PalArch's Journal of Archaeology of Egypt / Egyptology

An Approach for Rushing Attack Resolution in AOMDV Using Arbitrary Id in Manet

[1]Dr.B.Barani sundaram, [2]Mr.Tucha kedir, [3]Mr.Tesfaye tadele sorsa, [4]Mr.Rabira geleta,[5]Dr.Nune srinivas, [6]Adola haile genale

[1]professor & associate dean-ict-ce ,computer science department,college of informatics,bule hora university,bule hora, Ethiopia,

[2]dean ,college of informatics,bule hora university,bule hora, ethiopia,

[3]vice dean ,college of informatics,bule hora university,bule hora, Ethiopia,

[4]lecturer,department of computer science, college of informatics,

[5]assistant professor,school of electrical and computer engineering,addis ababa institute of technology, addis ababa university,addis ababa,Ethiopia,

[6] lecturer, department of information science ,college of informatics, bule hora university, ethiopia

Email: [1]bsundar2@gmail.com,[2] tuchakedir@gmail.com, [3]ttadele14@gmail.com, [4]rabirageleta2@gmail.com,[5]ns_maruthi@yahoo.com,[6]adolahaile2007@gmail.com/[6]adolahaile2019@gmail.com

Dr.B.Barani Sundaram, Mr.Tucha Kedir, Mr.Tesfaye Tadele Sorsa, Mr.Rabira Geleta,Dr.Nune Srinivas, Adola Haile Genale: An Approach For Rushing Attack Resolution In Aomdv Using Arbitrary Id In Manet -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(6). ISSN 1567-214x

Keywords: AOMDV, MANET, Rushing Attack, Simulation Network (NS2).

ABSTRACT

Mobile ad-hoc network (MANET) is a collection of mobile nodes connected by wireless links and that forward information from one node to other node without a wired connection. Since there is no central authority responsible for routing packets, the security of communication is dependent only on mutual trust between nodes. This leads MANET to be vulnerable to different attacks. Rushing Attack is among one of the existing MANET attacks that results in denial-of-service (DoS) against all on-demand ad hoc network routing protocols. It uses the duplicate suppression mechanism thus the response time of the malicious node is extremely fast

and can send a route discovery to the sender, and gain access on the forwarding data. The attackers can rush the route request packets in many ways such as removing MAC (media access control) and network delays in packet transmission. In this research, we propose Multipath-AODV (AOMDV) protocol, and deploy rushing attack prevention method in route discovery phase. It enhances the security features of AOMDV protocol. This research provides solution for rushing attack using Rushing Attack prevention (RAP) method for AOMDV protocol.

RAP uses the concept of average delay value, collects a number of RREQs then selects a request at random message forwarding to mitigate the attack. Trust evaluating node takes the decision based on request arrival time, then it decides whether a node is trustable or malicious, by using threshold concept in every pre-request in routing path.

We have used NS2 simulator for simulating the proposed method. The simulation results show that the proposed security solution is effective in detected and preventing rushing node attack in the mobile ad-hoc networks. After incorporating mitigation method is to detect and prevent the rushing attack, this research achieves significant improvement in the PDR (performance metric –Packet Delivery ratio) up to in average is 93.9%..

1. Introduction

1.1 Background

In wireless communication technology, mobile devices are known to provide different services. Better communication is also one of the benefits of these devices. By definition mobile ad hoc networks (MANETs) differentiate themselves from existing networks by nature. In ad hoc networks, the nodes themselves are responsible for routing and forwarding of packets. If the mobile nodes are within range of each other, no routing is necessary. But, on the other hand, if the nodes have moved out of range from each other, and therefore are not able to communicate directly, intermediate nodes are needed to make up the network in which the packets are to be transmitted. All network functions are performed by the nodes forming the network; each node performs the functionality of host and router, relaying data to establish connectivity between source and destination nodes not directly within each other's transmission range (V. Muthupriya and K. M. Mehata 2015).

Most of the time in situations where there is an urgent need for wireless communications, mobile ad hoc networks are well-suited for the purpose. Examples include emergency operations where there exists no fixed infrastructure and military operations where the existing infrastructure is unavailable. Since mobile nodes are not controlled by any other controlling entity; they have unrestricted mobility and connectivity to others. MANET has many characteristics which make it suitable for some important applications and it can provide services well in such cases. Mobile ad hoc networks have a wide range of application usage today, due to its great services, easy installation and configuration, and its other distinctive characteristics. Mobile ad hoc network have become an important part of our life due to its vital services it provides to the population and society. It’s used at home, at work, in

emergency situation, and natural disasters (Wilson Prakash. S 2015, Neetika Bhardwaj1, Rajdeep Singh2, 2014).

When MANETs are used in the absence of infrastructure, routing and network management are done cooperatively by each one of the nodes. The routing in MANET is classified as either proactive (Table-driven) or reactive (On-demand) (Palwal, Haryana , 2015). In proactive routing, all the nodes maintain the network status of their neighbor nodes by exchanging it for every defined time interval. Thus, by using this information, the routing path between the source and destination is predetermined and available in the routing table. Due to exchange of control packets in the network there will be increase of network overhead in proactive routing. In reactive routing the routing path between the source and destination is founded only during the time of transmission. This is done by initially forwarding Route Request (RREQ) packet in the network. Ad hoc On Demand Vector Routing (AODV) and Dynamic Source Routing (DSR) is the common on-demand routing protocols used for routing in MANET (Satyam Shrivastava 2014).

Security is an essential requirement in mobile ad hoc networks to provide protected network communication. One of the many threats that affect the MANET is rushing attack. This research work focuses on detection and prevention of this rushing attack. Rushing attack exploits duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group (Satyam Shrivastava 2014). When an attacker receives a route request message from a genuine source node S, it immediately broadcasts the same route request message throughout the network before the other mobile nodes receive the route request message from the original source node (Ankita Rathore, 2015).

1.2 Statement of the problem

By nature, a wireless network signal is traveling in free air, shared broadcast radio channel, insecure operating environment, with lack of central authority and association among users and physical vulnerability. Security is one of the most important concerns on MANETs, because MANET system is vulnerable to different attacks relatively compared with infrastructure-based wireless network. Security is a major concern in a potentially hostile environment; for this reason, MANET is one of security focuses area. Many nodes perform many kind of misbehavior. The focus of this thesis is to research built-in threshold value and random forward for detection and prevention in mobile ad hoc network. First clear understanding the behavior and impact of rushing attack, additionally detecting the malicious node on an infected mobile ad hoc network is important. In this research work the proposed approach to mitigation of rushing attack is implemented on the AOMDV route discovery phase

1.3 objective

1.3.1 General objective

The main objective of this research is to detect and mitigate rushing attack in Mobile Ad hoc Networks in AOMDV Protocol and by creating trusted neighbor nodes to enhance the security and performance of the network.

1.3.2. Specific Objectives

In order to achieve the aforementioned general objective, the following specific objectives need to be achieved.

i. To analyze various attacks in MANET with AOMDV
ii. To simulate AOMDV in MANET with rushing attack
iii. To detect rushing attack using the Threshold value
iv. To prevent rushing attack using Random forwarding Technique
ii. To test the performance of the system through various scenarios.
vi. To evaluate the performance of the system using metrics such as end-to-end delay, packet delivery ratio, throughput

2. Literature review

2.1. Introduction

Many researches have been done on the security of mobile ad hoc network protocols and they contributed to security enhancement and draw new idea on strengthening the security of MANET protocols. AOMDV is one of the protocols on which different researchers worked and proposed different ways of security enhancements. Therefore, AOMDV related research papers have been reviewed in detail to know the current level of the research's output to the security and research problem has been drawn for this research. In this section different papers on the impact of rushing attack in the performance of MANET protocol/s are discussed.

Many international level literatures have been reviewed with regard to rushing attack's impact in communication network and implementation along with some mitigation method on different reactive routing protocols on NS-2. Among these literatures, we have chosen a few of the most recent and related papers in rushing attack.

Vasudevan Muthupriya and K.M. Mehata (2015), Mobile ad hoc networks are mostly susceptible to various routing attacks due to their open access wireless medium. The researcher only described the impact of a rushing attack on AOMDV routing protocol is analyzed and its results were compared to other attack in order to prove that the rushing attack is more significant than other routing attack.

The researcher proposes the study of impact of a rushing attack in AOMDV routing protocol is analyzed and its results were compared to a black hole in order to prove that the rushing attack is more significant than other routing attack. AOMDV is one of reactive protocol; to enhance AODV where in multipath is discovered to minimize the delay in data packet transmission. The Rushing attacks in overall performance of the AOMDV under the impact of rushing attack is dangerous than black hole attack.

Some of the challenges in mobile ad hoc networks concerned to routing are mobility, bandwidth constraint, error prone and shared channel, resource constraints and insecure hop-to-hop data transmission. This enforces several security mechanisms in the network to ensure reliable packet delivery in the network. In reactive routing the routing path between the source and destination is founded only during the time of transmission. This is done by

initially forwarding Route Request (RREQ) packet in the network. Ad hoc On Demand Vector Routing (AODV) routing protocols used for routing in MANET. The routing can be categorized as a single path and multipath routing depending on the number of paths discovered during the route discovery phase. Multipath routing is comparatively reliable and secure because if there is any link breakage due to any attack or resource depletion in nodes, it can take alternate path for data transmission. In AODV according to the requirement of the source, a single path is discovered between source and destination by flooding the RREQ packets via intermediate nodes (V. Muthupriya and K. M. Mehata 2015).

The two main phases of AODV protocol are route discovery and route maintenance phase. The first one is route discovery phase in MANET when any node wants to have a data transmission it will broadcast a Route Request (RREQ) packet to its neighboring nodes. The RREQ packet contains the information of (Source address, Source sequence, Broadcast id, Destination address, Destination sequence and Hop count). The source address and broadcast id together form a RREQ identification to prevent the loop formation in the route and also avoids intermediate nodes to accept RREQ with the same identification and the second one is route maintenance phase **t**he Route Error (RERR) message is sent to the sender by the intermediate node if there is any link breakage between itself and sender. This interrupts the data transmission till it finds the available alternate path otherwise it repeats the route discovery phase to establish a new path. This will avoid loss of data during transmission. Since for every link failure the route has been rediscovered it induces more delay in AODV protocol. And provides control message are RREQ, RREP and RERR.

Ad Hoc On Demand Multipath Distance Vector (AOMDV**):-** an extension of AODV is proposed by Mahesh et al (Vasudevan Muthupriya and K.M. Mehata (2015)), which is intended to reduce packet loss by up to 40% and achieves a remarkable improvement in the end-to-end delay. In this multiple paths are discovered between the source and destination which enables reliable transmission at the times of link breakage. Multiple paths are guaranteed to be loop-free and disjoint. Like AODV it also has two phases route discovery and route maintenance phase.

In route discovery phase the AOMDV protocol aims to find node disjoint and link disjoint multipath. The node disjoint multipath is where no routing path will have a common node, whereas in link disjoint multipath, a node can be in common but no link is common in alternate paths. The node disjoint paths are more reliable than link disjoint as the link breakage due to loss of energy in any particular node is less. The route discovery phase in AOMDV is also initiated by broadcasting the RREQ from the source. Unlike AODV the neighbor nodes and destination nodes will accept duplicate RREQs and send multiple RREPs to sender node. Though the protocol sends multiple RREPs it follows AOMDV route update rule for finding loop free and disjoint routes between any sender and receiver nodes.

The route maintenance phase in AOMDV is similar to AODV where an intermediate node generates and forwards RERR towards upstream nodes whenever there is a link failure. Unlike AODV alternate routes are available and so it transmits the packets without much delay. When all the alternate paths are exhausted a new route discovery phase is initiated. The main advantage of AOMDV is, it reduces overall end-to-end delay during the period of link breakage by resuming the process with alternate paths.

As it is described in this thesis, the AOMDV unlike AODV does not possess duplicate suppression nature, they generate loop free disjoint multipath. In this thesis research work, rushing attack in AOMDV is focused, where number of routes discovered at route discovery phase is reduced due to this attack. Whenever there is route drop in an AOMDV during transmission time, it searches for available alternate route and forwards the packet through it. Since number of available alternate path is considerably very less due to rushing attack, the protocol need to discover new routes when the available routes are exhausted. This causes increase in end-to-end delay in the network. Due to increase in end-to end delay the throughput of AOMDV protocol decreases.

Consistent link failures occur in mobile ad-hoc networks because of node's mobility and use of fickle wireless channels for data transmission. Based on AOMDV protocol approach is to obtain all available node-disjoint routes from source-destination with minimum delay and high throughput. Node-disjoint multipath routing allows the establishment of multiple paths, each consisting of a unique set of nodes between a source and destination. This link failure causes two main problems. Firstly, when a route break occurs, all packets that have already been transmitted on that route are dropped and it decreasing the average packet delivery fraction. Secondly, the transmission of data traffic is halted for the time till a new route is discovered and it increasing the average end-to-end delay. AOMDV will minimize the effect of link failure. Hence, the above mentioned two problems caused by frequent link failures are addressed.

In general, propose AOMDV protocol to evaluation the performance and impact rushing attack in network. Using AOMDV protocols with rushing attack and compare by black hole attack over AOMDV.This work is over all better from other protocols because less packet loss compare with AODV. The researcher, more and detail discussed about for the impact of rushing attack in MANET. However, in this work not used any security method.

Finally, this thesis research work proposes a better solution than previous work because the case of rushing attacks, increase in end-to end delay and throughput of AOMDV protocol decreases, then to reduce the above mention problem by implement rushing attack prevention method in AOMDV routing discovery phase (V. Muthupriya and K. M. Mehata 2015).

3. Methodology

3.1Introduction

The applied mitigation mechanism is discussed in detail in this section. Before that, the network simulator and the implementation of AOMDV in NS-2 are introduced. Network Simulator Version 2, widely known as NS2, is an event

driven simulation tool that is useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community.

3.2. TOOLS- NS-2 (NETWORK SIMULATOR -2)

Network simulator is basically used for the purpose of research work in the field of networking. Network simulator plays an important role in simulation of routing protocols and mobility models. Code of Network simulator-2 is written in C++ programming language and with an object oriented version of Transmission Control Language (TCL, known as OTCL). NS-2 was developed by Monarch research group in Carnegie Mellon University (CMU) for the simulation of multi-hop wireless networks. Installation of NS-2
includes all the software extensions needed in simulation nile.wpi.edu/NS/overview.html, 2oo6).

NS2 is an object-oriented simulator written in OTcl and C++ languages. While OTcl acts as the frontend (i.e., user interface), C++ acts as the backend running the actual simulation. From Figure 4.1 class hierarchies of both languages can be either standalone or linked together using an OTcl/C++ interface called TclCL. The OTcl and C++ classes which are linked together are referred to as the interpreted hierarchy and the compiled hierarchy, respectively. Object construction in NS2 proceeds as follows. A programmer creates an object from an OTcl class in the interpreted hierarchy. The class embedded Tcl translates OTcl scripts into C++ codes.

3.3. Implementation of Rushing Attack in AOMDV

Since NS-2 network simulator does not support the rushing attack, we have to implement some protocols on NS-2 for simulation purposes.

Rushing attack described in previous chapter 3.6.2.5, rushing attacks are known to penetrate even the most secure routing protocols. When an attacker receives a route request message from a genuine source node, it immediately broadcasts the same route request message throughout the network before the other mobile nodes

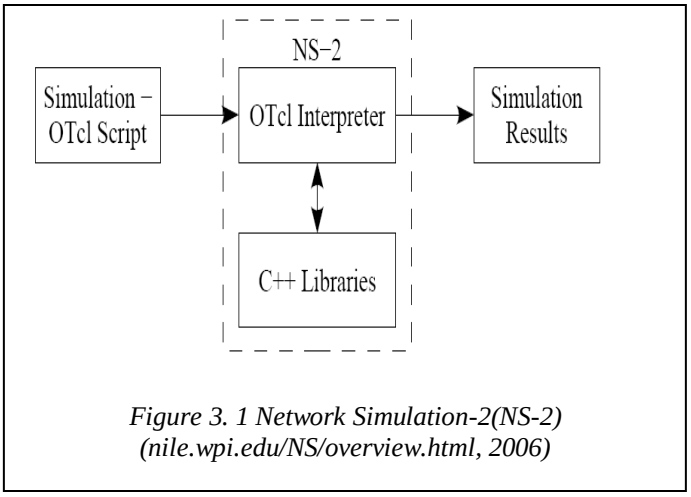

Figure 3. 1 Network Simulation-2(NS-2) (nile.wpi.edu/NS/overview.html, 2006)

receive the route request message from the original source node (JIANGYI, 2007).We simulate rushing attacks by introducing a simulated processing delay at every honest node. The node delays for a certain amount of time varying from 10 ms to 40 ms before broadcasting it. Meanwhile, the nodes that are designated as rushing attackers have their simulation processing delay set to zero. A rushing attacker is considered successful in a route discovery interval if and only if it has forwarded a fake RREQ and later receives a reply in the same interval. On other hand, rushing attack is not the only method enabling access to a multicast forwarding group. For multicast protocols that do not use a duplicate suppression mechanism such as AMRIS (C.W. Wu, Y.C. Tay ,1999), CAMP and BEMRP , route invasion can be done by modifying or advertising false routing information (Hoang Lan Nguyen *,2006). Once an attacker has invaded into forwarding routes, it may launch other attacks such as dropping data packets (black hole attack), or delaying them (jellyfish attack), corrupting or illegally accessing confidential data. In this thesis, we consider only route invasion by means of rushing attack since there exist many multicast routing protocols that use some form of duplicate suppression, and are thus vulnerable to rushing attack. To explain the rushing attack we add a malicious node that exhibits rushing attack behavior.

3.4. Prevention mechanism of rushing attack.

Depend on attacker behaviors and consider the attacker rushing method, then built solution to reduce rushing attack from mobile ad hoc network. In general terms, an attacker that can forward ROUTE REQUEST is quicker than legitimate nodes can do so, this can increase the probability that routes that include the attack will be discovered other valid routes. The detection and prevention of the rushing attack, is known or defined so the mitigation method is described with examples below.

We used timeout for prevention from higher transmission power or by wormhole; we can specify timeout at node before forward RREQ to neighbor's node. We set some timeout which is normal time for transmission from previous node to that node. Each time a data packet is sent to the destination of this route, the timeout for the route is extended to this value. If no data packet is sent during this timeout interval, the route is disabled but not deleted.

3.4.1. Threshold Values

In this thesis work we used threshold value concept to detect the rushing attack by fixed threshold value by pre-defined in each mobile node this minimizes the chances of rushing attack in mobile ad hoc network. The entire nodes in the network have the instruction that the packet must reach to the neighboring node at the fixed interval. Each node should check the RREQ of the neighboring node. If there is any rushing attack then it will try to transmit the packet quickly and thus the neighboring node can identify the attack node and inform about it, then discard the attack node from the network. The route request arrived before threshold value; assume the RREQ packet is coming from rushing attack, and then the request is discarding. Figure 4.2, shows the small network topology with rushing attack and the RREQ send from source node to destination node, then the attack (node 2) is wait in track genuine RREQ to

received and forward the fake RREQ to destination. The threshold value taken from our simulation result, after running so many time at that time we compare the rushing attack routing request time arrived most of time ,arrived to destination less than from genuine node route request time. Using total time by the number of nodes we get the average threshold value, in our case (t_1, t2, t_3 …tn)/n, the output of this assigned threshold value.

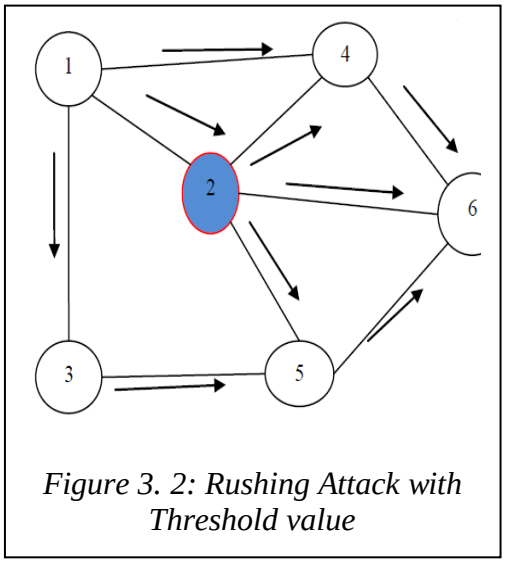

Figure 3. 2: Rushing Attack with Threshold value

Figure 3.2, shows the detection of the attack route request by using threshold value, then the RREQs is attack or not attack given decision based upon threshold value compare with incoming RREQ time from source node. In the topology 6 nodes are included in the network, i.e. node 1, 2, 3, 4, 5 and 6, and then node 1is assigned source node, node 6 assigned as destination node. Figure 3.2, shows the detection of the attack route request by using threshold value, then the RREQs is attack or not attack given decision based upon threshold value compare with incoming RREQ time from source node. In the topology 6 nodes are included in the network, i.e. node 1, 2, 3, 4, 5 and 6, and then node 1is assigned source node, node 6 assigned as destination node. The source (node 1) sends
the route request packet to destination (node 6). Using this threshold value is decided. In our case, now the threshold value for this network is 0.001sec or 10 ms (milli second), means a packet will take 10 ms in traveling to complete a hop. Node 1 sends a packet to 2, 3 and 4. The packet will reach in 10 milli second then node 2 sends a packet to 4 and 5; it will also reach in 10ms and 4 sends a packet to 6, then which will also reach in 10 ms. Node 5 send packet to 6 in 10ms. Assume node 2 is a rushing attack, so it will quickly send the packet to node 6 and this packet reach in 9.5ms to node 6. Node 6 knows that the threshold value is 10ms and packet comes in 9.5 ms, means there is an attack so it inform to other node about the attacker and discard this RREQ packet. So that receiver node 6 will accept the packets which come from 5 and 4.
According to our flow chart shown in Figure 3.3, combines two algorithm, those are threshold value concept and randomly forward technique algorithm.

This algorithm used to reduce the chance of rushing attack from MANET. The aim of the flow chart will generate the random value and randomly forward RREQ for every time data transmission so that the malicious node cannot continue to harm our data. Secondly, used calculate the average travel time from source to the adjacent node for detect the attack RREQ packet. As stated above t_1, t_2, t_3... t_n are travel time from source to adjacent node. Tavg = $(t_1+t_2+t_3+\ldots t_n)/n$ .If any packet which is taking time less than Tavg (average time) the node will discard RREQ packets, because the receive request packet assume from attacker. A packet which received after taking time at least equal or greater than Tavg times that packet will only be acceptable unless discard of RREQ packet from network.

3.5 Randomized Message Forwarding.

The threshold value concept techniques are not sufficient to thwart the rushing attack, since an adversary can still get an advantage by forwarding ROUTE REQUESTs very rapidly. We use a random selection technique to minimize the chance that a rushing adversary can dominate all returned routes

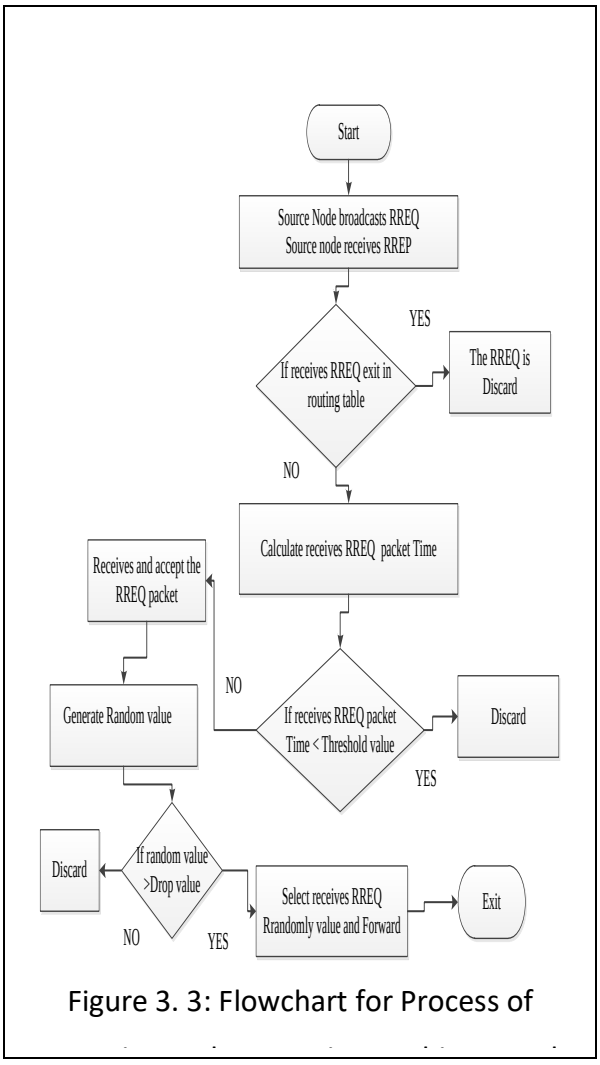

Figure 3. 3: Flowchart for Process of

3.6. Simulation Scenario

In our simulation scenario we generally focus on three scenarios for AOMDV routing protocol. All three scenarios are provided with the same simulation time, the same packet size and the same simulation network area. the scenarios include 11 nodes, node zero assigned Source node, node 10 assigned Destination node .The two nodes or (source and destination) assigned by blue color, then the ramming nodes or (intimidated nodes) assigned by red color in each scenario .Those are: - (i) Normal AOMDV (no attack), (ii) Rushing attack on AOMDV (with attack) and (iii) with mitigation attack on AOMDV (secure AOMDV).

3.6.1. First Scenario: Normal AOMDV (no attack) Scenario

In the first simulation scenario AOMDV without attack, connection between Source node and Destination is correctly data flow when we observe at the network animation of simulation using NAM. The network size is 11 nodes and is randomly distributed in 1200m× 700m area. TCP connections are established between the sending and receiving nodes and the data packet are transmitted by source node to destination node via node 0, 1, 3, 5, 4 and 10 nodes. In this normal network, the routing request packet (RREQ) transmissions without any interruption from source (node 0) to destination (node 10). `

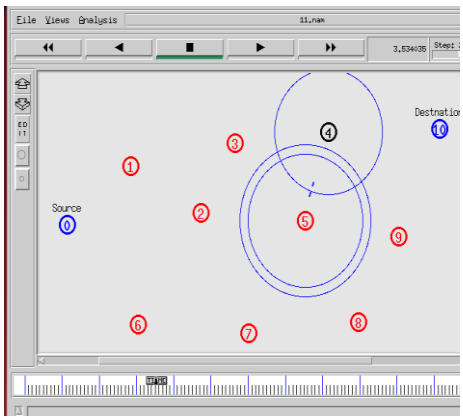

Figure 3. 4: Normal AOMDV scenario in MANET

3.6.2. Second Scenario: Rushing attack on AOMDV scenario

In this section based on the rule of on-demand routing protocol, only receives the first RREQ packet and accepted, the same RREQ packet arrived later to destination then discard even if in normal case. The rushing attack using this advantage, the attacker receive genuine node and send fake RREQ quickly forward to destination before honest node, then the honest RREQ arrived to destination later and discard.

In the second simulation scenario, we added the behavior of rushing node attack to Node 4. Then, node 4 is indicate rushing node attack ,after receive

routing request packet (RREQ) and forward fake RREQ quickly by using high transmission speed and the attacker RREQ arrived to destination before genuine node RREQ ,then the destination is discard the genuine RREQ because the destination getting the RREQ from attacker nodes subsequent REQUESTs.

3.6.3 Third Scenario: With mitigation attack on AOMDV (secure AOMDV).

In the third scenario, after incorporating threshold value concept and forward random technique to mitigate the rushing attack behavior from the MANET environment by finds other alternative path or (other route) to destination. In our cause, employed threshold value concept and randomly select forward technique apply in receive request class on AOMDV protocol. The destination node before accepted RREQ, first check if it is in route table because they arrived RREQ available or not, then the similar RREQ exit in routing table then discard the arrived RREQ and they arrived RREQ is not exit in routing table also check the arrive time and compare with threshold value, then the RREQ time less than threshold value, assume in our case the RREQ is rushing attack so discard because the request coming from rushing attack.

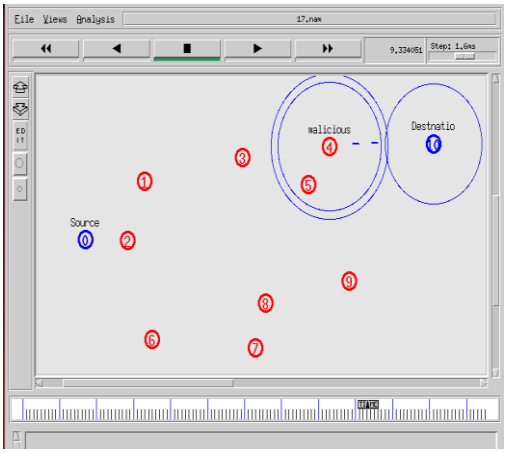

Figure 3. 5: AOMDV protocol with Rushing attack in MANET

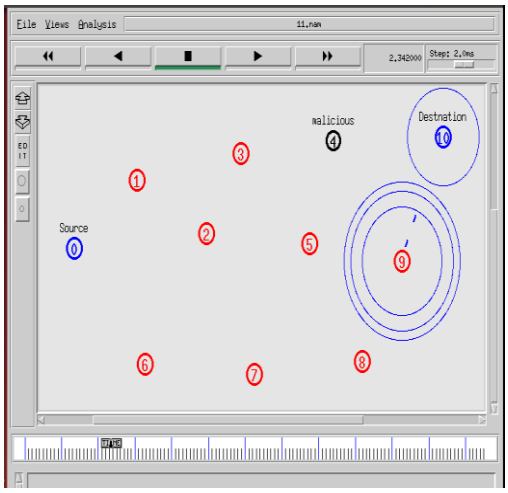

Figure 3. 6: Rushing attacks with mitigation

The second method using randomly forward method, this also one important method to reduce the chance of rushing attack from network .A genuine node receives RREQ packet from source, then before forward the receives RREQ packet firstly generate the random value and compare with drop factor value.If the random value greater than the drop factor value then random value selected forward the RREQ packet to destination node else discard the RREQ packet in our case. In Figure 3.6 shows, topology provide 11 nodes, node 4 assigned malicious (or rushing attack) and data packets are transmitted from S to D node via node 0, 6, 7, 8, 9 and node 10. Finally, after mitigation the RREQ packet transmissions time not used rushing attack node (node 4), so RREQ packet change other alternative path. This is the result of threshold value concept and forward random technique on AOMDV protocol.

4. Results And Discussion

Summary of the data

We also measured the impact of the introduction of security on the performance of both protocols. Moreover on our analysis, we have measured the impact (fault tolerance) due to the introduction of a threshold number of malicious nodes with in a network. Accordingly we have summarized the results of our findings below.

Table 5.2 with the presence of security

No. Malicious Nodes	Throughput		PDF		Average End-to-End Delay	
	AOMDV	MDART	AOMDV	MDART	AOMDV	MDART
0	23.97	23.55	1.0000	0.9957	0.009271	0.009781
1	23.97	23.11	1.0000	0.9616	0.009271	0.009493
2	22.39	20.68	0.9216	0.8536	0.009158	0.009671
3	20.55	18.11	0.8580	0.7543	0.009212	0.009446
4	20.06	17.54	0.8360	0.7279	0.009258	0.009639
5	18.76	14.60	0.7736	0.6085	0.009381	0.009425
6	17.23	13.78	0.7351	0.5798	0.009256	0.009525
7	16.33	12.13	0.6783	0.4987	0.009334	0.009324
8	15.80	11.43	0.6595	0.4840	0.009353	0.009349
9	14.38	9.32	0.6031	0.3812	0.009431	0.009368
10	13.84	8.48	0.5746	0.3542	0.009423	0.009380
11	12.40	6.92	0.5167	0.2852	0.009568	0.009360

Table 5.3 Varying pause time

Pause Time	Throughput		PDF		Average End-to-End Delay	
	AOMDV	MDART	AOMDV	MDART	AOMDV	MDART
5	23.94	23.25	1.0000	0.9947	0.006375	0.007047
10	24.24	23.53	1.0000	0.9939	0.006367	0.006891
15	23.94	24.05	1.0000	0.9966	0.006244	0. 006812
20	24.17	23.51	1.0000	0.9931	0.006390	0. 006835
25	24.42	24.06	1.0000	0.9966	0.006405	0.006899
30	23.85	23.97	1.0000	0.9966	0.006380	0.007170

Table 5.4 Varying size network

No. of Nodes	Throughput		PDF		Average End-to-End Delay	
	AOMDV	MDART	AOMDV	MDART	AOMDV	MDART
50	23.77	24.01	1.0000	0.9974	0.006410	0.006966
55	23.88	23.82	1.0000	0.9949	0.006057	0.006996
60	24.28	23.86	1.0000	0.9932	0.006392	0.007631
65	24.03	23.88	1.0000	0.9940	0.006089	0.007971
70	24.01	24.03	1.0000	0.9949	0.006408	0.008711
75	23.98	23.64	1.0000	0.9923	0.006097	0.012892
80	23.92	23.47	1.0000	0.9896	0.006422	0.034144

5. Conclusion, Limitation And Recommendation

Conclusions

From our simulation and analysis we arrive at the following conclusion:

- Multipath protocols are preferable for fault tolerance.
- The introduction of security doesn't severely impact the performance of our network and yet the absence of authentication mechanism can dramatically affect the performance of networks.
- That AOMDV performs better than MDART in networks of smaller size.
- The introduction of authentication security based on threshold scheme with elliptic curve cryptographic primitives seems to be the more ideal preference for deploying in MANETs over RSA primitives.

Recommendations

The study can be more complete if it expands into wider scope to assess the faults due to node energy, the faults due to link failures, and jamming of signals in the context of two lower layers.

Furthermore the results of the study can be more practical if the simulations are done on hardware platform kits specifically designed for such tests. In addition the study needs to proceed to the exploration of the authentication protocols in light of how well it identifies malicious nodes and segregates them, and in terms of how quickly it enables the network to recover from decrease in packet delivery ratio and throughput.

The study also can be made more complete by exploring the performance of the AOMDV and MDART protocols for large scale networks.

Reference

M.S. Corson, J.P. Maker, and J.H. Cernicione, “Internet-based Mobile Ad Hoc Networking”, IEEE Internet Computing, pages 63–70, July-August 1999.

“CISCO system. International Technology Handbook”, 2002.

Qing CHEN, Zhisheng NIU,” A Delayed Adaptive Retransmission Scheme for a False Route Failure in MANET”, 5th international symposium on multi-dimensional mobile communication proceedings, 2004.

S. Mueller R. P. Tsang and D. Ghosal, “Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges”, In Lecture Notes in Computer Science, Vol. 2964, Maria Carla Calzarossa and Erol Gelenbe (Eds.), 2004.

Chun-Yen Hsu, Jean-Lien C. Wu, Member IEEE, and Shun-Te Wang, “Finding Stable Routes in Mobile AdHoc Networks”,18th international conference ,vol-2,march 2004.

M.A. Razzaque, Simon Dobson and Paddy Nixon, “Cross-Layer Self Routing: a self-managed routing approach for MANETs”, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2008. WIMOB '08.

S. Capkun, L. Butty, and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," IEEE Transactions on Mobil Computing, vol. 2, pp. 52-64, 2003.

Haas J.D.Z., Liang B., P. Papadimitatos and S. Sajama, "Wireless ad hoc networks," in Encyclopedia of Telecommunications J. W. John Proakis, Ed., 2002.

Zhou L. and Haas Z.J., "Securing Ad Hoc Networks," IEEE Network:special issue on network security, vol. 13, pp. 24-30, 1999.

T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, and L. Viennot. “Optimized Link State Routing Protocol,” in Proceedings of IEEE INMIC, Lahore, Pakistan, December 2001.

A. Laouiti, A. Qayyum, and L. Viennot. “Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks,” in Proceedings of the 35th Annual Hawaii InternationalConference on System Sciences (HICSS’ 2002), Waikoloa, HI, January 2002.

Eriksson J, Faloutsos M, Krishnamurthy SV. Scalable ad hoc routing: the case for dynamic addressing. INFOCOM 2004. Twenty-third Annual Joint

Conference of the IEEE Computer and Communications Societies, Vol. 2, 2004; 1108–1119.