Route reply message
$TReq_x$	Route request table available in node x
T_{Sr}	Sequence of IP addresses specifying the route to IT_{Dst}
V_{Src}	IP address of the node initiating RREQ
TR_x	Route cache of the node x
V_{tar}	IP address of the target node whose route is requested
V_{own}	IP address of the processing node
$Num_{Seq}(i)$	Sequence number of node i; uniquely identifies the route request within the mobile node
$R_{Len}(l, m)$	Hop count between nodes l and m
TTL	Time to live field in IP header
N_m	Set of neighbours of node m
$TTop_x$	Topology table in node x

Every node in the MANET receiving the route request message packet, processes it in the following way.

Processing the route request messages in DSR

```
If $IP_{Dst} = IP_{Home}$ then
Prepare RREP;
Send back to previous hop node;
Update $TR_{Home}$ based on hop count;
Else if $IP_{Home} \trianglelefteq$ source route then
Discard RREQ;
Else if $TReq_{Home} \in$ entry for this RREQ then
Discard RREQ;
Else
Make entry in $TReq_{Home}$;
Add current address in the source address of RREQ;
Transmit as link layer broadcast;
End if;
```

When a node is unable to verify the reachability of a next-hop node after reaching a maximum number of retransmission attempts, it sends RERR message to the IP source address of the packet.

The attacker performs one of the following to deploy the sinkhole attack.

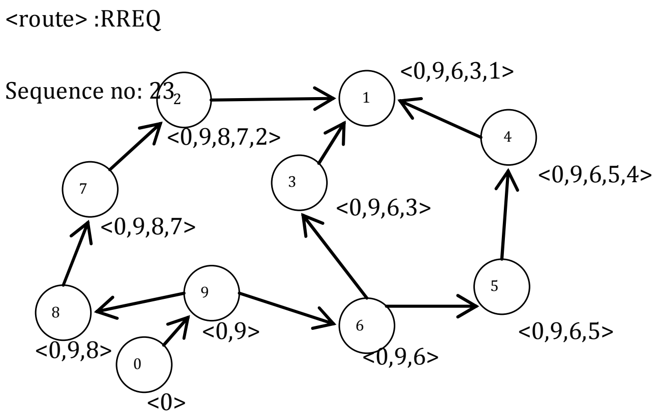
a The attacker identifies the victim node and initiates the RREQ by providing the identity of the victim as the *initiator*. The route in the RREQ holds the identity of the victim as the first node, followed by the identity of the attacker. After carefully analysing the sequence number of the victim node, this bogus RREQ is prepared with higher sequence number and broadcasted through the network. Any node receiving this RREQ update its route cache with the source route present in the bogus RREQ. Because, it has the shortest route to the *initiator* node and higher sequence number meaning a fresh route.

b When the attacker receives a RREQ for a *target* node, it prepares a malicious RREP. The *target* node is placed at one hop distance from itself in the source route of the RREP. This RREP is sent back to the *initiator* victimising the target node.

c By broadcasting a malicious RERR message that the victim is unreachable and sending out a bogus RREQ placing the victim in a one hop distance from itself.

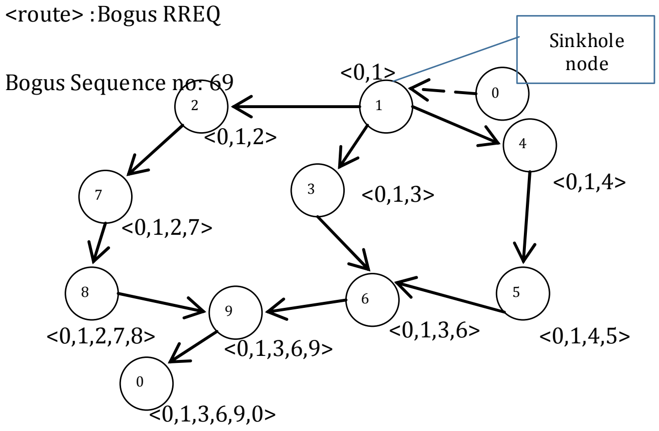
Figure 1 shows the normal DSR operation where the node 0 initiates the RREQ message with the sequence number as 23 requesting the route for the node 1. Figure 2 represents the sinkhole attack scenario. Node 1 is the attacker victimising the node 0. The RREQ is sent with high sequence number of 69 by node 1 having node 0 as the initiator. But, node 0 is not present in the one hop distance with node 1. Thus, node 1 poisons the route cache of the other nodes in the network.

Figure 1 Propagation of RREQ



Note: 0, SN: 23

Figure 2 Propagation of bogus RREQ (see online version for colours)



Notes: Sinkhole node: 2; target (victim): 0; SN: 69.

3 Related works

According to Karlof and Wanger (2003), the aim of sinkhole attack is to lure nearly all the traffic from a particular area of the network through a compromised node, creating a metaphorical sinkhole with the adversary at the centre. Tseng and Culpepper (2005) proposed two sinkhole detection indicators for MANETs which use the DSR protocol. They are sequence number discontinuity and route add ratio. To avoid the flooding of RREQs in the network, node processes an RREQ only if it has not already processed the packet, and its own address is not present in the source route of the packet. The sequence number discontinuity is the overall average difference between the current and the last sequence number from each node, added with a penalty that is proportional to the number of observed duplicate sequence numbers.

However, the attacker may use sequence numbers that are not unusually high, but only just high enough to cause the route overriding effect. The route-add ratio is the proportion of routes that traverse a particular node to the total number of routes added to this node's routing table. The sinkhole attack causes nodes in the MANET to add routes that pass through the sinkhole (Mohanapriya and Krishnamurthi, 2013). The system issues an intrusion alert if sequence number discontinuity and route add ratio values exceed a threshold (Jebadurai and Rajsingh, 2011).

Ramaswamy et al. (2003) proposed a solution which uses a data routing information table containing a trusted nodes list. The source node uses only the trusted nodes with good transmission history for sending the data packets. If the source node does not possess enough history of the intermediate nodes, the source node will send an additional request message to the next hop of the intermediate node in order to identify the trustworthiness of the intermediate node. The performance this method decreases in cooperative sinkhole attacks.

Marti et al. (2000) proposed watchdog to mitigate the presence of a sinkhole problem in the MANET. To identify a misbehaving node, sending node promiscuously checks if the next node forwards its data packet. If the next node does not forward the packet, it suspects that the node is misbehaving and watchdog increments a failure counter. As soon as this counter value exceeds a certain threshold, watchdog concludes that the node is malicious and sends a notification to the source. The performance of the watchdog decreases if it has less transmission power. In addition to this, it will be difficult to identify the misbehaviour if the node selectively forwards the packet.

Marchang and Datta (2008) proposed a collaborative technique which uses a monitor node for the detection of the malicious nodes. This approach burdens the monitor node. The mobility of the nodes in the MANET worsens the performance of this approach.

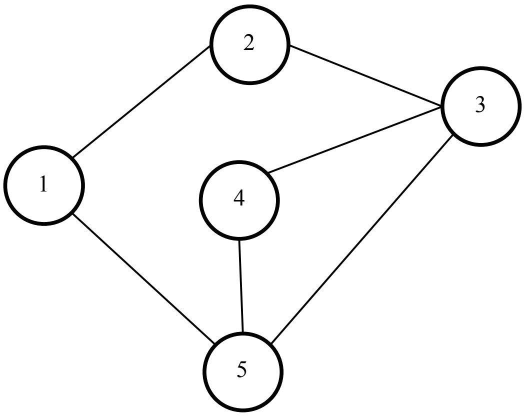
Kim et al. (2010) proposed the cooperative method. This method uses three kinds of packets for isolating sinkhole nodes. They are sinkhole alarm packet (SAP), sinkhole detection packet (SDP) and sinkhole node packet (SAP). The sinkhole node will be left undetected, if the bogus RREQ does not reach the victim node.

Cluster analysis method for sinkhole detection was proposed by Shim et al. (2010). This works by grouping data such that objects in a given group are similar to each other and different from other groups. In this approach, false RREQs are separated from normal RREQs. This requires a central controlling point. The cryptographic functions are also not effective as there is no centralised authority available in the MANET.

4 Enhanced DSR protocol to defend against the sinkhole attack

This section proposes an enhanced version of the DSR protocol for preventing the sinkhole attack. In the proposed protocol, every mobile node running DSR protocol maintains a data structure called topology table. The structure of the topology table is designed following the adjacency list. A simple mobile ad hoc network and the corresponding topology are shown in Figure 3.

Figure 3 A simple graph representing a network and its topology table



1	2	3	4	5
2	1	2	3	1
5	3	4	5	3
		5		4

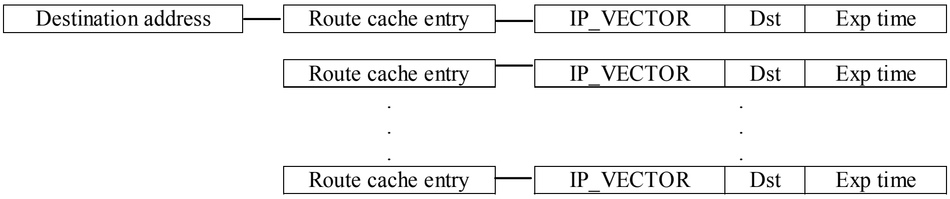
The MANET is modelled as an undirected graph G: {V, E} where V represents the set of nodes and E represents the edge between the nodes. There exists an edge between two vertices if the corresponding nodes are within the radio distance of each other nodes.

The topology table contains the entries for the routes received through the RREQ, RREP or RERR messages. Every node has a column. The values in the column contain the identity of the neighbouring nodes.

The topology table shall be updated whenever the nodes receive new routing information. This ensures that the topology table always contain relatively fresh entries. It is obvious that the topology table require a maximum of 8*N*(N-1) bits for the storage of the adjacency lists in the MANET having mesh topology. N denotes the total number of nodes in the MANET. However, in practical applications, every node may not be connected directly to every other node in MANET. Hence, at any given time the storage requirement is less than 8*N*(N-1) bits.

The structure of the route cache entry in DSR protocol is given in Figure 4.

Figure 4 Structure of route cache entry in DSR



The proposed solution to detect the sinkhole node utilises the 'non-propagating' route request technique (Johnson et al., 2007). The 'non-propagating' route request uses the hop limit as 1. This limits the route request not to be propagated beyond one hop distance. The target node field in this request contains the address of the node to which the source route is required.

Upon receiving this request, if the receiving node is the target node, the receiver replies with the route information; otherwise, the node fetches the source route from its route cache if available and replies with the routing information; otherwise, the request packet is simply discarded resulting in the request not being propagated further in the network.

When a node in the MANET has data packet to be sent to the destination, it places the data packet in the *sendbuffer* and looks into its route cache to determine the best available route to the destination. If it could not find any route to the destination, route discovery process is initiated.

It is obvious that RREQ is used by the malicious node to setup the sinkhole attack in MANET. Hence, the RREQ needs to be handled appropriately to prevent the sinkhole attack. When a node $V_i \in V$ receives a RREQ packet, it checks whether the V_{Src} of this RREQ is present in any of the routes in the route cache of the neighbours. If it is present, non-propagating route request is initiated.

V_{Src} is the IP address of the node which initiates the RREQ. TR_x represents the route cache of the node x. This can be achieved by sending the RREQ with TTL value as 1 in the IP header with the V_{Src} as the $V_{tar.}$ V_{tar} is the IP address of the target node whose route is requested. Once a neighbour V_j receives this RREQ, it checks the V_{own} and the V_{Src}.

Processing of route request packets in the one hop neighbours

```
If ($V_{own} = V_{Src)}$ then send RREP;
Else if ($TR_j \ni V_{src)}$ then send RREP;
Else drop RREQ;
End if;
End if;
```

In neither cases, the node V_i processes the RREP received from the node(s) $V_x \ni V_{sr}$. T_{sr} represents the source route present in the original RREQ.

On receiving the RREP from the one-hop neighbours, the routing information is updated in the topology table. The routes available in the topology table are not reflected in the route cache of DSR protocol. The route cache is updated based on the validity of the routes in the topology table. To check the validity of the routes, the route length R_{Len} is calculated using the Dijkstra's shortest path algorithm.

Generally, the shortest path algorithm uses the link weights to find the shortest path. But, DSR protocol uses the hop count to determine the shortest path. The graph-theoretic distance between two nodes is defined as the length of a geodesic that connects them. Shortest path algorithm provides the shortest path between the nodes. The links are given unit weights. Dijkstra' shortest path algorithm is used to calculate the shortest path from the V_i to V_{Src} on the topology table. The shortest path is the series of nodes from the V_i to V_{Src}.

This series of nodes is represented as a singly list. The R_{Len} from V_i to V_{Src} is calculated by traversing the linked list from V_i till V_{Src} and incrementing a counter while visiting each node.

The value R_{Len} (V_i, V_{Src}) shows the distance from the V_i to V_{Src} in terms of the number of hops. This value is utilised in finding out the validity of the new route. The calculation of storing the nodes in a link list needs the running time of O (|V|^2 + |E|).

The stability of each other node in a node's stability table is initialised to 25 seconds (Johnson et al., 2007). In this context, the entries in the adjacency lists of the topology table are flushed every 25 seconds.

In the normal operation of DSR protocol, the routes received through RREP are updated in the routing table. The proposed protocol updates the newly received routes in the topology table first. The validity of the route is confirmed before any new route is added to the route cache. This approach eliminates the possibility of updating the route containing the attacker node in the route cache.

Processing of the route request message in enhanced DSR

Case i: processed RREQ is received

```
If ($IP_{Src}$ || $Num_{Seq} \in TReq_x$) then drop RREQ;
End If;
```

Upon reception of the RREQ message, one of the following operations is performed. If the received RREQ is already processed by this node, the RREQ packet is discarded.

Case ii: source ID matches with processing node' ID

```
If ($IP_{Src} = IP_{Home}$)
If ($Num_{Seq}(IP_{Src}) > Num_{Seq}(IP_{Home})$ then raise alarm, isolate sinkhole node; ⇒ Sinkhole attack
Else drop RREQ;
End if;
Else process RREQ;
End if;
```

If the RREQ's source identity matches the processing node's identity and if the RREQ's sequence number is higher than the processing node's sequence number, it is a sinkhole attack (Kim et al., 2010).

Case iii: target ID matches with processing node' ID

```
If (($IP_{Dst} = IP_{Home}$) || ($T_{Sr} \ni IP_{Home}$)
Then Prepare RREQ with TTL = 1 and $IP_{Dst} = IP_{Src}$;
Broadcast RREQ;
Receive RREP from $N_{Home}$;
Update $TTop_{Home}$;
Calculate $R_{Len}(IP_{Home}, IP_{Src})$;
If ($R_{Len}(IP_{Home}, IP_{Src}) > \delta$)
Raise alarm and isolate sinkhole node;
Else
Add entry in $TReq_{Home;}$
Update $TR_{Home}$;
Prepare RREP;
If ($TR_{Home} \trianglerighteq$ route to $IP_{Src}$)
Then send RREP through route in $TR_{Home}$;
Else initiate RREQ or use Reverse route;
End if;
End if;
End if;
```

If the identity of the target node in the RREQ message matches with the processing node and/or the source address field contains the source route giving the complete path from the source node of this RREQ to this node, non-propagating RREQ is sent out.

The optimal value of δ is found to be 3.

5 Experimental results and analysis

The proposed enhanced DSR protocol for MANET was implemented and the simulation results were obtained for the proposed protocol. The enhanced DSR protocol is compared with DSR protocol to investigate the performance of the proposed protocol in terms of packet delivery ratio and routing overhead.

Packet delivery ratio is defined as the ratio of the number of packets that are successfully delivered to a destination to the number of packets that have been sent by the source.

Routing overhead is defined as the total number of routing packets transmitted in the MANET.

Table 2 Simulation parameters

Parameter	*Value*
Coverage area	750 × 750 m
Mobility model	Random way point model
Load	5 kb UDP CBR data payload: 512 bytes
Connections	20 pairs (40 nodes)
Traffic type	UDP – CBR
Transmission range	250 m
Routing protocol	DSR, enhanced DSR

If the packet delivery ratio is higher, the performance of the routing protocol is better and vice versa. If the routing overhead is lower, the performance of the routing protocol is better.

The proposed protocol for MANET was simulated using network simulator 2. The values of the parameters that are used in the simulation are given in Table 2.

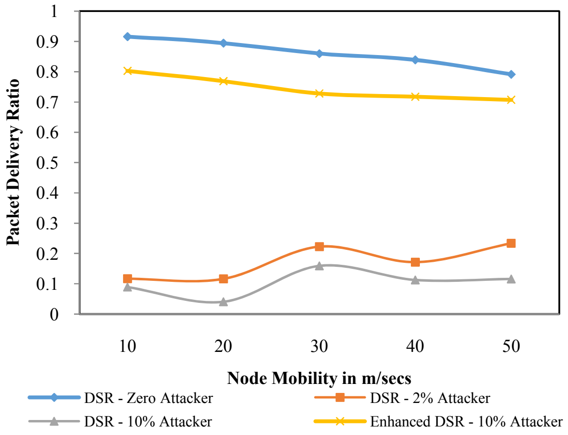
5.1 Performance analysis on the effect of node mobility in enhanced DSR protocol

5.1.1 Performance in terms of packet delivery ratio

The number of MANET nodes and number of flows were fixed at 50 and 20 respectively. The mobility of the nodes was varied from 10 m/sec to 50 m/sec by 10 m/sec in each step.

Initially, the packet delivery ratio in ideal condition for DSR protocol for different mobility of the nodes was obtained and is shown in Figure 5. The sinkhole nodes were induced in MANET such that 2% of the nodes were sinkhole nodes and the packet delivery ratio was obtained. The result is shown in Figure 5. Then the percentage of sinkhole nodes was increased to 10% of the nodes in the MANET. The packet delivery ratio for enhanced DSR protocol and DSR protocol were obtained and the results are shown in Figure 5.

Figure 5 Node mobility vs. PDR (see online version for colours)

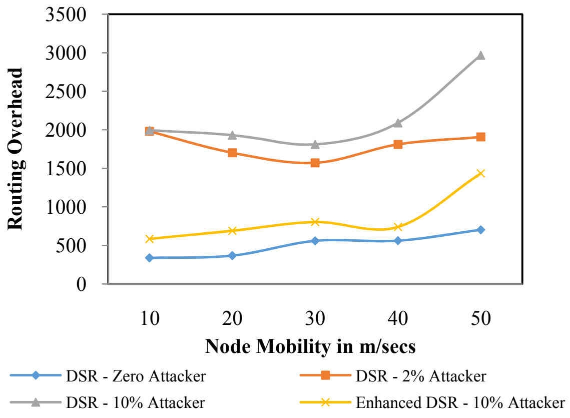


It is observed that the enhanced DSR protocol improves the packet delivery ratio as compared to DSR protocol. This is due to the fact that the proposed protocol detects the sinkhole nodes and isolates them quickly thereby enabling the normal nodes to transmit their data successfully.

5.1.2 Performance in terms of routing overhead

The routing overhead of the enhanced DSR protocol was investigated for varied node mobility. The mobility was varied from 10 m/s to 50 m/s. The routing overhead was obtained for DSR protocol in the ideal condition.

Figure 6 Node mobility vs. routing overhead (see online version for colours)



The sinkhole nodes were introduced in the MANET such that 2% of the nodes were sinkhole nodes and the routing overhead was obtained for DSR protocol. The routing overhead was obtained for enhanced DSR protocol and DSR protocol in the MANET with 10% of the nodes as sinkhole nodes. These results are shown in Figure 6.

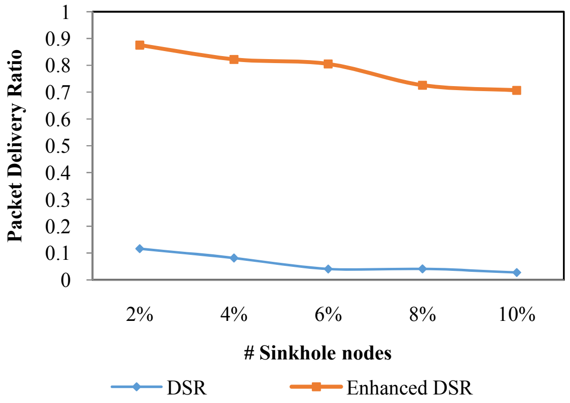
It is found that the routing overhead for the enhanced DSR protocol is very minimal and the proposed protocol provides significant improvement in the routing overhead.

5.2 Performance analysis on the percentage of sinkhole nodes in enhanced DSR protocol

5.2.1 Performance in terms of packet delivery ratio

The number of network nodes and the flows were fixed at 50 and 20 respectively. The node mobility was kept at 20 m/sec. The simulation time was 300 seconds. The sinkhole nodes were stimulated in the network such that 2% of the nodes were sinkhole nodes. The packet delivery ratio was obtained for DSR protocol and enhanced DSR protocol. Similarly, the packet delivery ratio was obtained for DSR protocol and enhanced DSR protocol in the MANET having 4% of nodes as sinkhole nodes, 6% of nodes as sinkhole nodes, 8% of the nodes as sinkhole nodes and 10% of nodes as sinkhole nodes separately. The results are given in Figure 7.

Figure 7 % of sinkhole nodes vs. PDR (see online version for colours)



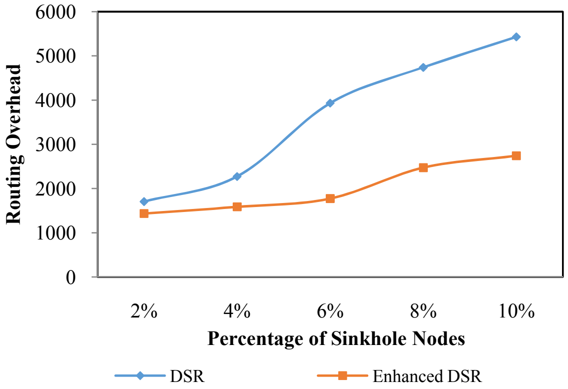
It is evident from Figure 7 that enhanced DSR protocol provides higher packet delivery ratio as compared to DSR protocol. This is due to the fact that the sinkhole nodes are identified efficiently and isolated from the MANET quickly.

This paves way for the other nodes to perform their normal operation. In addition, the isolation of the sinkhole node causes transient network partition. Hence, packet delivery ratio decreases for every increase in the percentage of attackers.

5.2.2 Performance in terms of routing overhead

The behaviour of DSR protocol and enhanced DSR protocol in terms of routing overhead is investigated. The number of network nodes was 50. The number of flows was fixed at 20. The simulation time was set at 300 seconds. The node mobility was 20 m/sec. The sinkhole nodes were stimulated in the MANET. Initially, the percentage of the sinkhole nodes was set at 2% of the nodes in the MANET.

Figure 8 % of sinkhole nodes vs. routing overhead (see online version for colours)



The routing overhead was obtained for DSR protocol and enhanced DSR protocol. The results are shown in Figure 8. Similarly, the routing overhead was obtained for DSR protocol and enhanced DSR protocol in the MANET having 4% of nodes as sinkhole nodes, 6% of nodes as sinkhole nodes, 8% of the nodes as sinkhole nodes and 10% of nodes as sinkhole nodes separately. The results are shown in Figure 8.

The results show that even at high stressful condition, routing overhead of enhanced DSR protocol is much lesser than DSR protocol.

This is primarily because enhanced DSR protocol detects and isolates the sinkhole nodes quickly thereby reducing the packet loss in the network. As a consequence, the necessity of routing packets is considerably reduced in enhanced DSR protocol.

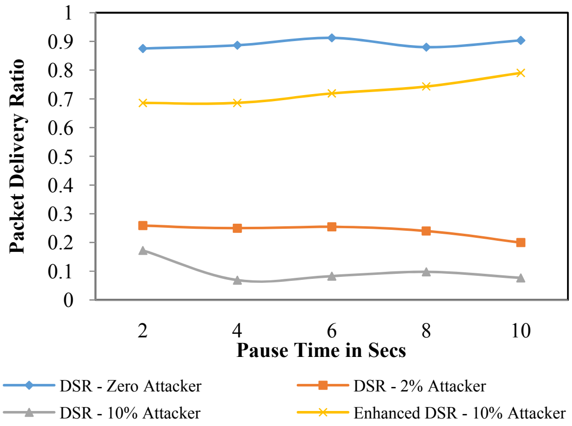
5.3 Performance analysis on the effect of varied pause time in enhanced DSR protocol

5.3.1 Performance in terms of packet delivery ratio

The number of MANET nodes was fixed at 50. The node mobility was kept constant at 20 m/sec. The number of flows was 20. The simulation time was 300 seconds. The pause time of the nodes was varied from 2 seconds to 10 seconds. Pause time is the amount of time a node stops before moving in the particular direction.

Initially the packet delivery ratio was obtained for DSR protocol in the MANET for ideal conditions. Then the sinkhole attack was injected in the MANET such that 2% of the nodes were sinkhole nodes. The packet delivery ratio of DSR protocol was obtained. The percentage of the sinkhole nodes was increased to 10%. The packet delivery ratio of DSR protocol and enhanced DSR protocol were obtained. These results are shown in Figure 9.

Figure 9 Pause time vs. PDR (see online version for colours)



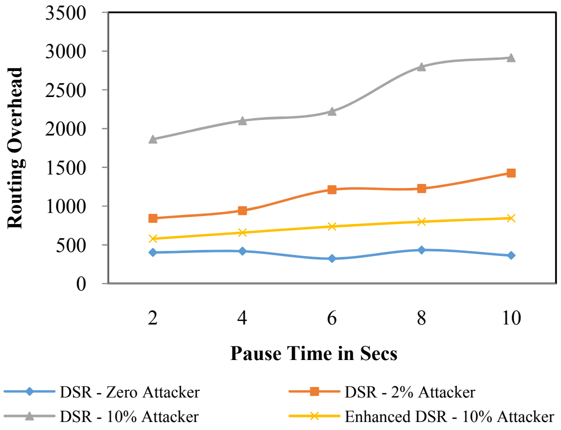
It is observed from Figure 9, the packet delivery ratio of enhanced DSR protocol is much higher than DSR protocol. This is due to the fact that enhanced DSR protocol isolates the sinkhole nodes quickly thereby enabling the other nodes to carry out normal operations. In addition, the packet delivery ratio of the enhanced DSR protocol is improved with the increase in the pause time.

5.3.2 Performance in terms of routing overhead

The number of MANET nodes was 50. The mobility of the nodes was kept at 20 m/sec. The number of flows was 20. The simulation time was 300 seconds.

The pause time of the nodes was varied from 2 seconds to 10 seconds. The routing overhead of DSR protocol in MANET for ideal conditions was obtained and is shown in Figure 10.

Figure 10 Pause time vs. routing overhead (see online version for colours)



The sinkhole attack was induced in the MANET such that 2% of the nodes were sinkhole nodes. The routing overhead was found for DSR protocol. Then 10% of the nodes were changed as attacking nodes in the MANET. The routing overhead was found for DSR protocol and enhanced DSR protocol. The results are shown in Figure 10.

The results show that the routing overhead for enhanced DSR is very minimal as compared to DSR.

This is primarily because of the efficient detection and quick isolation of the sinkhole nodes by enhanced DSR protocol. After the isolation of the sinkhole nodes from the MANET, the number of route discovery messages are reduced in enhanced DSR protocol.

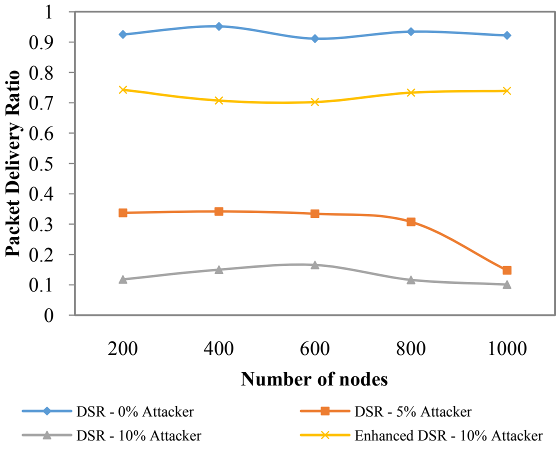
5.4 Performance analysis in terms of scalability on enhanced DSR protocol

5.4.1 Performance in terms of packet delivery ratio

The number of network nodes was varied from 100 to 500. The simulation time was set at 300 seconds. The node mobility was fixed at 20 m/sec.

The packet delivery ratio was obtained for DSR protocol in ideal MANET conditions. Then the sinkhole nodes were stimulated in the MANET. Initially, the percentage of the sinkhole nodes was set at 5% of the nodes in the MANET. The packet delivery ratio was obtained for DSR protocol. The results are shown in Figure 11. Similarly, the packet delivery ratio was obtained for DSR protocol and enhanced DSR protocol in the MANET having 10% of nodes as sinkhole nodes. The results are shown in Figure 11.

Figure 11 Number of nodes vs. PDR (see online version for colours)



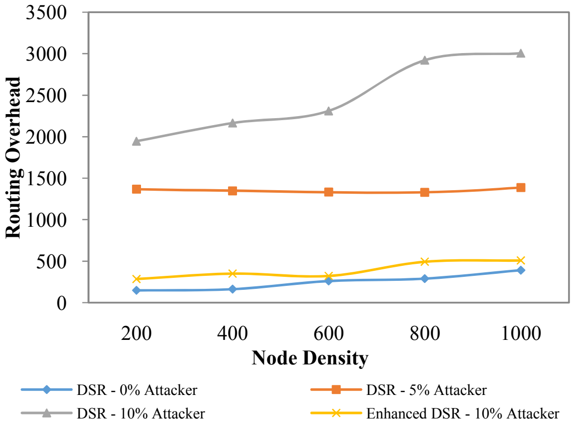
It is found from Figure 11 that the enhanced DSR protocol outperforms DSR protocol in terms of packet delivery ratio. Enhanced DSR protocol scales well. Enhanced DSR protocol maintains high packet delivery ratio with the increase in the number of mobile nodes in the MANET.

5.4.2 *Performance in terms of routing overhead*

The number of network nodes was varied from 100 to 500. The simulation time was set at 300 seconds. The node mobility was fixed at 20 m/sec. The routing overhead was obtained for DSR protocol in the ideal condition. The sinkhole nodes were introduced in the MANET such that 5% of the nodes were sinkhole nodes and the routing overhead was obtained for DSR protocol.

The routing overhead was obtained for enhanced DSR protocol and DSR protocol in the MANET with 10% of the nodes as sinkhole nodes. The results are shown in Figure 12.

Figure 12 Number of nodes vs. routing overhead (see online version for colours)



It is evident from Figure 12 that the routing overhead is kept minimal even with the increase in the number of nodes in the MANET. This is due to the fact that the proposed protocol detects and isolates the sinkhole nodes immediately from the MANET and less number of retransmissions is required. Hence the number of route discovery messages is reduced in enhanced DSR protocol.

Figure 11 and Figure 12 shown that the enhanced DSR protocol provides high scalability.

6 Conclusions

In this paper, an enhanced DSR protocol for routing in MANETs was proposed. This uses adjacency tables to calculate the validity of the new route and thus efficiently detects the sinkhole behaviour of the nodes and isolate them quickly. The proposed model does not require the nodes to work in promiscuous mode and it does not demand any additional hardware requirement. The proposed methodology was simulated and the experimental results on the packet delivery ratio and routing overhead were obtained for the proposed enhanced DSR protocol. The experimental results prove that the proposed protocol is efficient.

References

Boudriga, N. (2010) *Security of Mobile Communications*, Auerbach Publications, Taylor & Francis Group, Boca Raton, Florida, USA.

Jebadurai, I.J.R. and Rajsingh, E.B. (2011) 'A survey on sinkhole attack detection methods in mobile ad-hoc networks', *ICMLC 2011: Proceedings of 3rd IEEE International Conference on Machine Learning and Computing*, Singapore, Vol. 4, pp.430–433.

Johnson, D., Hu, Y. and Maltz, D. (2007) 'The dynamic source routing protocol (DSR) for Mobile ad hoc networks for IPv4' RFC 4728'.

Karlof, C. and Wagner, D. (2003) 'Secure routing in wireless sensor networks: attacks and countermeasures', *Ad Hoc Networks*, Vol. 1, Nos. 2–3, pp.293–315, Elsevier.

Kim, G., Han, Y. and Kim, S. (2010) 'A cooperative sinkhole detection method for mobile ad hoc networks', *AEU – International Journal of Electronics and Communications*, Vol. 64, No. 5, pp.390–397, Elsevier.

Marchang, N. and Datta, R. (2008) 'Collaborative techniques for intrusion detection in mobile ad-hoc networks', *Ad Hoc Networks*, Vol. 6, No. 4, pp.508–523, Elsevier.

Marti, S., Giuli, T., Lai, K. and Baker, M. (2000) 'Mitigating routing misbehavior in mobile ad hoc networks', *ACM Mobile Computing and Networking, MOBICOM 2000*, pp.255–265.

Mohanapriya, M. and Krishnamurthi, I. (2013) 'Modified DSR protocol for detection and removal of selective black hole attack in MANET', *Computers and Electrical Engineering*, Vol. 40, No. 2, pp.530–538, Elsevier.

Ozleyis, O., Burak, B. and Albert, I. (2004) 'A probabilistic routing disruption attack on DSR and its analysis', *Third Annual Mediterranean Ad Hoc Networking Workshop*, pp.300–306.

Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J. and Nygard, K. (2003) 'Prevention of cooperative black hole attack in wireless ad hoc networks', *ICWN'03: Proceedings of International Conference on Wireless Networks*, Las Vegas, Nevada, USA, pp.570–575.

Shim, W., Kim, G. and Kim, S. (2010) 'A distributed sinkhole detection method using cluster analysis', *Expert Systems with Applications*, Vol. 37, No. 12, pp.8486–8491, Elsevier.

Tseng, H.C. and Culpepper, B.J. (2005) 'Sinkhole intrusion in mobile ad hoc networks: the problem and some detection indicators', *Computers & Security*, Vol. 24, No. 7, pp.561–570, Elsevier.