International Journal of Chemical Sciences

Research | Vol 15 Iss 4

Secure Routing-Solution to Diminish DOS Attack in AODV Based MANET

Philomina S[1*] and Ramesh R[2]

[1]Research Scholar, ECE Department, Bharath University, Chennai-600073, Tamil Nadu, India

[2]ECE Department, Saveetha Engineering College, Chennai-602105, Tamil Nadu, India

[*]**Corresponding author:** Philomina S, Research Scholar, ECE Department, Bharath University, India, Tel: 9080143665; E-mail: philomina.november83@gmail.com

Received: June 10, 2017; **Accepted:** August 29, 2017; **Published:** September 04, 2017

Abstract

MANET has exceptional individuality like changing topology, reduced bandwidth, wireless radio medium, limited resource and no centralized control. It is composed of mobile nodes which traverse through wireless link by agreeing to route message for each other. Securing ad hoc routing is a great challenge. The mobile ad hoc network is subjected to various types of attack at different layers of the protocol stack. In this proposed work, our focus is on the attack on the network layer. DOS (Denial of Service) attack affects the network performance by causing data loss. Many solutions have been proposed to encounter DOS, but the issues still persist because it is not prevented or avoided completely. We propose a solution for DOS in MANET using AODV without affecting the network performance.

Keywords: SRAODV; DOS; End to end delay; MANET

Introduction

MANETs are formed by a group of mobile nodes which communicate through wireless links by agreeing to route message for each other. Ad hoc networks depend on co-operation and trust between nodes. Trusting criteria in MANET makes it vulnerable to attacks. All ad hoc routing protocols must ensure that the path from source to destination works correctly, i.e. routing signals cannot be spoofed, routing loops cannot be formed and route cannot be altered from the shortest path by spiteful action. A node is malicious if it can perform arbitrary actions that do not follow normal or expected behavior and it cannot validate itself as a truthful node to other nodes. MANET is subjected to challenges like availability, integrity, confidentiality, authentication and nonrepudiation. MANET doesn't have centralized administration and they have restricted resources like bandwidth and power. Wireless link, dynamic topology makes MANET prone to security issues. The success of a MANET depends on its security. MANETs can be attacked on any layer of the network protocol stack. Network layer attacks are most important attack to be solved. Attacks are grouped into two types such as active attacks and passive attacks.

Citation: Philomina S, Ramesh R. Secure Routing-Solution to Diminish DOS Attack in AODV Based MANET. Int J Chem Sci. 2017;15(4):188

Active attacks can be internal or external [1,2]. They inject packets in network or routing protocol. Malicious nodes, which enter the network take complete control of the network and change its behavior. Passive attacks silently capture valuable data during transmission silently without damaging the network. They are threat against privacy. AODV is more efficient in terms of network performance, but they easily allow attackers to advertise falsified route information to redirect the route and launch DOS attack. Ad hoc on-demand distance vector routing protocol has two functionalities such as route discovery and route maintenance. In route discovery phase the protocol will establish a route by broadcasting the route request (RREQ) packet across the network. The intermediate nodes after receiving the RREQ packet will check whether it is the designated node for the received packet. If it is the designated node, then it will generate a RREP packet to the source node or it will broadcast the received packet to its neighboring node. In the route maintenance phase, if any node detects any broken link in the network, then a route error (RERR) packet will be forwarded to the source node. After receiving an error packet, the source node will update its routing table and then go for an alternate route for communication.

Experimental

Layer specific attacks

Attack on different layers of protocol stack [3-5].

Physical layer

Eaves dropping: Intercepting and reading a conversation by unintended receiver. In a MANET, since the mobile host shares the wireless medium, messages can be eavesdropped and fake messages can also be injected into the network.

Data link layer

This layer maintains one hop connectivity among neighbors so attacks like monitoring and analyzing traffic and exploiting wired equivalent privacy (WEP) weakness can be made.

Network layer

Attackers mostly concentrate on this layer; they intrude, absorb and control the network traffic flow. They create routing loops, cause network congestion and performance degradation. Wormhole, black hole, gray hole, Byzantine, rushing, resource consumption are some of the attacks encountered in this layer. All the attacks aim at denial of service. Wormhole attack, two attackers are needed, they reside at different location. One records the packet and tunnels them to the other attacker. It disturbs normal routing by short circuiting the normal flow. It is difficult to identify this attack because they do not modify any data packet or generate false traffic.

In black hole attack [6] after receiving the RREQ the attacking node will exploit the MANET routing protocol like AODV to advertise itself as it is having a valid route to destination by increasing the sequence number. When the data is transmitted through the malicious node it will drop the entire packet without forwarding it to the destination. Gray hole attack, It is also same as black hole attack but the attacker does not get into the path but it also does not forward any data packet that goes through it. In Byzantine attack [7] the intermediate nodes will work alone or in groups to carry out the attack in the network. In this type of attack the malicious node will forward packets through a non-existing path or it will selectively drop the packet which results in performance degradation of the routing services. In rushing attack [8] two colluded attackers will make use of the tunnel procedure and form a wormhole. The tunneled packet propagates faster than the normal multi-hop

route. In resource consumption attack [3], the attackers will consume the battery power by requesting excessive route discovery or by forwarding unnecessary packet to the victim node.

Transport layer

Session hijacking is done by the attacker in this layer. SYN (synchronization) flooding attack is a denial of service attack. The attacker creates a large number of half opened TCP connection with the victim node but it never completes the handshake to open the connection. In the TCP session hijacking, the attacker will spoof the victims IP address and then perform the denial of service attack. Impersonation of node is done by the attackers in this layer.

Application layer

Major attackers are mobile viruses, worm attack and repudiation attacks.

Attacks on multiple layers

The attackers targeting the multiple layers will cause the denial of service. The attacker will cause a signal jamming at physical layer which will disturb the normal communication. In the link layer, the malicious node will occupy the channels through capture effect and prevent the other nodes from accessing the channel. In the network layer, the routing is interrupted through control packet modification, selective dropping and table overflow. In Transport and application layers the malicious node will cause the denial of service.

Denial of service by black hole attack

Black hole attack will adversely affect the reactive routing protocols. This attack targets the network layer. In this type of attack the malicious node deletes all the received data packets instead of forwarding it to the receiver. This attack reduces the PDR. Black hole attack is divided into single and cooperative black hole attack. In single black hole attack, the attack is generated by a single malicious node. In co-operative black hole attack, there will be a group of malicious nodes which act in coordination to generate the attack in the network. When a neighbor node immediately reply for a RREQ from the sender without checking the routing table with a RREP having highest sequence number, the source sends the data packet thinking that the reply has come from the destination. The malicious node drops the packet instead of forwarding it to the destination.

Discussion

Solution for MANET security attack

Physical layer can be protected by applying spread spectrum technology like frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) [9]. The Frequency changes in random fashion to spread energy to a wider spectrum so that the transmission power is hidden behind the noise level. The data link layer can be protected by ERA 802.11. Traffic analysis of the network can be prevented by encryption. Wired equivalent privacy (WEP) [10] uses link encryption to hide end to end traffic information. The transport layer is secured by protocols like SSL (secure socket layer), TLS (transport layer security) and PCT (private communication transport). All are based on public key cryptography [11]. In network layer, wormhole attack is prevented by packet leash protocol [12] and sector mechanism [13]. Directional antennas [14] can also

prevent wormhole. SAR [11] (security aware ad hoc routing) prevents black hole attack. ARAN [15] defends against impersonation and repudiation using predetermined cryptographic certificates.

Related studies

A cluster based scheme BHAPSC [16] is used to prevent black hole attack in MANET. In this method, the malicious node can be detected along with its exact location. BHAPSC maintained a friend table and a trust estimate are invoked to calculate trust values. If the value of the node exceeds the threshold level then it will be broadcasted as a black hole. Limitation in this method is the overhead encountered in the generation of the friend table. Two step co-operative mechanism [17] is used to detect black hole attack. In this method (SnT) table and status (ST) table are maintained to track the neighbors Sequence and its status along with this a neighbor list is also maintained. Voter table is also maintained by the source for gathering votes for the suspicious node. Drawback in this method is the added overhead for each node to maintain numerous tables. Watchdog method [5,18], in this method when a node forwards a packet the watchdog ensures that whether the next node forward the packet. If the next node does not transmit then it is a malicious node. In DPRAODV [19], a threshold level for the sequence number is fixed. If the RREP sequence is greater than threshold then the node is malicious. This is a simple method because no modification is made to the AODV protocol. In BDSR [20], a nonexistent destination address is sent and if any node replies then it is denoted as malicious. Advanced algorithm [21] aimed to detect and prevent cooperative black hole and gray hole using end to end checking with prelude and postlude messaging. The data flow is monitored and if the data loss is out of tolerable range and exceeds the threshold level then a backbone network of trusted nodes collects the outcome of the monitoring nodes and detects the malicious node. In this method, the drawback is that the nodes lose energy by monitoring. There will be a significant data loss before detecting the malicious node. Anti-black hole mechanism (ABM) [22] aims to detect malicious nodes. ABM calculates the abnormal difference between routing message from the node. A node will be malicious if it replies with RREP but it would not have broadcasted any RREQ at all in the network. Modified AODV [23] routing protocol aims to improve security and performance against black hole attack. It eliminates one or more black hole nodes from the network designed using AODV protocol. Two reply packets are generated by the intermediate node. The sequence number of the second generated RREP should be greater than the first generated RREP sequence number by 1. Every node after receiving the RREP, check for the verify field in the packet, if it is 0 then the packet is not verified. Then the sequence number is checked, if it satisfies the condition then it is a valid node and the verify field is set as 1. On the off chance if the intermediate node gets a RREP from a node with a higher sequence number, then a similar procedure is repeated and after that it sets the verified field as 0 and it ignores the packet. Solution to handle DDOS attack [24] proposes that a monitoring node sends hello packet to neighbor node and wait for a reply. If the node does not receive any reply within the prescribed time limit, then the node is considered as a victim node and its id is disabled.

Proposed prevention technique

An ad hoc network is subjected to security issues. In this paper, we propose a method to solve the issue. Communication time is the time taken for a packet to reach the destination from source. It can be calculated using a heartbeat timer. In our proposed scheme, we find the attacking node by instructing the source node to check the acknowledging node id. This checking is done only if the communication time taken by the packet to reach the destination does not fall within the

calculated threshold value. The threshold value is the average value of the communication time taken from the initial set of packets to reach the destination.

Case 1: If the time taken by a packet to reach the destination falls within the calculated threshold limit then the communication continues. If it does not match the threshold value, then case 2 will be executed.
If the communication time taken by the packet to reach the destination exceeds or falls below the threshold value, then we check the acknowledging node id. If the id matches with the original id saved in the source then it continues transmitting the packet. If it doesn't match, then the node is isolated from the network and declared as malicious.

This proposed scheme helps in securing transmission in MANET. It is time consuming to check the acknowledging node id for every packet so in this proposed scheme we are checking the id only if the communication time taken by a path exceeds the calculated threshold value. The flow chart representing SRAODV is shown in FIG. 1.

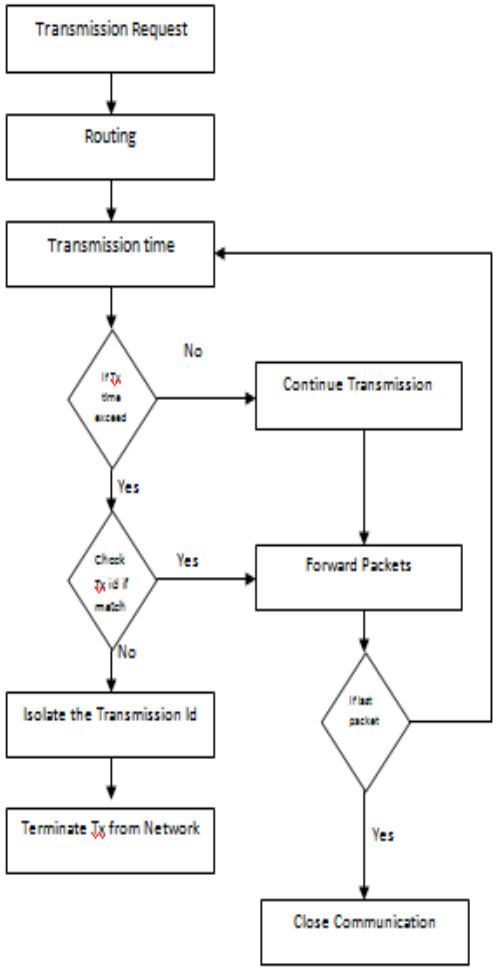

FIG. 1. **Flowchart representing SRAODV.**

Simulation

The proposed scheme is simulated in NS2 with following configuration shown in TABLE 1.

Simulation metric

The performance of SRAODV is compared with AODV. Performance parameters such as end to end delay, throughput, and packet loss are evaluated. SR-AODV gave increased throughput, reduced end to end delay and reduced packet loss when compared to AODV. The comparison graph for end to end delay, throughput and packet loss is shown in FIG. 2, FIG. 3 and FIG. 4.

TABLE 1. **Simulation parameters.**

Parameters	**Value**
Routing protocol	AODV
Number of nodes	35
Mac	Mac/802_11
Rx power	0.3 Joules
Tx power	0.3 Joules
Packet size	512 bytes
Simulation time	100 s
Environment size	500 × 500
No of attackers	3
Mobility model	Random way point

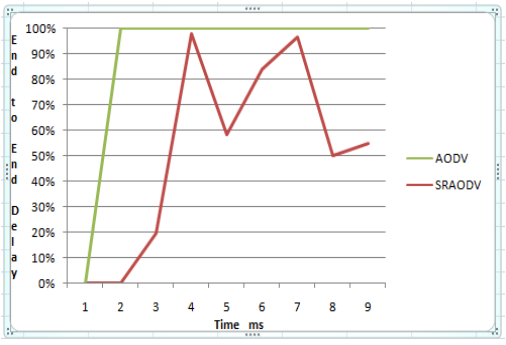

FIG. 2. **End to end delay vs. time.**

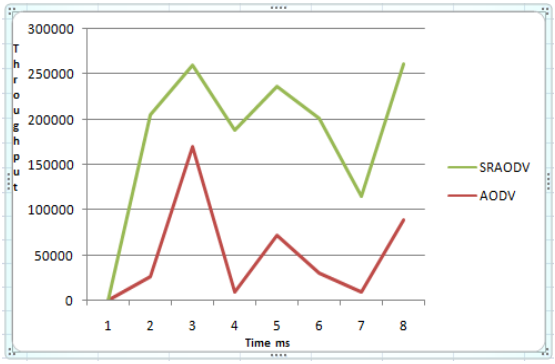

FIG. 3. **Throughput vs. time.**

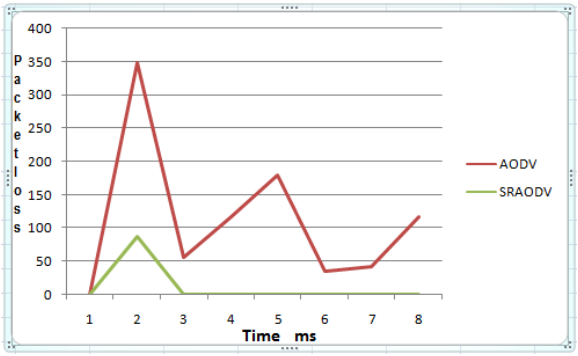

FIG. 4. **Packet loss vs. time.**

Conclusion

MANET is a self-configuring network without any specialized infrastructure. Security is a challenging issue faced by MANET. Most of the existing work has developed solution to the existing problem but more issues have arisen when the existing issues are addressed. The simulation result shows that the proposed solution is implemented and the problem caused by the attack during communication is solved. The performance parameters such as end to end delay, throughput and packet loss are analyzed. The proposed solution for DOS attack is achieved without affecting network performance. It takes care of existing and future issues.

REFERENCES

1. Siva Ram Murthy C, Manoj BS. Ad hoc wireless networks architectures networks architectures and protocols. Pearson Education. India. 81:5905-9.
2. Perkins C, Belding Royer E, Das S. Ad-hoc On-Demand Distance Vector (AODV) routing. IETE, RFC 2003;3561.
3. Wu B, Chen J, Wu J, et al. A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Wireless Mobile Network Security. Springer. 2006.

4. Kumar S, Pruthi G, Yadav A, et al. Security protocols in Manet. Second International Conference on Advanced Computing & Communication Technologies. IEEExplore.org. 2012;pp:530-534.
5. Ramaswamy S, Fu H, Sreekantaradhya M, et al. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. North Dakota State University. White paper. 2009.
6. Awerbuch B, Holmer D, Nita-Rotaru C, et al. An on-demand secure routing protocol resilient to Byzantine failures. Proceedings of the ACM Workshop on Wireless Security. 2002;pp:21-30.
7. Hu Y, Perrig A, Johnson D. Rushing attacks and defense in wireless ad hoc network routing protocols. Proc. of the ACM Workshop on Wireless Security (WiSe). 2003;pp:30-40.
8. Stallings W. Wireless communication and networks. Pearson Education. 2002.
9. Perrig R, Canetti Tygar J, Song D. The TESLA broadcast authentication protocol. Internet Draft. 2000.
10. Kaufman C, Perlman R, Speciner M. Network Security Private Communication in a Public World. Prentice Hall PTR. 2002.
11. Hu YC, Perrig A, Johnson D. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. Technical Report TR01-384. Rice University. 2002.
12. Srdjan Apkun C, Buttyan L, Hubaux JP. SECTOR: Secure tracking of node encounters in multihop wireless networks. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN). Washington, USA, 2003.
13. Hu L, Evans D. Using Directional Antennas to Prevent Wormhole Attacks, Network and Distributed System Security Symposium. San Diego. 2004;pp:5-6.
14. Sanzgiri K, Dahill B, Levine BN, et al. A secure routing protocol for ad hoc networks. In: Proc. of IEEE International Conference on Network Protocols (ICNP). 2002.
15. Kannammal A, Sujith Roy S. Survey on secure routing in mobile adhoc networks. International Conference on Advances in Human Machine Interaction (HMI-2016). Bangalore, India, IEEE 2016.
16. Marti S, Giuli TJ, Lai K, et al. Mitigating routing misbehavior in mobile ad hoc networks. 6th MobiCom, Boston, Massachusetts. 2000.
17. Su MY. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Elsevier, Computer Communications. 2011;pp:107-117.
18. Moudni H, Er-rouidi M, Mouncif H, et al. Modified AODV routing protocol to improve security and performance against black hole attack. International Conference on Information Technology for Organizations Development. 2016.
19. Nath I, Chaki R. BHAPSC: A new black hole attack prevention system in clustered MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2:113-21.
20. Deb M. A cooperative black hole node detection mechanism for ADHOC networks. In: Proc. of the World Congress on Engineering and Computer Science. 2008.
21. Po-Chun TSOU, Jian-Ming C, Yi-Hsuan L, et al. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. ICACT. 2011.
22. Payal Raj N, Prashant Swadas B. DPRAODV: A dynamic learning system against black hole attack in AODV based MANET, IJCSI. International Journal of Computer. 2009;2.

23. Jain S, Jain M, Kandwal H. Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. International Journal of Computer Applications. 2010;7:37-42.
24. Meghna Chhabra, Brij Gupta, Ammar Alomamani. A Novel solution to handle DDOS attack in MANET. Journal of Information Security. 2013;4:165-177.