EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.238-245
SANA ACADEMIC PRESS

Practicing MANET Security Using Bait Detection Scheme for Sleep Derivation and DOS Attack

G.S. Nishanthi[1], Sivakumar[2], R. Latha[3]
[1]Research Scholar, St.Peter's University, Chennai.
[2]Asst.Prof. & Head., Dept. of Computer Applications, St.Peter's University, Chennai
[3]Prof. & Head., Dept. of Computer Applications, St.Peter's University, Chennai
nishanthi04naidu@gmail.com

Abstract*—*With the production of Mobile Technology, the wireless communication is becoming more common among the general public than ever before. This is because of the technological advances in laptops & wireless data communication devices such as wireless modems & wireless LANS. It has finally led to the reduction of prices and higher the data rates which has been resulted in rapid growth of the Mobile Computing. The security threats may vary from active impersonation attacks to passive eavesdropping. Implementing Security and To Mitigate Threats in MANET has significant challenges because its dynamic properties make it complicated to be secures than the other types of static networks.

Keywords: *MANET, iMANET ,VANET, InVANET, AODV*

I. INTRODUCTION

MANET is a collectiom of mobile, decentralized, and self organized nodes. The distributive nature, infrastructure less and dynamic structure make it an easy prey to security related threats. A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each and every device in a MANET is free to move randomly in any of the directions, and will atlast change its positions to other devices simultaneously. Every device must send the traffic unrelated to its own use, and atlast can acts as router for the nodes. The major challenge in implementing a MANET is making each and every device to look upon and maintain the information which is required to traffic routing.The objective of this paper is to intend a cooperative bait detection scheme to struggle sleep deprivation and denial of service attack over MANET. This scheme merges both the proactive and reactive attack architecture in MANET by using the first hop neighbor node address as destination address to bait the malicious nodes which were causing the attack. A Susceptibility to attack is a weakness in security system. A particular system may be susceptible to unauthorized data access because the system does not verify a user's identity before allowing database to access. MANET is more susceptible than wired network. Some of the susceptibilities are as follows;

A. Lack of centralized management
B. Resource availability
C. Scalability
D. Cooperativeness
E. Dynamic configuration

F. Limited Power Supply

There are different types of attacker present in MANETs, which tries to decrease the performance of network by consuming more battery.

Types of MANET

Manet could be classified under three categories:

1) Internet Based Mobile Ad-hoc Networks (iMANETS) are an ad-hoc network that connects the mobile nodes to the fixed internet gateway nodes. Internet-based mobile ad hoc networking is an upcoming technology that supports self-organizing, mobile networking environment.

2) Vehicular Ad-hoc Networks (VANET) are used for communication among vehicles and roadside equipments. VANET, is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as
roadside equipment. Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network.

3) Intelligent Vehicular Ad-hoc Networks (In VANETS) are type of artificial intelligence techniques that help vehicles during collisions, accidents & etc. InVANET is an Intelligent Vehicular Ad Hoc Networking uses WiFi IEEE 802.11 and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility.

ROUTING PROTOCOLS IN MANET

(a) Proactive and Reactive MANET protocols: Proactive MANET protocols keeps on updating network topology information constantly ensuring that its available to all the nodes. These protocols reduce network latency and increases data overhead by updating routing information constantly. Reactive MANET protocols determines the routing paths only when required. Example of reactive protocol is AODV (Ad-hoc On Demand Distance Vector)

(b) Hybrid MANET routing protocols: Hybrid protocols is the integration of both reactive and proactive MANET protocols. Hybrid protocols combines the advantages of both reactive and proactive protocols resulting in better performance protocols that could adjust dynamically to different network conditions.

(c) High-Level MANET protocols: High-Level MANET protocols automates processes involved in establishing the Wi-Fi connection between the mobile devices allowing them to send and receive messages among them.

II RELATED WORK

In this paper the author tries to solve the problems of blackhole and grayhole attacks caused by malicious nodes by designing a Routing mechanism known as Cooperative Bait Detection Scheme (CBDS). It combines the advantages of both the proactive and the reactive detection schemes to detect malicious nodes where the proactive detection scheme traces nearby nodes and avoids the attacks in initial stage and the reactive detection scheme triggers only when detection node finds significant drop in delivery ratio. It achieves its goal with the use of Reverse tracing technique. Cooperative Bait Detection scheme is proposed to detect malicious nodes in Mobile Ad-hoc Network for the grayhole and blackhole attacks. Attacks might be in both active or passive ways.

According to the OSI model the security architecture of the MANET can be divided into four layers such as;

- Infrastructure layer
- Network security layer
- Application layer and
- Security layer

Which describes the functions of each layer in detail. Security architecture of MANET is designed according to OSI model. Relationship between each layer of security architecture of MANET and that of OSI is provided that helps in planning and designing reliable and secure MANET design. The main disadvantage of the existing theme is that the reverse tracing program sent by the Bait detecting Scheme is very slow.

III PROPOSED ALGORITHM

Every node sends a request signal (NReq) to transmit the data. If the neighbour node receives the NReq signal, then it replies with a NRep signal back to the node. If the NRep signal is received back by the transmitter node, then the system is working normal and fine and the data transmission can be started. If the transmitter node does not receive back its NRep signal, then its hop limit is to be checked. If the hop limit has not exceeded the lower threshold limit, then NReq is again resent or it is below the lower threshold limit then the NReq sending is terminated.Once the system starts transmitting data signal normally, packet delivery ratio of the packet will be scanned. If the packet delivery ratio is above the threshold limit, then no malicious nodes are present and the process terminates. But if the packet delivery ratio is below the threshold limit that is if there is any drop then it is detected and a bait NReq is sent and response is awaited. If there is no response then the packet delivery ratio drop may be due to inefficient routing and so CBDS is terminated. But if the transmitting node receives a NRep response to the bait NReq, then a reverse tracing program is triggered and test packet data and recheck messages are sent to confirm malicious node detection. After the confirmation of malicious node, source node updates the list of detected malicious node with this new entry and casts an alarm signal inside the network for all the other nodes to follow it. When all the n odes have updated their list of malicious nodes, the detected node is blacklisted and further communication to the node are stopped.

SYSTEM FLOW DIAGRAM

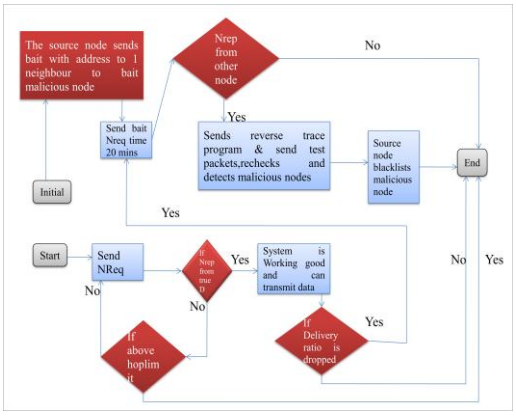

Figure 1: Flowchart of Proposed System

PSEUDOCODE

Step 1: Send NReq;
Step 2: if (NRep == true D) \\ if the NRep is from the True Destination
Step 3: then;
Step 4: System=G; \\ Syetem is working Good
Step 5: Data can be transmitted;
Step 6: else
Step 7: if (Time > hoplimit) \\ if it exceeds the hoplimit
Step 8: end process
Step 9: else
Step 10: Send NReq again;
Step 11: end if;
Step 12: end if;
Step 13: if (DR < TH) \\ if the Packet Delivery Ratio drops to a certain Threshold
Step 14: Send Bait NReq;
Step 15: else
Step 16: end process;
Step 17: end if
Step 18: if (NRep = True) \\ If NReq is Yes
Step 19: TTM = 20mins; \\ Trigger Trace Mechanism time
Step 20: else
Step 21: end process;
Step 22: end if;
Step 23: Initiate T Mechanism;
Step 24: Malicious Nodes Detected;
Step 25: MN = Black List;

IV SIMULATED RESULTS

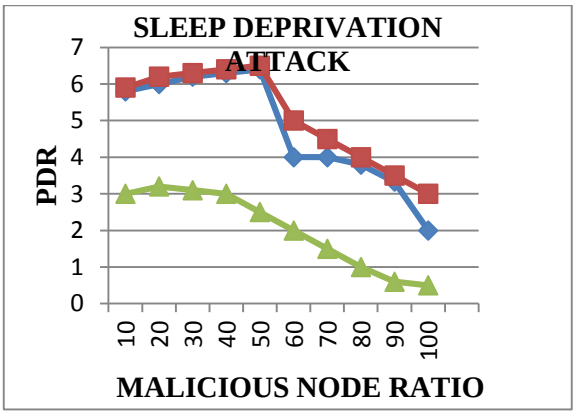

Figure 2: PDR vs. malicious node ratio for DOS Attack

Figure 2: shows the differentiation of Packet Delivery Ratio (PDR) with malicious node ratio for Denial of Service (DOS) attack. Packet delivery ratio is the ratio of the number of data which is delivered to the destination node. This shows the level of delivered data to the destination node. The higher value of packet delivery ratio means the better performance of the protocol. PDR = Σ Number of packet receive / Σ Number of packet send In optimal conditions the DR value for different malicious node ratio is high. When the system is under DOS attack the PDR value becomes lower than that in optimal conditions. However applying CBDS increases the corresponding PDR value further to optimal conditions.

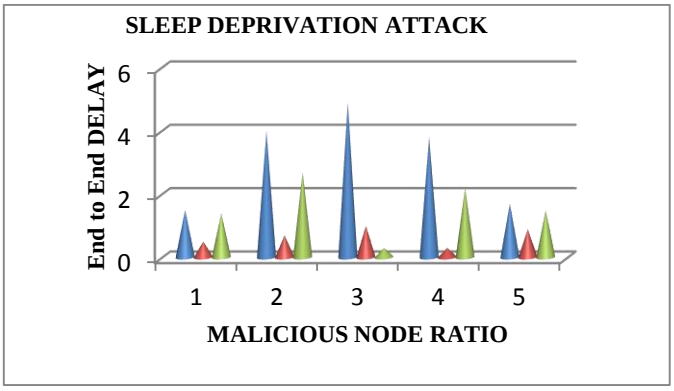

Figure 3: End to End delay vs. malicious node ratio for DOS attack

Figure 3 shows the differentiation of end to end defer Versus the malicious node ratio in case of Denial Of Service attack. End-to-end defer is defined as the average time taken by a data packet to come in the destination node. It also includes the defer caused by route discovery process and the queue in data packet transfer. Only the data packets that successfully gets delivered to the other nodes. The lower data of end to end defer means the better performance of the protocol. However DOS attack is gushing type attack and low values of end to end defer means less time for analysis of data. Hence the values should be greater. End to End defer = Σ (receive time – send time) / Σ Number of connections:

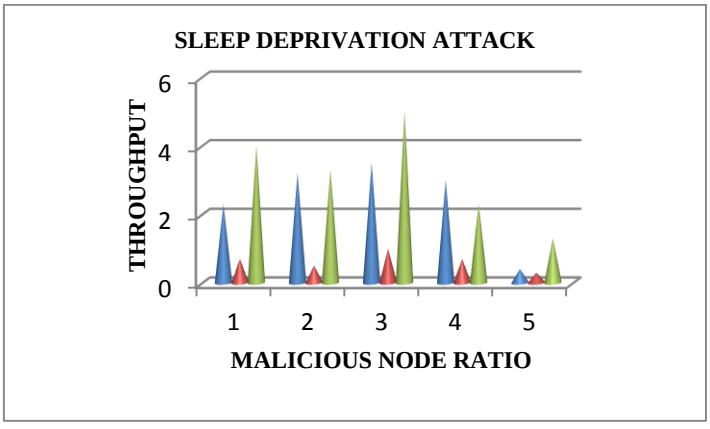

Figure 4: Throughput vs. malicious node ratio for DOS attack

Figure 4 shows the differentiation of throughput with change in malicious node ratio in case of DOS attack. Throughput is the rate of successful message delivery through a communication channel. How much higher the throughput better will be the protocol. The throughput is low in case of optimal condition. RCA raises the value of throughput which is further gets higher by CBDS. The throughput after CBDS however shows a varying trend. This too remains an area for further improvement.

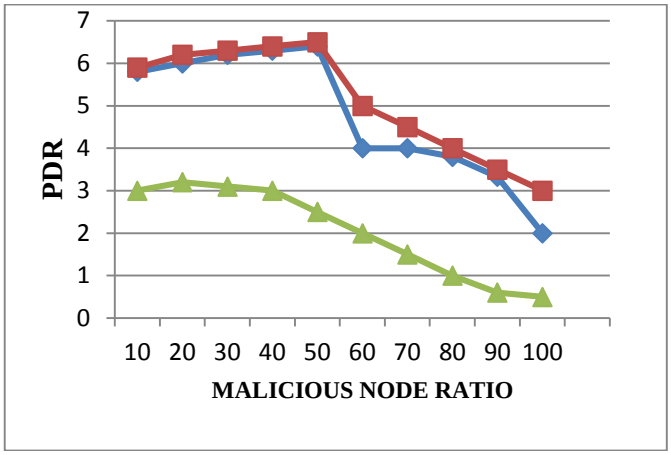

Figure 5: PDR vs. malicious node ratio for Sleep Deprivation Attack with CBDS time

Figure 6 shows the varied Packet Delivery Ratio with malicious ratio for Sleep Deprivation Attack. Packet delivery ratio is the ratio of the number of delivered data packet to the destination. This shows the level of data which is delivered to the destination. The higher value of packet delivery ratio refers the better performance of the protocol.

PDR = Σ Number of packet receive / Σ Number of packet sent

In optimal conditions The Packet Data Ratio value for different malicious node ratio is high. When the system is for sleep deprivation attack the PDR value becomes lesser than that in optimal conditions. while applying CBDS increases the corresponding PDR value even further to optimal conditions.

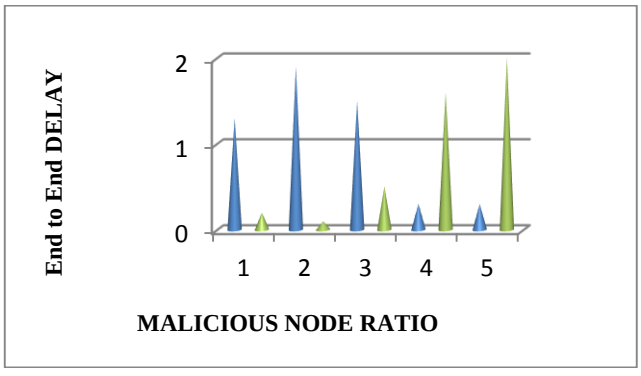

Figure 6: End to end delay vs. malicious node ratio for SDA

Figure 6 shows the differentiation of end to end defer with respect to malicious node ratio in case of sleep deprivation attack. End-to-end defer is defined as the average time taken by a data packet to be received by the destination. It also includes the defer which is caused by route discovery process and the queue in transmitting the data packet. Only the data packets which are successfully sent to other nodes. The lesser value of end to end defer tells the better achievement of the protocol. However SDA is gushing type attack and lower values of end to end defer means less time for analysis of data. Thus the values should be greater.

End to End defer = Σ (receive time – send time) / Σ Number of connections

For optimal conditions the end to end defer is shown to be greater (shown in orange). Whereas for sleep deprivation attack the value comes down (as shown by red bar). Application of CBDS changes the end to end defer value to bring it closer to the optimal conditioned values. The optimal graph increases first until malicious node ratio of 3 and then gradually comes down. At malicious node ratio 3, we notice that the value of end to end defer after implementation of CBDS is still lower than before the practisation This remains the area of future improvement to work on these exceptions and improve the efficiency of CBDS scheme.

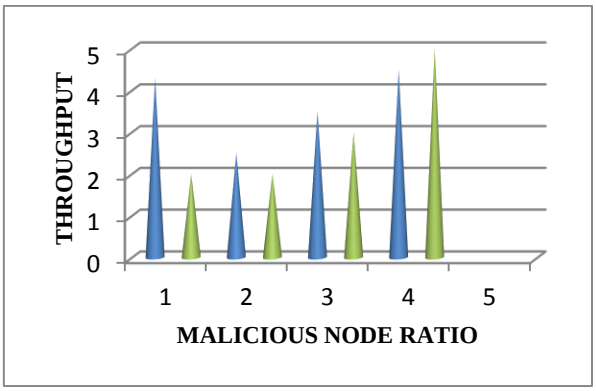

Figure 7: Throughput vs. Malicious node ratio for SDA

Figure 7 shows the varied throughput with change in malicious node ratio if it is sleep deprivation attack. Throughput is the rate of successful data sent through a communication channel. Higher the throughput better is the protocol.The throughput is high in case of optimal condition. SDA brings down the value of throughput which is again cleared and changed by CBDS with the given time. The throughput value after practising CBDS is in fact greater than that in case of optimal condition.

V CONCLUSION

In this paper, it is analyzed that the security threats of an ad-hoc network faces and presented the security objective that need to be achieved. On one side, the security-sensitive applications of an ad-hoc network requires high measurement of security. The research on MANET security is still in its early stage. The existing proposals are typically attack-based in that they first identify various security threats and then enhance the existing protocol or propose a new protocol to prevent such threats but these were

done with a little or slight slow process. Because the solutions are designed explicitly with the CBDS technique that combines both proactive and reactive detection schemes which enhances its efficiency of detection. It can be prepared and arranged for both self prepared and arranged node topologies as well as randomly prepared and arranged node topologies. It is a network wide detection scheme whereas on detection of malicious node the whole network is told about the detection by giving a Trace Time. CBDS has been successfully implemented on black hole and grey hole attacks before and has proved to be equally efficient in case of DoS attacks and Sleep deprivation attacks in our experiment too. Simulation result have shown an enhanced response and increased detection for CBDS.

REFERENCES

[1]Akinlemi Olushola.O, Cooperative Bait Detection Scheme (CBDS) To Avoid the Collaborative Attacks of Nodes in MANET, Visvesvaraya Technological University, Belgaum, Karnataka, Impact Factor (2014).

[2]Divjot Kaur, International Journal of Advances in Computer Science and Communication Engineering Rayat College Of Engg. & IT, Ropar, Punjab, Vol 3, Issue 1 (August 2015).

[3]Kailashchandra.D, Detection of Black Hole and Worm Whole Attacks in MANETS, SSRG International Journal of Mobile Computing & Application, Jawaharlal Nehru Technological University College of Engineering, Kakinada, June 2015.

[4]Khushboo Sawant, Flooding Attacks over MANET Environment, Lakshmi Narayan College of Technology Indore, Vol. 4, Issue 5(Version 6), May 2014.

[5]Navdeep Kaur, Implementing MANET Security using CBDS for Combating Sleep Deprivation & DOS Attack, Maharishi Ved Vyas Engineering College Jagadhari, 2014.