ADVISEDLY DELAYED PACKET ATTACK ON TCP-BASED MOBILE AD-HOC NETWORKS

Romil Nehra[1], Narendra Yadav[2]

[1, 2]*Department of Computer Science and Engineering, Sri Balaji College of Engineering and Technology, Jaipur, Rajasthan, India,* ***romil.nehra@gmail.com, narensinghyadav@yahoo.com***

Abstract

Efficient routing in mobile ad-hoc networks (MANETs) is a challenging task due to its varying physical channel characteristics, dynamic topology and un-centralized communication. Furthermore, multihop routing is required when the source-destination pairs are not in each other's communication range. Due to the above challenges these networks are vulnerable to various types of attacks on various layers of the TCP/IP protocol stack. In this thesis, we implement and analyze an attack called advisedly delay packet attack on ad-hoc on-demand distance vector (AODV) routing protocol. The advisedly delay packet attack is an attack that effects the TCP-based as well as UDP-based data transmissions but in this thesis we will also see how it exploits the TCP congestion control mechanism to decrease the throughput of the network. In this attack, the attacker exploit the period of retransmission time out (RTO) of the sender and attack in such a way so the sender is always transmitting in the slow start phase.

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

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

1. INTRODUCTION

Mobile ad-hoc network is a dynamic network formed by independent system of randomly moving mobile nodes. Nodes are connected through wireless links without utilizing the existing network infrastructure or any form of centralized administration. Each node is able to communicate directly with nodes in its transmission range. For nodes outside communication range, intermediate nodes are used to relay the message hop by hop. Hence, such networks are called "multi-hop" networks.

In an ad-hoc network, it is required that a node forwards or routes data packets on behalf of other nodes. Each node, therefore, acts as a host and a router, necessitating use of routing protocols to make routing decisions. Many routing protocols have been proposed by the researchers. The biggest challenge for routing protocols is to establish and re-establish routes in the face of dynamically varying network topology and network partitions due to node mobility. Depending on how the mobile nodes acquire and maintain routing information, MANET routing protocols can be classified as either reactive or proactive.

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.

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 advisedly delayed data packets attack an attacker node delays some or all packets with randomly or selectively chosen delay periods during the data communication process. The attacker node should be one of the intermediate nodes on the route between the source destination pair to effectively perform this attack. The attacker can perform the proposed delaying attack in one of the following two ways:

a) The attacker can delay a percentage of the total number of packets it receives in a fixed amount of time all the delay time can be chosen same or differently over a range. For example, the attacker can delay 200 data packets from every 1000 data packets it receives for the forwarding towards the destination. Also, it can delay 100 packets from these 200 packets with the fixed delay period say 200 milliseconds while the other 100 packets are delayed by selected a random period from 100 to 300 milliseconds.

b) The second way in which the attacker node can perform the delayed attack is by delaying all data packets that are arrived for a fixed period of time each time from a fixed amount of time. For example, the attacker node will start delaying all the packets it receives in the first 100 milliseconds of every second. Again the delayed period can either be fixed or variable chosen from a given interval of time.

When the above mentioned packet delaying attack is performed on a data communication session that is transmitting data packets using the TCP protocol The following can be result: due to the data packets delays at intermediate nodes the retransmission time out of delayed data packets triggers their retransmissions at the source node either due to the time out of the RTO used by the source TCP.

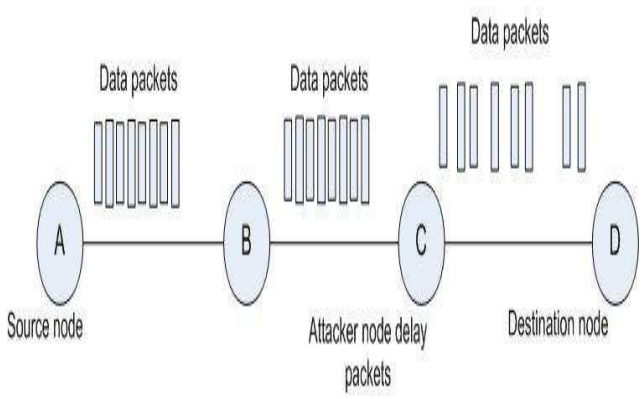

Figure1 Packet dropping attack

Pseudo Code for proposed Delay-Aware Routing Protocol

Processing of data packet received by an attacker node

Variable used:
////////////////////////////////////
S = Source node
D = Destination node
A = Attacker node
I = Intermediate node
T_window = time window from which the attacker node selects the delay period
T_period = delay duration selected randomly from the T_window
////////////////////////////////////
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 packet towards *D*
ELSE
WHILE (output queue has data packet to send)
A selects the T_period from T_window
A pauses the fetch function for next T_period duration
A forwards the data packet once the timer set at the time of the start of the fetch pause expires
ENDWHILE
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	800 x 800 meter square
Simulation time	700 Seconds
Application Layer Process	Generic File transfer protocol (FTP)
Transport Layer Protocols	TCP (Tahoe, Reno, NewReno) and UDP
Routing protocol	AODV
Number of Nodes	30
Mobility model	None
MAC specification	IEEE 802.11
Network Bandwidth	12 Mbps
Performance Metrics	Network Throughput, 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.

B. Performance Evaluation

1. Effects of Increase in Packet Delayed Period

In figure 2, we have shown the effects on network throughput for three variants of TCP protocol when the attacker increases its delay period time. As it can be seen from Figure 2 that the throughput of the network decreases with the increase in the delay period time because as the delay period of the data communication increases the number of data packets that are delayed intentionally instead of forwarding them without introducing any delay by the attacker also increases.

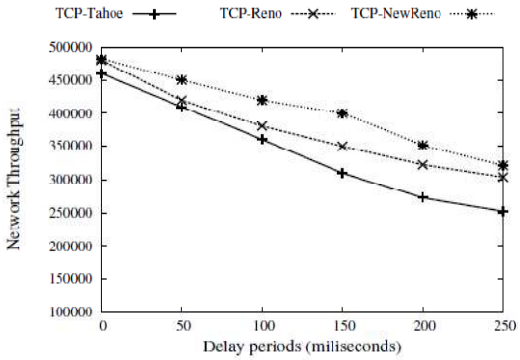

Figure 2 Throughput with increase in delayed period time of attackers (TCP-based MANET scenario)

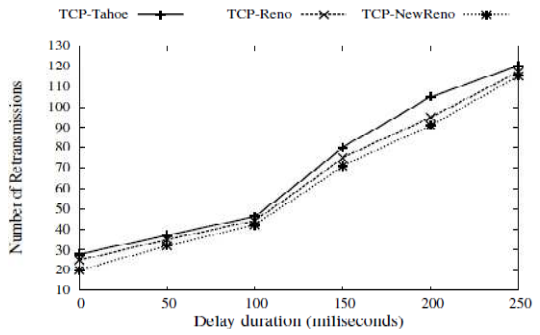

Figure 3 Number of retransmissions with increase in percentage drop time of attackers (TCP-based MANET scenario)

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.

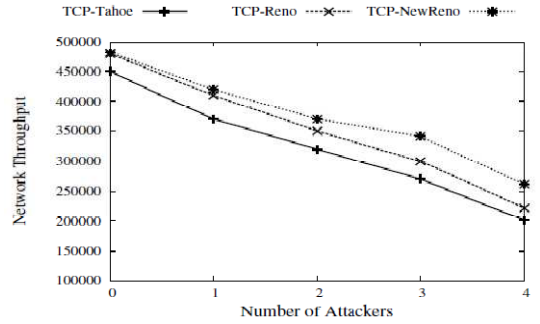

Figure 4 Throughput with increase in number of attackers on the route (TCP-based MANET scenario)

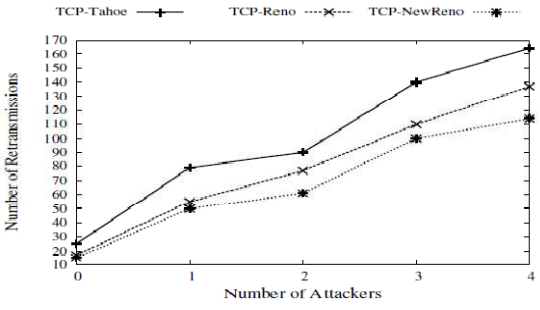

Figure 5 Number of retransmissions with increase in number of attackers on the route (TCP-based MANET scenario)

CONCLUSIONS AND FUTURE WORK

In this section, we have presented the conclusion and future work for the paper. To perform the work proposed in this thesis we start with the basics of the mobile ad-hoc networks. We have studied about the MANETs and its characteristics and its challenges and issues that are faced by the researchers when performing the routing over these networks. After the in-depth introduction of MANETs we started the related work which is similar to our proposed work in this thesis. For this we have studied all forms of existing attacks over Mobile ad-hoc networks. As it can be easily seen from the work presented in Chapter 4 that the proposed Advisedly Delaying Packet (ADP) attack is a simple yet very powerful denial of service (DoS) attack that is effective on both TCP and UDP based MANETs. The simulation results clearly show the impact of proposed attack on the network throughput, bandwidth wastage and end-to-end delay data quality. It has also been observed that even though the TCP congestion control is adaptable to the packet losses but in case of the forced delayed attack it is fully unable to detect whether the packet is dropped or delayed and these are the result of the attacker misbehaving or it is due to the congestion or other wireless environmental problem. 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.

For the future work, we will try to discover a detection mechanism for the attacker nodes so that they can be removed from further communications. Once detected the source node or network has to make sure that this attacker will not become the part of any active routes in the network. Also, we will try to figure out the other closely related attacks that can be possible to induce by a simple modification on our attack.

REFRENCES

[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=JP1376002 U.

[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.