Research Journal of Mathematics and Computer Science
(ISSN:2576-3989)

Session Hijacking in Mobile Ad-hoc Networks: Trends, Challenges and Future

Kuyoro Shade O., Okolie Samuel O. and Oyebode Aduragbemi*
Department of Computer Science, Babcock University, Nigeria

ABSTRACT

Technological advancement in the field of telecommunication has led to the creation of highly dynamic networks, one of such is Mobile Ad-Hoc Networks which can be described as an autonomous collection of devices (mobile devices) that offers dynamic topologies, no central administration, dynamic and ever mobile nodes and so on, information becomes easy to disseminate. Mobile Ad-Hoc Networks and the various features it provides affects the security of the network. A network with dynamic nodes and no central administration can be prone to network attacks one of such is session hijacking. Integrity is paramount in any network, session hijacking affects the integrity of data on a network, important information is leaked also due to the sensitive application of MANETs especially in the military these has to be avoided. This paper looks into session hijacking in MANETS, reviewed various existing solutions to find out gaps and also proposing an optimised IDS which offers more flexibility and also dynamic applications in any network traffic environment.

Keywords: Session Hijacking; Intrusion Detection System, Information Sharing, Security, Confidentiality

***Correspondence to Author:**
Oyebode Aduragbemi
Department of Computer Science
Babcock University, Nigeria
oyebodeaduragbemi @ hotmail .com

How to cite this article:
Kuyoro Shade O., Okolie Samuel O. and Oyebode Aduragbemi. Session Hijacking in Mobile Ad-Hoc Networks: Trends, Problems and Future. Research Journal of Mathematics and Computer Science, 2017; 1:2

eSciencePublisher

eSciPub LLC, Houston, TX USA.
Website: http://escipub.com/

INTRODUCTION

In the field of telecommunication and networking specifically wireless communication, sporadic advancements in technology has led to rapid growths and development in this field of Computer Science. The need for connectivity and information sharing has grown beyond the conventional methods of creating networks which includes having a central administrator, base stations, and defined topology and so on. The need to have dynamic networks which can evolve to the ever-changing demands of humans with mobile or changing nodes capable of handling multiple topologies.

Mobile Ad Hoc Networks (MANETs) was developed to handle such needs by operating in an environment with no central administration. Figure 1 depicts three nodes communicating, NODE 1 can send packets to NODE 2 because its within transmission range also NODE 2 can route packets to NODE 3. NODE 2 acts as a router routing packets between the two other nodes. Furthermore, NODE 1 and NODE 2 are capable of routing packets to other nodes within their transmission range.

Although MANETs provide dynamic routing with changing nodes it is very vulnerable to security threats (Geetha & Sreenath, 2016). This is a generic issue; one cannot isolate any network system from security threats but MANETs which are infrastructure-less network provide no centralized control and this serves as a disadvantage when it comes to security. MANETs are been targeted by a huge number of attacks each of which vary in the mood of attack and also the layer been attacked.

Network security threats are broadly categorized into two main categories which include Passive and Active Attacks. (Agrawal & Chauhan, 2014) These classification is done considering the behaviours and modes of these attacks on the MANET networks.

> A) Passive Attacks: These group of attacks are such that they do not alter data being transmitted over the network or led to network crash, instead it monitors the traffic for sensitive information. Connections are being monitored for unauthorized data. The attacker obtains vital information and tries to cover up the traces or footprint left behind to ensure a successful attack. Examples of such attacks include; Eavesdropping, Traffic Analysis, Snooping etc.
>
> B) Active Attacks: These group of attacks are very severe to network operations. They are very destructive to network nodes, they prevent information and data transfer between network elements and could lead to a network crash. These group of attacks could further be categorized further into two subgroups which are internal and external attacks. Attacks are grouped under internal attacks when the malicious nodes responsible for the attacks are apart or internal to the network. Such group is harder to detect and also could do far more damage to the network. External attacks are attacks carried out by external influences. The source of the attack is not part or external to the network. Examples of such attacks include Denial of Service (DoS) attacks, Packet Modification attacks, Congestion attacks, Fabrication attacks etc.

This study aims to critically analyse an active attack pertinent to MANETs, which is Session Hijacking. A session using literal terms means having a formal meeting or time set aside for a particular activity, this relates to how sessions are viewed in network terms. In telecommunication or networking, sessions are simply interactions (Wage & Patil, 2014). Interactions between two or more communication devices or a computer and a server. One endpoint mostly a client requests for a connection session with another end point typically a server, once the connection is agreed upon a session can takes place.

The most commonly used protocol on the internet today, Transmission Control Protocol/Internet Protocol (TCP/IP) which provides the most reliable service on the internet (R.Ragupathy & Sharma, 2014), a session begins when the client sends a request to the server, the server sends an acknowledgement to the client and thus a communication session can start. Also, to terminate a communication session an End Communication packet is also sent to the server which is also followed with an acknowledgment (Zanoon, Albdour, Hamatta, & Al-Tarawneh, 2015). A typical example of this is communication session that customers have with their banks.

A request is sent to the server; it should also be noted that during the process of receiving the request, the server authenticate the customer and also authorized them to be able to perform certain operations on their bank account. Thus, imagine a scenario in which after the authentication and authorization has taken place and a session has started, an attacker takes control of the session deceiving the server and acting like the authenticated user, this can be described has a session hijacking attack. (Singh & Kaur, 2013)

Mobile ad hoc networks are described to be more susceptible to attacks compared to other types of networks, this article studies session hijacking in relation to MANETs. MANETs are highly sensitive network which is mostly used and applied in military environments and also their operations and they often transfer sensitive information and security had to be optimized.

This study also aims to see how Intrusion Detection Systems can be used to make MANETs more secured. An Intrusion Detection System can be said to be a software or hardware, deployed on a network to detect malicious activities and also malicious nodes. An IDS basically detects undesirable and also intruder activities. It's a highly effective wat to detect malicious events on the network. It functions has an integrated system capable of detecting attacks of different various types by analysing network events and activities and also monitoring. (Meenatchi & Palanivel, 2014)

In fixed network systems in which topologies are not dynamic and there is a central administration, IDS behave like another layer of defence beyond that of the firewalls that is installed on the network, but in MANETs IDS do not behave this way. In MANETs, the IDS is the first means of protection, IDS are placed at the front line. Due to the lack of a central administration IDS is placed and deployed in each nodes of the network.

RELATED WORKS

A lot of researches has gone into security in Mobile ad hoc networks, in this section we present a general review of new trends in MANETs as it tends to being more secured and reliable. Session hijacking is but one the numerous attacks associated with MANETs, and solutions for addressing such attacks have been postulated, but due to the tenacity and resourcefulness of attackers this solution are fast becoming obsolete.

Ragupathy et al in 2014 postulated the deployment of an Intrusion Detection System (IDS). An Intrusion Detection System is a piece of software or hardware employed and deployed on a network to detect malicious and unwanted activities on networks. This form of security provides a means by which cracker, hacker, malware and other forms of attacks can be detected on the system, and also malicious sessions can be detected. The Intrusion Detection System may not be able to prevent such activities but a means of detection is possible. Although, using an Intrusion Detection System provides a means by which malicious activities can be detected, it is often useless and impossible to detect malicious activities if the traffic is well encrypted. Malicious sessions can go undetected and unnoticed when the traffic is properly encrypted.

Ehsan et al in 2013 did a review on IDS in MANETs, existing IDS architecture was postulated also various IDS algorithms was also compared. The problem of IDS being unable to work effectively in encrypted traffic wasn't addressed. This can be said to be one big drawback for IDS in MANETs. Meenatchi et al in 2014 did a survey on IDS in MANETs, they also reviewed various algorithms and critically analysing their various merits and demerits. The fact that IDS are impeded by encrypted traffic is also not addressed.

Pratibha et al 2014 postulated a new intrusion detection method EAACK, Enhanced Adaptive Acknowledgment designed to handle three major weakness in traditional IDS methods, the three-major weakness include: Limited Transmission Power, Receiver Collision and False Misbehaviour. EAACK provides a higher level of security to the network system, demonstrating high detection of malicious nodes and activities on networks also not affecting the network performance in any way. Also, the system is also impeded by encrypted traffic and can totally be vulnerable. This is a major defect in the design and also architecture of various Intrusion Detection Systems.

Vikaram et al in 2014 gave a different view towards making MANETs more secured. During a network session, messages (which are basically

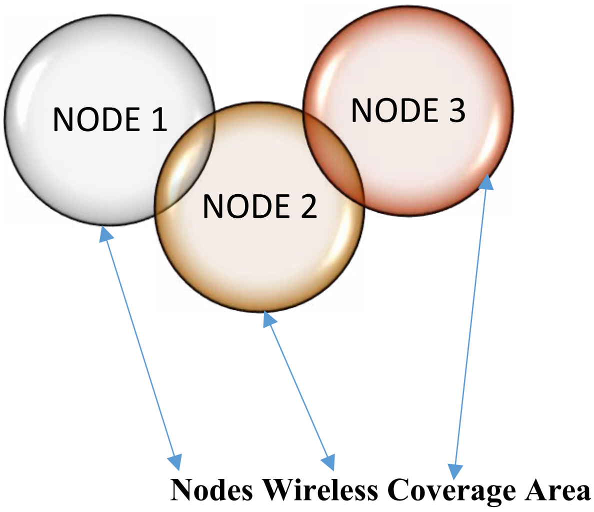

Figure 1. Example of Mobile Ad-Hoc Networks

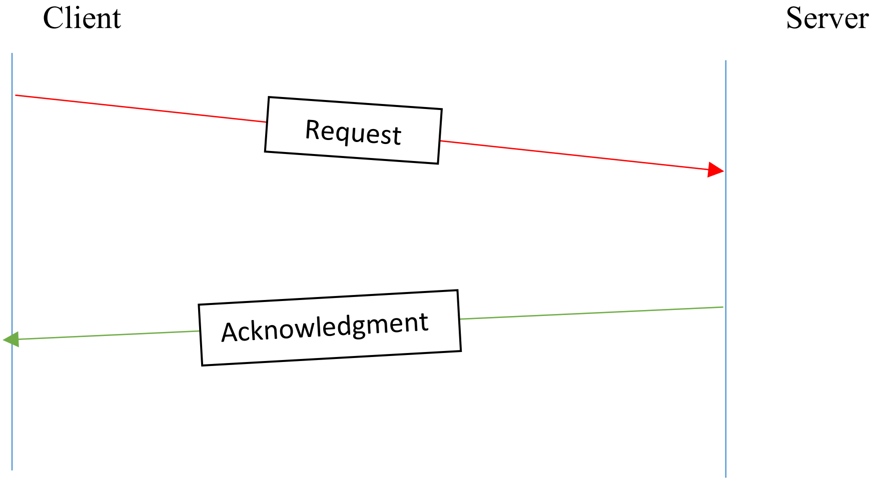

Figure 2. TCP/IP Operations

a collection of data packets), are broken down into packets, this is known as packet switching and these packets travel through what are called routes to the destination where the packets are reassembled into the original message. They postulated that the routes through which these packets travel can be made secured and these would make it difficult for attackers to get networks session when the routes packets travel is well secured. Various protocols will be employed to determine the routes through which the packets will travel, but the protocols are also vulnerable to attacks and might not be the most effective way to tackle the problem of security in MANETs due to the dynamic architecture of MANETs. Augustine et al also proposed routing has a means of improving security in MANETs. They went on to develop algorithms, these algorithms ensure selection of routes from source to destination. A secured randomized route selection method was developed which provides improved security for source, destination and also the routing path.

Noureldien et al in 2015 carried out a survey of MANET attacks and came up with a new classification scheme. Session hijacking was classified into Confidentiality attacks only. Confidentiality simply means setting and placing authorized level of access to a piece of information making it available to persons authorized to have them. Therefore, Confidentiality attacks are attacks targeted at the disclosure and reviling of messages by unauthorized individuals on the network. Session hijacking falls under this category, basically an attacking trying to hijack a session wants to get access to unauthorized messages thereby reducing the confidentiality requirement of such messages. Although solutions to attacks where not explicitly given, they tried to give network administrators a guide to understanding of attacks and their features also the security requirement targeted.

Geetha et al 2015, reviewed security threats and also the various means to counter act these threats in MANETs. Threats were analysed based on 5 major security attributes which are:

1.Availability: These assures that the services provided by the network is made available at all times and also it must be able to address errors in other to have a stable connection

2.Authenticity: These feature of network elements to validate the data sent and also data received by nodes in other to make it impossible to for attackers to get access to nodes and obtain sensitive information.

3.Confidentiality: This involves restricting information from being leaked to unintended parties, just authorized users should have access to data.

4.Integrity: Data shouldn’t be changed or altered during transmission.

5.Non-Repudiation: These ensures that both the sender and the receiver of massages cannot deny that the exchange took place. (Geetha & Sreenath, 2016)

Manjeet et al in 2015 carried out a survey on attacks on MANETs, identifying various vulnerabilities associated with this type of network. Some of the identified vulnerabilities include:

1.Lack of Centralized Management: The absence of a central administration makes the detection of attacks hard and highly difficult due to the fact that the lack of a centralized management system impedes trust management of nodes. Monitoring traffic in a highly dynamic and large-scale ad-hoc network is even more difficult without a central administrator.

2.Resource Availability: The availability of resources is a big vulnerability issue in MANETs, providing a secure line of communication in an unpredictable environment such has MANETs and also ensuring protection of these resources from threats and attacks.

3.Scalability: Nodes in MANETs are ever changing and also mobile providing issues of scalability which further affects security.

4.Dynamic Topology: Moving and changing nodes resulting in a dynamic topology may disturb the trust relationship among nodes. Also, if a node is termed as compromised the trust between nodes can be affected.

5.Limited Power Supply: Inadequate power supply restricts the effectiveness of MANETs, nodes could be visible and other might not and a complete section of the network might be down. (Singh & Kaur, 2013)

Also, Manjeet et al 2015 discussed attacks in MANETs and how they affect the operations of MANETs. Although solutions were not provided in the study, security threats pertinent to MANETs were analysed, concluding that MANETs are plagued by a variety of issues which needs to be addressed to make them more secured. Nabeel et al also carried out a study similar to Manjeet et al, in the fact that they both reviewed attacks related to MANETs. Nabeel et al went further to postulate security solutions for MANET networks, he proposed certain properties for MANET security solutions which include:

1. The solution provided must cut across all network elements, they must be applied to all network nodes for a complete collective protection of the network.

2. The solution must take into consideration all layers of the network and also how these different layers complement each other.

3. The solution has to provide adequate means to avoid network threats be it internal or external, the solution must be able to protect the network from these attacks.

4. The solution has to apply to all mechanism of security taking into consideration prevention, detection and also interaction.

Nabeel et in 2015 addressed the structure on MANETs, the structure of MANETs is very vital to understanding why they act the way they do and also why they are so vulnerable to attacks. The study proposed building a sort of security wall to protect MANET network elements form the risk of an attack, attacks occur when the security placed in place is very weak. Session hijacking was also addressed, the study suggested improving the encryption and also authentication between the parties in communication which is a viable way of defending against session hijacking but not permanent. Attackers are getting more skilled in what they do, simply improving on the encryption and also the authentication level on the network doesn't make it free from attacks, attacks are extremely resourceful and also in MANETs nodes could be infiltrated and this could pose a serious problem.

Raja et al in 2014 did and overview of MANETs, giving a detail history of how MANETs came into existence by grouping them into generations, first second and third generations of MANETs. The various applications of MANET technology were listed, which include applications in the military, commercial sector, networking and so on. The study further went on to analyse attacks in MANETs, the study used the network layers to group various attacks pertinent to MANETs. It mentioned that Session Hijacking takes advantage and exploits unprotected sessions. The attacker spoofs for a node's address and with this malicious node's ip, the attacker tries to gain secured data such has passwords, encryption keys, login names and so on. Although explicit solutions to the attacks was not given in the article, the study gives a general overview of what MANETs are and also how they work and behave pointing out the fact that MANETs are vulnerable to attacks.

Session hijacking as earlier stated falls under confidentiality attacks (Geetha & Sreenath, 2016), due to the fact that sensitive sessions (messages) are been made available to unintended persons, just like Noureldien et al, Geetha et al also postulated the securing of routes, and the protocols used to secure these routes are vulnerable to attacks. Aarti et al, also postulated securing the routes in other to make it impossible to attack, it went further to classify attacks based on their behaviours either internal or external, and also on the layer affect or targeted.

When we try to analyse Session hijacking, two layers in the network protocol stack are vital and considered highly important. These layers involve the transport and the session layer. At the transport layer, this is the lowest level where messages instead of packets are handled, these messages are addressed to communication ports and also check errors, the session layer is the layer where sessions between end to end applications or nodes is opened and also managed. Session hijacking occurs at the transport layer leading to the session layer, both layers are involved in the session hijacking attacks.

RESEARCH GAP AND DISCUSSION

Mobile Ad-Hoc Networks are very vulnerable to attacks (Aarti & Tyagi, 2013), this is due to various reasons ranging from its dynamic topologies, no central administration and so on. (Singh & Kaur, 2013) Session hijacking on MANETs is also a pertinent problem which could lead to the dissemination of sensitive information to third parties who should not have access to such information, considering the sensitive nature of MANETs and also its application in military, paramilitary, business etc. there is need to secure information or packets been transmitted through the network. Information integrity is an important virtue of a network and MANETs must provide means to insure data integrity. The literatures reviewed provided different means of securing MANETs and protecting the network from session hijacking. The solutions provided all have their pertinent flaws.

Session hijacking could be prevented by securing the protocols used for communication. This ensures that attackers would not be able to get access to packets transmitted over the routes taken by the packets. This is important when trying to prevent session hijacking, if the routes taken by packets are secured well enough it's possible to prevent session hijacking from ever taken place. There are various protocols available to secure routes. Some of these protocols include:

1. Ad-Hoc On-Demand Distance Vector Routing (AODV)
2. Dynamic Source Routing (DSR)
3. A-SAODV – Adaptive Secure AODV
4. SEAD – Secure Efficient Ad-Hoc Distance Vector

These are but a few of the protocols used in MANETs to secure the routing of packets in MANETs, but a major drawback of this is that, if we look at these protocols closely we find out that they also have their individual drawbacks (Geetha & Sreenath, 2016), an example is the Ad-Hoc on Demand Distance Vector Routing (AODV) may not sense misbehaving or malfunctioning nodes, also fails to detect wormhole attacks, also Dynamic Source Routing (DSR) is vulnerable to attacks if the attacker is along the route taken by the packet. Also, looking at using protocols to secure the routes in packets generally, they are vulnerable to attacks and might not be the most effective way to tackle the problem of security in MANETs due to the dynamic architecture of MANETs.

Intrusion Detection Systems (IDS) also can provide a means to combat session hijacking, IDS help monitor networks for malicious activities and malicious nodes. They help provide means by which we can detect network issues also malicious sessions can be detected and this can prove to be vital to network administrators. IDS are very effective for detecting and securing network but also, they could be highly ineffective when the traffic is properly encrypted (R.Ragupathy & Sharma, 2014) and this renders the IDS useless and not the best means to secure sessions.

In this work, we propose that an Intrusion Detection System capable of decrypting encrypted traffic should be built (Augustine & Sebastian, 2016). A module which decrypts network traffic could be added to the architecture. Although this might make the design more complex and also the implementation more tedious, it would an optimised intrusion detection system capable of working in any environment making it better at analysing network traffic and detecting malicious nodes and also nodes.

In order to have a comprehensive solution to deal with session hijacking in MANETs we have to consider some issues. Problems must be looked at critically, looking at how the problem itself originates. Two network layer abstractions are of importance when trying to deal with session hijacking in MANETs and also in other network types available, the two layers are the transport layer where messages rather than packets are addressed to communication ports and also the session layer where active sessions occur between communication nodes. A session hijacking attack has to at first get through these two layers. Securing these layers of abstraction is now of vital importance. Adequate security techniques which involves the creation of firewalls could help protect these layers. Furthermore, protocols could be adopted to help secure the routes through which packets travel also to encrypt the traffic also. One method or solution might prove inadequate to address the issue of session hijacking, but a combination of various solutions can help make the network more secured.

CONCLUSION AND RECOMMENDATION

FOR FUTURE WORKS

In this paper, how session hijacking affects MANET operations was presented. MANET are very vulnerable to attacks due to various reasons which include dynamic topologies, no central administration, mobile nodes and so on, these makes securing such a network tedious and tasking. Various solutions that have been postulated in this area was analysed and the existing gaps are presented. The following recommendations are suggested:

1. In order to come up with a comprehensive solution to session hijacking, no one solution is enough, a variety of solutions is needed to ensure a secured network system. Some of these solutions include, building firewalls, encrypting traffic and also using protocols to secure the routes for packets.

2. An Intrusion Detection System capable of decrypting encrypted network traffic can also be developed.

REFERENCES

Aarti, & Tyagi, S. S. (2013). Study of MANET: Characteristics, Challenges, Application and Security Attacks . *International Journal of Advanced Research in Computer Science and Software Engineering* .

Agrawal, V., & Chauhan, H. (2014). An Overview of security issues in Mobile Ad hoc Networks . *International Journal of Computer Engineering and Science*.

Alkharashi, A. (2016). Wireless & Telecommunication. *2nd International Conference and Business Expo* . Saudi Arabia: Open Access Jorunal.

Amiria, E., Keshavarzb, H., Heidaric, H., Mohamadid, E., & Moradzadehe, H. (2013). Intrusion Detection Systems in MANET: A Review . *Elsevier*.

Augustine, A., & Sebastian, E. (2016). Routing Mechanism for Mobile Ad Hoc Networks with Improved Security Features. *Journal of Telecommunications System & Management*.

Geetha, A., & Sreenath, N. (2016). Review of Security Threats and its Countermeasures in Mobile Adhoc Networks. *AENSI Journals* .

Mangrulkar, N. S., Patil, A. R., & Pande, A. S. (2014). Network Attacks and Their Detection Mechanisms: A Review . *International Journal of Computer Applications* .

Meenatchi, I., & Palanivel, K. (2014). Intrusion Detection System in MANETS: A Survey . *International Journal of Recent Development in Engineering and Technology* .

R.Ragupathy, & Sharma, R. (2014). Detecting Denial of Service Attacks by Analysing Network Traffic in Wireless Networks . *International Journal of Grid Distribution Computing*

Raja, L., & Baboo, S. S. (2014). An Overview of MANET: Applications, Attacks and Challenges. *International Journal of Computer Science and Mobile Computing* .

Scheme, S. o. (2015). Noureldien A. Noureldien; Saeed K. Saeed; M. Ahmed Salih; Alsawi M. Ahmed. *British Journal of Mathematics & Computer Science* .

Singh, M., & Kaur, G. (2013). A Surveys of Attacks in MANET. *International Journal of Advanced Research in Computer Science and Software Engineering* .

Wage, P., & Patil, C. (2014). INTRUSION-DETECTION SYSTEM FOR MANETS: A SECURE EAACK . *International Journal of Research in Engineering and Technology*

Zanoon, N., Albdour, N., Hamatta, H. S., & Al-Tarawneh, R. (2015). SECURITY CHALLENGES AS A FACTOR AFFECTING THE SECURITY OF MANET: ATTACKS, AND SECURITY SOLUTIONS . *International Journal of Network Security & Its Applications*