Performance Evaluation of Byzantine Rushing Attack in ADHOC Network

Neha Agrawal
Maharana Pratap College Of Technology
Gwalior, Madhya Pradesh

Krishna Kumar Joshi
Maharana Pratap College Of Technology
Gwalior, Madhya Pradesh

Neelam Joshi
Maharana Pratap College Of Technology
Gwalior, Madhya Pradesh

ABSTRACT

The MANET incorporates mobile nodes that forward information or packets from node to node without a wired connection. The topology changes rapidly and unproductively, there is no central control for routing of packets hence the communication is on mutual trust. There are many proposed routing protocol in which on-demand routing is most preferable among all as its overhead is very low. Thus attention has been paid on developing a secure reactive protocol against various attacks. In this proposed work effect of rushing attack is presented over AODV. This attack results in denial-of-services and is effectively damaging as it can also be performed by weak attacker.

General Terms

Mobile Ad-Hoc Network (MANET).

Keywords

MANET, Byzantine Rushing Attack, Reactive Protocol, AODV

1. INTRODUCTION

Ad-hoc network is collection of autonomous nodes where all the nodes are dynamically configured without any centralized management thus form of network without any pre-existing infrastructure. Such networks is applicable in many fields like military & police exercises,, disaster relief, operations, robot data accumulation, mine site operations etc. MANET [1, 3, 4,] is prone to various types of attacks as compared to wired networks, but is used largely due to the reason that the network can be setup at any place & anytime without any pre-existing infrastructure.

Attacks in MANET:

A. Passive attack: It does not disrupt the operation of data or data is not altered.

B. Active attack: It alters the data or destroys the data that is being transmitted.

Some common types of attacks in MANET:-

i. **Wormhole attack**: In this attack two malicious node tunnels between and traffic and transfers packet.

ii. **Blackhole attack**: The attacker reply for the route request with the short path and thus get access to the data.

iii. **Byzantine attack**: In this attack the intermediate node perform collision of data, forming loops dropping of packets thus degrading the routing services.

iv. **Rushing attack**: This attack provides a denial-of-service, which uses duplicate suppression mechanism & quickly forward route discovery and gain access on data.

2. RELATED WORK

AODV is the type of reactive protocol which is on demand protocol. As its name implies it works only when user demand for communication related to the transmission and receiving the data packets. The AODV routing protocol is the up gradation of the destination sequenced distance vector routing. The main advantage of the AODV is that, it provides the better communication in the network without any congestion. The noteworthy contribution related is as follows:

Yin-Chun Hu et al [2] presented in year 2003 a new type of attack " Rushing attack", this attack results in denial of services (DoS) when used against on-demand routing protocol. All on demand protocols are unable to detect this attack. This attack can also be performed by weak attacker. Thus a generic rushing attack prevention (RAP) have been developed it exploits no cost unless the underlying protocol fails to find a working route .This method provide provable prevention even for strong attackers.

S. Albert Rabara, and S. Vijayalakshmi [3] proposed how rushing attacker works in multicasting network. Rushing attack is the processes of disturbing routing mechanism by pumping a high speed malign MRREQ (Multicasting Route Request) to reach the last node, thus increasing the network traffic . The solution suggested is threshold technique (D_3UT_3) in which a alarm is triggered when the number of requests is greater than the defined threshold value.

Rusha Nandy, and Debdutta Barman Roy [4] presented how rushing attack works on DSR protocol. Self organized clustering technique schemes have been proposed. A parameter k has been defined for number of hop away from the cluster head. Thus the hop forms a cluster with its cluster head and routing is performed by transferring data within the cluster or between the clusters. A rushing attack detection technique have been suggested in which the cluster examine the nodes of cluster. If the RREQ transmission frequency is greater than normal frequency than the node is malicious and hence removed from the cluster.

Desilva et al [7] proposed rushing attack prevention technique aka RAP. This paer have proposed an adaptive method of threshold value calculation where value is not fixed and predefined . Threshold value can also be statically calculated.

V. Palanisamy and P.Annadurai [10] presented the rushing attack, in this attack the malicious node exploits duplicate suppression mechanism and quickly forwarding route discovery packets to gain access on the forwarding data .Thus attacker provide route discovery first and hence the possibility of false route selection increases .This paper compare the performance of attacker and its success rate in three scenario: near sender ,near receiver ,anywhere in network.

Hyojin Kim et al. [11] proposed here a novel, robust routing scheme to defend ad hoc networks against rushing attacks. This scheme utilizes the "neighbor map mechanism". This methodology focuses on route maintenance rather than using route discovery. By using this methodology path recovery delay is reduced and thus provide energy efficient solutions.

Swarnali Hazra and S.K.Setua [14] extended the AODV protocol which is based on trust model and provide secure network. This model is based on threshold value of trust ,the network consist of trust evaluating node which takes the decision to include or not to include the trustee node in routing path depending on the final trust value computed by the trust model . AODV is enhanced with different functional modules: Node Manager, Trust Module and Decision Manager. Trust based AODV secures the routing path by isolating the rushing attacker, based on their trust value.

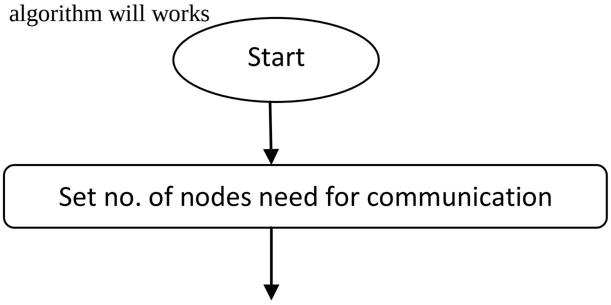
3. BYZANTINE RUSHING ATTACK IMPLEMENTATION

Byzantine Rushing attack is a zero delay attack nd more effective when the attacker nearby source or destination node. On-Demand routing protocols like AODV and DSR are more Vulnerable to this attack, because whenever source node floods the route request packet in the network, an adversary node receives the route request packet and sends without any hop count update and delay into the network. Whenever the legitimate nodes receive the original source request packet s, they dropped because legitimate nodes , would have already received packet from the attacker and tret the currently received packet as duplicate. so the adversary node is included on yhe active route and it disturbs the data forwarding phase. This attack can take place source side or destination side or at middle .

In the following condition the rushing attacker not include in active route

1. If source and destination have direct communication link.
2. if source and destination nodes have better route than attackers route

Here I am presenting the flow chart which describes how the algorithm will works



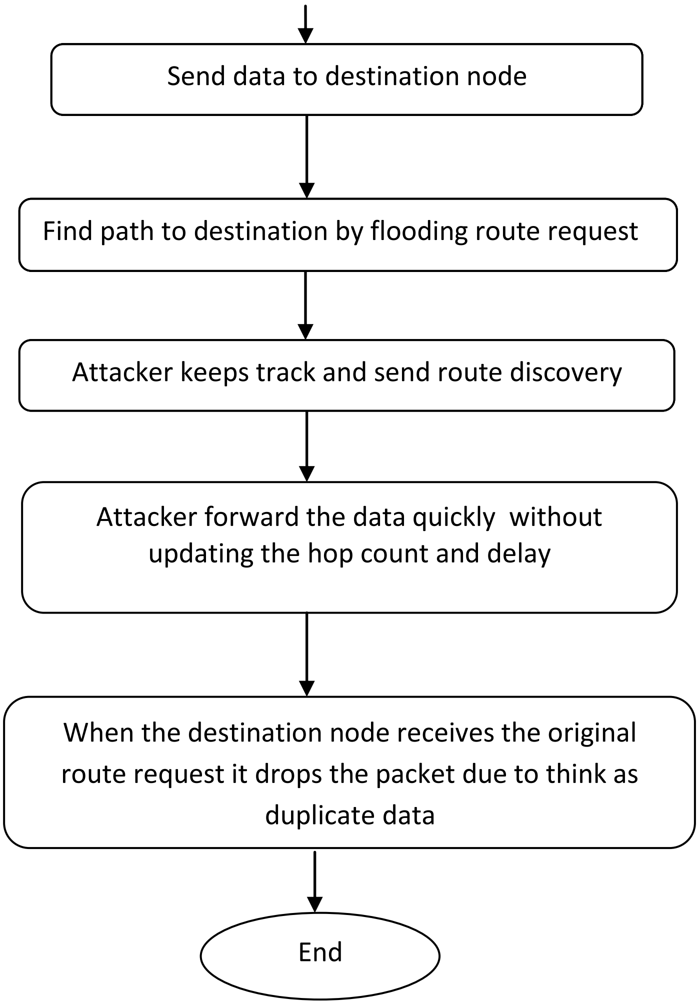

Send data to destination node
Find path to destination by flooding route request
Attacker keeps track and send route discovery
Attacker forward the data quickly without updating the hop count and delay
When the destination node receives the original route request it drops the packet due to think as duplicate data
End

fig. 1 Byzantine Rushing attack formation Algorithm

4. SIMULATION PARAMETRES AND RESULTS

Simulation parameter details are required the parameters are as follows And generated results using ns-2.35 simulator.

4.1 Simulation Parameter

The simulation parameters are given in the table 1 below:

Parameter	Values
Channel Type	Wireless Channel
Radio-Propagation Model	Two Ray Ground
Network Interface Type	Wireless Phy
Mac Type	802_11
Interface Queue Type	Drop tail/PriQueue
Link Layer type	LL
Antenna Model	OmniAntenna
Max packet in Ifq	50
Number of mobile nodes	25
Routing Protocol	AODV
Time of Simulation End	100ms

For the simulation NS-2.35 simulator is used as a simulator. The performance comparison of AODV can be done under:

- **Without attacks:** As a Normal AODV.
- **With attacks:** Where the Rushing attacks with one attacker, two attackers and three attackers.

4.2 Simulation Scheme

- 25 nodes
- MANET
- Reactive protocol: AODV
- Attack: Byzantine Rushing Attack
-

The scenarieo for attack implementation on 3 nodes are given in fig 2 below:

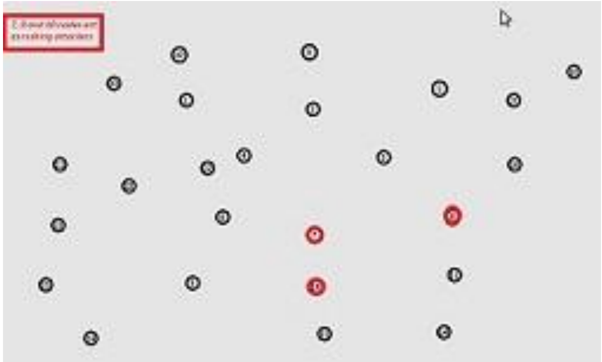


Fig 2: showing the implementation

4.3 Experimental Evaluation of Flood Rushing Attack

Figure 3 shows Throughput where x-axis defines different systems with number of adversaries present in the network, and y-axis defines throughput in kilo-bits per second(kbps). The larger this metric, the more efficient network will be.

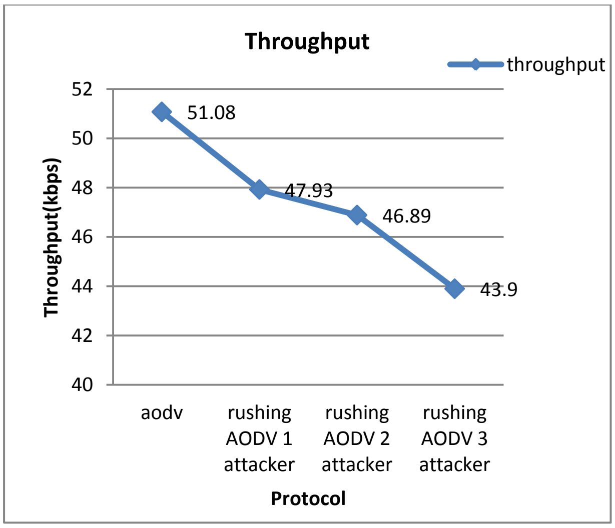
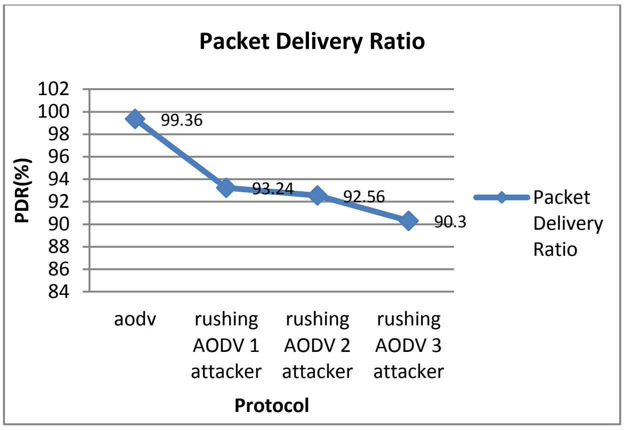


Figure 4 shows Packet Delivery Ratio (PDR) where x-axis defines different systems with number of adversary present in the network, and y-axis defines PDR. The larger this metric, the more efficient network will be.



5. CONCLUSION

In this paper, we had evaluated Byzantine Rushing attack on entire network performance, in the presence of different number of adversarial nodes. From the simulation outcome and result analysis we can conclude that, with ascending increase in number of adversarial node, throughput decreases, and PDR decreases. Moreover, the experimental evaluation of Byzantine attack having colluding nodes is comparatively more efficient that former. The paper concludes that Byzantine Rushing attack is most significant factor for an efficient attack against insecure on-demand protocols, mainly when adversaries collude. The most effective property of flood rushing attack is it amplifies any attack that merge with it, as it permit adversaries to have control over route discovery and overall network.

6. FUTURE WORK

Implementation of an efficient IDS (Intrusion Detection System) for and Byzantine Rushing attack may be considered as future work. The way in which network should behave once any node is identified as malicious may be considered as future scope. Moreover future scope of research on security protocol will incline approach towards MANET security.

Another scope is to determine the allocation of bandwidth in MANET environment with limited resource. Moreover, future work also includes the optimal way over the constraints on the resource and power of adversaries.

7. REFERENCES

[1] B. A. David Holmer, Reza Curtmola, “Mitigating byzantine attacks in ad hocwireless networks”, Technical Report Version 1, March 2004.

[2] Wikipedia: Attack (computing) August 2012 “http://en.wikipedia.org/wiki/Attack(computing)”, August 2012.

[3] C. X. Lujie Zhong, “Byzantine attack with anypath routing in wireless mesh networks,” IEEE Proceedings of IC-BNMT, vol. 1.0, pp. 711–715, 26-28 Oct 2010. 3rd IEEE International Conference.

[4] S. E. S. Steven R Snapp, “The distributed intrusion detection system prototype,” In Proceedings of the Summer USENIX Conference, pp. 227– 233, June 1992.

[5] G. F. Calvin Ko, “Automated detection of vulnerabilities in privileged programs by execution monitoring,” In Proceedings of the 10th Annual Computer Security Applications Conference, IEEE Computer Society Press, vol. xiii, pp. 134–144, May 1994.

[6] S. C. S. Stani ford Chen, “Grids-a graph based intrusion detection system for large networks,” In Proceedings of the 19th National Information Systems Security Conference, 1996.

[7] G. White and V. Pooch, “Cooperating security managers: Distributed intrusion detection systems,” Computers & Security, Elsevier Science Ltd., 1996.

[8] F. G. Y. Frank Jou, “Architecture design of a scalable intrusion detection system for the emerging network infrastructure,” Department of Com-puter Science, North Carolina State University, Releigh, N.C, USA, April 1997.

[9] P. A. Porras and P. G. Neumann, “Automated detection of vulnerabilities in privileged programs by execution monitoring,” In Proceedings of the 10th Annual Computer SecurityMApplications Conference, IEEE Computer Society Press, October 1997.

[10] Cabrera, Gutierrez, and Mehra, “Infrastructures and algorithms for dis-tributed anomalybased intrusion detection in mobile ad-hoc networks,” Military Communications Conference, 2005. MILCOM 2005,IEEE, vol. 3, pp. 1831–1837, October 2005.

[11] S. Marano, V. Matta, and L. Tong, “Distributed detection in the presence of byzantine attack in large wireless sensor networks,” Military Com-munications Conference, 2006. MILCOM 2006, IEEE, pp. 1–4, October 2006.

[12] A. R. Sangi, J. Liu, and L. Zou, “A performance analysis of aodv routing protocol under combined byzantine attacks in manets,” Computational Intelligence and Software Engineering, 2009. CiSE 2009, IEEE, vol. 3, pp. 1–5, December 2009.

[13] P. Yi, Y. Wu, and J. Ma, “Experimental evaluation of flooding attacks in mobile ad hoc networks,” Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference, pp. 1–4 ISBN:978–1– 4244–3437–4, 2009.

[14] A. S. ALshahrani, “Rushing attack in mobile ad hoc networks,” Third International Conference on Intelligent Networking and Collaborative Systems, pp. 752–758 ISBN: 978– 1–4577–1908–0, 2011.

[15] M. H. Rehmani, S. Doria, and M. R. Senouci, A Tutorial on the Implementation of Ad-hoc On Demand Distance Vector Protocol in Network Simulator. June 2009.

[16] Prof. S.B. Javheri and Shwetambari Ramesh Patil, “Attacks Classification in Network”, International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 4, Issue 3, 2013, pp. 1 - 11, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.

[17] Nada M. Badr and Noureldien A. Noureldien, “Review of Mobile Ad Hoc Networks Security Attacks and Countermeasures”, International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 6, 2013, pp. 145 - 155, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[18] Neha Kaushik and Ajay Dureja, “A Comparative Study of Black Hole Attack in Manet”, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 4, Issue 2, 2013, pp. 93 - 102, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.

[19] Sharada Valiveti, Hetuk Upadhyay and Dr. K Kotecha, “Analyzing The Performance of Bandwidth Starvation Attack in Lan”, International Journal of Advanced Research in Engineering & Technology (IJARET), Volume 5, Issue 1, 2013, pp. 145 - 153, ISSN Print: 0976-6480, ISSN Online: 0976-6499.