Mitigation of black hole attack in MANETs: A sequence no-based approach

L. Maheshavel and C. Senthilkumar.

1,2 Department of Computer Science and Engineering, Thiagarajar college of Engineering (TCE), Madurai, India.

Emails: maheshavel@gmail.com

Abstract. MANET (Mobile Ad-hoc network) is type of network which is comprised of moveableness vertices which are connected to form a wireless network. The connected vertices can move very freely as there is no fixed infrastructure for the network. Black hole attack is a DOS attack where one of the vertices in the network is mischievous which tries to capture all the datagrams passing through it by sending a false reply to the origin vertex. In this paper an improvement is made to the existing AODV protocol to mitigate the black hole attack in Manets. The proposed method finds the mischievous vertex and avoids the delivery route through the mischievous vertex. The simulations were experimented in ns2 and the observations prove that the implemented approach works well for various performance metrics like Packet delivery ratio, End to End delay and throughput.

1. Introduction

As the improvements in wireless are increasing a lot, Huge reaches were started to bloom in the area of MANETs. MANET accounts for set of mobiles vertices that are non-uniformly located across the network and are able to transmit messages among them without any fixed infrastructure or a centralised management. In MANETs the vertices do not need a centralised vertex for its communication between the vertex despite they employ in a cooperative kind of stuff to pass on the data between them which are quite distant from each other’s. Owing to that, for the purpose of communication each vertex needs to finds itself a way or path. In spite of the flaws in the vertices, it is used in areas where the network needs to the implemented very without any infrastructure in advance, for example, communication needed for military purposes, mobile conferencing, etc. To establish the communication between the vertices in a trusted and efficient manner there are quite a few routing protocols like AODV protocol and DSV protocol.

Despite the usefulness and the effectiveness of MANETs, there are still areas which needs to be improved. The security issues in the routing protocols like AODV and DSR is one among them. This security issue is the one which has been always looked after. The traditional routing protocols are designed in such a way that the vertices that the network established among the vertices is a trusted one and all the vertices in the network works in a co-operative manner which actually leads to various security attacks to the network. One among them is the DOS attack. The DOS attack mainly tries to find the services that are available in the various routing protocols to mitigate the network capacity. Packet Dropping attack is one of such kinds of attack. The main topic of black hole attack which the proposal
addresses come under the Packet dropping attack. Black hole attack is also called as the Full packet attack in which when a origin vertex broadcasts a RREQ packet, a mischievous hole vertex gives a fake answer to the origin vertex by affirming that it owns the shortest approach to the terminus vertex with a untrue RREP packet to the origin vertex. and hence the origin vertex transmits all the packets to that mischievous vertex. Owing to which a black hole is produced inside the network by the fake vertex and all the transmitted data carriers are being scraped from the network instead of forwarding them towards the required terminus. The most vulnerable attack against the AODV protocol is the black hole attack because there is no existing way in AODV protocol to identify the misbehaving mischievous vertex

Lots of proposals were made to mitigate the security issue in MANETs, yet, quite a few unfulfilled vacuum available in MANETs which are uncovered by the researchers. The previous research works done in MANETs were focussed on how to minimize the effect of black hole without worrying about the performance of the network with various performance metrics like delivery ratio, throughput, etc. Therefore, making a change to at least one of the existing protocols is mandatory to address the above issues. In this methodology the authors aimed to enhance the performance of AODV protocol. The proposal is made by segregating the mischievous vertices by the seq. no in the (RREP) route reply packet given by the vertices. The origin vertex gets all the RREP from various vertices and then calculates a peak value from the difference of sequence no from the terminus to the origin vertex and dividing it with the total no of reply or RREP packets. The conventional AODV protocol finds the route with minimum no of hops and maximum sequence no. The mischievous vertex obviously replies with less hops and then with a higher sequence no. Hence the vertices which were given the seq. no bigger than that of the peak can be neglected. Thus, the proposed method gives an optimisation and enrichment to the AODV protocol

2. Black hole attack

In AODV, the discovery of routes by the vertices occurs in a cyclic manner. When a vertex is willing to transmit a message, it broadcasts RREQ packets to all of its neighbours. An RREQ is being is returned to the requested vertex by a neighbour vertex when it has no track to the terminus vertex through it by remembering the reverse track to the requested vertex when can be user later for sending further RREQ packets. Until the transmitted RREQ reaches an inter-located vertex through which a track exists to the terminus vertex or to the end vertex itself the above cyclic process gets repeated. The origin vertex is replied with a RREP by that corresponding vertex. This RREP is unicast along all the available intermediate vertices till the originally requested vertex. Thus, after each cycle a bidirectional path has been established between the vertices at both ends. The AODV keeps a routing table at each vertex. The routing table contains 3 essential columns for each terminus vertex, they are an immediate adjacent hop vertex, a seq.no and a count of hops resides along the track. All packets to be transmitted to the terminus are sent to the adjacent hop. The seq.no acts like time-stamping which is a computation of how much recent the route is. The count of hops indicates the no of inter-located vertices to the terminus vertex. when multiple RREPs are obtained by a origin vertex, only the vertices with highest sequence no is selected, the vertex with the lowest hop count is selected in case of two vertices with same sequence no.

The efficiency of MANET can be easily degraded by the Black hole attack as it can be caused by either a single mischievous vertex or by a pack of mischievous vertices [1]. Since the newness of the route is being estimated only based on the sequence no, the black-hole vertex in the network always demands that it has a newer route to all the required terminus vertices, by specifying a highest sequence no in the route reply [2]. Whenever a broadcast is initiated for route discovery by the origin vertex, the mischievous vertex replies quickly with a fake RREP specified with a highest sequence no for the required terminus, [3] that is believed as an honest answer from an inter-lying vertex possessing the shortest route.

The vertices residing in MANET are made to work in a cooperative manner due to the reason of which the origin vertex has a belief in the reply sent by the mischievous vertex as a genuine one and
transmits all the packets to the mischievous vertex instead of the genuine vertex having a correct route to the terminus. The origin vertex actually assumes that it is the optimal route but the mischievous vertex is the black hole in the network and hence all the data carriers are being lost without being forwarded to the terminus. The black hole attack is an example of DOS in the network, as it can deny the services between the start and end vertices. There are various kinds of black hole attacks in the networks they are, single vertex, multiple vertices, collaborative and smart black hole attack. Single or multiple vertex attack is caused by only one mischievous vertex in the network or multiple mischievous vertices in the network, where the collaborative attack is caused by the mutual cooperation among the vertices. A smart black hole attack is an intelligent attack which is smart as it can even go through the security patterns featured in a routing algorithm.

Consider the above scenario where “M” is the mischievous vertex. Vertex “A” wants to pass on the data carrier to vertex “E” hence it sends the RREQ to its neighbours. The vertex “E” transmits RREP to the vertex “A” with a minimum count of hops and a large seq.no, hence vertex “A” will consider that the path to “E” from “A” is shortest when it sends the packet via vertex “M” but the vertex “M” being the mischievous vertex will not forward the data instead the packet will be lost and hence a black hole is created at the vertex “M”.

3. Related Works

Ananthakumaran S et al. proposed a way of mitigating the black hole effect through trust-based approach in that all existing vertex is given a faith value based on the victory and flop rates of packet transmissions through the vertices. Vertices with trust value less than zero are considered as mischievous and are being put in the blacklist. RREP packets from the vertices in the blacklist are rejected. The maintenance of an extra trust table called the black table by all the vertices can increase the overhead.[4]

Pathan, M.S. et al. A proposed a way that, a fake route request is transmitted in the network such that the origin ode sends a broadcast as to pass on the data carriers to the vertex which is not at all available in the network. Those vertices which provide a reply to the origin as there is a path through this vertex to the non-existing terminus vertex are considered as mischievous vertices [5]

Yasin, A et al, proposed a method that, a dummy RREQ is sent with a small life time called a Bait time. The vertices which send the RREP within the Bait time are considered as mischievous vertices. There a few chances where the reply from the mischievous vertex may come a little late than Bait time [6]

Tamilselvi et al. provided a new way that can neglect the black hole vertices in the course of track founding and picks safe track alone for data channellization. In this proposed methodology, the origin vertex picks the address of the neighbour vertex as the required terminus vertex's address and broadcasts RREQ with the selected address to its neighbours along with an encrypted key. The vertex which has the terminus route through it will reply to the origin vertex with the decrypted information of the encryption key provided by the correspondence vertex whereas the mischievous vertex will not contain the public key of the origin vertex and hence reply the same encrypted key to the origin vertex which helps the start vertex to identify and ignore the mischievous vertex. The method can be failed in cases where any of the black vertices may contain information like public key about all the available vertices in the network. In these cases, the malevolent vertex can easily surpass the proposed methodology and hence an improvement is needed.[7]

Dorri Ali et al. provided a new approach for locating and neglecting the misbehaving vertices residing in
the network. This approach uses a data control packe(DCP) like the past routing protocol along with a black hole check (BCh) table for the identification of mischievous vertex in the network. All the existing vertices in the net. There are two fields in the BCh table they are, vertices ID and “Trustable” where trustable is a boolean variable that has a value of 0 indicating that the particular vertex is a mischievous vertex whereas a value of 1 indicates that the vertex is not mischievous which can be trusted. The neighbour vertices send the RREP to the origin along with the BCh of the corresponding vertex. On getting all the RREPs from the inter-lying vertices, a reliable route is being chosen on the basis of the BCh table of the respective vertices. A DCP is being sent to all the chosen routes by the origin to check the validity of the path. In case, if it encounters a mischievous vertex the data carrier is being dropped and the respective path is ignored or else the respective path is considered for transmission. The overhead is increased due by using the huge no of DCPs and also the delay in the course of routing also gets increased due to the maintenance of the BCh table for each vertex in the network [8].

Kumar et al. provided a scheme to locate the misbehaving vertices by using IDS kind of vertices. The fore-most outcome of this employment was to employ a method to locate black-hole attack and also minimize the impact of the mischievous vertex on non-mischievous vertices. In this proposal, the passage of data among vertices are monitored by keeping IDS vertices residing in network. The approach identifies the black hole on the basis of volatality of the sequence no. In the course of monitoring, when the special vertex identifies that the sequence number is replicating with a sequence no larger that the set threshold, then the vertex is included in a respective table of IDS and a packet is channelized as an alert in the network possessing the I.D of a mischievous vertex to avoid further transmissions through it. There is an overhead due to the usage of extra IDS vertices can be a limitation of the above approach. An improper implementation of IDS may lead to false identification of attacker vertices.[9]

Jhaeveri et al. provided a way to locate the mischievous centered on the greatest seq no in the RREP sent by the vertex. This proposal requires two changes in each vertex's routing table, one is the "Vertex Status" which is used to contain the behaviour of the vertex and the other is "Last Reply time" designates to the desired terminus vertices’ s sequence no which is updated in any vertex's final RREP. In this approach, 3 variant attacking models with distinct routing behaviours are taken into account. A pre-mentioned value is determined at each vertex in the course of the tracking process. When an RREP packet of a vertex contains the sequence no which is more than the computed value, the vertex is interpreted as sceptical as of now. To affirm the estimation of vertex which is sceptical of now, the corresponding vertex is forwarded with a bait request packet contains the terminus address. The terminus address sent is the address of vertex which is not at all in the network. If a reply is made by the vertex to this fake bat request packet, the sceptical estimation is switched to mischievous state, and none of the packets are either forwarded or received to that vertex from thereafter. Hence neglecting the respective vertex. Delay may be increased by the computation of threshold value at each vertex [10]

Naveena s et al provided a scheme centered on faith on the vertices residing in the network. In the course of routing, a data retrieval tables is being maintained by this methodology to monitor the passage of vertex data among the vertices. There is another phase called routing formation which is to locate a track to the terminus vertex which is more secured among the available paths[11].

4. Proposal

The foremost aim of the proposed algorithm is to locate, isolate and eliminate the harmness of misbehaving vertices in the network. In the AODV protocol the origin vertex sends the RREQ to the neighbours and the neighbours sends the RREP with the updated seq.no with the count of hops needed to reach the terminus. The mischievous vertex sends the RREP with a maximum sequence no and with a less no of count of hops. In this proposal a new value called the “Peak sequence no” is calculated from the seq.no of the both RREQ and the RREP packets. The peak value is the division of cumulation of the subtraction between the RREP and the RREQ packets with the total no of RREPs.

$$\text{sum} = \sum_{i=1}^{N} (\text{seqno in ith RREP} - \text{seqno in RREQ})$$
Peak value = \text{sum}/N

Where,
- \( N \) is the total no of RREPs
- RREP is the route reply packet
- RREQ is the route request packet

The normal AODV protocol checks only whether the sequence no in RREP is as high or not but the proposed method checks if that is lesser than that of Peak or not. If a vertex has a route reply with minimum no of hop-counts and also with the higher sequence no but only those vertices with the sequence no less that the peak value will be considered as non-mischievous vertex, other vertices will never ever be considered by the origin vertex for packet delivery. So, this proposal will help locating secure tracks and segregating Blackhole vertices in the network.

5. Simulation Results and Discussions

To estimate the perfectness of the proposed approach a simulation is done on ns2.35 simulator. We have accomplished 3 protocols namely, AODV, BAODV which is the simulation of AODV with black hole vertices and then the AODV protocol with the proposed the mechanism. Thirty vertices were created and simulated in ns2 among which 3 vertices were mischievous vertices.

5.1 Performance metrics
- Packet Delivery Ratio (PDR): PDR may be defined as the division of the packets acquired no by the terminus vertex to the packets sent no by the origin vertex;
- Average End to End Delay (AEED): AEED may be defines as the delay of sending packets by the origin and acquiring it by the terminus;
- Throughput: Represents the total no of packets transmitted and received successfully for a given simulation time.
### Packet Delivery Ratio

| Simulation time | AODV     | AODV with black hole | Proposal |
|-----------------|----------|----------------------|----------|
| 20              | 0.9875   | 0.1583               | 0.6654   |
| 40              | 0.9959   | 0.1751               | 0.7971   |
| 70              | 0.998    | 0.1732               | 0.9345   |

### Throughput

| Simulation time | AODV     | AODV with black hole | Proposal |
|-----------------|----------|----------------------|----------|
| 20              | 71.26    | 18.22                | 48.34    |
| 40              | 71.44    | 18.94                | 48.65    |
| 70              | 71.44    | 19.03                | 48.98    |

### Average End to End Delay

| Simulation time | AODV     | AODV with black hole | Algorithm |
|-----------------|----------|----------------------|-----------|
| 20              | 19.9507  | 21.5563              | 20.4452   |
| 40              | 20.0461  | 28.8326              | 23.65     |
| 70              | 20.0564  | 29.1839              | 24.98     |
Packet delivery ratio: It can be inferred from the Fig 1 that, when there is no attacker vertex resides in the network the PDR is highest i.e) it ranges between 0.9875 and 0.998. When we introduce some attacking vertices to the network, there is a fair fall in the PDR as it ranges between 0.1583 and 0.1751. The reason for this reduction in PDR is due to the non-availability of any mechanism to monitor the misbehaviour of vertices in the course of the process of routing. The PDR is improved when the proposed algorithm is employed as it ranges between 0.6654 and 0.9345

End to end delay: More the no of vertices reside in network, the more is the delay of routing, inside the network. From the results it can be inferred from Fig 2 that the ED of AODV is the lowest without any misbehaving vertices as it ranges between 19.9057 ms and 20.0564 ms due to the presence of protocol which always choses the shortest path towards the end vertex. When black vertices were added to the network, the ED rises up abruptly as it ranges between 21.5563 ms and 29.1839 ms. The cause for this volatility in the network is due to the absorption of packets along the way by the attacker vertices and also the protocol is designed in a way to constantly search for newer routes to improve the security of the network. The proposed changes made to the protocol behaves better and the results are well and good in terms od ED, the delay ranges between 20.448 ms and 24.98 ms. The proposed algorithm showed better performance even black hole vertices are included.

Network throughput: From Fig 3, it can be interpreted that the NTP of the routing protocols are always reduced by the inclusion of black hole vertices in the network. From the inference of Fig 3, the NTP of AODV is very high when black vertices are excluded from the network as it ranges between 71.26 kbps and 71.44 kbps. But by the inclusion of attacking vertices the AODV’s NTP gets reduced as it ranges between 18.22 kbps and 19.03 kbps. The proposed approach results are better considering the throughput i.e there is an improvement as it ranges between 48.34 kbps and 48.98 kbps. The improved results indicates that comparatively large amount of packets were delivered to the terminus within the given unit of time. Hence the proposed method is more effective of the isolation of vulnerable vertices before the transmission of data.
6. Conclusion

In this project, a sequence no-based proposal is made which tries to eliminate the presence of misbehaving black hole vertices in the MANET and improves the performance of the network. The improvement showed by the project has been proved with the simulation results from ns2. The future work is to reduce the calculation overhead which happening in the course of routing in the proposed approach in terms MANETs.

References

[1] Bhagat, Swapnil P., Puja Padiya, and Nilesh Marathe. "A generic request/reply based algorithm for detection of blackhole attack in MANET." In Smart Technologies For Smart Nation (SmartTechCon), 2017 International Conference On, pp. 1044-1049. IEEE, 2017.

[2] Singh, Kulwinder, and Shilpa Sharma. "A new technique for AODV based secure routing with detection black hole in MANET." In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 1528-1534. IEEE, 2017.

[3] Shashwat, Yugarshi, Prashant Pandey, K. V. Arya, and Smit Kumar. "A modified AODV protocol for preventing blackhole attack in MANETs." Information Security Journal: A Global Perspective 26, no. 5 (2017): 240-248.

[4] Ananthakumaran.S, Sathishkumar. M, Bhavani. R, Ravinder Reddy. R. “International Journal of Advanced Trends in Computer Science and Engineering”9(3) (2020), pp. 4022-4029.

[5] Pathan, M.S., HeJ., Zhu, N. (...), Memon, M.Q. Azmat, A. "International Journal of Advanced Computer Science and Applications"10(1),(2019) pp. 243-251.

[6] Yasin, Adwan, and Mahmoud Abu Zant. "Locating and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique." Wireless Communications and Mobile Computing 2018 (2018).

[7] Tamilselvi, P., and C. Ganesh Babu. "An efficient approach to circumvent black hole vertices in manets." Cluster Computing (2017): 1-9.

[8] Dorri, Ali, Soroush Vaseghi, and Omid Gharib. "DEBH: locating and eliminating black holes in mobile ad hoc network." Wireless Networks 24, no. 8 (2018): 2943-2955.

[9] Kumar, Sudheer, and Nitika Vats Doohan. "A modified approach for recognition and eradication of extenuation of gray-hole attack in MANET using AODV routing protocol." In Colossal Data Analysis and Networking (CDAN), Symposium on, pp. 1-5. IEEE, 2016.

[10] Jhaveri, Rutvij H., and Narendra M. Patel. "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks." Wireless Networks 21, no. 8 (2015): 2781-2798.

[11] Naveena s, Senthilkumar C, Manikandan T. “Analysis and Countermeasures of Black-Hole Attack in MANET by Employing Trust-Based Routing”. 6th International Conference on Advanced Computing & Communication Systems (ICACCS) 2020