A SURVEY ON DIFFERENT CROSS-LAYER ATTACKS AND THEIR DEFENSES IN MANETS

Khaleel Husain[1], Premala Patil[2]

[1]PG Student, ECE Department, Guru Nanak Dev Engineering College Bidar, Karnataka, India
[2]Assistant Professor, ECE Department, Guru Nanak Dev Engineering College Bidar, Karnataka, India

Abstract

A Mobile ad hoc network (MANET) is a self-configuring network that has no infrastructure. Each device in a MANET is free to move independently in any direction and will therefore change its links to other devices frequently. It is an emerging technology that has the potential to be applied in applications like battlefields and also in many commercial applications. With great features MANET also has some limitations like unreliability of wireless links, constantly changing topologies and more. Due to this vulnerable nature of MANET, they are exposed to various security threats that cause problems in using them. The attackers takes advantage of these vulnerabilities to launch various kinds of security attacks on MANETs. Among the security attacks, the attack of most concern is Cross-layer attack that initializes at MAC layer and launches attack on routing layer which causes serious degradation in network performance. This attack emerges from lack of interaction between MAC and routing layer. In this paper, we focus on surveying various Cross-layer attacks that were discovered till now and their defense systems. Finally we highlight what could be done in future to improve the defense systems.

Keywords: *Cross-layer attack, Defense, MANET, MAC, Routing, Security.*

---***---

1. INTRODUCTION

A mobile ad hoc network (MANET) is different from normal cellular network, it has no fixed base station, very rapid deployment, highly dynamic topologies with multi-hop. In addition these networks forms and adapts to changes in the environment. The assumption that makes all these features possible is that not all nodes can directly communicate with each other, so nodes are needed to relay packets on behalf of other nodes in order to deliver data across network. These networks are used in military services, space exploration, under sea operations and rare animal tracking [1].

Although MANET has some good features it also has some drawbacks. Lack of reliability of wireless links between nodes, which is due to the limited energy supply for the nodes and the mobility of nodes results in inconsistency of wireless links for the communication participants in the ad hoc network. While dynamically changing topologies can be good sometimes, it can also cause problems where the nodes move in and out of the radio range of the other nodes in the ad hoc network. For these reasons mobile ad hoc networks are more prone to suffer malicious behavior than the conventional wired networks [2]. In these paper, we study a new breed of attack known as Cross-layer attack that initializes at one layer and aims at another layer. We survey various types of Cross-layer attacks at present and their proposed defense mechanisms.

The rest of the paper is organized as follows is organized as follows. In section 2 we provide a short overview of security attacks in MANET and in section 3 we briefly study a particular security attack known as Cross-layer attack and its effect on MANET. In section 4 we survey the work carried out till now in the field of discovering Cross-layer attacks and their defense mechanisms. Finally, in section 5 we provide some insight of what future work can be done to improve the Cross-layer attack detection systems.

2. SECURITY ATTACKS IN MANET

There are various attacks that target the weakness of MANET. Broadly we can classify these attacks as Active and Passive attacks.

In Active attacks, the attacker tries to modify the behavior of the network, the type of modification depends on the type of attack. Active attacks are further classified into External and Internal attacks. In External attack, the attacker tries to cause congestion, propagate false routing information or disturbs the nodes from providing services. In Internal attack, the attack is carried out from the compromised node within the network. Some examples of active attacks are Black-hole attack, Worm-hole attack and information disclosure.

In Passive attack, the attacker does not modify the behavior of the network but extracts date exchanged in the network. Snooping which refers to the illicit use of another person’s information is an example of passive attack [2] [12].

3. CROSS-LAYER ATTACK

Former attack techniques target either MAC layer or routing layer. In case of Cross-layer attack technique, most of the attacks are initialized at MAC layer but aim at routing layer [5]. The main reason for Cross-layer attack is the lack of interaction between MAC and routing layer. This attack can cause serious degradation of network performance in terms of achieved throughput, latency and connectivity. The result of this attack may cause congestion in the network, which they may achieve either by generating specific patterns that prevent certain nodes from communicating with the other nodes [3].

This type of attack exploits the vulnerability of particular layer (attack point) to launch the attack, but ultimately aspires to disrupt then operations of another layer (target point). This attack is stealthy and difficult to detect because the point of attack and target point reside in different layers of the protocol stack [13]. By using the concept of Cross-layer design, attackers can launch attacks in multiple layers simultaneously. Intelligent attackers can coordinate the attack activities in different layers to achieve their goal [14]. This attack can also be used on anonymizing networks where in, if the attacker gets information on any layer of the communication system, he can use this information in order to reduce the anonymity on the other layer as well [7]. This attack reduces the probability of detection of attacker. It also reduces the cost to conduct the attack successfully and achieve the attack goals that may not be feasible through single layer attack activities [12].

4. OVERVIEW ON VARIOUS CROSS-LAYER ATTACKS AND THEIR DEFENSES

4.1 Interlayer Attack in MANET

Lei Guang et al [5] discovered a new type of attack in which the attacker installs a malicious node in the MAC layer and uses it to launch attacks on on-demand routing mechanisms. This attack is able to carry out routing shortcut and detour attacks, while completely following the specification of IEEE802.11 standard. They extensively studied the effects of such attacks on AODV and DSR on-demand routing protocols. After analyzing the effects of such attacks, they put forward a technique which prevents shortcut and detour attacks.

4.2 Cross-Layer Denial of Service (DOS) Attack

Svetlana Radosavac et al [3] concentrated on a type of attack known as Denial of service (DOS) attack whose impacts on network performance are difficult to mitigate. In this case, the attack is planted at MAC layer and then used to target routing layer with an intention of breaking critical routes. They analyzed various possibilities in which an attacker can launch DOS attack in either one or more than one nodes in MANET, while following the rules of the MAC protocol IEEE802.11. Attacks with low-rate traffic patterns, whose aim is to either prevent one or more particular nodes from working or dividing the network were more focused by them. Finally, by using the notion of Extended Finite State Machines (EFSM), they modelled the MAC protocols with which they were able to design an attack detection scheme. They also gave a generic representation for detection system that not only can produce possible attack patterns but also verify the authenticity of the communication patterns in the network.

4.3 Cross-Layer Attack against the MANET Co-Operation Enforcement Tools

Vincent Toubiana et al [6] introduced a type of cross-layer attack that is usually applied against MANET cooperation enforcement tools. This kind of attack depends on CSMA/CA model with an intention of leaking information about the possible easy targets. This species of cross-layer attacks are very dangerous because they take benefit of security enforcement solutions, thereby instituting new violations in security of MANET. They evaluated the effects of these attacks on various cooperation mechanisms by carrying out simulations. Finally, they made a conclusion that for the cooperation mechanism tool to be more secure, they should only depend on the validated information.

4.4 Cross-Layer Attack on Anonymizing Networks

In conventional attacks on anonymity networks, network layer was the sole focus of attack for attackers. However, Andriy Panchenko et al [7] presented a new cross-layer attack applied in anonymizing networks, known as predecessor attack, in which the attacker takes benefit of universal nature of network and can even target the data transmitted in application layer. The attack will be more speedy and accurate if the attack is carried out on both layers. The main weakness of anonymizing network is that lower layer provide perfect protection but the higher layer does not. This drawback can be used by attackers to leak information from the application layer, thereby destroying the whole effort of the network. In order to improve the security of anonymous networks, the authors extended the current work by taking in the additional information leakage from the application layer into account. Additionally, they also showed how this information can be used not only to build a low cost extensive user profile, but also to speed up the attacks at network layer.

4.5 Cross-Layer Attack in Cognitive Radio Network

Olga Leon et al [10] discovered a new breed of cross-layer attack known as lion attack that is especially applied on Cognitive Radio Networks (CRNs). Here, the operation band of CRN is jammed in order to coerce frequency handoffs. The result of these handoffs is that there are interruptions in connection which leads to packet loss and also artificial increase in round trip time thereby reducing the TCP throughput or even completely stopping it. For this reason, counter measures were taken to compromise this attack and the methods used ranged from applied cryptography to cross-layer protection mechanism. To minimize the attack effectively, all methods should be used effectively. First step they took was they indicated some alterations to the TCP protocol with an aim to avoid throughput degradation due to frequency handoffs. The above stated can only be achieved if cross-layer data is utilized between physical/link and transport layer. The usage of this data is during frequency handoff, it permits the CRN participants to stop the TCP connection parameters and adjust to the new media connections, which were known before the handoff. To prevent the attackers from eavesdropping present and future actions of CRN, they showed reasons for securing control data. To cope with this problem, a technique that supply group security with more emphasis on efficiency and group dynamism, which is known as group key management (GKM) was proposed by them. Finally, they suggested for CRNs, an intrusion detection system which is specifically adapted to them should be used.

Wenkai wang et al [14] proposed a new strategy for cross-layer attack that makes an attacker more powerful by decreasing its risk of being detected. The small-back-off-window attack (MAC layer) and the coordinated report-false-sensing-data attack (PHY layer) was thoroughly explored by them. Additionally they suggested a trust-based cross-layer defense framework that depends on abnormal detection in individual layers and cross-layer trust fusion. They carried out simulations, whose results demonstrated that the maximum damage caused by attacker was considerably decreased by this suggested defense framework.

4.6 Cross-Layer Dropping Attack in Video Streaming

Min Shao et al [8] found out a new attack in video streaming known as cross-layer dropping attack. General IP layer dropping attack was identified first and then the dangerous effects that an attack can have by holding the application layer information (e.g. video streaming) was showed. The impact of the attack as a function of various performance parameters such as hop number, number of attacker and delivery ratio was calculated through simulations. The result of the attack was that even with 94% delivery ratio, the receiver was not able to watch video which was quite astonishing. They also suggested various workable solutions to deal with dropping attack.

4.7 Stasis Trap attack

One of the major security threats to MANET is the denial of service (DOS) attack. The fluency of the operation of network itself depends on the correct placements of DOS countermeasures in an adequate durable form. A new breed of DOS attack which is not only covert but also incorporates cross-layer architecture, known as Stasis Trap attack was outlined by Kaigui Bian et al [13] and they also explained countermeasures to mitigate their impacts. The working of attack starts by initializing at MAC layer and then using it as a launch station to disrupt the operation of transport layer by reducing the end to end throughput of flows by making use of TCP congestion control mechanism. Although the attack is very effective but it has negligible impact on the MAC layer which is its launch point, and hence it is very difficult to detect thereby justifying its covertness. They showed the effect of this attack through simulations and then in order to counter it used the approach of mini-max robust decentralized detection to design a detection framework that solves all the problems that were present in the scheme of traditional MAC layer detection that usually employed a centralized detection approach.

4.8 Joint MAC and Routing Attack

Soufiene Djahel et al [11] extensively examined two kinds of attack that can be applied on ad hoc networks that runs Optimized Link State Routing (OLSR), known as false validation and joint virtual link attack. These attacks can be applied to any routing protocol in MANET, but their damage impacts depends on the type of the protocol. Here two conspiring malicious nodes work collaboratively, wherein one acts at MAC layer and other at routing layer. These attacks are very dangerous as they can achieve huge losses of data packets by drastically altering the routing protocols. After analyzing the impact of these attacks, they suggested some solutions, whose efficiencies were proved through simulation results.

4.9 Integrated CRADS in MANET

John Felix Charles Joseph et al [9] designed a defense framework to counter the routing attacks known as cross-layer based routing attack detection system (CRADS) for wireless ad hoc networks, which has the ability to make use of attributes of multiple protocols over distinct layers. Despite greater detection accuracy of CRADS, it has a drawback and that is its complexity is more, which comes into consideration when using nonlinear pattern algorithm, such as SVM algorithm. For this problem to overcome, the authors have not only improvised a set of data reduction techniques but also showed the impact of these data reduction techniques though simulations. Furthermore, they analyzed the detection capability of CRADS by using OLSR routing protocol to simulate all possible routing scenarios. These results clearly showed the supremacy of CRADS over traditional protocol specific detection systems.

4.10 Cross-Layer Attack Detection Systems based on Swarm Intelligence

Rajani Muraleedharan et al [4] proposed a Cross-layer security mechanism which uses swarm intelligence to detect DOS attacks and the countermeasures taken to avoid the same without comprising any network resources.

G.Indirani et al [12] proposed a swarm based detection and defense technique for routing and MAC layer attacks in MANET. The swarm intelligence algorithm used here is Ant Colony Optimization (ACO). Using forward and backward ants, the technique obtains mean value of nodes between the first received RREQ and RREP packets. Based on this estimation, the source node decides the node as valid or malicious. The MAC layer parameters namely number of neighbors identified by the MAC layer, number of neighbors identified by routing layer, the number of recent MAC receptions and the number of recent routing protocol receptions are used to determine the node state. The source node uses these two node state estimation techniques to construct the reliable path to the destination. This proposed technique improves the network performance and at the same time prevents attackers intelligently.

5. FUTURE WORK

In future, we would like to extend the work of [12], by replacing Ant Colony Optimization (ACO) with another swarm intelligence algorithm known as Particle Swarm Optimization (PSO), which is based on the characteristics of particles moving in space. We will carry out simulations and find out based on results, whether PSO provides better network performance and prevention of attackers than ACO or not.

6. CONCLUSIONS

In this paper, we carried out a survey of various Cross-layer attacks and their defenses in MANETs. First, we briefly introduced the concept of MANET and their vulnerabilities. Then we discussed about various security attacks that can happen in MANETs. We then briefly studied an important security attack known as Cross-layer attack and its impact on MANET. We then surveyed the work carried out till now in discovering various Cross-layer attacks and their proposed solutions. Finally, we provided some insight on what future work can be done in order to improve the detection systems for Cross-layer attacks.

ACKNOWLEDGEMENTS

First of all I would like to thank Almighty and my beloved parents by degree of whom I reached the stage of completion of this paper. I express my deep sense of gratitude to my guide Prof. Premala Patil for her valuable suggestions and guidance in preparing this paper.

REFERENCES

[1]. Ram Ramanathan and Jason Redi, “A Brief Overview of Ad Hoc Networks: Challenges and Directions”, IEEE Communication magazine-50th anniversary commemorative issue/May 2002.
[2]. Wenjia Li and Anupam Joshi, “Security Issues in Mobile Ad Hoc Networks - A Survey”.
[3]. Svetlana Radosavac, Nassir Benammar and John S.Baras, “Cross-layer attacks in Wirelerss ad hoc networks”, 38th conference in Information sciences and systems (CISS), Princeton university, March 17-19-2004.
[4]. Rajani Muraleedharan and Lisa Ann Osadciw, “Cross Layer Denial of Service Attacks in Wireless Sensor Networks using Swarm Intelligence”, 40th Annual Conference on Information Sciences and Systems, 2006.
[5]. Lei Guang, Chadi Assi, and Abderrahim Benslimane, “Interlayer Attacks in Mobile Ad Hoc Networks”, Springers, Mobile Ad-hoc and Sensor Networks Lecture Notes in Computer Science volume 4325, Pp 436-448,2006.
[6]. Vincent Toubiana and Houda Labuiod, “A Cross layer attack against MANET Cooperation enforcement tools”, 16th IEEE International Conference on Networks (ICON), 2008.
[7]. Andriy Panchenko, Lexi Pimenidis, “Cross-Layer Attack on Anonymizing Networks”, IEEE International Conference on Telecommunication (ICT), Pp 1-7,2008.
[8]. Min Shao, Sencun Zhu, Guohong Cao, Tom La Porta and Prasant Mohapatra, “A Cross-layer Dropping Attack in Video Streaming over Ad Hoc Networks”, SecureComm 2008.
[9]. John Felix Charles Joseph, Amitabha Das, Boon-Chong Seet, Bu-Sung Lee, “CRADS: Integrated Cross Layer approach for Detecting Routing Attacks in MANETs”, WCNC Proceedings, 2008.
[10]. Olga Leon, Juan Hernandez-Serrano and Miguel Soriano, “A new cross-layer attack to TCP in cognitive radio networks”, Second International Workshop on Cross Layer Design (IWCLD) 2009.
[11]. Soufiene Djahel, Farid Nait-Abdesselam and Ashfaq Khokhar, “A Cross Layer Framework to Mitigate a Joint MAC and Routing Attack in Multihop Wireless Networks”, 5th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks (P2MNET), Zurich, Switzerland, 20-23 October 2009.
[12]. G.Indirani and K.Selvakumar, “Handling Cross-Layer Attacks using Neighbors Monitoring Scheme and Swarm Intelligence in MANET”, International journal of Computer Application Technology and Research volume 2-Issue 1, 41-48, 2013.
[13]. Kaigui Bian, Jung-Min Park and Ruilang Chen, “Stasis Trap: Cross-Layer Stealthy Attacks in Wireless Ad Hoc Networks”, In Proceedings of IEEE GLOBECOM, 2006.
[14]. Wenkai Wang and Yan (Lindsay) Sun, Husheng Li, Zhu Han, “Cross-Layer Attack and Defense in Cognitive Radio Networks”, IEEE GLOBECOM, 2010.

BIOGRAPHIES

Khaleel Husain completed his Bachelor’s degree in Electronics and Communication engineering in 2012. He is currently pursuing his Master’s degree in Digital Communication and Networking. Email: khsan075@gmail.com

Premala Patil is currently working as an Assistant Professor (ECE Department) in Guru Nanak Dev Engineering College Bidar. Email: kashipremala@gmail.com