Study of Performance Under Attack for ZRP Protocol Compared to DSR Protocol In MANET

Er. Namisha
M. Tech. Student
Department of Computer Science & Engineering
GIMT, Kanipla

Er. Sahil Batra
Assistant Professor
Department of Computer Science & Engineering
GIMT, Kanipla

Abstract

Mobile Ad-hoc network is characterized by Infrastructure Less nature. It is a collection of wireless mobile nodes dynamically forming a temporary network. Each node in MANETs can act as a router or host on the network. The nodes are free to move randomly. Mobile ad hoc networks (MANET) are characterized by rapid change, dynamic multi-hop topology. The main types of routing strategies are proactive, reactive and hybrid. Traditionally, routing protocols for ad-hoc wireless networks provide a non-adversarial environment and an environment of cooperative network. In practice, there may be malicious nodes seeking to disrupt network communication by the attacks launched in the network or the routing protocol itself.. The variation of the transmit power causes more fatal and difficult to detect the Sybil attack. In this paper, the Sybil attack is applied in two protocols viz. DSR and ZRP. Comparison of these two protocols under attack is made to analyze the behavior of the proactive and reactive protocol under attack.This paper, is a contribution in the field of MANET security and their requirements of applications. To access limitations, the mobile nodes have been studied in order to design a secure routing towards different kinds of attack.

Keywords: Mobile Ad Hoc Network, Network Security, Sybil Attack

I. INTRODUCTION

Most computers communicate with one another through the use of cable networks. This approach is well suited for desktop computers, but not suitable for mobile devices. Mobile devices can use wireless networks almost anywhere and anytime using one or more wireless networking technologies, such as mobile ad-hoc networks. An ad-hoc cooperative coupling network is a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. Are Mobile nodes communicate directly via wireless links within radio range, while these being distant depend on other nodes to transmit messages. Mobile networks were of primary interest in military communications and disaster relief because of their "The infrastructure-less" nature. However, in the last decade these networks won popularity as personal area networks and civil networks. One of the most demanding and challenging aspects of ad-hoc networks is routing. Routing can be defined as the process of finding a path from the source to the destination to deliver packets to the destination nodes while network nodes They move freely. Therefore, each node acts as a router and an end node or to retransmit receiving packets in the network [46]. Routing is a difficult task in mobile ad-hoc networks due to many reasons such as node mobility, lack of predefined infrastructure, media and within limited range of peer-to-peer. Actually, there is no standard for a routing protocol for ad-hoc networks, however it is a work in progress.

Secure routing is also a vital factor for ad-hoc mobile networks, due to the sensitive applications of these networks. However, achieving security objectives, such as confidentiality, authentication, integrity, availability and access control in these networks is a difficult task. In general, a mobile ad-hoc network is especially vulnerable to attack by its key features half open, dynamic topology, distributed cooperation, limited capacity, and the absence of center authorities.Security is also a major concern in the ad hoc mobile networks. The use of wireless channel open and shared broadcast brings new security challenges in MANETs. Moreover, due to the distributed nature of the network, the centralized security control is difficult to implement. These characteristics of MANET pose challenges and opportunities in achieving security objectives, such as confidentiality, authentication, integrity, availability, access control and non-repudiation.

There is a wide variety of attacks that target weak MANET routing protocols. The most sophisticated and subtle attacks routing have been identified in some recently published as Blackhole [4] documents, Rushing [5], Byzantine [6], wormhole [7] and Sybil [8] attack, etc. Sybil attack is an attack [8] in which a malicious node asserts multiple identities illegally impersonating other nodes or by claiming fictitious identities. Sybil attacks are also able to alter the routing mechanisms in mobile ad hoc networks. Karlof and Wagner have been shown in [9] multipath routing and geographic routing plans are affected by this attack. If multi-path routing, there is a possibility that a supposedly set of paths may be disjoint passing through multiple identities Sybil of a single malicious node. Instead based routing a malicious node can have multiple nodes with different positions Sybil his neighbors.Therefore a legitimate node can choose any of the Sybil nodes while sending the packet at the base of the nearest location to the destination node; but in fact the packets are passed through the malicious node.

II. RELATED WORK

Sybil attack was first introduced by J. R. Douceur [8]. According to Douceur, the Sybil attack enables the attacker to control a substantial fraction of the sstem by representing itself as multiple identities in the network [8].

In other words, a simple presentation of multiple identities for a single physical node can be considered to be a Sybil attack. The Sybil attack can occur in a distributed system that operates without a central authority to verity the identities of each communicating entity.

III. RESEARCH OBJECTIVES

The following steps are followed to implement the attack.

1) VANET is designed to perform attack.
2) A VANET node which represent the attacker is appointed to perform the Sybil attack.
3) This network scenario is not changed in any of the case.
4) The attack is performed under running VANET.
5) At first the DSR protocol is applied on the VANET for analysis.
6) After this the ZRP protocol is applied on the VANET for analysis.
7) The comparisons are made by using the XGRAPH and creating dat files from the trace file generated by the simulation of the network.
8) The comparison graphs are studied and analysed.

IV. RESULTS & ANALYSIS

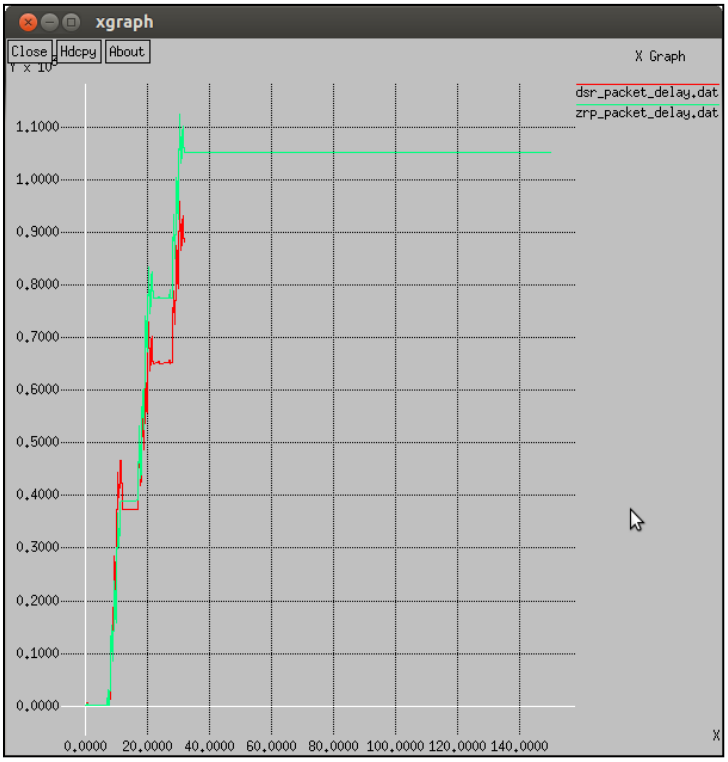

Fig. 1: Comaprison of Packet Delay for Two Types of Protocols

For the comparison purpose the four performance parameters i.e. packet delay, dropped packets, throughput, packet delivery ratio are compared for the two protocols DSR and ZRP. In the analysis phase the study is done while network under the Sybil attack for these two protocols and having the same network configuration i.e. network topology, number of nodes, number of cbr agents, number of null agents, the connections between source and destination nodes and connection patterns for these connections. Fig 1 shows the comparison of the packet delay for these two protocols. The green plot is for ZRP and red Plot is for DSR. The convention of having these colors is followed for remaining three graphs.Packet delay performance is approximately similar as the plot for these two is similar in the Fig 1.

Dropped packet for ZRP is greater than that of DSR as the plot for it is dominates the red line throughout the graph. In Fig 3, throughput comparison summarizes the overall performance as the plot for throughput is having higher values for DSR as

compared to ZRP. In Fig 4, packet delivery ratio is plotted , In accordance with the throughput comparison the the plot of DSR dominate the plot for ZRP.

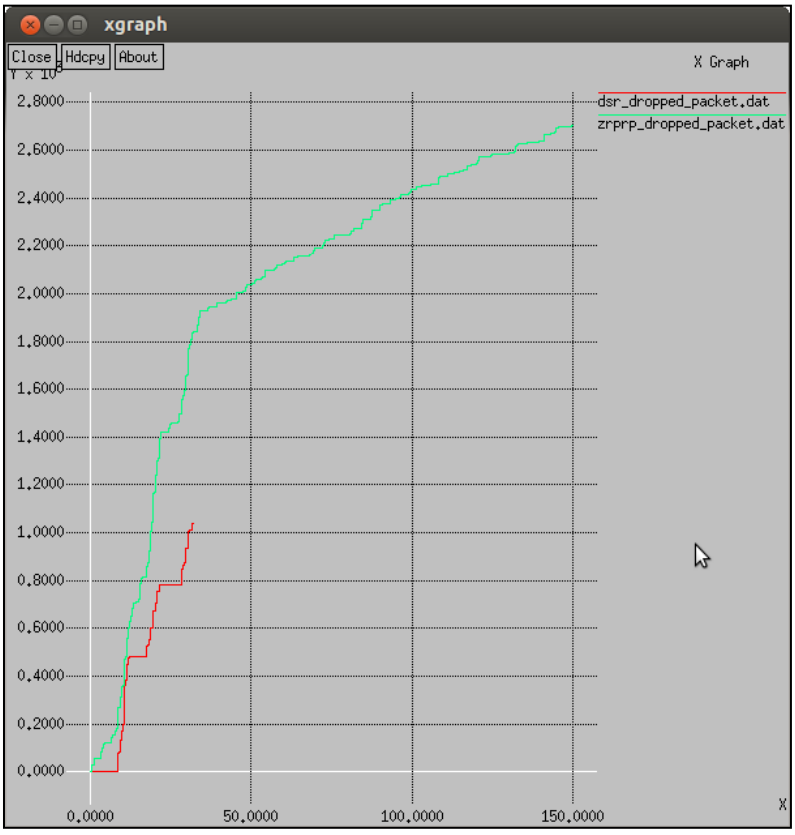

Fig 2:- Comparison of Dropped Packets for Two Types of Protocols

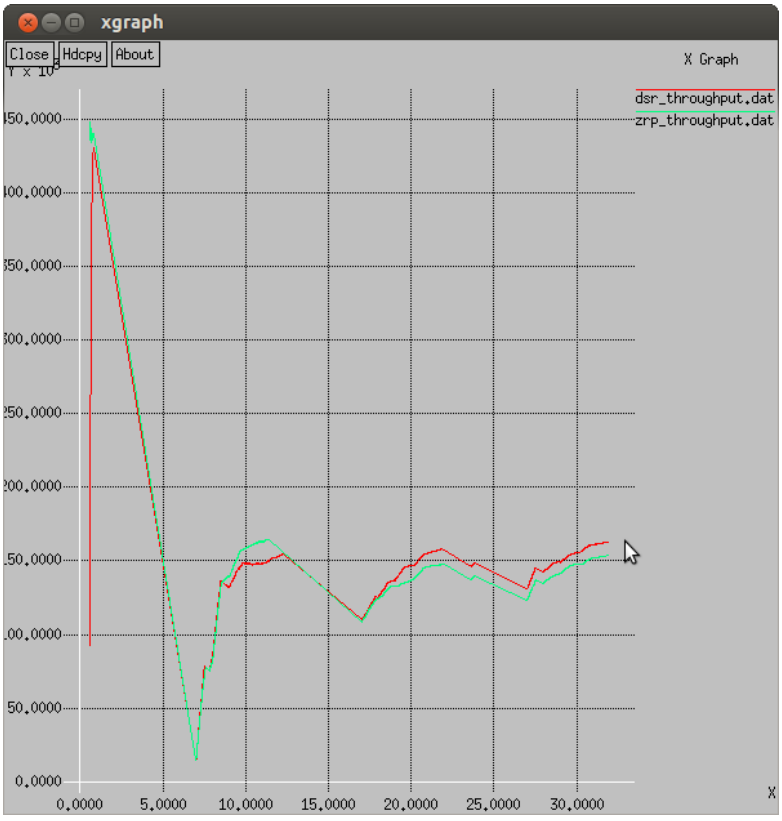

Fig. 3: Comparison of Throughput of Two Types of Protocols

Fig. 4: Comparison of Packet Delivery Ratio for Two Types of Protocols

V. CONCLUSION

The Sybil attack is made misleading packets to a node that is not authorized for acceptance. The robustness of a protocol can be measured by its ability to identify the exact destination of the package. The protocol, which is unable to detect the exact identity of destiny will be unable to resist this attack. The change of identity may be conducted on the network now depends only on the protocol to allow the route change is not identifying the newly generated node on the network that does not exist on the network. Due to the dynamic nature of ad hoc networks is an acceptable route training mechanism to adjust the network, according to adding new nodes and nodes prior removal. This characteristic of the MANET makes it hard to resist this type of attack without any external mechanism.

REFERENCES

[1] C. -K. Toh, (2002), "Ad Hoc Mobile Wireless Networks: Protocols and Systems", Prentice Hall PTR.
[2] E. M. Royer and C. -K. Toh, (1999), "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE Personal Communications.
[3] L. Buttyan and J. P. Hubaux, (2002), "Report on a working session on security in wireless ad hoc networks", Mobile Computing and Communications Review.
[4] M. Al-Shurman, S. -M. Yoo, and S. Park, (2004), "Black Hole Attack in Mobile Ad-Hoc Networks", ACM Southeast Regional Conference.
[5] Y. C. Hu, A. Perrig and D. B. Johnson, (2003), "Rushing Attacks and Defense in Wireless Ad Hoc Networks Routing Protocol", In Proceedings of ACM WiSe2003.
[6] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, (2002), "An On-demand Secure Routing Protocol Resilient to Byzantine Failures", Proceedings of the ACM Workshop on Wireless Security, pp. 21-30.
[7] Y. Hu, A. Perrig and D. Johnson, (2002), "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", Proc. of IEEE Infocom.
[8] J. R Douceur, (2002), "The Sybil Attack", IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251–260, Springer Verlag, London, UK. [9] C. Karlof and D. Wagner, (2003), "Secure routing in wireless sensor networks: Attacks and Countermeasures", Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, Vol. 1, No. 2-3, pp. 293-315.