ISSN 0975-3303
Mapana J Sci, **11**, 4(2012), 65-76
https://doi.org/10.12725/mjs.23.5

Mitigating Black Hole Attacks in AODV Routing Protocol Using Dynamic Graph

Arunangshu Pal,[*] Anita Pal[†] and Prasenjit Choudhury[‡]

Abstract

With the advancement of wireless technologies, Mobile Ad hoc NETwork (MANET) has been an important field of study. MANETs find useful applications in the real world, for example in military battlefield and disaster management. Since MANET is dynamic in nature, it must be represented by dynamic graph. Evolving graph, a form of dynamic graph, may be used for the purpose. When we talk about a network, a routing protocol comes into the question, and one of the most popular routing protocols is AODV. However, since AODV suffers from a drawback that it may be a victim of black hole attack, we need to find a technique to eliminate the possibility of the phenomenon. This paper makes a study of MANET and an efficient way of representing MANET by dynamic graph. It explains the AODV routing technique and the black hole attack. It then extends the idea of dynamic graph to propose a technique to solve the problem of black hole attack in AODV.

1. Introduction

Mobile Ad hoc NETwork (MANET) is an interesting field of study in modern times. It can be used to solve communication problems in many real world scenarios like military battlefield, disaster

[*] Department of Computer Applications, NIT Durgapur, arunangshupalinbox@gmail.com

[†] Department of Mathematics, NIT Durgapur, anita.buie@gmail.com

[‡] prasenjit0007@yahoo.co.in

Received: July 2012, Reviewed: Aug. 2012

management, educational programmes and multimedia services [4]. MANET, as the name suggests, is dynamic in nature, i.e. its topology keeps on changing randomly and frequently. This inherent property makes it difficult to handle this type of networks as far as routing data through the network is concerned. When a node needs to send a packet of data through the network to some destination node, it needs to find the correct path so that packet loss is minimised and the transmission is efficient. One of the popular routing protocols for MANET is Ad hoc On Demand Distance Vector routing (AODV) [5]. AODV is a reactive protocol – it finds a route only when it is required. Its technique is to broadcast a route request packet and discover the route after receiving a route reply packet that has the next hop information. It uses a time-out during it which it waits for the route reply. The expiry of the time-out causes it to rebroadcast the route request. The discovered routes are assigned with sequence numbers which denote the freshness of the routes. The route with the highest sequence number is selected to route data packets.

AODV suffers from a drawback that it is prone to black hole attack [7]. Black hole attack is made by some malicious node that drops all packets received by it and results in huge amount of packet loss. It launches the attack by sending a route reply with an updated sequence number. The source node, due to the property of the protocol of selecting the route with the highest sequence number, routes the data packets through the route containing the malicious node, resulting in the successful implementation of the attack.

We aim to eliminate the possibility of black hole attack by using dynamic graph to discover the route. Evolving graph [1], a form of dynamic graph, can efficiently represent a MANET. Using evolving graph, if we can predict the future topology of a MANET, we may avoid the use of sequence numbers to find the correct route. We may modify the AODV protocol in such a way that it selects the correct route by using the predicted topology of the network. Thus the protocol will be saved from the black hole attack.

In section 2, we explain MANET and its applications. In section 3, we describe what the evolving graph is. In section 4, we show how MANETs can be represented by evolving graph. In section 5, we describe the AODV protocol and black hole attack in AODV (section 5a). We propose the technique of mitigating black hole attacks in AODV routing protocol using dynamic graph in section 5b.

2. Mobile Ad Hoc Network

Wireless computer or cellular networks can be classified into two types – Infrastructure based network and Infrastructureless network [3]. In Infrastructure based wireless network, the nodes of the network, that may be mobile or immobile, communicate with one another through fixed base stations. The base stations work as routers between the communicating nodes. When a node goes out of range of one base station, it enters the range of another base station. The whole communication in the network is controlled by the base stations. On the other hand, in infrastructureless network, there are no fixed base stations, i.e. the network is not provided beforehand with an infrastructure. The communicating nodes are mobile and communicate with each other while moving. The nodes themselves act as routers. The nodes form a dynamic network by sending, receiving and forwarding data packets without the help of any base station. Mobile Ad Hoc Network (MANET) is an example of infrastructureless network.

In Mobile Ad Hoc Network (MANET), the mobile nodes create the dynamic network on the fly [3], i.e. they create the network by themselves by acting as routers without the help of any base station. The network is temporary and its topology is dynamic, meaning the topology may randomly change frequently, since the nodes are mobile often exhibiting random movements.

With the advancement in wireless communication technology, MANET has grown popular in real life scenarios and has a wide range of important applications. MANETs are necessary in those situations where an infrastructure based network is not possible to establish. Examples of applications of MANETs [4] can be as follows:

1. Military operations: In military regions, it is not possible always to set up an infrastructured network. MANETs come into play in these scenarios when soldiers need to

create a communication network instantly for wartime activity or other military operations.

2. Disaster management: During natural disasters like earthquakes and floods, when the network infrastructure fails, MANETs have to be used for rescue operations. MANETs make it possible to render emergency services to the victims.
3. Public network services: MANETs can be used to serve people in public places like classroom, conference hall, sports stadium, train, aircraft, etc. Educational, news or multimedia information can be provided by MANETs at these places.
4. Personal networks: MANETs can be used to set up temporary network among personal devices like cellphones, laptops or PDA's to transfer data or even connecting to the Internet whenever people require.

3. Evolving Graph

Let us see what an evolving graph is like. The evolving graph is an indexed sequence of a number of subgraphs of a given graph where the subgraph with a particular index is a representation of the network topology at that time interval represented by the index number [1]. The following subgraphs represent four snapshots of the topologies of a MANET.

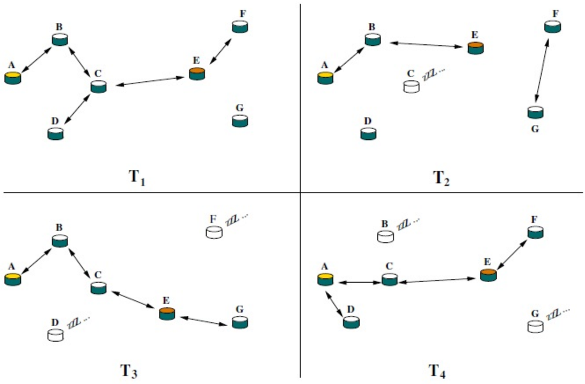

Figure 1: Snapshots of a MANET at the four time periods T_1, T_2, T_3 and T_4.

These four subgraphs of the time periods T_1, T_2, T_3 and T_4 constitute the evolving graph shown below:

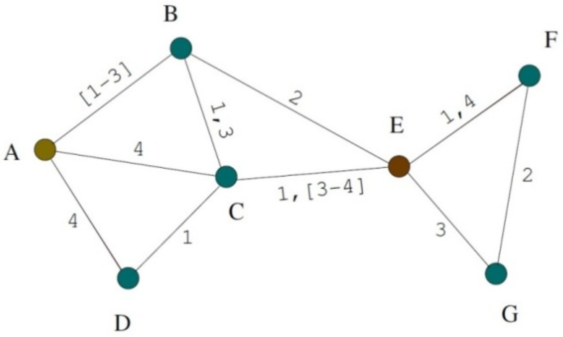

Figure 2: Evolving graph of MANET shown in figure 1.

Here, the edges are labelled with numbers representing the presence time intervals. For example, the edge CE is labelled with 1,[3-4] – this means that there is an edge from node C to E at time intervals 1, 3 and 4 only. A journey in the evolving graph is a sequence of edges with non-decreasing edge time-labels, i.e. a path at a particular time interval cannot be constructed by using edges that existed in past subgraphs. Thus the time domain is incorporated in the evolving graph model.

4. Representation of MANET by Evolving Graph

Now, there arises the question of how to represent MANETs so that they can be studied with the aim of improving their efficiency. Since MANETs are dynamic in nature, i.e. their topology frequently changes, they must be represented by some dynamic entity. A network is generally represented by a graph. Now since a MANET is a dynamic network, it must be represented by a dynamic graph. Here comes the concept of using evolving graph to represent MANETs.

Julian Monteiro, Alfredo Goldman and Afonso Ferreira, in their work [1, 2] have used the evolving graph concept to represent MANET and to design and evaluate routing protocols in MANET. The researchers have implemented the foremost and shortest journey algorithms by the evolving graph model and call the routing protocols originated from them as $EG_{Foremost}$ and $EG_{Shortest}$ respectively. The protocols are then compared with four main MANET routing protocols, DSDV, DSR, AODV and OLSR through extensive simulations.

In figure 1 above, the four subgraphs of the evolving graph can be used to represent the four snapshots of the topologies of a MANET at time periods T_1, T_2, T_3 and T_4. The nodes in the graphs represent the mobile nodes of the MANET and the edges of the graphs represent the links between the mobile nodes. Thus the graphs represent the connectivities between nodes over a span of time. The resultant evolving graph, shown in figure 2 above, has edges labelled with numbers that denote the time periods at which the links exist between nodes. In this way, an evolving graph can represent the dynamic topology of a MANET that changes over time and space. Here, we note that there is a journey from A to F through the path A, B, C, E, F and also through the path A, B, E, F. Now the latter path may have less number of hops but we see that it takes 4 time intervals, while the former path takes only 1 time interval. Thus a path with more number of hops may be a quicker one than the one that takes a less number of hops, due to the dynamic nature of the network over time and space.

5. Ad Hoc on Demand Distance Vector Routing

Ad hoc On Demand Distance Vector Routing (AODV) is a routing protocol used in mobile ad hoc networks and other wireless networks [3, 5, 6]. AODV is a reactive or on-demand protocol [3], meaning that it discovers route only when it is required. It has the property of using sequence numbers for the discovered routes so that old routes are discarded and fresh routes are used. It also prevents the counting-to-infinity problem by using time-out values in route requests. This means that when a route request packet is broadcasted, the source node will wait for a particular period of time before it rebroadcasts the next route request packet with a new sequence number and longer time-out value. Let us see what happens in this routing technique by considering a simple network represented by the following graph:

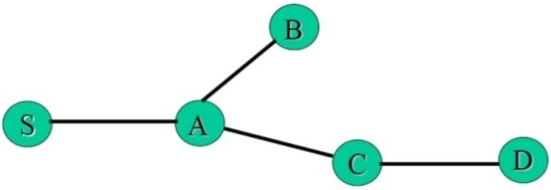

Figure 3: Sample network to show AODV.

Here let S be the source node that wants to discover a route to the destination node D. S broadcasts a RREQ (Route Request) packet to its neighbours. If its neighbours have a route to the destination, they reply with a RREP (Route Reply) packet. If not, they broadcast the RREQ packet to their neighbours. Here, A broadcasts the RREQ to B and C. Now C has a route to D, so it replies with an RREP and sends to A. A then sends the RREP to S. The RREP has information about the next hop and the hop count to the destination. Thus S discovers the route to D. Now whenever a new route is discovered, it is assigned a sequence number which is an incremented value of the last sequence number. The route with the largest sequence number is selected for routing packets. Thus the fresh route is always selected, while the older routes are discarded.

a) Black Hole attack in AODV

The AODV protocol always selects the fresh route to transmit data packets. The freshness of a route is determined by the sequence number of the route. When the source node receives multiple RREP (Route Reply) packets, it uses the RREP packet with the highest sequence number. This property of AODV makes it prone to black hole attacks [7]. Let us see how a black hole attack can be set up. Consider the following graph representing a MANET topology:

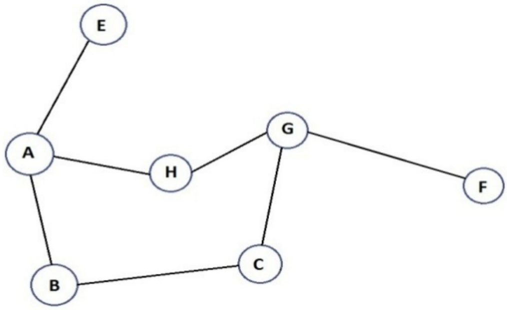

Figure 4: Sample network without malicious node.

Here, let A be the source node and F be the destination node. When A broadcasts the RREQ (Route Request) packet, it receives two RREP packets from H and B respectively that denotes two routes as follows:

1. A-H-G-F; Sequence number – 50.
2. A-B-C-G-F; Sequence number – 100.

Now, route reply containing the highest sequence number is considered as a fresh route. Since route 2 is fresher than route 1, it is selected as the preferred route. All this happens at time period 1. Now at time period 2, node D comes into the scene. See the following graph that represents the topology at time period 2.

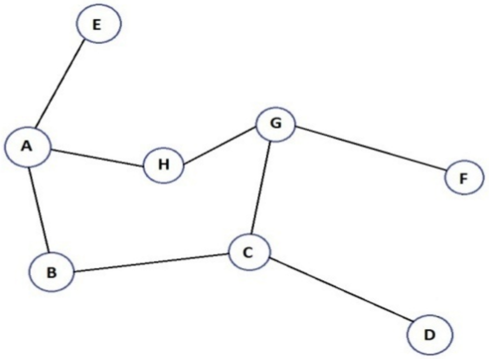

Figure 5: Sample network with malicious node D.

Here, D is a malicious node that launches the black hole attack. At time period 2, D sends an RREP packet to C with an incremented sequence number as 150, although D does not have a route to the destination F. Consequently, A receives another RREP packet that denotes the following route.

1. A-B-C-D-F; Sequence number – 150.

Since route 3 is fresher than routes 1 and 2 because of a higher sequence number, it will be selected as the preferred route. When A sends data packets along this route, D will discard or drop the packets thereby successfully implementing the black hole attack.

b) Eliminating the Black Hole Attack by Dynamic Graph

Since the property of AODV to always select the freshest route as the preferred route is mainly responsible for the protocol to be a victim of black hole attack, we may eliminate the property and take a different approach in selecting the route. We may use evolving graph, which is a dynamic graph, to predict beforehand the topology of a MANET in the near future. The topologies represented by the two graphs above would be denoted by the evolving graph shown below:

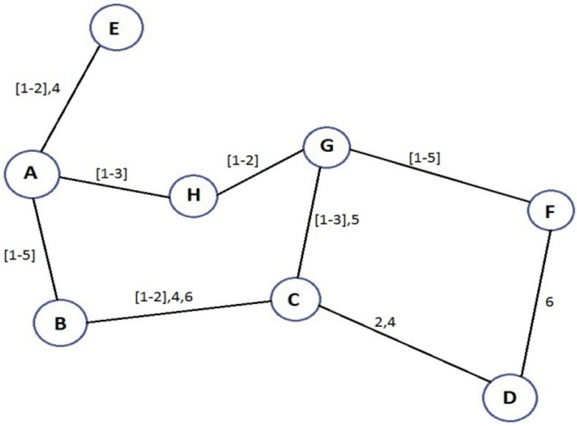

Figure 6: Evolving graph of sample network of figure 5.

From the evolving graph, we see that at time period 2, there is no route from D to the destination F. So whatever be the sequence of the RREP packet received from D, source A will not send its data packet along the route through D. Rather, we are not anymore bothered about the freshness of the discovered route. We may modify the AODV protocol in such a way that a route is selected only after foreseeing the topology of the network in the near future with the help of the evolving graph. In this case, since we already know that there is no route from A to F through D during the time periods 1-5, we will not select any route through D. By investigating the edge labels of the evolving graph, that denote the existence of the links between nodes, we can determine the best route to be taken at a given time period.

In dynamic environment like MANET, frequent change of topology may occur due to:

- Node mobility.
- Addition of new nodes.

The topology changes that may occur because of mobility can be predicted using the following mobility prediction algorithm. The dynamic graph at instance 't' can be obtained by predicting the mobility of the nodes using this algorithm. If new nodes join the network, the topology can be designed from the neighbour list of the individual nodes. The objective is to select the route based on the topology of the dynamic graph.

Mobility prediction algorithm:

Each node monitors its neighborhood. Let x denote the node and N be its neighborhood set of nodes at time t where N_t comprises of two categories of node: Nodes which were also neighbor of x at time (t-1) denoted by N_{t-1}. Nodes which are neighbors of x at time t but was not neighbors during time t-1 denoted by N_t Mobility of a node at time t:

m^{t}_{x} = $[N_t/N_{t-1}]$.Where m^{t}_{x} is the mobility of x at time t.

$$R_x^t = \frac{1}{s}\sum_{i=t-x}^{t}(m_x^t)$$

Relative mobility of a node at time t is stored for the last s time steps. The algorithm for mobility prediction is as follows:

Step 1: Find current neighbor list

Step 2: Calculate change in neighbours using below equation

$$\frac{|\,\text{Previous Neighbor List}\,|\cap|\,\text{Current Neighbor List}\,|}{|\,\text{Current Neighbor List}\,|}$$

Step 3: Store the obtained values in array

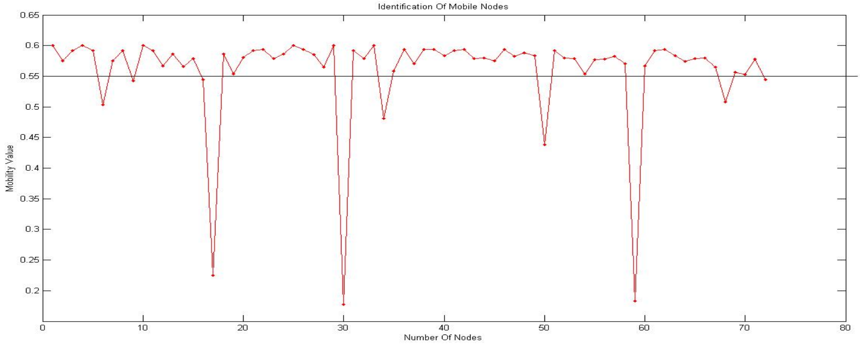

Figure 2: Identification of Mobile Nodes (Number of Nodes: 72)

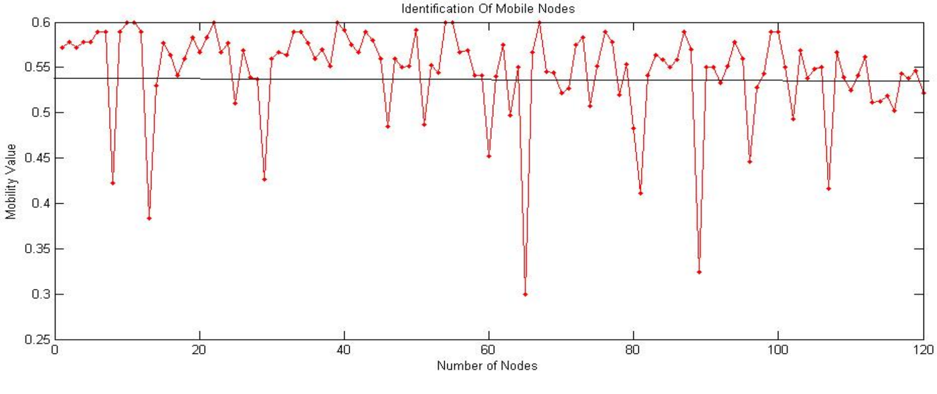

Figure 3: Identification of Mobile Nodes (Number of Nodes: 120)

The above graphs indicate the static nodes having more mobility value than the mobile nodes. There is line in middle of graph, which indicates the average of value of prediction value. Nodes below this line treated as mobile nodes having more mobility with respect to other nodes.

6. Conclusion and Future Work

We have shown here how the AODV protocol can be a victim of the black hole attack and proposed a method to eliminate this phenomenon. Our idea is to use evolving graph, a form of dynamic graph, to predict the network topology beforehand and then select a route based on this prediction. We are avoiding the use of freshness of the route to select the path, thereby mitigating the black hole attack. Our proposed solution is only for AODV protocol. Further research can be made to find out the solution in case of other routing protocols as well. Also, the tool of dynamic graph can be used to devise more efficient routing protocols that would find the correct path by using the predicted future topology of the network. Thus we see that dynamic graph can be made a powerful tool in routing operations in MANETs and to cope with other routing attacks in MANET [8].

References

[1] J Monteiro, *The use of evolving graph combinatorial model in routing protocols for dynamic Networks*. Instituto de Matematica e Estatistica - Universidade de Sao Paulo (IME-USP).

[2] J Monteiro, A Goldman and A Ferreira, *Performance Evaluation of Dynamic Networks using an Evolving Graph Combinatorial Model*. WiMob '06 – Montreal/Canada.

[3] S Taneja and A Kush, A survey of routing protocols in mobile ad hoc networks. *Int. J. Innovation, Management and Technology*, vol. 1, 2010.

[4] K Lego, P K Singh and D Sutradhar, Comparative study of adhoc routing protocol AODV, DSR and DSDV in mobile adhoc network. *Indian J. Computer Science and Engineering*, vol. 1, 364-371.

[5] L Klein-Berndt, *A Quick Guide to AODV Routing*. National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce.

[6] B Awerbuch and A Mishra, Ad hoc on demand distance vector (AODV) routing protocol, *Advanced Topics in Wireless Networks*. Department of Computer Science, Johns Hopkins.

[7] M Al-Shurman and S Yoo, S Park, *Black Hole Attack in Mobile Ad Hoc Networks*.

[8] R H Khokhar, M A Ngadi and S Mandala, A review of current routing attacks in mobile ad hoc networks. *Intl J. Comp. Sci. and Security*, vol. 2. No.3, pp. 18-29, 2008