International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol 1 Issue 4 August 2015

Prevention of DOS-attack for AODV Routing Protocol in MANET Scenario

Akshay Jain[1], Prof. Priyanka Dhasal[2]
[1] Research Scholar, [2]HOD IT, PCST Indore

ABSTRACT:- In Mobile Ad hoc Networks (MANET), various types of Denial of Service Attacks (DoS) are possible because of the inherent limitations of its routing protocols. Considering the Ad hoc On Demand Vector (AODV) routing protocol as the base protocol it is possible to find a suitable solution to over-come the attack of initiating / forwarding fake Route Requests (RREQs) that lead to hogging of network resources and hence denial of service to genuine nodes. In this paper, a proactive scheme is proposed that could prevent a spe-cific kind of DoS attack and identify the misbehaving node. Since the proposed scheme is distributed in nature it has the capability to prevent Distributed DoS (DDoS) as well. The performance of the proposed algorithm in a series of simu-lations reveal that the proposed scheme provides a better solution than existing approaches with no extra overhead.

Keywords: MANET, AODV, Routing

INTRODUCTION

In an ad hoc wireless network where wired infrastructures are not feasible, energy and bandwidth conversation are the two key elements presenting re-search challenges. Limited bandwidth makes a network easily congested by control signals of the routing protocol. Routing schemes developed for wired networks seldom consider restrictions of this type. Instead, they assume that the network is mostly stable and the overhead for routing messages is negli-gible. Considering these differences between wired and wireless network, it is necessary to develop a wireless routing protocol that restricts congestion in the network.

DoS Attack Due to RREQ Flooding

In AODV, a malicious node can override the restriction put by *RREQ_RATELIMIT* (limit of initiating / forwarding RREQs) by increas-ing it or disabling it. A node can do so because of its self-control over its parameters. The default value for the *RREQ_RATELIMIT* is 10 as proposed by RFC 3561. A compromised node may choose to set the value of parameter *RREQ_RATELIMIT* to a very high number. This allows it to flood the net-work with fake RREQs and lead to a kind of DoS attack. In this type of DoS attack a non-malicious node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs. This leads to the following problems:

- Wastage of bandwidth
- Wastage of nodes' processing time (more overhead)
- Exhaustion of the network resources like memory (routing table en-tries)
- Exhaustion of the node's battery power

These further results in degraded throughput. Most of the network resources are wasted in trying to generate routes to destinations that do not exist or routes that are not going to be used for any communication. This implies that the existing version of AODV is vulnerable to such type of malicious behavior from an internal node (which is then termed as a compromised node

PROPOSED METHOD

Overview- As mentioned earlier, the default value for *RREQ_RATELIMIT* is 10 RREQs/sec. This means each node is expected to observe some self-control on the number of RREQs it sends in one sec. A compromised node may choose to set the value of parameter *RREQ_RATELIMIT* to a very high num-ber or even disable this limiting feature, thus allowing it to send large number of RREQ packets per second. The proposed scheme shifts the responsibility to monitor this parameter on the node's neighbor, thus ensuring the compli-ance of this restriction. This solves all of the problems (mentioned in section 2) caused due to flooding of RREQs from a compromised node. Thus instead of self-control, the control exercised node's neighbor results in prevent-ing the flooding of RREQs.

RREQ_ACCEPT_LIMIT and RREQ_BLACKLIST_LIMIT

The proposal is based on the application of two parameters:

RREQ_ACCEPT_LIMIT denotes the number of RREQs that can be accepted and processed per unit time by a node. The purpose of this parameter is to specify a value that ensures uniform usage of a node's resources by its neighbors. RREQs exceeding this limit are dropped, but their timestamps are recorded. This information will aid in monitoring the neighbor's activities. In the simulations carried out, the value of this parameter was kept as three (i.e. three RREQs can be accepted per unit time). This value can be made adap-tive, depending upon node metrics such as it memory, processing power, bat-tery, etc.

The RREQ_BLACKLIST_LIMIT parameter is used to specify a value that aids in determining whether a node is acting malicious or not. To do so, the number of RREQs originated/forwarded by a neighboring node per unit time is tracked. If this count exceeds the value of RREQ_BLACKLIST_LIMIT, one can safely assume that the corresponding neighboring node is trying to flood the network with possibly fake RREQs. On identifying a neighboring node as malicious, it will be blacklisted. This will prevent further flooding of the fake RREQs in the network. The blacklisted node is ignored for a period of time given by BLACKLIST_TIMEOUT after which it is unblocked. The proposed scheme has the ability to block a node till *BLACKLIST_TIMEOUT* period on an incremental basis. The *BLACKLIST_TIMEOUT* period is doubled each time the node repeats its malicious behavior.

In the simulations the value of *RREQ_BLACKLIST_LIMIT* is kept as 10 (i.e. more than 10 RREQs per unit time results in flooding activity). By blacklisting a malicious node, all neighbors of the malicious node restrict the RREQ flooding. Also the mali-cious node is isolated due to this distributed defense and so cannot hog its neighbor's resources. The neighboring nodes are therefore free to entertain the RREQs from other genuine nodes. Nodes that are confident about the malicious nature of a particular node, can avoid using it for subsequent network functions. In this way genuine nodes are saved from experiencing the DoS attack.

ADVANTAGES OF THE PROPOSED SCHEME

- The proposed scheme incurs no extra overhead, as it makes minimal modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV (RFC 3561).
- Also the proposed scheme is moreefficient interms of its resultant routes established, resource reservations and its computational com-plexity.

- If more than one malicious node collaborate, they in turn will be re-stricted and isolated by their neighbors, since they monitor and exer-cise control over forwarding RREQs by nodes. Thus the scheme suc-cessfully prevents DDoS attacks.

ALGORITHM ILLUSTRATION

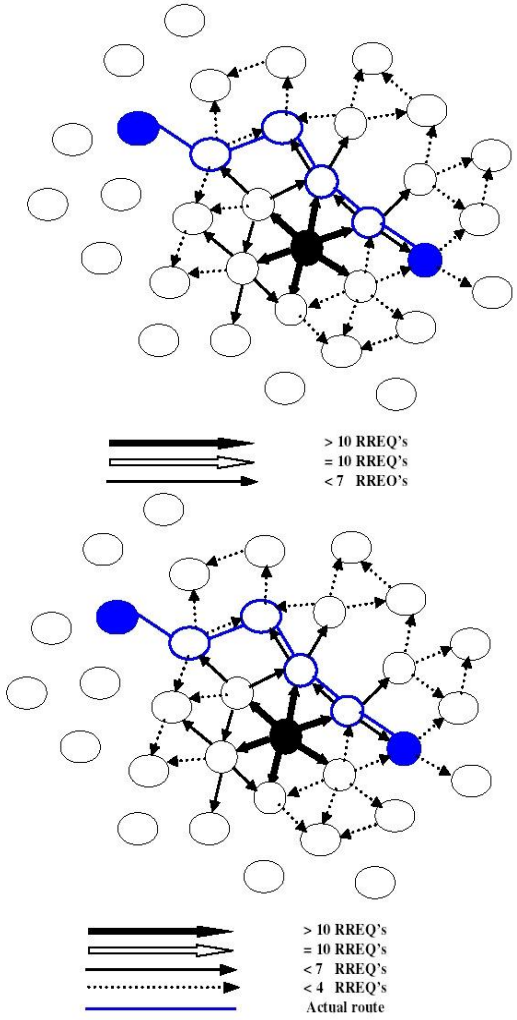

Figure 1. Illustration in original AODV

Figure 1 depicts the working in pure AODV routing protocol when an in-ternal malicious node launches a DoS attack by flooding the network with RREQs. The black node depicts the malicious node and the blue nodes depict two genuine nodes that want to communicate with each other. The optimal route consists of four intermediate nodes including the malicious node and three of its neighbors. The malicious node floods the network by generating 10 RREQs per second as shown. Its immediate neighbors, (who are not mali- cious) observe the

RREQ_RATELIMIT and hence each forward 10 RREQs only. Since at max three RREQs will be accepted from these nodes within one second, the neighbors of these nodes need to forward < seven RREQs and their neighbors in turn need to forward < four RREQs, as shown. Since the resources of the malicious node's neighbors are completely occupied in proc-essing and forwarding the RREQ's originating from it, the route between the blue nodes, if it is established, will consist of greater number of intermediate nodes. Thus in effect a DoS attack is launched as the genuine nodes are de-prived of the services of nodes whose resources are wasted due to flooding.

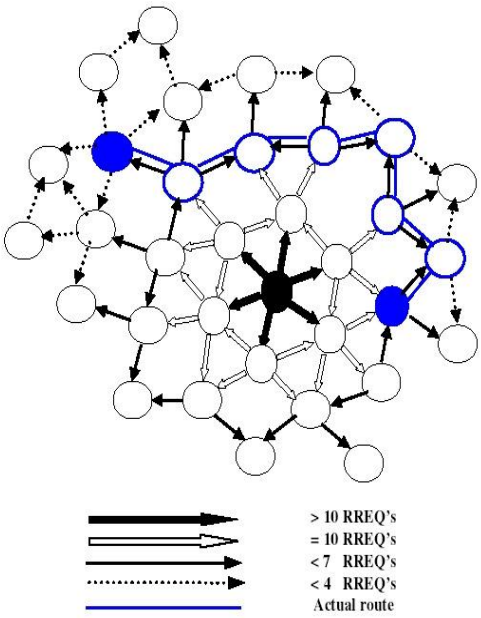

Figure 2. Illustration of the proposed AODV

Figure 2 illustrates the working procedure in the proposed AODV scheme. As shown in the figure, malicious node (depicted by the black node) floods RREQs in the network and two genuine nodes (depicted by blue nodes) want to communicate with each other. In this scheme, the no. of RREQs that can be accepted from a neighbor is limited. Hence, the neighbors of the malicious node, will only accept and forward three RREQ packets received from it within a time interval of one sec. This rate limit of three packets is to ensure fair share of a node's resources to all the neighbors. Moreover, whenever the malicious node crosses the RREQ_BLACKLIST_LIMIT of 10 RREQ pack-ets within a time interval of one sec, its neighbors will blacklist it. Thus, in addition to limiting the clogging up of resources in the network, the proposed scheme also, isolates the malicious node. The route established in this scheme is expected to be the optimum route, which consists of minimum number of intermediate nodes. Thus, no DoS attack is experienced in the developed scheme.

IMPLEMENTATION & RESULTS

We have implemented our work i.e. Creation of MANET Scenario for NS-2 and then to detect denial of service attack for AODV routing protocols with the use of Various performance matrices Like Packet Delivery Ratio, End to End delay, Residual Energy, Routing overhead and Overall Throughput. In our case firstly we have created scenario file for DOS attack standard which has to be used along with our TCL Script than we have created a TCL script consist of various routing protocols in our case these are AODV, WAODV and TAODV than a particular MANET scenario or topology in our case it consist of 21, 41 and 61 static nodes with 300sec simulation time.

In this section, three scenarios are described with three different protocols which are AODV, WAODV and TAODV, presented in tabular form.

EVOLUTION OF RESULTS

For our work to be done successfully we have used MANET scenario with varying node density which are 21, 41 and 61 nodes and constant 300 sec under static scenario using various routing protocols. We have reached to the results with the help of various performance matrices for now we have used following performance matrices.

1. Packet Delivery Ratio
2. Residual Energy
3. Throughput

Packet Delivery Ratio:- Figure shows the packet delivery ratio for AODV, WAODV and TAODV.

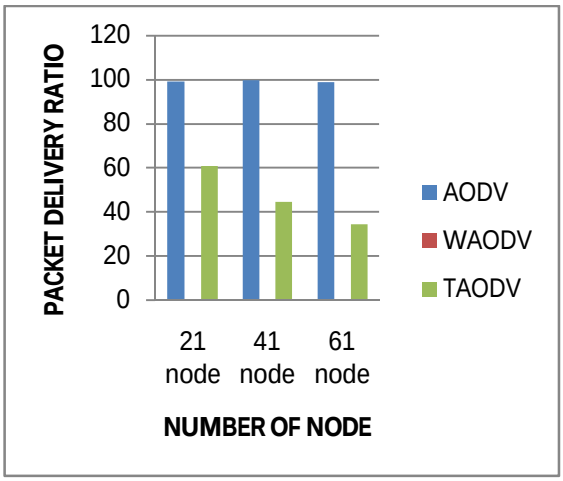

Figure 3. Packet Delivery Ratio

Throughput: Figure shows the Throughput for AODV, WAODV and TAODV.

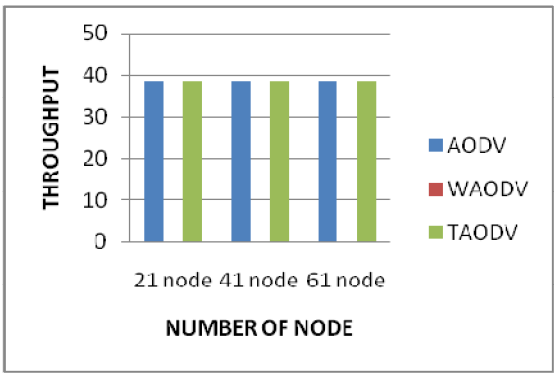

Figure 4. Throughput

Residual Energy: Figure shows the Residual Energy for AODV, WAODV and TAODV.

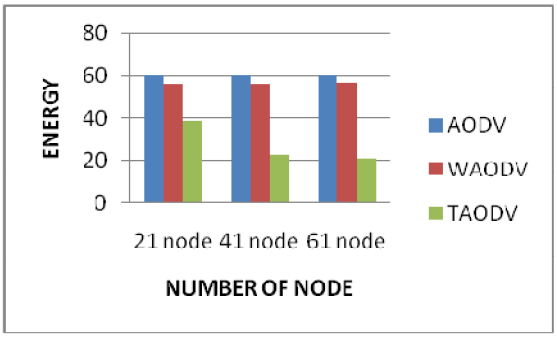

Figure 5. Residual energy

CONCLUSION

In this work we analyzed all parameter which are Packet Delivery Ratio, End to End Delay, Routing Overhead and concluded that the TAODV routing protocol secured to DOS attack where as WAODV protocol affected by DOS attack so we can say that TAODV is good as compare to the WAODV routing protocol for different node.

REFERENCES

[1] S.A.Arunmozhi and Y.Venkataramani, A Flow Monitoring Scheme to Defend Reduction-of-Quality (RoQ) Attacks in Mobile Ad-hoc Networks, Information Security Journal: A Global Perspective , Vol.19, No.5, 2010, pp. 263- 272.

[2] Jelena Mirkovic and Peter Reiher, D-WARD: A Source-End Defense against Flooding Denial-of-Service Attacks, IEEE Transactions On Dependable And Secure Computing , Vol. 2, No. 3, 2005, pp. 216-232.

[3] Ping Yi, Zhoulin Dai, YiPing Zhong and Shiyong Zhang, Resisting Flooding Attacks in Ad Hoc Networks, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), Vol. 2

[4] Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song, Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks, IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, May 2010, pp. 579-582.

[5] N. Karthikeyan, V. Palanisamy and K. Duraiswamy, Optimum Density Based Model for Probabilistic Flooding Protocol in Mobile Ad Hoc Network, European Journal of Scientific Research ,Vol.39, No.4, 2010, pp.577-588.

[6] Xuan Yu, A Defense System On Ddos Attacks In Mobile Ad Hoc Networks, Ph.D dissertation, Auburn University, Alabama, May 2007.

[7] Ming-Yang Su, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems, Computer Communications , Vol. 34, 2011, pp. 107–117.

[8] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal, Antonio Nucci and Edward Knightly, DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks, IEEE/ACM Transactions On Networking , Vol. 17, No. 1, February 2009, pp. 26-39.

[9] Amey Shevtekar and Nirwan Ansari, A router-based technique to mitigate reduction of quality (RoQ) attacks, Computer Networks, Vol. 52, 2008, pp. 957–970.

[10] Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong, A New Routing Attack in Mobile Ad Hoc Networks, International Journal of Information Technology , Vol. 11, No. 2, 2005, pp.83-94.