Implementing MANET Security using CBDS for Combating Sleep Deprivation & DOS Attack

Navdeep Kaur* and Mouli Joshi **

***Pursuing M.tech (CSE), **Assistant Professor**

Maharishi Ved Vyas Engineering College

Jagadhari, Yamuna Nagar 135003

(Received 10 June 2014 Accepted 17 June 2014)

***Abstract-** With the proliferation of mobile technology, the wireless communication is becoming more popular than ever before. This is due to technological advances in laptops & wireless data communication devices such as wireless modems & wireless LANS. It has lead to lower prices & higher the data rates which has resulted in rapid growth of mobile computing. The security threats may vary from active impersonation attacks to passive eavesdropping. Implementing Security & mitigating threats in MANET has significant challenges because its dynamic properties make it harder to be secured than the other types of static networks.*

***Keywords:** MANET(Mobile Ad-Hoc Network), iMANET (Internet MANET),VANET(Vehicular MANET), InVANET (Intelligent Vehicular MANET), AODV (Ad-hoc On Demand Distance Vector).*

I INTRODUCTION

MANET is a collection 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.

Figure 1 shows how data is send from transmitter to receiver.

Each device in a MANET is free to move randomly in any direction, and will therefore change its links to other devices again and again. Each must forward traffic unrelated to its own use, and therefore can acts as router. The major challenge in building a MANET is making each device to monitor and maintain the information required to traffic routing ..The objective of this paper is to propose a cooperative bait detection scheme to combat sleep deprivation and denial of service attack over MANET. This scheme merges the proactive and reactive defence architecture in MANET by using the first hop neighbour address as destination address to bait the malicious nodes which were causing the attack.

A vulnerability is a weakness in security system [2]. A particular system may be vulnerable to unauthorized data access because the system does not verify a user's identity before allowing dataease to access. MANET is more vulnerable than wired network. Some of the vulnerabilities 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 emerging 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

Chin-Feng Lai et al, IEEE [2014]. In this paper the author[1] tries to solve the issues of blackhole and grayhole attacks caused by malicious nodes by designing a Dynamic Source Routing (DSR) mechanism known as Cooperative Bait Detection Scheme (CBDS). It combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique. Cooperative Bait Detection scheme is proposed to detect malicious nodes in Manet for the grayhole and blackhole attacks.[2]

Cooperative Bait Detection Scheme (CBDS) has been used to tackle blackhole and grayhole attacks caused by malicious nodes [1]. CBDS combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique.

In Game theory mechanism each node needs to know only its own state information and aggregate effect of the other nodes in the MANET network. It's a fully distributed scheme. In future the mechanism could be extended to multiple attackers and multiple defenders.

Some devices in network might be interested in computing some functions of their private inputs without disclosing the inputs to the other devices, such type of computation is Secure Multiparty Computation (SMC) [4]. The solution to this problem could be by modification of data inputs to prevent eavesdropping. Other approach is by making the identity ambiguous to hide it from other parties. The major focus in the paper is made on that how the SMC solutions can be used for preserving the privacy during the computation.

Attacks might be active or passive. According to hierarchy idea of OSI model the security architecture of the MANET can be divided into five layers [5] as infrastructure layer, network security layer, application layer and security layer describing functions of each layer in detail. Security architecture of MANET is designed according to OSI hierarchy. Relations 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.

III PROPOSED ALGORITHM

A. DESIGN CONSIDERATION

- 1) Number of Nodes :
- 2) Network area:
- 3) Radii of node:
- 4) Energy:

B. DESCRIPTION OF PROPOSED ALGORITHM

Each node sends a route request signal (RREQ). The neighbour nodes receive the RREQ signal and reply with a RREP signal. If the RREP signal is received back by the transmitting node, the system is judged as normal and data transmission can begin. However if the transmitting node does not receive back RREP signal delivery hop limit is checked. If the delivery hop limit has not exceeded the threshold, RREQ is resend. Otherwise, the RREQ sending is terminated.

Once the system starts transmitting data signal normally, packet delivery ratio is scanned. If the packet delivery ratio is above threshold limit, then no malicious nodes are present and the process terminates. However if packet delivery ratio drop is detected, a bait RREQ 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 RREP response to the bait RREQ, reverse tracing program is triggered and test packets and recheck messages are sent to confirm malicious node detection. On confirmation of malicious node, source node updates its list of malicious node with this new entry and broadcasts an alarm signal inside the network for all the nodes to follow suit. When all the nodes have updated their list of malicious nodes, the detected node is blacklisted and further communication to the node are stopped.

In a randomly deployed node topology source node chooses the cooperative bait address randomly from its one hop neighbour nodes and sends the bait RREQ.

Figure 2: Flowchart of Proposed Work

IV PSEUDO CODE

```

Step 1: Send RREQ
Step 2: if ( RREP == D true) \\ If RREP is from true destination
Step 3: system=1; \\ system is working
Step 4: else
Step 5: if (Time > T) \\ T is the discovery time threshold
Step 6: end process;
Step 7: else
Step 8: send RREQ again;
Step 9: end if
Step 10: end if
Step 11: if (PDR < T1) \\ if packet delivery ratio drops to a certain threshold
Step 12: Send Bait RREQ'
Step 13: else
Step 14: end process
Step 15: end if
Step 16: if (RREP == true) \\ if any RREP
Step 17: Trace Mechanism = 1 ; \\ Trigger trace mechanism
Step 18: else
Step 19: end process;
Step 20: end if ;
Step 21: Initiate trace mechanism;
Step 22: MN detected;
Step 23: MN = black listed; \\ malicious is black listed
  
```

V SIMULATION RESULTS

DOS

Figure 3: PDR vs. malicious node ratio for DOS attack

Figure 3 shows the variation 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 delivered data packet to the destination. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol.

$$PDR = \frac{\sum \text{Number of packet receive}}{\sum \text{Number of packet send}}$$

In ideal conditions the PDR value for different malicious node ratio is high. When the system is under DOS attack the PDR value becomes lower than that in ideal conditions. However applying CBDS increases the corresponding PDR value further to ideal conditions.

Figure 4: End to End delay vs. malicious node ratio for DOS attack

Figure 4 shows the variation of end to end delay with respect to malicious node ratio in case of DOS

attack. End-to-end delay is defined as the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. The lower value of end to end delay means the better performance of the protocol. However DOS attack is flooding type attack and low values of end to end delay means less time for analysis of data. Thus the values should be higher.

$$\text{End to End delay} = \frac{\sum (\text{arrive time} - \text{send time})}{\sum \text{Number of connections}}$$

Under ideal conditions the end to end delay is shown to be high (shown in blue). When under DOS attack this value increases (as shown by green bar). Application of CBDS changes the end to end delay value to increase it further. At malicious node ratio 3, we notice that the value of end to end delay for DOS attack is lower than ideal conditions. The value is increased by implementation of CBDS attack

Figure 5: Throughput vs. malicious node ratio for DOS attack

Figure 5 represents the variation of throughput with change in malicious node ratio in case of DOS attack. Throughput is the rate of successful message delivery over a communication channel. Higher the throughput better is the protocol.

The throughput is low in case of ideal condition. RCA raises the value of throughput which is further increased by CBDS. The throughput after CBDS however shows a varying trend (it is lower than the throughput value before implementing CBDS in some cases while in other it is higher). This too remains an area for further improvement.

Sleep Deprivation

Results for implementation of Cooperative Bait Detection Scheme (CBDS) technique on Sleep Deprivation Attack (SDA) and Denial Of Service Attack (DOS) are graphically discussed below:

- The line/bar in blue represents the ideal condition, i.e. without any attack.
- The line/bar in green represents the results measured after the specific attack.
- The line/bar in red represents the results after implementation of CBDS on the specific attack.
- Malicious node ratio = number of malicious node / total number of nodes

Figure 6: PDR vs. malicious node ratio for SDA

Figure 6 shows the variation of Packet Delivery Ratio (PDR) with malicious node ratio for Sleep Deprivation Attack (SDA). Packet delivery ratio is the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol.

$$PDR = \frac{\sum \text{Number of packet receive}}{\sum \text{Number of packet sent}}$$

In ideal conditions The PDR value for different malicious node ratio is high. When the system is under sleep deprivation attack the PDR value becomes lower than that in ideal conditions. However applying CBDS increases the corresponding PDR value even further to ideal conditions.

Figure 7: End to end delay vs. malicious node ratio for SDA

Figure 7 shows the variation of end to end delay with respect to malicious node ratio in case of sleep deprivation attack. End-to-end delay is defined as the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. The lower value of end to end delay means the better performance of the protocol. However SDA is flooding type attack and low values of end to end delay means less time for analysis of data. Thus the values should be higher.

$$\text{End to End delay} = \frac{\sum (\text{arrive time} - \text{send time})}{\sum \text{Number of connections}}$$

Under ideal conditions the end to end delay is shown to be high (shown in blue). When under sleep deprivation attack this value decreases (as shown by green bar). Application of CBDS changes the end to end delay value to bring it nearer to the ideal condition values. The ideal graph increases initially until malicious node ratio of 3 and then gradually decreases. At malicious node ratio 3, we notice that the value of end to end delay after implementation of CBDS is still lower than before the implementation. This remains the area of future improvement to work on these exceptions and improve the efficiency of CBDS scheme.

Figure 8: Throughput vs. Malicious node ratio for SDA

Figure 8 represents the variation of throughput with change in malicious node ratio in case of sleep deprivation attack. Throughput is the rate of successful message delivery over a communication channel. Higher the throughput better is the protocol. The throughput is high in case of ideal condition. SDA brings down the value of throughput which is again improved by CBDS. The throughput value after implementation of CBDS is in fact higher than that in case of ideal condition.

VI CONCLUSION

In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of security on the other hand, ad-hoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with The CBDS technique combines both proactive and reactive detection schemes which enhances its efficiency of detection. In can be deployed for both self deployed node topologies as well as randomly deployed node topologies. It is a network wide detection scheme

wherein on detection of malicious node the entire network is informed about the detection by Alarm signal. 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.

VII FUTURE SCOPE

The networking opportunities for MANETs are intriguing and the engineering tradeoffs are many and challenging. This paper presented a description of ongoing work and a vision for the future integrating of mobile networking technologies into the Internet. There is a need for standardized, secure, and interoperable routing and interface solution(s) for mobile networking support. The future holds the possibility for deploying inexpensive, IP internetworking compatible solutions to form self-organizing, wireless routing fabrics for commercial and military use. In future work, CBDS can be deployed on various other security threats in MANET and it results could be checked for validation. A slight variation in throughput and end to end delay is observed in case of CBDS which remains an area of further improvement.

REFERENCES:

- [1] Chin-Feng Lai, Han-Chieh Chao, Jian-Ming Chang, Isaac Woungang, and Po-Chun Tsou, *Member, IEEE*. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach.
- [2] S. M. A. Pari, M. Noormohammadpour, M. J. Salehi, B. H. Khalaj, H. Bagheri, and M. Katz, "A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks," 2013 IFIP Wireless Days (WD), Valencia, 2013, pp. 1-3. doi: 10.1109/WD.2013.6686475
- [3] Rakesh kumar Sahu, Narendra S chaudhari "performance evaluation of ad hoc network under black hole attack 978-1-4673-4805-8/\$31.00, IEEE 2012
- [3] Richard Yu, Helen Tang, Minyi Huang and Yanwei Wang, *Member, IEEE*. A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks.
- [4] Durgesh Kumar Mishra (Acropolis Institute of Technology and Research, Indore, India). Mahakal Singh Chandel (Arjun Institute of Advanced Studies and Research Centre, Indore, India), Rashid Sheikh. Security Issues in MANET: A Review.
- [5] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng College of Computer Science Chongqing University Chongqing, China. Research on MANET Security Architecture design.