ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

Scheme of security in Mobile Ad Hoc Networks using Route Blacklist Limit Mechanism

Hemant Kamle, Geetika Dubey
Computer Science And Engg. ,SATI , Vidisha,RGPV
kamle_hemant@yahoo.co.in
M.Tech (Student)

Abstract. Routing protocols play an important role for communications in Mobile Ad Hoc Network Mobile Ad hoc Networks (MANET) has various types of Denial of Service Attacks (DoS) are possible because of the inherent limitations of its routing protocols. Denial-of-Service (DoS) and Distributed Denial-of Service (DDoS) are widely known security attacks which attempt to make computer resources unavailable to its intended users. Considering the Ad hoc On Demand Vector 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 specific 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 as well. DoS attacks consume the resources of a remote host or network that would otherwise be used for serving legitimate users. The performance of the proposed algorithm in a series of simulations reveal that the proposed scheme provides a better solution than existing approaches with no extra overhead.

According to our proposal we apply RREQ limit and check through that limit and prevent our network.

Keyword :-

RREQ_Accept_limit, AODV, Radio range, MANET, DOS.

1. 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 [1][2][3].

This paper proposes minor modifications to the existing AODV routing protocol (RFC 3561) in order to restrict congestion[4][5] in the network during a particular type of DoS attack[6]. In addition to this it incurs absolutely no extra overhead [7]. The rest of this paper is organized as follows. In section 2, we describe the DoS attack caused due to RREQ flooding and its implications on the existing AODV driven MANET [8][9]. To combat this DoS attack a pro- active [10] scheme is proposed in section 3. Section 4 presents an illustration to describe the implications of RREQ flooding on pure AODV and the modified AODV. To quantify the effectiveness of the proposed scheme, a DoS [11] attack was simulated in the mobile environment and its performance results are reported in section 5.

2. Related Work

The security difference between wired infrastructure networks and mobile ad hoc networks [12] motivated researchers to model an IDS that can handle the new security challenges such as securing routing protocols. A cooperative intrusion detection model has been proposed in [13], where every node participates in running its IDS in order to collect and identify possible intrusions. If an anomaly is detected with weak evidence, a global detection process is initiated for further investigation about the intrusion through a secure channel. This model suffers from performance penalties and false alarm rates. An extension of this model was proposed in [14], where a set of intrusions can be identified with their corresponding source. Moreover, authors addressed the problem of run-time resource constraint by IDS through modeling a repeatable and random head cluster election framework. Watchdog and pathrater were proposed in [15] to improve the throughput in MANET in the presence of misbehaving nodes. Watchdog goal is to identify the compromised nodes in the network while pathrater goal is to notify the routing protocols from using misbehaving nodes. This model did not propose any punishment procedure that could motivate nodes to behave normally. Hence, misbehaving nodes can continue operating in the network and benefiting from others' services. CORE [16] is a cooperative enforcement mechanism based on a monitoring and reputation systems. The goal of this model is to detect selfish nodes and enforce them to cooperate. Each node keeps track of other nodes' cooperation using reputation as the cooperation metric. CORE ensures that misbehaving nodes are punished by gradually stopping communication services and provides incentives for nodes, in the form of reputation, to cooperate. Note that, reputation is calculated based on data monitored by local node and information provided by other nodes involved in each operation.

Game theory [20] was successfully used in many disciplines including economics, political science and computer science. Currently, it has been used to address problems where multiple players with different objectives can compete and interact with each other. To predicate the optimal strategy used by intruders to attack a network, the authors of [17] modeled a non-cooperative game theoretic model to analyze the interaction between intruders and IDS in wired infrastructure networks. In [14], the authors aimed at demonstrating the suitability of game theory for development of various decision, analysis, and control algorithms in intrusion detection. They accomplished this by addressing some of the basic network security tradeoffs, and giving illustrative examples in different platforms. They proposed two different schemes, based on game theoretic techniques. They considered a generic model of a distributed IDS with a network of sensors. Finally, one can conclude that game theory is a strong candidate to provide the much-needed mathematical framework for analyzing the interaction between the IDSs in MANET to reduce false positives.

In AODV, a malicious node can override the restriction put by *RREQ_RATELIMIT* [12] (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 [12] 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 nodes' processing time (more overhead)

Wastage of bandwidth

.Exhaustion of the network resources like memory (routing table en- tries)

•Exhaustion of the node's battery power

This 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 behav- ior from an internal node (which is then termed as a compromised node).

3. Proposed Scheme:

According to malicious node criteria, malicious node increase RREQ (Route request) limit from 10 to greater value per second and flooding it to neighbor nodes , if neighbor node work without checking this parameter so that neighbor node not fairly serve another packets, that means node work without checking RREQ_Limit and congested itself and to others.
So in our proposal we create a module for checking RREQ packet limit and forward to actual destination nodes, here we divide our proposal into two parts.

1) RREQ Accept Limit

2) RREQ Blacklist Limit

The proposed scheme shifts the responsibility to monitor this parameter on the node's neighbor, thus ensuring the compliance 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 by a node's neighbor results in preventing the flooding of RREQs.

3.1 RREQ_ACCEPT_LIMIT

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 adaptive, depending upon node metrics such as it memory, processing power, battery, etc

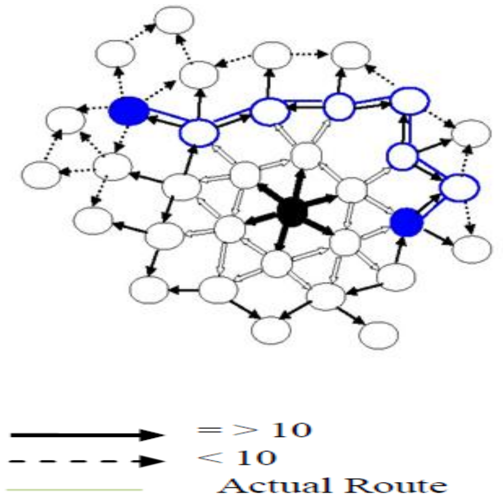
3.2 RREQ_BLACKLIST_LIMIT

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

3.3 Algorithm Route Deployment

Figure 1 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 purple 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 packets 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.

Figure:1 Route Request Flooding with Blacklisted Node



4. Simulation Details

The simulation described in this paper was tested using the ns-2 test-bed that allows users to create arbitrary network topologies [22]. By changing the logical topology of the network, ns-2 users can conduct tests in an ad hoc network without having to physically move the nodes. ns-2 controls the test scenarios through a wired interface, while the ad hoc nodes communicate through a wireless interface.

The AODV protocol incorporated in NS-2 by Uppsala University, Sweden, was used as the base protocol. Modifications were made to this version of AODV protocol that confirms to RFC 3561. TCP was used as the transport protocol Radio transmission range is set as 250 meters. Traffic sources used are Constant-Bit-Rate (CBR) and the field configuration is 800 x 800m with 40 nodes.

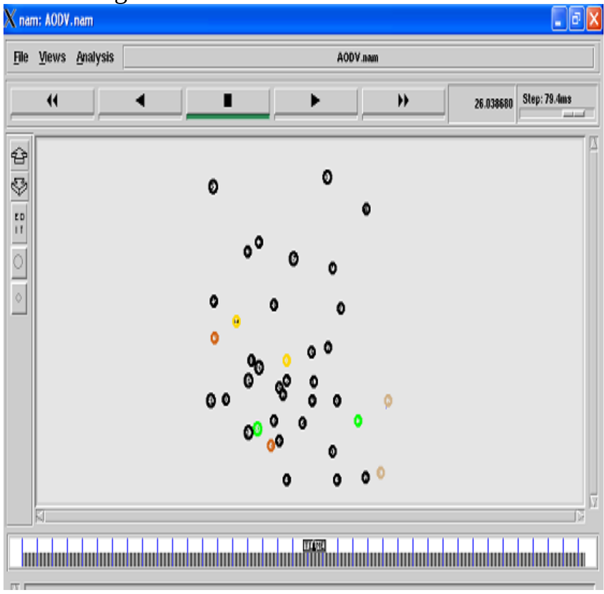


Figure: 2 A sample topology generated by ns-2

4.1 Simulation Parameter

Here we create the simulation parameter table, according to that given table we simulate the our result and analyze them. we use routing protocol as AODV with uni-casting mechanism and take the simulation time as 50 sec. Table-1

Metrics	**Parameter**
Number of nodes	40
Dimension of simulated area	800×800
Routing Protocol	AODV
Simulation time (seconds)	50
Traffic type	CBR
Packet size (bytes)	1000
Number of traffic connections	10
Maximum Speed (m/s)	30

We get Simulator Parameter like Number of nodes, Dimension, Routing protocol, traffic etc.

According to below table 1 we simulate our network.

4.2 UDP Comparison of 25 nodes with random movement

Figure 3 show UDP packet transmissions which includes packet receive, packet lost and total packet transmission and comparison normal case. Graph shows that the packet received is much more than the packet loss.

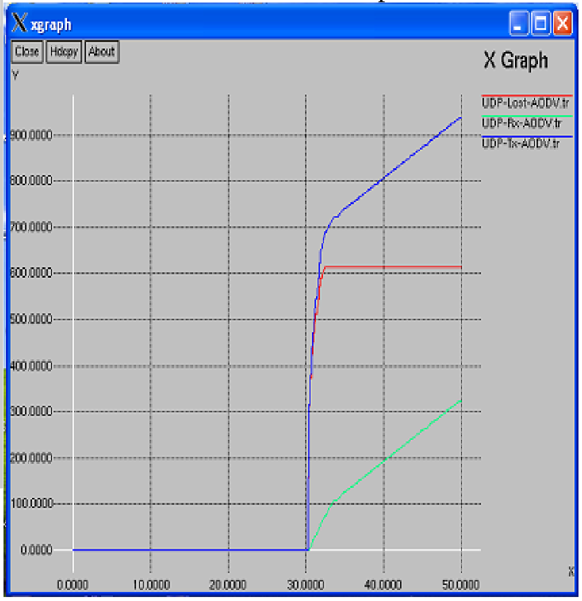


Figure 3 UDP packets Normal Case

4.3 UDP Comparison after Blacklist Node

Figure 4 show UDP packet transmissions which includes packet receive, packet lost and total packet transmission and comparison after blacklist node enter in our network. Graph shows that the packet loss is much more than the packet received.

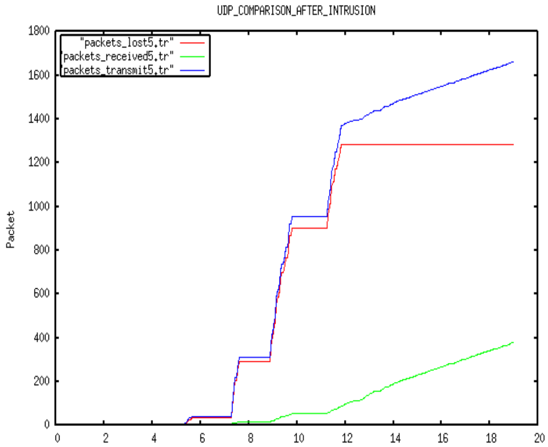


Figure 4 UDP packets after Blacklisted Node

4.4 TCP Comparison

Figure show TCP packet transmission which includes packet receives and total packet transmission and comparison before and after blacklisted node in network. Graph shows that the packet received is much large before blacklist node comes to our network than the entering blacklist node in our network.

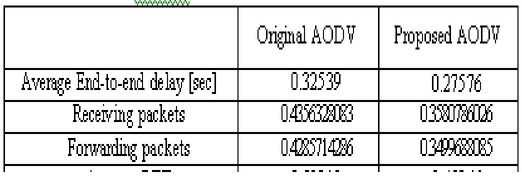


Table 2. Overall network simulation results

	Original AODV	Proposed AODV
Average End-to-end delay [sec]	0.32539	0.27576
Receiving packets	0.4356328083	0.3580786026
Forwarding packets	0.4285714286	0.3499688085

5. Conclusion and Future Work:

According to our result we find out if blacklist node comes to our network so network has been heavily congested and actual data packet sends percentage decreases that conclude blacklist node sense less bandwidth consume through mobile nodes, also drop rate has been increases. The malicious nodes identified are blacklisted and none of the genuine nodes in the network are wrongly accused of misbehaving. In the proposed scheme, there is an enhancement in the per- formance of the network in presence of compromised nodes.

Here we simulate our result through AODV routing protocol with a Blacklist node and analyze our results, in future we simulate our network through various routing attack effect like worm hole , selfish node and etc. and prevention mechanism for that type of attack so that no any intrusive process comes to our network, and network safe through unwanted activity, we also apply IDS mechanism with DSR , DSDV and other type of mobile ad-hoc routing and simulate our result.

References

[1] Peng Yang, Biao Huang,Multi-path Routing Protocols for Mobile Ad Hoc Networks, International conference on computer science & software engineering 2008.

[2] Dan Galatchi, Roxana Zoican, On-Demand Multicaste Routing Protocols in Dynamic Ad Hoc Networks,TELSIKS Serbia,Nis, October 7-9,2009.

[3] Broch J., Maltz D.A., Johnson D.B., Hu Y.C., and Jetcheva J., A performance comparison of multi-hop wireless ad hoc network routing protocols. In 4th International Conference on Mobile Computing and Networking (ACM MOBICOM’ 98), pages 85–97, Oct 1998

[4] Rahman A., Security issues in mobile systems, http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/ docs /sec-in-ob.html, 1995 (accessed on May 03, 2004).

[5] Royer E.M. and Toh C.K., A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications, vol. 6:46–55, Apr 1999.

[6] Perkins C.E. and Royer E., Ad-hoc on-demand distance vector routing. In 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90– 100, 1999.

[7] Perkins C.E., Das S.R. and Royer E.. Ad-hoc on-demand distance vector (aodv) routing. http:// www.ietf.org/internet-drafts/draft-ietf-manet-aodv-
05.txt, 2000 (accessed on May 03, 2004).

[8] Karpijoki V., Signaling and routing security in mobile and ad-hoc networks. http://www.hut.fi/vkarpijo/iwork00/, 2000 (accessed on May 03, 2004).

[9] Jacquetand P., Viennot L., Overhead in Mobile Ad-hoc network Protocols, INRIA Research Project RR-3965, 2000.

[10] Y. Zhang andW. Lee, "Intrusion Detection inWireless Ad-Hoc Networks", Proc. MOBICOM 2000, Boston, ACM press, pp:275-283, 2000.

[11]http//dolphin.eng.uc.edu/networks/thesis/laksmi%20thesis.pdf (accessed on May 03, 2004)

[12] Routing Security in Ad Hoc Networks, Janne Lundberg, Helsinki University of Technology.

[13] Perkins C.E., Terminology for Ad-Hoc Networking, Draft-IETF-MANET terms-00.txt, November 1997.

[14] A. Agah, S. Das, and K. Basu, "Intrusion Detection in Sensor Networks: A Non-cooperative Game Approach", Proc. 3rd IEEE International Symposium on Network Computing and Applications, IEEE press, 2004.

[15] T. Alpcan and T. Basar, "A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection", Proc. of 43rd IEEE Conference on Decision and Control (CDC), Paradise Island, Bahamas, 2004.

[16] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", Proc. 1st ACM Workshop Security of Ad Hoc and Sensor Networks, Virginia, ACM press, pp:135-147, 2003.

[17] M. Mehrandish., H. Otrok, M. Debbabi, C. Assi and P. Bhattacharya, "A Game Theoretic Approach to Detect Network Intrusions: The Cooperative Intruders Scenario", Proc. 49*th* annual of IEEE GLOBECOM, San Francisco, IEEE press, 2006.

[18] P. Michiardi and R. Molva, "Analysis of Coalition Formation and Cooperation Strategies in Mobile Ad hoc Networks", Journal of Ad hoc Networks, Elsevier, pp:193-219, 2005.

[19] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection inWireless Ad Hoc Networks", IEEEWireless Communications, IEEE press, pp:48-60, 2004.

[20] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. 6th annual international conference on Mobile computing and networking, Boston, USA, ACM press, pp:255 - 265, 2005.

[21] G. Owen, "Game Theory", 3*rd* ed. New York, NY: Academic Press, 2001.

[22] Nidhi S Kulkarni, Balasubramanian Raman and Indra Gupta, On Demand Routing Protocols for mobile Ad Hoc Networks; A Review,2009 IEEE International Advance Computing conference,Patiala,India,6-7 March 2009.