VOL. 11, NO. 11, JUNE 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

HANDLING TCP-SESSION HIJACKING WITH TRANSPORT LAYER DEFENSE METHOD (TLD) IN MOBILE ADHOC NETWORKS

K. Geetha
Department of Computer Science, Periyar Arts College, Cuddalore, India
E-Mail: kl.geetha@gmail.com

ABSTRACT

Mobile Adhoc Networks (MANETs) play the vital role in communication. It makes one to get the complete utilization of ubiquitous computing. That is data can be accessed from anywhere at any time using any devices. As the facility by using the MANETs are increased, the complications and issues are also increased. The main support to be strengthened is security. A variety of attacks exist in MANETs. The major attack which affects any communication is the Session hijacking attack. It is a multilayer attack. But, it generally affects the transport layer exploiting transmission Control protocol (TCP). It takes away the session between the source and destination. It affects the confidentiality and the Quality Of service (QOS). The attack has several variants like Active attacks, Passive attacks and Hybrid attacks. An analysis is performed to handle these attacks. Since the MANET communications are multimedia oriented, the multimedia messages are considered for transmission and study. The QoS analyses reveal that the TLD Method performs well and minimizes the effect of the attack.

Keywords: active attacks, hybrid attacks, mobile adhoc networks, passive attacks, security, quality of service, session hijacking attack.

1. INTRODUCTION

An attack is the potential violation of security due to flaws in design, implementation and operation [1]. Attacks from the attack nodes are generated with the intention to affect the performance of other nodes. A variety of attacks are there affecting each layer of MANET. But, the basic attacks which will affect the communication and takes away the session established in between the source and destination is session hijacking attack. There exist a variety of approximations or variations to this attack. This work aims to consider a few variations of the attack like active, passive hybrid attacks and combines the handling methods in to one approach called Transport Layer Defense Method (TLD) is explained in this paper. The section 2 explains the attack and its effect on MANET. Section 3 gives the related work. The handling methods are explained in section 4. A simulation is explained and QoS parameters are analyzed with attack and with the handling methods. This is explained in section 5. Section 6 concludes the paper.

2. TCP - SESSION HIJACKING ATTACK

When the connection is established between the nodes, the attacker spoofs the victim's address and acts like the victim. He terminates or delays the communication which has been already established and takes away the connection. Then, the connection is established between the source and the attacker as shown in the Figure-1.

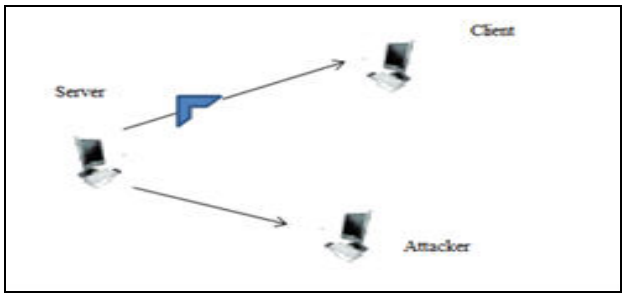

Figure-1. Session hijack scenario.

The TCP session hijacking attacks are launched by the attacker after knowing the sequence number in the TCP handshake and establishing the communication with the source by replacing existing connection with the destination. The source unaware of this sends the data continuously to an attacker instead of the actual client. The source unaware of this sends the data continuously to an attacker instead of the actual client. The following sequence of steps is carried out before a connection is established.

Step 1: The client sends a SYN request with i as the sequence number.
Step 2: The server acknowledges it with i+1 along with j with the next sequence number.
Step 3: Client then sends an acknowledgement to j with j+1 by incrementing the sequence number.

Guessing the sequence number is very easy by an attacker. The attacker after step 2 sends the next sequence number. If the attacker communicates at the same time sending SYN to the source node, which acknowledges to the client as well as to the attacker (the attacker uses the same IP address), makes the SYN RST to reset the connection. In order to avoid this, for a TCP session hijacking attack, the attacker tries to throw the client away

from the network. In such a case, the victim tries to communicate with the source repeatedly and the attacker has to throw away the victim every time. Instead of doing this, the attacker in turn establishes the communication with the victim and routes the data to the victim.

There are several variation of the attack exist. The session hijacking attacks may be passive, active or hybrid where the existing session may be taken away (active attacks), the existing session may be silently observed by the attacker and later the data may be used (Passive attacks) or the existing session may be watched and changes may be made in the data by the attacker (hybrid attack). In this type of session hijacking attacks the attacker takes away the session between the source and destination and starts communicating with the server by spoofing the address of the destination.

In active type of session hijacking attacks the attacker takes away the session between the source and destination and starts communicating with the server by spoofing the address of the destination. It behaves like the genuine client. Then, the attacker removes the client and establishes the connection with itself. This is given in the Figure-2.

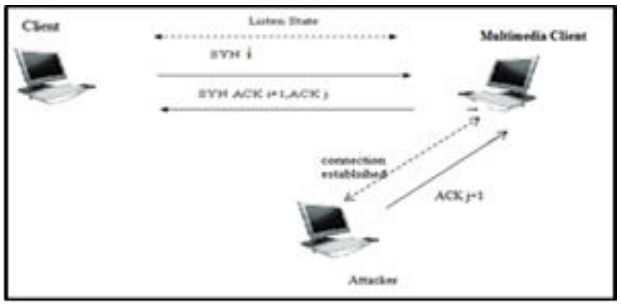

Figure-2. Active session Hijacking attack.

In passive session hijacking attacks, the attacker sniffs the traffic between the server and the client, and monitors the data exchange as in the Figure-3. Later the attacker use the information observed.

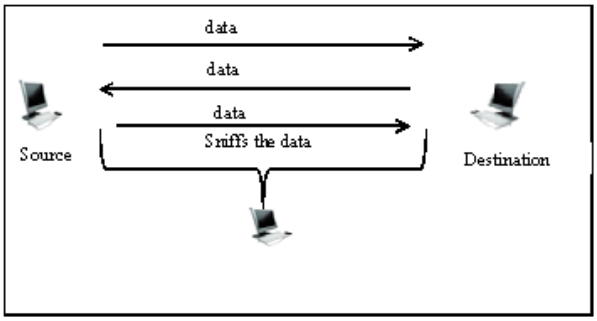

Figure-3. Passive session Hijacking attack.

Hybrid session hijacking attack is a combination of active and passive session hijacking attack. The attacker monitors the traffic between the source and the destination. If the attacker wants to replace the victim, then he takes away the session as shown in the Figure-3.

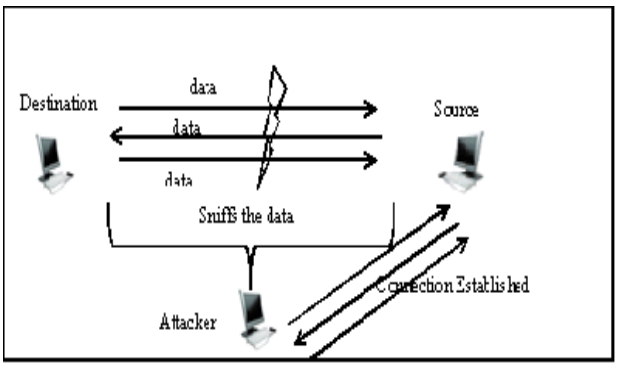

Figure-4. Hybrid session Hijacking attack.

3. RELATED WORK

Session hijacking attacks can be detected using sequence number analysis, transceiver finger printing and signal strength analysis [2]. Yong *et al.* [2] detect the attacks using received signal strength (RSS). The method identifies that the RSS readings follow a mixture of multiple Gaussian distributions Hall *et al.* [3] proposed to identify the attack using received radio frequency finger printing (RFF). Long *et al.* [4] proposed a method using continuous wavelet theory to identify the noise present in the signals received. Gill Rupinder *et al.* [5] used Received Signal Strength (RSS) and Round Trip Time values (RTT) to detect session hijacking attack. The RSS and RTT values are non spoofable characteristics of a nodeKai zeng *et al.* [6] devised an RSS based detection called Reciprocal Channel Variation based Identification (RCVI). Faria *et al.* [7] proposed a method to detect the session hijacking attacks using signal prints. Differential signal prints are used here. This increases the robustness of signal prints against various devices. Chen *et al.* [8] proposed a method based on statistical testing which utilizes the RSS values for detection. The RSS values are related to the transmitter's location.Under no attacks the RSS values of a transmitter will be close to each other and will not fluctuate too much. When there is hijacking or spoofing, the values vary very much from the mean and variance. Ahmad *et al.* [9] proposed a method which detects access points spoofing using partition based clustering. The client monitors and stores the profile of RSS values. These values collected from the same location fluctuate around a mean value. By applying clustering, the similar values are grouped. All the methods use the RSS values for finding the session hijacking attacks. These methods identify the spoofing at the MAC layer. The proposed method uses the transport layer and the TCP sequence number to prevent the attacks.

4. TRANSPORT LAYER DEFENCE METHOD (TLD METHOD)

The best way to handle the three session hijacking attack is to prevent the occurrence of the attacks. Figure-5 shows the concept of defence in our proposed method. It is divided in to three segments as shown in the Figure-5.

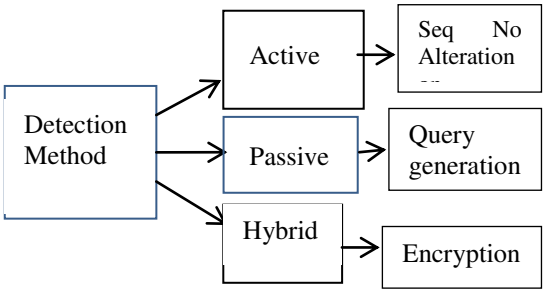

Figure-5. Transport layer defence method.

4.1 Active attacks defense

The active session hijacking occurs by replacing the victim after getting the sequence number sent along with the SYN requests. To avoid the guessing of numbers, the sequence number can be altered by the Multimedia source. For example, the number can be shifted left and incremented one as given in Figures 6(a) and 6(b). In Figure 6(b) the SYN with number 1 is sent from the client to source node. The acknowledgement 2 is given along with new SYN 5 generated from the source node. The client acknowledges by sending 6 as acknowledgement sequence number. By using the prevention method the sequence number 1 is shifted to the left and is incremented which yields 3.

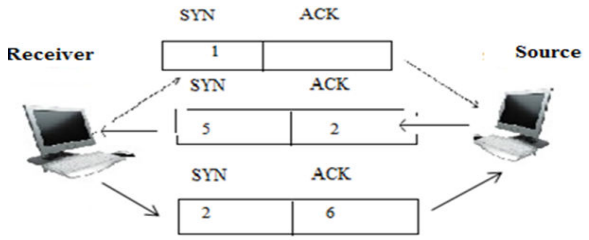

Figure-6(a). Unchanged sequence number before prevention.

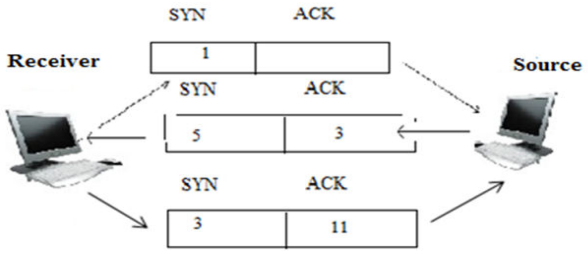

Figure-6(b). Shifted and incremented sequence number after prevention.

4.2 Passive attacks defense

Passive session hijacking attacks can be prevented by sending periodical query to the client from the source along with a time stamp.

The answer to the query can be given by the receiver only. The frame sequence number is also altered using transposition concept.

For genuine node

Step 1: Sender node generates the query
Step 2: Sender node adds time stamp and sends the query
Step 3: Sender node changes the frame sequence number S(n)=S(n')

Where n' represents the sequence number of the frame altered by any mathematical function applied on S(n).

Step 4: Source maintains the intermediate node counts in a table and checks when the messages pass through them with the help of Time To Live Value.
Step 5: Destination receives the query with time stamp
Step 6: Client responds with correct answer to the query within the time

If the attacker is present in the network and hijacks the session established with the victim then the attacker could not understand and answer the query. The attacker could not understand the frame sequence even if it tries to monitor the traffic. If the attacker tries to delay the communication the time stamp will reveal that.

4.3 Hybrid attacks-defense

The messages are encrypted using a key as, M=E(m) at the source side. The client decrypts it using M=D(m), The encryption method used is given by the source to the client already .

4.4 Algorithm

Source Side
Shift left the ACk number
Increment the ACk number
Apply the function s(n)=s(n') for changing the frame sequence number//Preventing active session hijacking
Put the time stamp
Check the source routing table with H(a) hop address count using TTL value
Generate the query Q(a) // Preventing Passive session hijacking
Encrypt the message E(m) // Preventing hybrid session hijack
Destination Side
Decrement the sequence number and shift right
Apply the reverse function s((n')'') to get the original sequence
Answer the query Q(a')
Decrypt the message D(m)

5. SIMULATION AND QOS ANALYSIS

The attack and the TLD Method are simulated using NS2. The different attacks are generated and launched in the MANET. The QoS parameters are analysed with MANET in an attack free environment. The parameters which affect the multimedia communication like packet delivery ratio, control overhead / node, throughput, delay, jitter are studied with attacks. The TLD

method for detecting the session hijacking is implemented and the results are analysed using graphs with AODV protocol. AODV protocol is Adhoc on Demand Distance Vector protocol. It is a reactive routing protocol which is the basic and well known protocol taken for study. The simulation parameters are shown in Table-1.

Table-1. Simulation parameters.

Number of Nodes	150
Simulation Area	1000 m x 1000 m
Buffer Size (Queue Length)	50 Pkts
Packet Size	1024 bytes
Application Traffic	Video traffic
Simulation time	200 Secs
Number of Connections	150
Connection duration (secs)	20
Data Intervel	0.01,0.02,0.03,0.04,0.05,0.06,0.07,0.08,0.09,1.00
Connection	10,20,30,40,50,60,80,100,120,140,150
Protocol used	AODV

Packet delivery ratio: It is calculated as the number of packets delivered to destination [10].

PDR = Number of packets delivered/Number of packets sent

Control overhead/node: Control Overhead/Node is the routing overhead produced per node [11]. This includes route requests, replies and error messages.

COH/node = Control packets produced/number of nodes

Throughput: Throughput measures the amount of data successfully delivered to the destination from the source. It is usually measured in bits / sec.
Throughput=Data delivered/time unit

End to end delay: End to End Delay includes all types of delays that occur during transmission like route discovery delay, processing delay, queuing delay and propagation delay. The delay is averaged by computing the ratio of the send time-received time with the number of received packets [12]. The delay is an important metric to be considered for multimedia applications [13]

ETE delay = (Sending time - Received time)/Number of packets received

Jitter: The most important and relevant metric for the multimedia data transfer analysis is jitter. Jitter (Delay variation) is the difference in end to end delay between selected packets in a single connection [14]. This occurs due to network congestion, and improper queuing.
Jitter=ETE (pkt_{i+1})-ETE (pkt_i)

With AODV protocol, with attacker, the PDR reduces to a minimum of 70%. Without attacker, a maximum of 100% PDR and minimum of 90% delivery is achieved. With our detection method, a maximum of 98% and minimum of 77% is achieved. This is shown in the Figure-7.a. The performance with throughput is similar to PDR. The attack, which takes away the session established and in turn makes a communication with the destination affects not only the PDR but also the throughput, delay, control overhead and jitter. Mainly the delay increases a lot and as such the jitter is also increasing. The control overhead is more when compared to the attack free environment. The TLD method, all the parameters are improved as shown in Figures 7.a to 7.e.

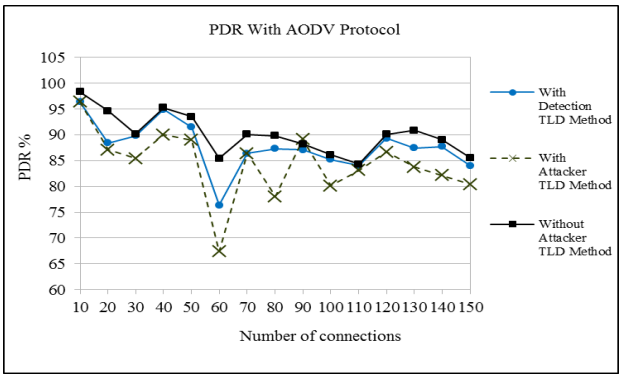

Figure-7(a). PDR with varying number of connections.

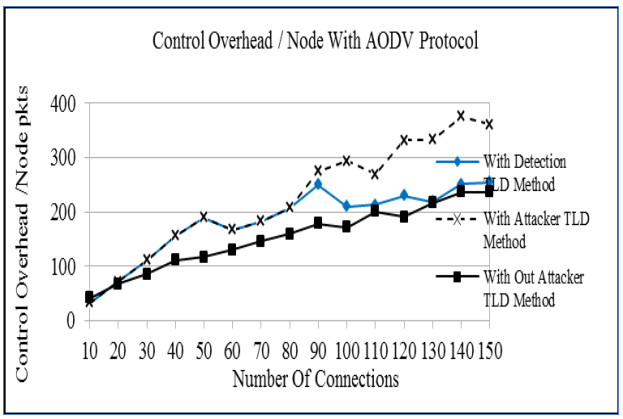

Figure-7(b). Control overhead/node with varying number of connections.

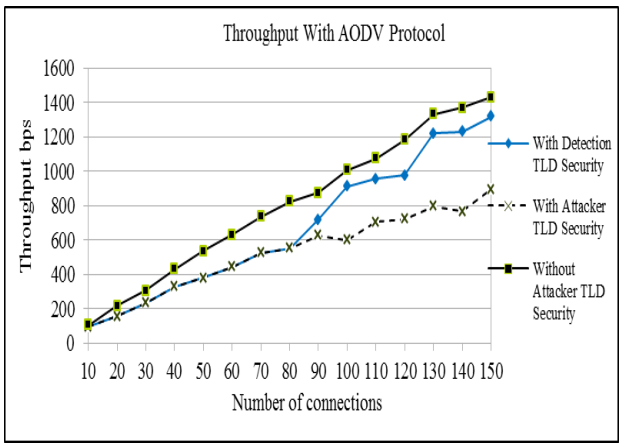

Figure-7(c). Throughput with varying number of connections.

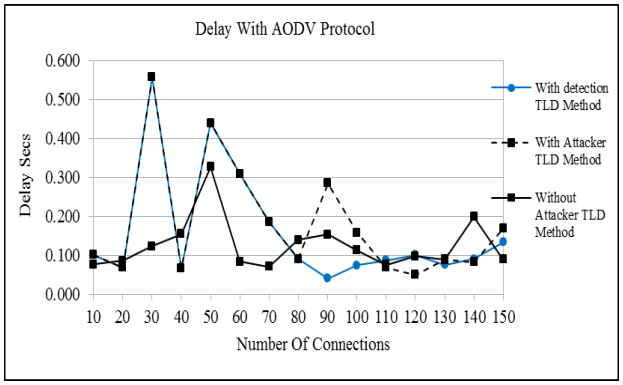

Figure-7(d). Delay with varying number of connections.

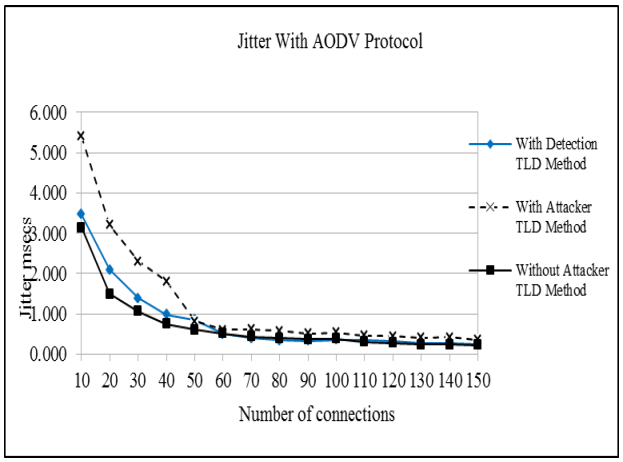

Figure-7(e). Jitter with varying number of connections.

6. CONCLUSIONS

The TLD method provides an efficient defense against the transport layer session hijacking attacks. The method provides security with quality of service. The parameters specific to a multimedia transmission are analyzed. This method constitutes the major session hijacking attack variations. The method may be extended to the session hijacking attacks which arise in the link layer. This is considered as a future research.

REFERENCES

Panaousis Emmanouil A. and Christos Politis. 2009. Securing ad hoc networks in extreme emergency cases. In: proceedings of the World Wireless Research Forum, Paris.

Sheng Yong, Keren Tan, Guanling Chen, David Kotz, and Andrew Campbell. 2008. Detecting 802.11 MAC layer spoofing using received signal strength. In: IEEE proceedings of the 27th Conference on Computer Communications. pp. 1768-1776.

Hall M. Bareau and E. Kranakis. 2004. Using transceiver prints for anomaly based intrusion detection. In: Proceedings of 3rd International Conference on Communications, Internet, and Information Technology. St. Thomas. pp. 22-24.

X. Long and B. Sikdar. 2008. Wavelet based detection of session hijacking attacks in wireless networks. In: Proceedings of IEEE Global Telecommunications Conference, New Orleans, United States of America. pp. 1-5.

Gill R, Smith J, Looi M. and Clark A. 2005. Passive Techniques for Detecting Session Hijacking Attacks in IEEE 802.11 Wireless Networks. In: Proceedings of Asia Pacific Information Technology Security Conference, Australia. pp. 26-38.

Zeng Kai, Kannan Govindan, Daniel Wu, and Prasant Mohapatra. 2011. Identity-based attack detection in mobile wireless networks. In: IEEE Proceedings of INFOCOM, pp. 1880-1888.

Faria Daniel B. and David R. Cheriton. 2006. Detecting identity-based attacks in wireless networks using signal prints. In: Proceedings of the 5th ACM workshop on Wireless security. pp. 43-52.

Chen Yingying, Jie Yang, Wade Trappe and Richard P. Martin. 2010. Detecting and localizing identity-based attacks in wireless and sensor networks. IEEE Transactions on Vehicular Technology, 59(5): 2418-2434.

Ahmad M, Nazrul, Anang Hudaya Muhamad Amin, Subarmaniam Kannan, Mohd Faizal Abdollah and Robiah Yusof. 2014. Detecting Access Point Spoofing Attacks Using Partitioning-based Clustering. Journal of Networks. 9(12): 3470-3477.

S. Corson and J. Macker. 1998. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations (Internet-draft), in Mobile Ad-hoc Network (MANET) Working Group, IETF.

Sun J. Z. 2001. Mobile ad hoc networking: an essential technology for pervasive computing. in proceedings of the International conference on Info-tech and Info-net, Beijing. 3: 316-32.

Perkins Dmitri D., Herman D. Hughes and Charles B. Owen. 2002. Factors affecting the performance of ad hoc networks. In: IEEE International Conference on Communications. 4: 2048-2052.

Bouras Ch, and Apostolos Gkamas. 2003. Multimedia transmission with adaptive QoS based on real-time protocols. International Journal of Communication Systems. 16(3): 225-248.

Adam Giorgos, Vaggelis Kapoulas, Christos Bouras, Georgios Kioumourtzis, Apostolos Gkamas and Nikos Tavoularis. Performance evaluation of routing protocols for multimedia transmission over mobile ad hoc networks.