A General Survey on Rushing Attack in MANETs

Prakash Kalita[1], James Deep Raj Hagjer[2] and Bobby Sharma[3]
[1,2,3]Don Bosco College of Engineering and Technology, Assam Don Bosco University
Airport Road, Azara, Guwahati - 781017, Assam. INDIA.
prakash.kalita@gmail.com, Jdraj.hagjer@gmail.com,esbobby@gmail.com

Abstract:*MANETs (Mobile Ad hoc Network) is a kind of network in which all the nodes are connected via wireless link. There is no fixed infrastructure because of which any node can join or leave the network at any point time. There is no central monitoring system. All the nodes are working as host as well as client at the same time. This makes the network vulnerable to different kind of attacks. Standard routing protocols are also not that secured to protect the network from all probable attacks. Attacker may attack the network and disrupt the network services abruptly. Some of the common attacks in MANETs are Rushing attack, Black hole attack, Sybil attack, Neighbor attack and Jellyfish attack etc. In this paper we are trying to accumulate different probabilities of getting rushing attack in MANETs. And also discuss about different counter measures to prevent as well as to detect rushing attack.*

Keywords: Rushing attack, MANETs, Security, Denial of Service (DoS), Security threats.

1. Introduction

Mobile ad hoc network is a collection of mobile nodes that communicates amongst themselves in a wireless media. If any node wants to communicate with any other node routing protocol finds a path between the nodes. Nodes forward packets in hop by hop fashion. Entire communication depends on node cooperation. It is a infrastructureless network. Basically such kind of networks are established in some places where it is very difficult to establish infrastructure or infrastructure is damaged due to some disaster. Usually such kind of networks are run in some untrusted environment. So, security becomes most essential part of routing.

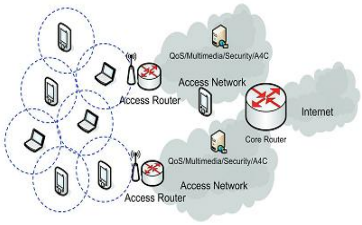

Figure 1. A MANET structure [From Web]

Structure of MANETs is shown in Figure 1. MANET routing protocols can be classified as either proactive or reactive. Reactive routing protocols such as AODV and DSR are now considered more effective and scalable compared to their proactive counterparts such as OLSR, because they have less routing overhead. AODV and DSR are designed under the assumption that all nodes trust each other and there are no malicious intruder nodes in the network. Therefore, the presence of any such node imposes security challenges. Hybrid protocol is a mix of both proactive and reactive protocol. Figure 2 shows the classification of protocol.

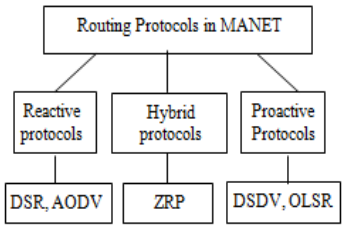

Figure 2. Routing protocols [From Web]

Rushing attack is a kind of routing attack. Figure 3 is a depiction of a simple rushing attack. It shows, when the sender sends a route request packet (RR packet) to another node in the wireless network. The attacker accepts the RR packet and send to its neighbor with high transmission speed as compared to other nodes present in the wireless network. Destination node accepts this RR packet and drop other RR packets. As a result, receiver adopts this route as a valid routeand starts communication via this route. This helps the attacker to successfully gain access in the communication between sender and receiver.

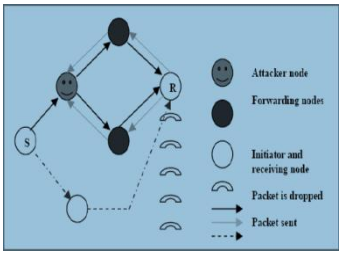

Figure 3. A simple rushing attack [From Web]

2. Literature Review

In paper [1], the authors have studied the different MANET's security issues, and have shown that the features of this new environment make it more vulnerable to threats. The solutions developed for standard networks are often unsuitable in this environment. The threats are divided into two categories; attacks and misbehavior. DjamelDjenourix and NadjibBadachez, have presented how the attacks can affect the MANET's security in different layers, especially in the network and the Medium Access Control (MAC) layers. For the network layer, the authors have presented different kinds of attacks on routing protocol and have classified and discussed the proposed solutions . The paper also presented the key distribution issue that can be an underlying mechanism for securing both lower and upper layers, and finally Intrusion Detection Systems (IDSs) that are essential when preventive measures fail. The authors think securing ad hoc networks is a great challenge that include many open problems of research, and receives more and more attention among ad hoc networks community. In paper [2], the authors presented RAP (Rushing Attack Prevention), a new protocol that thwarts the rushing attack. They found that the widely

used duplicate suppression technique makes the rushing attack possible, and designed a new Route Discovery protocol called RAP that came with a new proposal to prevent the rushing attack.. Though RAP incurs higher overhead than the standard route discovery techniques, still it is more efficient than other existing standard protocols. This paper also shows that the existing on-demand routing protocols can be retrofitted using the proposed technique to resist the rushing attack. In paper [3], the authors propose a generalized intrusion detection and prevention (GIDP) mechanism. The author combined both the anomaly based and knowledge based intrusion detection system to secure the network. It is also capable to detect new unforeseen attack. Simulation results for a specific case shows that the proposed mechanism can successfully detect attacks.The authors also investigate the impact on the MANETs performance of the various attacks and the type of intrusion response, and demonstrate the need for an adaptive intrusion response.In paper [4], the authors proposed a security framework called ECCEA by incorporating security aspects into the AODV protocol to provide data integrity and authentication against the adversary effects. The simulation results show that ECCEA outperforms AODV in terms of Packet Delivery Ratio, Average End-to-End Delay, Throughput, and Normalized Routing Load for different MANETs scenarios under adversary attack conditions. Simulation results proved that proposed ECCEA protocol outperforms the reputed AODV protocol by enhancing the Packet Delivery Ratio (PDR) from 20% to more than 85%. The newly proposed security scheme, built on top of normal AODV routing protocol, achieves an overall good results. Thus, the proposed scheme is successfully securing AODV routing protocol in defending against both malicious and unauthenticated nodes and also proved to be more efficient and less power consuming.

In paper [5], the authors V. Palanisamy and P. Annadurai,say that if the number of multicast receivers is large and/or the number of multicast sender is small, then such kind of attackers are seem to be more successful. Author found the best place to launch the rushing attack is at the near receiver. It shows the highest success rates. On the other hand, attack near sender have the low success rate and attack in anywhere in the network seem to be least success rate.In paper [6], the authors analyze the DSR and Secured Dynamic Source Routing (SDSR) protocols. This protocols have been designed to address rushing attack, to reduce overhead in the network and the time required. They also highlight the drawbacks and strengths of the Secured Dynamic Source Routing protocol, and finds that this is the best solution to address the rushing attack problem. The authors proposes two algorithms, that will reduce the overhead and time in the DSR and SDSR protocol and ensure all neighbors in the network are receiving safe data.

3. Analysis of Results

Below is some analysis of counter measures for rushing attack as mentioned in [8],

Table 1. Strength and weakness of different counter measures

Counter measures	Strength	Weakness
Firewall as semitransparent Gateway	No delays introduced for legitimate connections	It is necessary to select the timeout period in such a way that access is not denied to legitimate connections with long response times.
Firewall as relay	Host is fully protected from DoS attacks and no spoofed SYN packets are received.	New delays are introduced for legitimate connections
Request dropping	In both low and high congestion, random dropping worked well by keeping client performance losses below 10%, even under very high spoofed SYN rates.	An attacker hardly denies a genuine connection request
Intrusion detection	ID systems are designed to detect violations to usage policies, virus activity, and pre-attack probes, and other malicious hacking activities	Any ID systems which are capable of retaliatory attacks, the ID system may be tricked into retaliating a host that has not perpetrated any attacks

Elliptic Curve Cryptography Enabled AODV (ECCEA) [4]. It provides security features such as integrity, authentication, confidentiality and nonrepudiation of routing data. The simulation results prove that proposed ECCEA protocol outperforms the reputed AODV protocol by enhancing the Packet Delivery Ratio (PDR) from 20% to more than 85%. The simulation results also showed that the new protocol ECCEA drastically double the throughput and less Normalized Routing Load against AODV protocol under attack scenarios. As mentioned in [7], in cluster based intrusion detection technique, using the cluster formation protocols described above, a cluster head is selected to perform IDS functions for the whole cluster. It instructs the cluster citizens on how the feature computation is to take place. After cluster formulation the following criteria are the measured using LFSS (Local Feature Set Scheme) and CLFSS (Cluster head-Assisted Local Feature Set Scheme). Comparison of both LFSS and CLFSS with respect to CPU usage speed up network overhead and detection accuracy are given below in Table 2,

TABLE 2.COMPARISON OF LFSS AND CLFSS

Scheme	CPU usage speed-up	Network Overhead	Detection accuracy
LFSS	1%	>1400 Kbytes	87%
CLFSS	1.5%	>200 Kbytes	84%

Generalized Intrusion Detection Technique is tested under two scenarios according to the number of nodes present in the network.[3]

TABLE 3.4.ANALYSIS OF GENERALIZED INTRUSION DETECTION TECHNIQUE (GIDP)

	Success Rate		False Positive	
	25 nodes	50 nodes	25 nodes	50 nodes
GIDP	95%	90%	7%	10%

4. Conclusion

In MANETs, considerable amount of interest has recently been devoted to propose mechanisms to enforce security. Many proposals have been made in the literature to secure MANETs from various attacks.

The results show that all the various techniques applied by the researchers are good enough to prevent and detect the rushing attacks and along with it various other attacks. In Rushing attack, the attacker utilize the duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group. This affects the average attack success rate. As a result, the network performance parameters degrade in various way. In our future work, we will try to propose an algorithm by which rushing attack can be controlled

References

[1] DjamelDjenourix, NadjibBadachez, "A Survey on Security Issues in Mobile Ad hoc Networks," Laboratoire des Systemes informatics, February 2004, LSI-TR054.

[2] YihChunHu, Adrian Perrig, David B. Jhonson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, MobiCom 2002, pages 12–23, September 2002.

[3] Adnan Nadeem, Michael Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system," Telecommunication Systems, April 2013, Volume 52, Issue 4, Date: 27 Jul 2011.

[4] B. Prabhakara Reddy, Dr. M. N. Giri Prasad, "Efficient Lightweight Hybrid Cryptography Solution to Secure Mobile Ad hoc Networks," International Journal of Research in Computer andCommunication Technology, Vol 3, Issue 3, March- 2014, ISSN 2320-5156.

[5] V. Palanisamy, P. Annadurai, "Impact of Rushing attack on Multicast in Mobile Ad Hoc Network," International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[6] Aakanksha Jain, SamidhaDwivedi Sharma, "An Efficient Rushing Attack Prevention Algorithm for MANETs Using Random Route Selection," International Journal of Science and Research (IJSR),ISSN (Online): 2319-7064.

[7] Yi-an Huang, Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc

[8] Networks," Proceedings of the 23rd International Conference on Distributed Computing Systems, Providence, RI, May 2003.

[9] Safdar Ali Soomro, Sajjad Ahmed Soomro, Abdul GhafoorMemon, Abdul Baqi, "Denial of Service Attacks in Wireless Ad hoc Networks," Journal of Information & Communication Technology, Vol. 4, No. 2, (Fall 2010) 01-10

[10] K. Tamizarasu, A.M. Kalpana, Dr. M. Rajaram, "Maliciousness in mobile ad hoc networks: aperformance evaluation," Journal of Theoretical and Applied Information Technology, 31st July 2014. Vol. 65 No.3, ISSN: 1992-8645, E-ISSN: 1817-3195

[11] G.S. Mamatha, Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETS," International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010, 1793-8201

[12] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security

[13] Measures in Mobile Ad-Hoc Networks," Journal of computing, volume 3, issue 1, January 2011, ISSN 2151-9617.

[14] DeepeshNamdev, Monika Mehra, "Detection Approach for Denial of Service Attack in Dynamic Wireless Networks," Journal of Electronics and Communication Engineering Research, Volume 2 ~ Issue 6(2014), pp. 01-06 ISSN (Online): 2321-5941.

Authors Profile

Dr. Bobby Sharma is a faculty member of Dept. of Computer Science and Engineering & Information Technology of School of Technology, Assam Don Bosco University. Prior to this she was a faculty member of Dibrugarh university. Her subjects of interest are Computer Network Security, Artificial Intelligence, Compiler Design.

Mr. Prakash Kalita was a student of Dept. of Computer Science and Engineering & Information Technology, School of Technology, Assam Don Bosco University .His subjects of interest are Computer Network Security, Artificial Intelligence, Compiler Design.

Mr. James Deep Raj Hagjer was a student of Dept. of Computer Science and Engineering & Information Technology, School of Technology, Assam Don Bosco University.His subjects of interest are Computer Network Security, Artificial Intelligence, Compiler Design.