International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-6,June 2016
ISSN: 2395-3470
www.ijseas.com

A SURVEY ON SECURE SCHEME AGAINST SLEEP DEPRIVATION ATTACKS ON MANET

A.Theresa Vinothini[1] , S.Madhurikkha[2]
[1]PG student-Department Of Computer Science,
[2]Associate Professor-Department Of Computer Science
Jeppiaar Engineering College,Chennai-119

Abstract - *MANET is a collection of mobile which are decentralized and self-organized nodes. Securing MANET is a problem that has become a critical one. This is because MANET properties make it tough to be secured than the other types of static networks. It suffers from a variety of security attacks and threats such as: Denial of Service (DoS), flooding attack, selfish node misbehaving, routing table overflow attack, wormhole attack, blackhole attack etc. MANET is open to vulnerabilities,no point of network management; topology changes vigorously, resource restriction, no certificate authority or centralized authority. Sleep deprivation attack in MANET makes frequent request to the node to deplete the power source. Sleep deprivation attack is a type of flooding attack in which a particular node or a group of nodes is chosen whose resources are to be exhausted. This attack can be implemented by forcing the chosen node to use its vital resources e.g. battery life, network bandwidth and computing power by frequently sending false RREQ requests for existent or non-existent destination nodes. In the mean time it will not be able process the requests coming from genuine nodes. This attack cannot be distinguished from original request, it is difficult to prevent and identify it.The main aim of the malicious node is to minimize the genuine nodes lifetime by wasting its valuable resources this attack cannot be distinguished from original request, it is difficult to prevent and identify it. We are going to present the application of sleep deprivation attack over AODV protocol .This paper objective is to summarize in doing a detailed survey on sleep deprivation attack.*

Key words: *Denial of Service(DoS),MANET,Sleep deprivation attack, Route REQuest(RREQ),Routing protocols,AODV.*

1.INTRODUCTION

A MANET is a collection of nodes that do not rely on a predefined. Infrastructure to keep the network connected.the functioning of Ad-hoc networks is more relied on co-operation of each node in the participating network. Each node in the MANET acts both as a host and a router and takes part in forwarding packets to the correct node in the network once a route s established. A malicious node in MANET has the potential to do great harm .Routing protocols for mobile ad-hoc network generate a large amount of contr5ol traffic when node mobility cause link state and the network topology to change frequently.

Routing is one of the key issues in MANET due to their highly dynamic and distributed nature .In particular energy efficient routing may be the most important design criteria for MANET mobile nodes will be powered by batteries with limited capacity . We are going to present the application of sleep deprivation attack over AODV Routing protocol. AODV is a self reactive self-starting and large scale routing protocol. In sleep deprivation attack the attacker exploits the route discovery process in AODV by broadcasting RREQ packet in order to notify each node continuously and consume its limited source of energy, bandwidth and memory .Simulation results shows that the energy consumption of network is less after applying various algorithm and our network gets more stable and that proposed technique has better packet delivery and improved throughput.

2.LITREATURE SURVEY

Ching-Tsung Hsueh[1]has proposed a cross-layer design of secure scheme integrating the MAC protocol. The analyses show that the proposed scheme can counter the replay attacks and forge attacks in an energy efficient way.The detailed analysis of energy distribution shows a reasonable decision rule of coordination between energy conservation and security requirements of WSN.

Maha Adlhaq[2]has introduced a simulation-based study for the impact of Resource Consumption Attack (RCA) on MANET performance. RCA is one of the Denial of Service attacks (DoS) in which the attacker keeps broadcasting Route Request (RREQ) packets in order to degrade the network overall performance. Specifically, this paper examined how differing the number of attackers and their positions could affect MANET packet delivery ratio and delay jitter. The paper results open the door for suggesting

an intrusion detection system in order to mitigate and prevent RCA terrible effects on MANET.

Muhammad Saleem Khan [3] has provided a comprehensive evaluation of the four well-known MANET routing protocols (OLSR, DSDV, AODV, and DSR) and the impact of security attacks on their performance. In this study, quantitative evaluation of routing protocols has been carried out using NS-2 simulator by comparing Packet Delivery Ratio (PDR),Average end to end delay and Normalized Routing Load(NRL).

Shivashankar[4] has proposed an efficient Power Aware Routing (EPAR), EPAR identifies the capacity of a node not just by its residual battery power, but also by the expected energy spent in reliably forwarding data packets over a specific link. This paper evaluates three ad hoc network routing protocols (EPAR, MTPR and DSR) in different network scales taking into consideration the power consumption. Indeed, our proposed scheme reduces for more than 20 % the total energy consumption and decreases the mean delay especially for high load networks while achieving a good packet delivery ratio.

Esubalew Yitayal[5] In this paper he has introduced a new energy efficient algorithm called BBU-AODV, which maximizes the life time of a MANET by avoiding routing of packets through nodes with low residual energy and balance the total energy consumption among all nodes in the network while selecting a route to the desired destination, is proposed. BBU routing protocol is developed on top of the popular AODV routing protocol.

Jin Zhu[6]. we propose a power consumption model for wireless sensor nodes that take into account the power consumption characteristics of the radio transceiver. We then obtain the parameters by fitting the model to the actual measurement data for some commercially available sensor node devices. We use this model to determine the optimal range that maximizes the transmission energy efficiency.

Kasturiniva Das[7] has analyzed various attacks like Gray hole, Rushing and Sleep Deprivation attacks in Adhoc On-Demand Distance Vector (AODV) based MANETs. Various performance metrics have been used to study the effects of different DoS attacks in MANETs and a comprehensive analysis is presented. NS-2.35 has been used extensively to simulate these attacks.

K. Gomathi[8] The trustworthiness of the node is evaluated by direct trust evaluation technique. The proposed Trust based Clustering Algorithm(TBCA) is proved its superiority with Existing Enhanced Distributed Weighted Clustering Algorithm(EDWCA) based on some metrics like delay, PDR, packet drop and overhead etc.

Rosilah Hassan [9] This paper utilizes one of the danger theory intrusion detection algorithms, namely, the dendritic cell algorithm (DCA) to detect the sleep deprivation attack over MANET. In this paper, DCA is plugged in a proposed mobile dendritic cell algorithm called MDCA which represented through a proposed MDCA architecture.

Girish Paliwal[10] this paper presents a review study of different types of vulnerable attacks on different network layers of MANET .MANET attacks are broadly classified according to the TCP/IP layer architecture. This study gives us the scope of developing secure Intrusion Detection Prevention SystemIDPS for the MANET.

Sabitha[11] In this paper, we discuss the security mechanisms, namely data routing information (DRI), cross-checking, and retard-mode operations, to defend against packet dropping attack in MANET with results simulated in ns-2 to show the improvement in packet delivery ratio

Alaa Zain[12] The main purpose of this paper is to study different MANETs routing protocols with three scenarios of Denial of Service (DoS) attacks on network layer like Optimized Link State Routing (OLSR) ,Ad hoc On-Demand Distance Vector (AODV), Geographic Routing Protocol (GRP). A comparative analysis of DoS attacks for throughput, Data loss, delay and network load is taken into account.

Meenu Talwar[13]has analyzed with the main concern to to maintain a counter of the number of requests served by various nodes. On the basis of number of requests in a particular time interval the decision will made whether to serve the node's request or not. The threshold values to control the packet-traffic and maintain various criteria.

Surendra Kumar[14] This paper objective is to summarize different types of attacks over MANET, and concerns with studying sleep deprivation attack. Our objective is to design an artificial immune system to secure from sleep deprivation attack and is based on biological Danger Theory.

Shikha Jain[15] Many routing protocols like AODV, DSR etc have been proposed for these networks to find an end to end path between the nodes. These routing protocols are prone to attacks by the malicious nodes. There is a need to detect and prevent these attacks in a timely manner before destruction of network services.

3.SYSTEM DESCRIPTION

1. Two-Tier Energy – Efficient Secure Scheme(TE_2S)

This cross-layer design involves coupling two layers at design time without creating new interface for information sharing at runtime. This paper proposes a two-tier secure transmission scheme. This scheme uses the hash-chain to generate the dynamic session key, which can be used for mutual authentication and the symmetric encryption key.

2.Packet Delivery Ratio and Delay Jitter

The simulation experiments were carried out using Qualnet 5.0.2 [17 The preliminary goal of the experiments' scenarios is to assess the impact of RCA on the network performance .Therefore, the number of attackers varies in the experiments' scenarios from zero to ten attackers. Also, each certain number of attackers has been tested in three attack positions which are: near sender, near receiver, and random

3. Normalized Routing Load(NRL)

NRL is shown in Fig with varying pause time. Under no attack scenario, NRL of OLSR and DSDV is higher compared to other two routing protocols. This is because of the number of control packets and routing information that is periodically exchange among the nodes and recalculation of MPR nodes particularly when link changes.

4. Energy Efficient power aware routing (EPAR)

EPAR identifies the capacity of a node not just by its residual battery power, but also by the expected energy spent in reliably forwarding data packets over a specifc link. Using a mini-max formulation, EPAR selects the path that has the largest packet capacity at the smallest residual packet transmission capacity. Indeed, our proposed scheme reduces for more than 20% the total energy consumption and decreases the mean delay, especially for high load networks, while achieving a good packet delivery ratio.

5. Balanced Battery Usage routing protocol (BBU)

The algorithm which we propose combines threshold, summation of residual energy, min Residual energy and hop count as a cost metric and integrates these metrics into AODV in an efficient way. This metrics ensure that all the nodes in the network remain up and running together for as long as possible

6. Power Consumption Model and Radio Propagation Model

A wireless sensor node consists of a microcontroller,a radio transceiver, and sensors and other peripherals. It is generally assumed the that radio transceiver is the dominant energy consumer in a wireless sensor node. Although some ultralow power microcontrollers are available with less than $1mW$ power consumption at active mode [13], a microcontroller is also considered as a major power consumption component in wireless sensor node.

7. Trust based Clustering Algorithm(TBCA)

Direct trust evaluation is used ,it will provide first hand information and at the same time transmission overheads are reduced. After finding the trust value of one particular node and that value will be compared with predefined threshold values. If the value lie in between minimum and maximum threshold value then the node announced as trusted otherwise distrusted and isolated from other work.

8. OPNET

The simulation setup of four scenarios comprising of 16 mobile nodes moving at a constant speed with mobility Random way point mobility is selected with constant speed of 10 m/sec and with pause time of constant 100 seconds. This pause time is taken after data reaches the destination only. Our goal was to determine the protocol which shows less

vulnerability in case of denial of service attack. We choose AODV, DSR, GRP and OLSR routing protocol, which are reactive and proactive protocols respectively.

9.Artificial Immune System

The basic protocol that we used in our work is AODV i.e Ad-Hoc On Demand Distance Vector protocol. It is one of the most basic protocols used in ad-hoc networks. Since MANET is also a class of ad-hoc networks so AODV is an obvious choice. The best thing about AODV is that it uses on-demand routing approach which implies that the network is functional only when a connection is required, otherwise it is silent.

10. SET-IBS and SET-IBOOS

The proposed SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. We introduce the protocol initialization, describe the key management of the protocol by using the IBS scheme, and the protocol operation onwards.

4.RESULT AND DISCUSSION

This paper presented a popular attack like DoS, sleep deprivation attacks in MANETs. Comparisons using different performance metrics for different attacks give a very clear picture of the effects of some of the DoS attacks on MANETs. This study could be very useful in understanding the impact of the four attacks on MANETs in general and AODV-based MANETs in particular. As this attack greatly degrades the performance of a MANET, hence lot of work can be done in the area of development of secure routing protocols for MANETs that can withstand DoS attacks. The analysis done in this paper will prove helpful for researchers who are engaged in proposing secure routing protocols for MANET.

TABLE 1
Comparison of Throughput and End-to-End Delay

PROTOCOL/ ALGORITHM	THROUGHPUT (Kbp/s)	END-TO-END DELAY (ms)
AODV	90	22
MDCA	72	43
Cross-Layer MAC	63	13
AODV,DSS	92	32
DSDV	52	30
BBU-AODV	70	17
ZRP	36	11

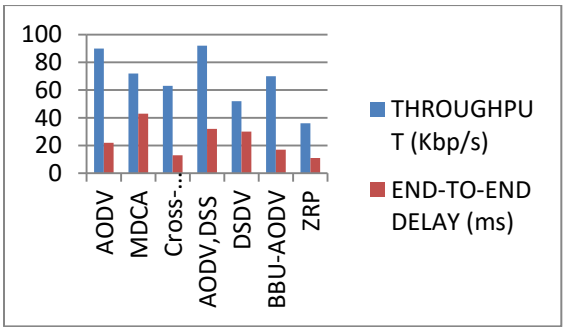

*Fig 1.*Throughput And End-To-End Delay Of Discussed methods

5.CONCLUSION

This paper had presented some of the methods to attack a network model along with some of the proposed solutions. Various issues that need to be addressed keeping in view the security of MANETS have also been highlighted. The need of the hour is to detect and prevent these attacks in a timely fashion in time .In the future work, the author would like to propose an integrated security system which will analyze the network for detecting the presence of these attacks. After detection of a particular attack author will try to pinpoint the attacker nodes and then mitigate their affect by excluding those nodes from the system. The analysis done in this paper will prove helpful for researchers who are engaged in proposing secure routing protocols for MANET.

6.REFERENCE

[1]Ching-Tsung Hsueh et.al, "A Secure Scheme against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks" Citation information: DOI10.1109/JSEN.2015.2395442, IEEE Sensors Journal,2015.
[2] Maha Abdelhaq et.al, "The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing"

International Journal of Network Security, Vol.16, No.5, PP.376-381, Sept. 2014.

[3] *Muhammad Saleem Khan et.al,"* A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks" © Springer-Verlag Berlin Heidelberg 2015K.J. Kim and N. Wattanapongsakorn (eds.), *Mobile and Wireless Technology 2015*, 137 Lecture Notes in Electrical Engineering 310, DOI: 10.1007/978-3-662-47669-7_16.

[4] Shivashankar et.al, "Designing Energy Routing Protocol With Power Consumption Optimization in MANET", 2168-6750 2013 IEEE. Translations and content mining are permitted for academic research only. VOLUME 2, NO. 2, JUNE 2014.

[5] Esubalew Yitayal et.al, "A Balanced Battery Usage Routing Protocol to Maximize Network Lifetime of MANET Based on AODV", S. Balandin et al. (Eds.): NEW2AN/ruSMART 2014, LNCS 8638, pp. 266–279, 2014. © Springer International Publishing Switzerland 2014.

[6] Jin Zhu et.al," On the Power Efficiency and Optimal Transmission Range of Wireless Sensor Nodes" ;978-1-4244-3355-1/09/$25.00©2009 IEEE,2009.

[7] Kasturiniva Das et.al," A Comprehensive Analysis of DoS Attacks in Mobile Adhoc Networks", 978-1-4799-3080-7/14/$31.00_c 2014 IEEE.

[8] Gomathi, et.al," *A Secure Clustering in MANET through Direct Trust Evaluation Technique", 978-1-4673-6618-2/15/$31.00 ©2015 IEEE.*

[9] Maha Abdelhaq et.al," Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm*" ,International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).*

[10]Girish Paliwal et.al," A Study on Various Attacks of TCP/IP and Security Challenges in MANET Layer Architecture", © Springer India 2015 K.N. Das et al. (eds.), Proceedings of Fourth International Conference on Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing 336, DOI 10.1007/978-81-322-2220-0_16.

[11] Sabitha et.al," Defensive Mechanism to Guard Against Packet Droppers in Mobile Ad Hoc Network", © Springer India2015.P. Suresh et al. (eds.), Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Advances in Intelligent Systems and Computing 324, DOI 10.1007/978-81-322-2126-5_77.

[12] Alaa Zain et.al,"MANETs performance analysis with DoS attack at different routing protocols" .

[13] Navneet Sandhu et.al," An introduction of sleep depriviation attack in AODV", International journal of Science Technology & Management (IJSTM) ISSN: 2229-6646,2015.

[14] Surendra Kumar et.al,"Prevention in Sleep DepriviatonAttack in Manet", Volume IV, Issue II, February 2015 IJLTEMAS ISSN 2278 – 2540,2015.

[15] Shikha Jain et.al,"SECURITY THREATS IN MANET: A REVIEW", International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.