IOP Conf. Series: Materials Science and Engineering **396** (2018) 012032 doi:10.1088/1757-899X/396/1/012032

A Study on Packet Loss Reduction methods and Node Registration methods in AODV for MANET

Achu Anna Antony [1], Bino Thomas [2]

[1]St. Joseph's College of Engineering and Technology, Palai
[2] Assistant Professor,St. Joseph's College of Engineering and Technology, Palai

E-mail: [1]achuannaantony2@gmail.com, [2]binothokar@gmail.com

Abstract. Mobile Ad-hoc NETwork (MANET) is a restless self-forming, infrastructure-less network of mobile nodes in a wireless connection. As there is a high hike in the use of mobile devices and wireless networks over past years, MANET has become one of the vital networks used for communication. A routing protocol is used for distributing information that allows selecting routes between two nodes in a network. Ad- hoc on- demand distance vector (AODV) protocol is widely used protocol for routing in mobile ad- hoc network. Packet loss is one of the significant problems that happen in the mobile ad- hoc networks while routing. A packet consists of the unit of data which is routed between source and destination in a network. Packet loss happens when one or more packets across devices in a network drop before reaching the destination node. A node density method is proposed in this study to alleviate the packet loss problem to an extent. Due to network infrastructure of MANET dynamically changes, mobile ad- hoc network is very vulnerable to attacks. As for the security purpose, we also propose a bloom filter method, which can be used to register the mobile nodes that are participating in a network in- order to restrict attacker nodes or foreign nodes to participate in the packet transmission.

Keywords- Bloom-filter, mobile ad-hoc network, routing protocol, neighbor node.

1. Introduction

Usage of mobile nodes these days has increased and the communication enhancement in its network becomes crucial. Ad hoc networks are generally used by military, rescue teams, personal electronic device networking, maritime communications etc. These users cannot rely on the centralized network [10]. The main factors affected in ad-hoc networks are routing and the characteristic of wireless communication. In ad hoc, a node can communicate only with nodes in its area and to communicate with other nodes uses a routing algorithm. [10]. Mobile Ad-hoc network (MANET) is a collection of mobile nodes that constitute a network with no central admin [1]. A MANET can change location and is a kind of ad-hoc network. MANET has its property that it can configure itself. The advantage of a decentralized network is that they are more robust than centralized networks due to its multi-hop pattern.

Packet loss in transmission is one of the major limitations in the mobile ad-hoc network. As one node moves away from the network, the connection gets lost and the packet drop may happen and also because of congestion packet loss happens. Congestion happens when many

demand request gathers and when there is a shared medium [11]. To send packets to the Internet, a MANET node acquires information about an Internet Gateway and establishes appropriate routes to this gateway [2]. There are generally three kinds of protocols used like proactive, reactive and hybrid and is shown in fig 1.

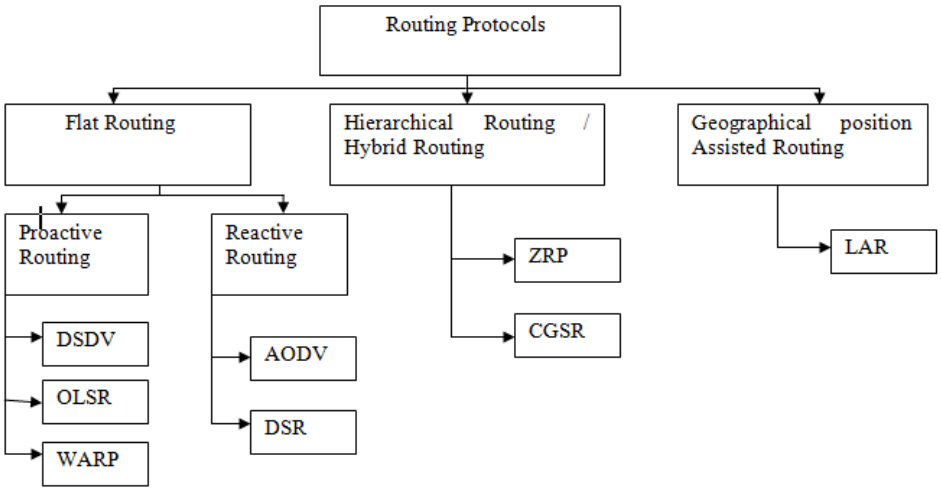

Figure 1. Ad- hoc routing protocols.

Considering AODV and DSDV routing protocols, AODV is better [11]. AODV routing protocol is a distance vector routing protocol and uses destination sequence numbers to determine the freshness of routes. AODV mostly maintain only active routes. Due to openness, dynamic, infrastructure-less nature, MANET is vulnerable to various attacks. One of these possible attacks is a Black Hole Attack.

A proposed node density method in this survey can be added along with the AODV protocol to send packets from node to destination with less packet loss. This survey paper adopts bloom filter technique, to reduce the attacks from foreign nodes by making member nodes to register into the bloom filter.

2. Background and Related Works

2.1. Type of Attack and Node Registration Method

2.1.1. Attack in AODV .

Black Hole Attack In AODV Protocol [13]: AODV Routing Protocol is used to find a path from source to the destination in an ad hoc network. All mobile nodes are needed to use routing control messages to find the path to the destination. There are three types of routing control messages in AODV protocol and they are Route Requests (RREQs), Route Reply (RREP), Route Error (RERR) which are used to find a path to the destination [14]. The AODV uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested to it. The principle of this protocol is higher the destination sequence number; fresher is the route [14]. When the source node S wants to communicate with destination D as shown in the figure2, it broadcasts RREQs messages to

the neighbor nodes. These neighbors check their routing table whether there is a path to the destination or not. If not then they also forward RREQs of the source node until the message is received by the intermediate node having a path to the destination or to destination node itself. If the node having a path to destination receives RREQ, it sends route reply message to the source node. In this way, source node selects the shortest path to the destination node with the greater sequence number of route reply message. If any link break occurs then RERR message send to the source node. In Black Hole Attack in MANET, assume malicious node M as Source S broadcasts its RREQs to connect with destination D, all intermediate node check their routing table whether there is a path to the destination D. Here Node M as malicious does not check its routing table and send false route reply packet to the source S with greater forged sequence number [15] than expected that it is having a path to destination D. As malicious node M does not check its route table, this reply reaches the source node faster than the normal nodes [16] source node select this path and send all of its data to the node M. The node M receives this data packets and deprive of the destination node. As this packets never reach the destination node D the attack is called as a black hole attack [17]. .

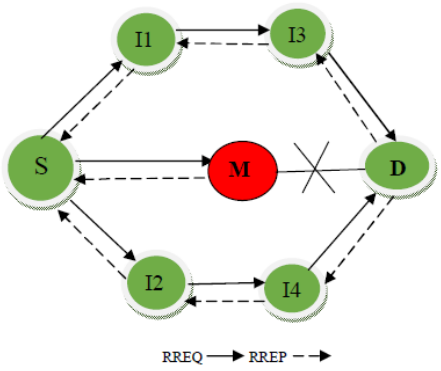

Figure 2. Black hole attack.

Spoofing Attack [12]: In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node.

Man- in- the- middle attack: A malicious node sites between the source and destination and then sniffs any information being sent between two nodes.

Denial of service [12]: Attacker tries to block the specific network service or network operation.

Jamming Attack [12]: In this attack, the malicious node determines the frequency at which destination node is receiving signal. And then it transmits signal on that the same frequency.

2.1.2. Node Registration .
For node registration security, the survey is done with three methods which are proposed in [8], [12] and [4]. Node registration method described in [8] is, admin of the network tries to configure the nodes to give access. When other nodes request access, a token is generated and this will be valid only for some constant time. The token is then generated and is distributed to the requested node. As we know MANET does not have any central admin that is fixed, this approach will not be much feasible.

MANETs security attacks and proposed nodes registration based technique explained in [12] by using cryptography functions. The registered nodes will only have the provision to assign tokens to validated nodes and are confirmed by the registered node from the node id and home address in a request packet. Token exchange can lead to delay in packet transmission. Steps in this method proposed is as follows:

(i) Node is registered(RN) and generates registration token
(ii) Request RN for nodes communication
(iii) Checks node id and address.
(iv) After confirmation, token is generated
(v) After tokens are received, communication is initiated.

The bloom filter algorithm for node registration purpose explained in [4], only need is to register the node while joining the network and the foreign nodes will not be allowed to register into the bloom filter. When you insert a new node in a simple array or list, the index, where this data would be inserted, is not determined from the value to be inserted. That means there is no direct relationship between the key(index) and the value(node). As a result, if you need to search for a value in the array you have to search in all of the indexes. Now, in hash tables, you determine the key or index by hashing the value. Then you put this value in that index in the list. That means the key is determined from the value and every time you need to check if the value exists in the list you just hash the value and search on that key.[19]

2.2. Protocols
There are different routing protocols in MANET and is categorized into flat routing, hybrid routing and geographic routing shown in fig 1.
In the flat routing protocol, Routing table represented each network Identity individually.Flat routing protocols are two types, Proactive Routing (Table Driven) Protocol and Reactive Routing (On demand) Protocols. Proactive Routing is divided among DSDV, WAR, and OLSR [18]. Hybrid Routing- As the size of the wireless network increases, flat routing protocols will produce much more overhead for the MANET so hierarchical Routing can be used instead.Protocols are ZRP and CGSR [18]. The geographical position of a moving node is used in Geographical position Assisted Routing algorithms. The study mainly focuses on reactive routing protocols. Rather than AODV protocol, there is DSR protocol that comes under reactive protocols topology. In table 1 in section 3, it is clearly shown why AODV is efficient than DSR protocol.

Packet Loss Comparison for AODV and DSDV: The comparison of different packet losses for AODV and DSDV is as follows [11].

- Total packet loss: The total packet loss for DSDV will be 10percent to 20percent higher than that of AODV regardless of pause time or a number of connections.
- Congestion-related packet loss: DSDV loses more packets compared to AODV due to congestion. Fig 3 from [11] shows packet loss variation graph between AODV and DSDV.

So we can choose AODV over DSDV

2.3. Packet loss reduction method
In [9] when source node receives Warning Message from any node in the route then it will stop sending packets on that route. Here extra parameters are needed to be defined rather than finding the route. But in the proposed study, a method to find the route is the only factor needed to be considered. The steps for this method[9] is as follows

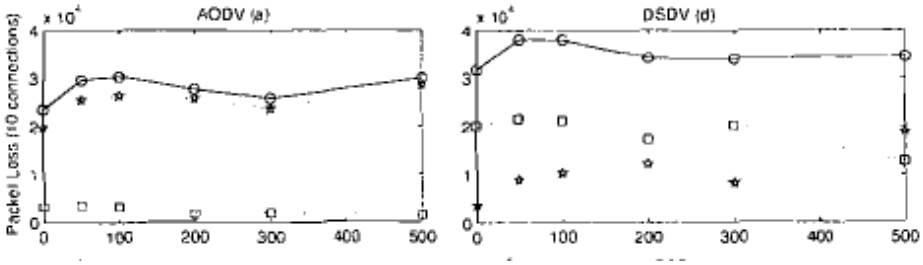

Figure 3. Packet Loss Comparison Graph.

(i) Transmit packets from source to destination.
(ii) For every node on the ongoing route do If the energy level is critical, then Node N will generate a Warning Message to the source. Here Node N is any node on the ongoing route.
(iii) If a Warning Message from any routing host is received, THEN
(iv) Source will not send a single packet in this current route.
(v) It will discard the current route from its cache.
(vi) If any messages need to be transmitted to the destination then the source will use another route from its cache. Else Source will forward packets on the current route.

3. AODV with Node Density Method and Node Registration method

3.1. Packet Loss Factors in Ad- hoc Network

Packet loss can occur in ad hoc networks where compromised nodes are not present. This packet loss happens mainly because of the following factors [7]:

3.1.1. Congestion in Network In mobile ad hoc networks, congestion is the main factor for packet loss. As the traffic increases packets may not reach the destination and packet loss happens.

3.1.2. Path Change and Noise In mobile ad-hoc networking, the path condition cannot be made unseen since it changes its path frequently. Presence of noise and fading of the transmitted signals are among the channel conditions that can lead to packet loss or bit errors in the transmitted signal. Because of these factors, packets can get dropped.

3.1.3. Energy Constraints Nodes in mobile ad hoc networks have limited energy resource. As the power of nodes decreases, the low energy nodes can get disconnected which may lead to packet loss.

3.2. Route Discovery by Neighbour Node Density Method

The mobile ad-hoc network is dynamic in nature the routing protocol will be preferred on the basis of administrative distance value allotted to each path in the network [3]. As an enhancement to AODV protocol, the node density feature can be embedded. When a node is about to get disconnected, the packets must be transferred to the neighbor node which has a maximum number of neighbors.

3.3. MANET Protocols

About MANET protocols, in section 2 it is explained in detail. MANET has mobile nodes and wireless links. As in MANET, the nodes move frequently which tends to change its topology frequently. These nodes have power constraints and are pervasive devices.

In MANET, dynamic routing is considered because, in dynamic routing, frequent topological changes are possible and also provides potential network partitions. There are proactive and reactive protocols based on topological routing. Proactive protocols like DSDV have high overhead independent of data traffic. But in reactive, on-demand routing enables overhead to scale with data traffic. Some reactive protocols are Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector (AODV). AODV can be used over DSR. Table 1 describes the difference between AODV and DSR.

Table 1. AODV and DSR difference.

Properties	AODV	DSR
Path Information	Limited	Detailed
Route Discovery times	Many	Few
Traffic when RREQ	Low	High
Route path life time	New	Unknown
Delete path when RERR	Delete all	Delete some nodes

The RREQ is the Route Request message and RERR is the Route Error message. By comparing both protocols, AODV is efficient that DSR.

The Ad hoc On-Demand Distance Vector (AODV) routing protocol offers fast conversion to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network [6]. The routing table of AODV protocol is shown in table 2.

Table 2. AODV routing table.

Routing Table
destination
sequence number
$\text{hop}_c ount$
$\text{next}_h op$
$\text{expiration}_t imeout$

So in this study, it is evident that AODV is better considering flat type routing protocols.

3.4. Bloom Filter

Bloom filter is an efficient method for registering nodes that help to know if any attacker node is trying to be the part of the network. The bloom filter is used for various network security areas [4]. In [4] a proposed method, an efficient identity-based key management (IBKM) scheme, which exploits the bloom filter to authenticate the communication sensor node with storage efficiency. Example of a bloom filter is shown in figure 1. The basic bloom filter supports two operations[19]: test and add. The test is used to check whether a given element is in the set or not. Add simply adds an element to the set. Add function can be used to add member nodes to the network. Test function can be used to check whether there are any attacker nodes present.

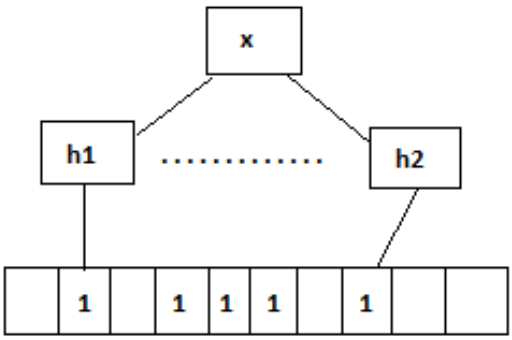

Figure 4. Example of Bloom Filter.

4. Conclusion

In this paper done a detailed study on packet loss reduction methods and node registration methods in AODV for MANET. Mobile ad-hoc network is a self-configuring, dynamic network of the mobile node in a wireless connection. AODV routing protocol is a distance vector routing protocol and uses destination sequence numbers to determine the freshness of routes. Bloom filter is the method adopted in this study and it will register all the member nodes in a network which transfer common packets and if any attacker node tries to join the network then the hash of group nodes will be different from the attacker node. Thus the attacker node will not be able to join the network. For routing, AODV protocol can be used which is already widely used a routing protocol. In order to reduce the packet loss in a network due to disconnectivity of nodes, the node density feature can be considered. In future, more on security and packet loss reduction methods will be concentrated.

5. References

[1] Aqeel Taha, Raed Alsaqour, Mueen Uddin, Maha Abdelhaq, and Tanzila Saba, May 24, 2017 *Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function* (IEEE access)

[2] Jain S Charles E. Perkin, Jari T. Malinen, Ryuji Wakikawa, Anders Nilsson 2002 *Internet connectivity for mobile ad hoc networks* (Wirel. Commun. Mob. Comput. 2:465482)

[3] V. Karthikeyan, A.Vinod P. Jeyakumar Y *An Energy Efficient Neighbour Node Discovery Method for Wireless Sensor Networks* (India)

[4] Achu Anna Antony, Ashily M Baby, Kavya Rajeev, Bino Thomas 2017 *Cooperative game theoretical approach for efficient node discovery in mesh network with bloom filter* (International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835)

[5] Zhongyuan Qin , Xinshuai Zhang , Kerong Feng, Qunfang Zhang and Jie Huang *An Efficient Identity-Based Key Management Scheme for Wireless Sensor Networks Using the Bloom Filter* (ISSN 1424-8220)
[6] C. Perkins, E. Belding-Royer, S.Das, *Ad hoc On-Demand Distance Vector (AODV) Routing* (Network Working Group)
[7] Kennedy Edemacu, Martin Euku and Richard Ssekibuule 2014 *Packet drop attack detection techniques in wireless ad hoc networks: a review*)Vol.6, No.5(International Journal of Network Security Its Applications (IJNSA))
[8] Manoj V. Mori1, G.B. Jethava 2013 *Node registration in MANET* (International International Journal of Emerging Trends Technology in Computer Science (IJETTCS)) Volume 2, Issue 1, January February 2013
[9] Rezvi Shahariar and Abu Naser *Reducing Packet Losses in Mobile Ad Hoc Network Using the Warning Message Generated from a Routing Node* (Dhaka Univ. J. Sci. 62(2): 141-145, 2014 (July)) April 2014
[10] Martinus Dipobagio *An Overview on Ad Hoc Networks* (Institute of Computer Science (ICS))
[11] Yi Lu, Yuhui Zhong, Bharat Bhargava 2003 *Packet Loss in Mobile Ada Hoc Networks* (Purdue University,Purdue e-Pubs)
[12] Rashid Jalal Qureshi,Khalid Haseeb,Muhammad Arshad , Huma Javed,Haleem Farman Sep 2012 *A Novel Technique Based on Node Registration in MANETs* (IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3)
[13] Nitesh Funde, P. R. Pardhi May 2014 *Analysis of Possible Attack on AODV Protocol in MANET* (International Journal of Engineering Trends and Technology (IJETT) Volume 11 Number 6)
[14] C. Perkins. July 2003 *(RFC) request for Comments-3561* (Category: Experimental, Network, Working Group)
[15] Dokurer,Seimih Septeber 2006*(RFC) Simulation of Black hole Attackin wireless ad-hocNetworks* (Masters Thesis Atihm University)
[16] Hsun Tseng Li-Der Chou and Han-Chieh Chao *A survey of black hole attacks in wireless mobile ad hoc networks Fan*
[17] Ebrahim Mohamad, Louis Dargin *Routing Protocols Security* (In:Ad Hoc Networks. A Thesis at Oakland University School)
[18] Neeraj Verma,Sarita Soni 2017 *A Review of Different Routing Protocols in MANET* (International Journal of Advanced Research in Computer Science)ISSN No. 0976-5697, vol 8
[19] Ahmed shamim hassan 2017*Probabilistic Data structures: Bloom* ([Online]: https://hackernoon.com/probabilistic-data-structures-bloom-filter-5374112a7832)