PERFORMANCE INVESTIGATION OF RE-SHUFFLING PACKET ATTACK ON TRANSPORT LAYER PROTOCOL IN MANET

Sonia Choudhary[1], Vandna Verma[2]

[1, 2]*Department of Computer Science and Engineering, Rajasthan College of Engineering for Women, Jaipur, Rajasthan, India,* ***sonia.choudhary.14@gmail.com, vermamtech@gmail.com***

Abstract

Over the past decade, the wireless world has experienced significant developments. The emergence and proliferation of radio frequency networking products, wireless devices like handheld, wearable and portable computers, Personal Digital Assistants (PDA)s, cellular phone have given rise to a kind of wireless revolution. A mobile ad hoc network is much more assailable to attacks than a wired network due to its limited physical security, high mobility and lack of centralized administration. In this paper, we present and analyze the effects of re-shuffling attack on TCP based mobile ad-hoc networks named as Packet Re-Shuffling. In the packet reshuffling attack the malicious node will reorder the packets in its FIFO buffer before forwarding them towards their destination. Due to the out of order delivery the retransmission time out of the packet is triggered and the source TCP and UDP has to retransmit the packet. In this way it also stops the TCP to perform the congestion avoidance technique. A malicious node will always participate in route setup operations. For example, if source routing is employed, malicious nodes always relay Route Request packets in order to have as many routes as possible flowing through themselves; if distance vector routing is employed, malicious nodes will also obey all control-plane protocol specifications. However, once a route is established, attacking nodes will thwart the end-to-end throughput of the flow via above mentioned attacks. The effect of the proposed attack is analyzed with the simulation results generated using the trial version of the simulator known as Exata Cyber 2.0. The simulation results are given in terms of metrics such as data flow throughput, Packet Retransmission, average end-to-end delay and packet delivery ratio. In this paper, we are giving The study on UDP and TCP.

Keywords: *MANETs; Multimedia Streaming; Routing protocols; QoS; Topology; Node Mobility; Network Scalability;*

----------***----------

1. INTRODUCTION

MANET routing protocols in general lack security mechanisms. For proper operation of routing protocol, it is assumed that intermediate nodes included in routing paths are trustworthy and follow protocol rules. It is required that each node in the network generate and forward routing control traffic according to protocol specifications. Absolute trust on intermediate nodes is a significant issue in networks that are characterized by dynamic topology. It is comparatively easy to eavesdrop wireless communication and to physically capture and compromise legal nodes. Without appropriate network level or link-layer security provisions, routing protocols are susceptible to many form of malicious activity that can freeze the whole network. In this chapter we study various attacks that can be launched on MANETs by exploiting the vulnerabilities inherent in routing protocols. We study how basic routing protocol functions like packet or message forwarding and routing can easily jeopardize the whole network.

This paper is organized in the following manner. In Section II, we present the related work done in our area which includes the papers that are proposed the effective routing methods. This is followed by the proposed work for efficient routing for delay-sensitive applications in Section III. We also summarize the key features, basic operation, as well as major pros and cons of our proposed approach. In Section IV, We will conclude the paper with present state of the art and future work.

2. RELATED WORK

In this section, we discuss the past works done in MANET that includes the evolution of many new attacks. It is imperative to secure networks - wired or wireless for its proper functioning. Wireless ad hoc network is more vulnerable to security threats than wired network due to inherent characteristics and system constraints. The nodes are free to join, move and leave the network making it susceptible to attacks - both from inside or outside the network. The attacks can be launched by nodes within radio range or through compromised nodes. The compromised nodes exploit the flaws and inconsistencies present in routing protocol to destroy normal routing operation of the network. A compromised node may advertise nonexistent or fake links or flood honest nodes with routing traffic causing Denial of Service (DoS) attacks that may severely degrade network

performance. Thus we see that routing protocols are one of the main areas of vulnerability. There is a need to study the vulnerabilities in routing protocols that may be exploited by malicious nodes to launch attacks.

In [1] and [2], the attack is one of the most serious attacks on MANETs. In wormhole attack at least two attackers are required to perform the attack very effectively. These two attackers resides on different areas of the network makes a tunnel through the network to communicate with each other. The attackers broadcast the wrong information to the other nodes in the network that the destination is only one hop away from them. Sometimes they also broadcast the wrong information that they are true neighbors of each other due to this the attacker one which is near to source node is easily selected on the route between the source destination pair when the route is discovered on the basis of lowest number of hops on the route.

In [3], the attacker when received a route request (RREQ) message it modifies the sequence number in the RREQ message to perform the attack. The attacker increases the sequence number more than the usual number and reply back to the source to make it believe that it has the better and fresher route to the destination node. Once the source node got this reply it start the transmission of data packet on the route which consists of the attacker i.e., one of the intermediate node of the established route is the attacker. Till now half of the attack is performed by the attacker by spreading the false information and making himself the part of the route. Now when the data communication is started using the route the attacker will drop all the data packets that reaches to it that is when the attacker got the data packet for forwarding it drops the packet without forwarding any of the data packets.

In [4], Flooding attack is the simplest attack to implement but it is one of the most dangerous attacks. In this attack, the attacker broadcast the false control or data packets in the network due to which the network bandwidth is wasted largely and the non-false packets are not able to reach their destinations.

In [5]: As the communication in MANETs is multi hop therefore the intermediate nodes plays an important role in data communication over MANETs. The intermediate nodes can become selfish by either using the wireless channel unnecessary due to which the other nearby channels has to contend more time to access the channel.

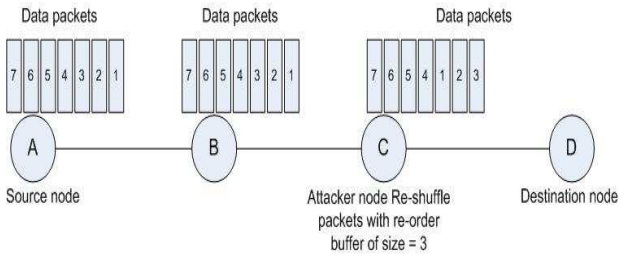
In [6] has analyzed the impact of packet re-ordering attack over various TCP-variants using the MANET routing protocols named AODV and DSR. Although authors claim that they have investigated various versions of TCP but the simulation results show graphs for TCP-Reno and TCP-NewReno. Furthermore, the effect of packet re-ordering is not analyzed in UDP-based data communications. Also, the author's uses only network throughput as an metric for the performance evaluation but other important metric such as number of retransmissions which greatly increases network congestion and delay in the network is not examined. Finally, it is not understandable that why the authors uses and compares AODV and DSR routing protocols in his paper because the re-ordering attack is used to effect the close-loop attacks only and are independent on the underlying protocol used for the routing.

3. PROPOSED METHODOLOGY

In proposed Re-shuffling data packet attack (RSA) an attacker node re-ordered a specified number of packets using a re-ordering buffer whose size is either selected randomly every time the buffer is empty or its size can be fixed at the start of the data communication and kept constant throughout the whole communication duration. To perform this attack the attacker node should be one of the intermediate nodes on the route between the source destination pair. The attacker can perform the proposed Re-shuffling data packet attack (RSA) using any one of the following two approaches:

a) In this method, the attacker node uses a fixed size of buffer and wait till the number of packets are equal to the size of the buffer once the number of data packets are equal to the used re-order buffer size the attacker shuffles all the packets and forward them one-by-one. For example, if the re-order buffer size is set to 3 then as soon as the re-order buffer has 3 data packets stored in it the attacker shuffles them in any random or predefined order and forward the data packets.

b) In the second method, the attacker node may vary the size of the reorder buffer during the communication duration and uses a random re-order buffer size for some duration while uses some other size for the rest or some other period. In this way, the attacker makes itself more secure from the detection mechanisms if applied by the source node to detect the attackers. To perform any attack method either first or second the attacker should be one of the intermediate nodes on the active TCP or UDP based route using for data communication process.



Pseudo Code for proposed Delay-Aware Routing Protocol

Processing of Data Packet Received by an Attacker Node

Shorthand used in the Algorithm:
////////////////////////////////////
S = Source node
D = Destination node
A = Attacker node
I = Intermediate node
IP_OQ(N) = IP output queue of node N
RO_buffer_size = x; where x is between 1 to 5
////////////////////////////////////
IF1 (*I* got a data packet)
I check its AODV routing table
IF2 (Route is present in the routing table)
IF3 (*I* != *A*)
I forward the data packets from its IP output queue using FIFO approach towards *D*
ELSE //this node is an attacker node
A checks whether the IP output queue has number of data packets that are greater than or equals to its RO_buffer_size
IF4 (RO_buffer_size (A) >= number of packets in IP_OQ(A))
A either send the data packet or it pauses the data packet till the re-shuffle buffer of its IP output queue is filled with the required packets
ELSE //attackers re-shuffle buffer is full
A re-shuffle the data packets either using a fixed re-order pattern or randomly
After re-shuffling send the packets from the re-order buffer using FIFO approach
ENDIF4
ENDIF3
ENDIF2
ENDIF1

4. SIMULATION RESULTS AND PERFORMANCE EVALUATION

In this section, we present the detailed performance analysis and impact analysis of the proposed Re-shuffling data packet attack (RSA) on different variants of TCP protocol over mobile ad-hoc networks. The network scenarios used in the simulation process are designed in such a way so that the effects of the wireless channel and environment can be mitigated. This is done to discover the exact impact of Re-shuffling data packet attack on the TCP-based MANETs. Therefore, we ignore the congestion and mobility induced situation from the network scenarios used for simulation process. As already mentioned above that the network simulator used for the simulation process is the trail version of the well knows network simulator called EXata.

Table1. Simulation Parameter Table

Parameters	Values
Simulator	EXata
Network Size	900 x 900 meter square
Simulation time	750 Seconds
Application Layer Process	File transfer protocol (FTP)
Transport Layer Protocols	TCP (Tahoe, Reno, NewReno) and UDP
Routing protocol	AODV, DSR, OLSR
Number of Nodes	30
Mobility model	None
MAC specification	IEEE 802.11
Network Bandwidth	15 Mbps
Performance Metrics	Network Throughput, Packet Delivery Ratio end-to-end delay and Number of Retransmissions
PHY Specification	802.11a/g
Parameters	Values

A .Simulation Setup

Furthermore, the performance measurement metrics used are as follows and the graphs will show that the attack is independent from the effect of routing protocol on both TCP as well as UDP:

a) **Network throughput:** The network throughput is defined as the ratio of the total number of data bytes received to the total duration of the communication process.
b) **Packet delivery ratio (PDR):** The ratio of the application data packets that are received without any error at destination nodes to the total data packets generated by the CBR sources are called Packet delivery ratio (PDR) of the network.
c) **Average end-to-end delay of data packets:** This metric is calculated by the destination node whenever it receives a data packet. The destination node will calculate the delay of each received data packet by using its send timestamp and its received timestamp at the destination.
d) **Number of retransmission (NOR):** This is the important evaluation metric as we are using TCP-based MANETs. In TCP a data packet is re-transmitted when its retransmission timer expires or the TCP receives the three acknowledgment packets for the same data packet. These retransmissions waste network bandwidth and lead to lower network throughput.

B. Performance Evaluation

1. Effects of Increase in Re-Shuffle Buffer Size

In this section, the effects of increase in the size of the re-shuffle buffer of an attacker node are analyzed using the two metrics (i.e., network throughput and number of retransmissions).

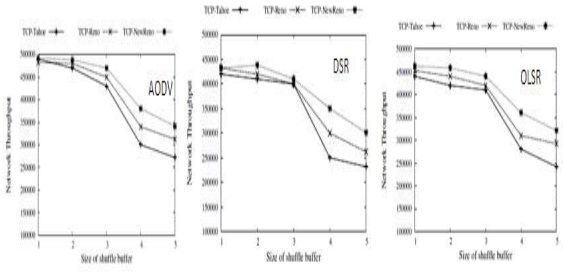


Fig.1 Network throughputs with increase in shuffle size when using all three routing protocols (TCP-based MANETs)

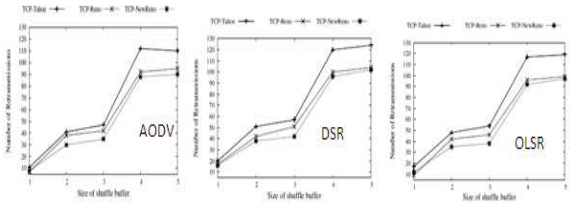


Fig.2 Number of Retransmissions with increase in shuffle size when using all three routing protocols (TCP-based MANETs)

2. Effects of Increase Number of Attackers in TCP-Based Manets

In this section, we analyze the performance of three TCP protocol variants with the increase in the number of attackers in an active route between any source-destination pair. The metrics used for the analysis are network throughput and number of re-transmissions caused during the whole duration of data communication of a data session.

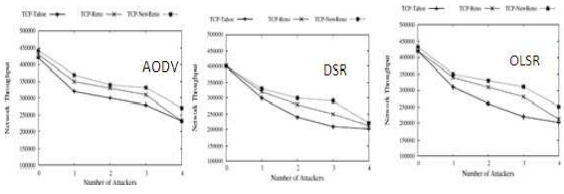


Fig.3 Network throughputs with increase in number of attackers when using all three routing protocols (TCP-based MANETs)

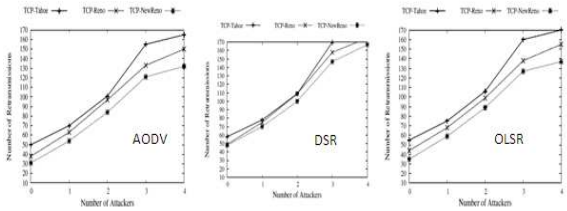


Fig.4 Number of Retransmissions with increase in number of attackers when using all three routing protocols (TCP-based MANETs)

3. Effects of Increase Number of Attackers in UDP-Based Manets

In the previous section, we have shown the effect of the proposed attack on TCP-based transmissions over mobile ad-hoc networks. In this section, we analyze the effects of the proposed attack on the UDP-based transmissions. As we are using UDP as a transport layer protocol therefore there is no re-transmission of data packets so we have used different metrics to analyze the effects of our proposed attack on the source-destination pair and overall network.

To show through the simulation process that the attack is independent on the routing protocol used, we have also configure the OLSR and DSR as the routing protocols in conjunction with the AODV protocol and the results are given below. This change is due to their different types of route discovery methods used for route discovery and different levels of routing overhead. These factors affect the network metrics values.

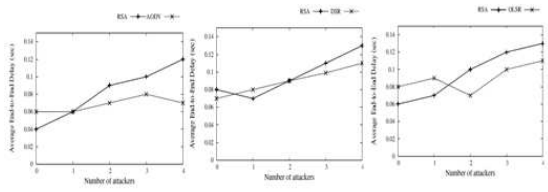


Figure 5 End-to-end delays with increase in number of attackers in all three routing protocols (UDP-based MANETs)

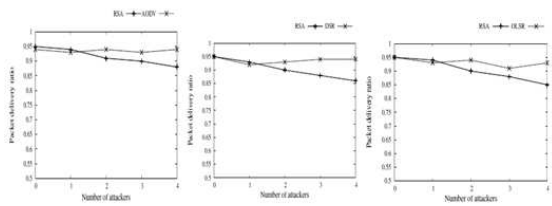


Figure 6: End-to-end delay with increase in number of attackers in all three routing protocols (UDP-based MANETs)

5. PROPOSED DETECTION METHOD FOR RE-SHUFFLING DATA PACKET ATTACK

In this section, we will propose an efficient yet simple method to detect the proposed Re-shuffling data packet attack. The source node TCP protocol uses the time-stamps to detect whether the re-transmission done by it is a false or true re-transmission. If the re-transmission done by the source is true than the TCP will work in the traditional way by applying its methods to control the congestion and network flow rates. On the other hand, if the re-transmission is detected as a false re-transmission the source TCP will not enter into the congestion control states. Due to this the network throughput of the network is maintained during the attack periods.

The proposed method for the detection weather the current re-transmission at the source is true or false type is explained below with the help of the Figure

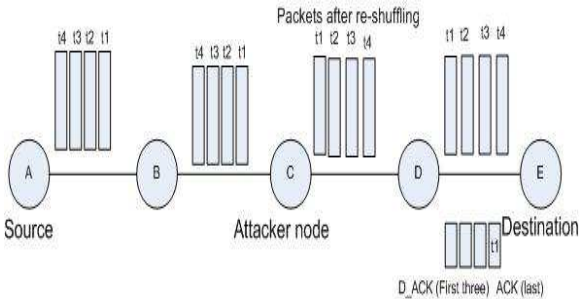


Figure 7 Detection methods for packet re-shuffling attack

When the source TCP sends a data packet, it also places a time-stamp in that data packet. The value of the time stamp is set equal to the current system time when the data packet is transmitted into the network. Let's assume that node A sends four data packets with the time stamps t1, t2, t3 and t4 respectively. As, it can be seen in Figure 4.13 that the attacker node re-shuffles the packets before forwarding them towards the destination node When the receiver node E receives the data packet with the time-stamped equal to t4 it generates the duplicate ACK because it is waiting for the data packet which has the timestamp equal to t1. In this way, the node E will generate three duplicate ACKs for the first three received out of order data packets.

CONCLUSIONS AND FUTURE WORK

In this section, we have presented the conclusion and future work for the paper. As we are using UDP as a transport layer protocol therefore there is no re-transmission of data packets so we have used different metrics to analyze the effects of our proposed attack on the source-destination pair and overall network. For this we have studied all forms of existing attacks over Mobile ad-hoc networks. The simulation results clearly show the impact of proposed attack on the network throughput, bandwidth wastage and received data quality. We have also seen that the proposed attack is independent on the underlying network protocol as the attack is done to interrupt the usual working of the TCP protocol. The attack exploits the TCP congestion avoidance algorithm and flow control process to disturb the regular data transmission process.

In the paper, we have analyzed the impact of packet re-ordering attack over various TCP-variants using the MANET routing protocols named AODV and DSR. Although authors claim that they have investigated various versions of TCP but the simulation results show graphs for TCP-Reno and TCP-NewReno. Furthermore, the effect of packet re-ordering is not analyzed in UDP-based data communications. Also, the author's uses only network throughput as an metric for the performance evaluation but other important metric such as number of retransmissions which greatly increases network congestion and delay in the network is not examined. Finally, it is not understandable that why the authors uses and compares AODV and DSR routing protocols in his paper because the re-ordering attack is used to effect the close-loop attacks only and are independent on the underlying protocol used for the routing.

REFERENCES

[1] George Hoffman, Yoko Ono, Akiko Kawakami, Kenichi Kusano, and Takashi Manabe Japan Communications 2012 Top 10 Predictions http://www.idc.com/getdoc.jsp?containerId=JP1376002U.

[2] Trends — Survey Says Wireless Net- works Expand for Mobile Growth. http://edtechdigest.wordpress.com/2011/10/18/trends-survey-says-wirele

[3] Raza, I. and Hussain, S.A. and Ali, A. and Hassan Raza, M. : Persistent packet reordering attack in TCP based Ad hoc wireless networks, Information and Emerging Technologies (ICIET), 2010 International Conference, 2010.

[4] C. Perkins and E. Royer. Ad hoc on-demand distance vector routing. 1999.

[5] A. Mishra, R. Jaiswal, and S. Sharma. A novel approach for detecting and eliminating cooperative black hole attack using advanced dri table in ad hoc network. In Advance Computing Conference (IACC), 2013 IEEE 3rd International, 2013.

[6] Yih-Chun Hu; Perrig, A.; Johnson, D.B., "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on , vol.24, no.2, pp.370,380, Feb. 2006.

[7] Hoang Lan Nguyen and Uyen Trang Nguyen. A study of different types of attacks in mobile ad hoc networks. In Electrical Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on, 2012.

[8] M.T.Refaei V.Srivastava L.Dasilva and M.Eltoweissy. A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In International Conference on Mobile and Ubiquitous Systems, Networking and Services, July 2005.

[9] Ping Yi; Zhoulin Dai; Yi-ping Zhong; Shiyong Zhang, "Resisting flooding attacks in ad hoc networks," Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on , vol.2, no., pp.657,662 Vol. 2, 4-6 April 2005.

[10] Carl, G.; Kesidis, G.; Brooks, R.R.; Rai, S., "Denial-of-service attack-detection techniques," Internet Computing, IEEE , vol.10, no.1, pp.82,89, Jan.-Feb. 2006.

[11] JOHNSON David B. The dynamic source routing protocol for mobile ad hoc networks (dsr). Internet-Draft, 2004.

[12] Chen, S., Nahrstedt, K.: Distributed quality-of-service routing in ad hoc networks. Selected Areas in Communications, IEEE Journal 17, 1488–1505 (1999).

[13] Zeadally, Sherali and Hunt, Ray and Chen, Yuh-Shyan and Irwin, Angela and Hassan, Aamir," Vehicular ad hoc networks (VANETS): status, results, and challenges", Telecommunication Systems, Springer US, 2012.

[14] Chakrabarti, S., Mishra, A.: QoS issues in ad hoc wireless networks. Communications Magazine, IEEE 39, 142–148 (2001).

[15] Imrich Chlamtac, Marco Conti, and Jennifer J.-N. Liu. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1):13 – 64, 2003.

[16] Tsu-Wei Chen and Gerla, M.: Global state routing: a new routing scheme for ad-hoc wireless networks, Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference.

[17] E.M. Royer and Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE, 6(2):46 –55, apr 1999.

[18] P. Jacquet, P. Mhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized link state routing protocol for ad hoc networks. 3626, 2001.

[19] Charles E. Perkins and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. SIGCOMM Comput. Commun. Rev., 24:234–244, October 1994.