Volume 5, Issue 9, September 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review on Acknowledgement Based Scheme of Intrusion Detection System on MANET

Amit Khatri
Research Scholar (CTA)
Dept. of Computer Science & Engg.
Gyan Ganga College of Tech. Jabalpur, India

Deepak Singh Rajput
Assistant Professor
Dept. of Computer Science & Engg.
Gyan Ganga College of Tech. Jabalpur, India

Abstract- Among all the wireless networks, Mobile Ad hoc NETwork is vital and a unique application as it does not require a fixed network infrastructure. In this type of infrastructure nodes communicates directly with each other when they are in a same communication range. As MANET is having a distributed architecture and changing topology, so a traditional centralized monitoring system is no longer feasible in MANET, and thus it is vulnerable to attacks. The main attacks are packet dropping or black hole attack and it is very hard to detect and prevent them. In this paper we are proposing an improvement over EAACK scheme by doing a comprehensive investigation on detection of misbehavior links and malicious nodes.

Keywords- MANET, Packet DroppingAttack, EAACK

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a type of Wireless ad hoc network. It is deployed in various applications such as research and rescue, military and disaster recovery. A Mobile Ad hoc Network is a collection of wireless mobile nodes that are able to communicate with every other nodes without any fixed infrastructure. They communicate via bidirectional wireless links either directly or indirectly and communication occurs within the transmission range. In MANET, pair of nodes exchange message either over a direct wireless links or over a sequence of wireless links including one or more intermediary nodes.

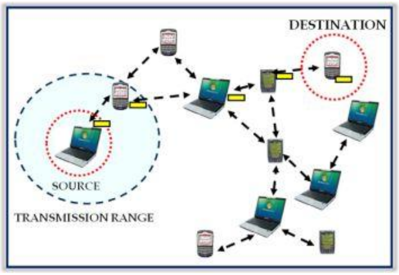

Fig:1 Mobile Ad hoc Network (MANET)

MANET is also capable of creating self-maintaining and self- configuring architecture without the need of any centralized infrastructure. These properties of MANET are used in emergency circumstances where such centralized infrastructure is unavailable. One of the major advantages of MANET is its ability to allow data communication between different parties and still maintain their mobility.

MANET are very popular in critical mission applications and because of optimum distribution of nodes and open medium makes it vulnerable to various types of attacks, at all layers, basically in the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network. Therefore network security plays an important role in MANET. Due to nodes lack of physical protection, malicious attackers can easily capture and capsulate nodes to achieve attacks. The assumption in MANET that every node in the network works cooperatively with other nodes, leaves the attackers with the opportunities to achieve significant on the network with just one or two compromised nodes. [1]

II. ATTACKS IN MANET

Mobile ad hoc (MANETs) are networks which are constructed on an ad-hoc basis, where the communication systems are mobile in nature and make use of wireless links for communication among each other. These do not rely on a centralized infrastructure or administration server to work. Open network architecture, shared wireless medium, resource constraints, and dynamic network topology are the few constraints which MANETs impose to achieve following security services i.e., integrity, anonymity, confidentiality, authentication and availability. There are several network layer attacks or intrusions which are known for MANET. Here we present a brief introduction of major network layer attacks and list the several possible types of attacks. Classification of Network Layer attacks in mobile ad-hoc networks is divided into two main divisions, known as passive attacks and active attacks.

Passive Attacks: Passive attacks are those where the operation of the routing protocol is not disturbed by the intruder but it tries to gets some important information through traffic analysis. This in turn can lead to the disclosure of critical knowledge of the network or nodes like the network topology, node locations or the identity of important nodes. Few examples of passive attacks are Eavesdropping and Traffic Analysis and Location Disclosure.

Active Attacks: In active attacks, intruders initiates activities such as forging, modifying, injecting, fabricating or dropping data or routing packets, which results in various disruptions to the network Some of these attacks are caused by a single activity or by a sequence of activities by colluding intruders. Active attacks disturb the operations of the network so severely that they degrade the network performance significantly or can bring down the entire network, as in the case of denial of service attacks. Some common active attacks are Malicious Packet Dropping, Routing Attacks, Sleep Deprivation Attack, Black hole attack, Grey hole attack, Rushing attack, Sybil attack, etc.

Packet dropping attack

In MANET, a packet dropping attack is a type of denial of service in which a node in the network will drop packets instead of forwarding them. The packet dropping attack [3], [6], [11] is difficult to detect and prevent because it occurs when the node becomes compromised due to a number of different causes. In terms of the strategy adopted by the malicious node to launch the attack the packet dropping attack can be classified into several categories:

- The malicious node can intentionally drop all the forwarded packets going through it.
- It can selectively drop the packets originated from or destined to certain nodes that it dislikes.
- A special case of black hole attack dubbed gray hole attack is introduced. In this attack, the malicious Node retains a portion of packets while the rest is normally relayed [2].

III. SCHEMES FOR SELFISH NODE DETECTION IN MANET

Various detecting and mitigating routing misbehavior schemes are Watchdog approach, Collaborative security architecture, Cross layer approach, Collaborative watchdog approach, TWOACK approach, Adaptive ACKnowledgment scheme (AACK), Enhanced Adaptive ACKnowledgment scheme (EAACK).

Enhanced Adaptive ACKnowledgment scheme (EAACK):

EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). EAACK scheme, assume that the link between each node in the network is bidirectional. Also, for each communication process, both the source node and the destination node are not malicious.

- *ACK*: It is mainly end to end acknowledgment scheme. It acts like a fraction of the cross scheme aim to decrease network transparency as no network misbehavior is detect.
- *S-ACK*: Secure- acknowledgment scheme is an enhanced report of the TACK scheme. The standard is to let each three following nodes works in a grouping to identify misbehavior nodes. For each three following nodes in this way, the third node is necessary to send an S ACK packet to the first node. The meaning of introduce S-ACK mode is to identify misbehavior nodes in the existence of receiver collisions or limited transmission power
- *MRA*: The Misbehavior Report Authentication (MRA), scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. By adopting an alternative route to the destination node, the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehavior re-port and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

IV. VULNERABILITIES IN EXISTING SCHEME

Node Misbehavior in collusion:

Scenario of collusion attack is explained by the figure given below:

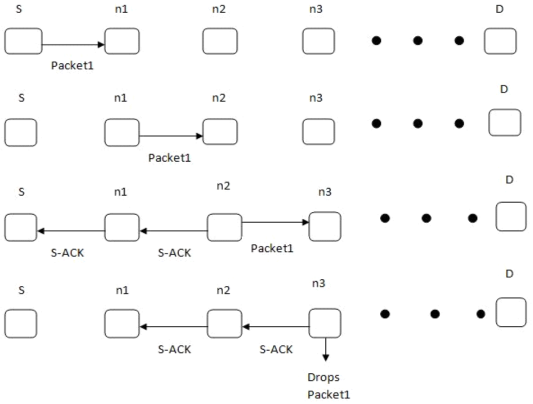

Fig:2 Collusion Attack

Source node S sends a Packet1 to node n1 then n1 forwards this packet to n2. Since, n2 is two hop away from S it redirects S-ACK packet to S following the reverse path and forwards Packet1 to n3. By receiving this digitally signed S-ACK from n2, S is ensured that till node n2 there is no misbehavior. Now, n3 is two hops away from n1 so it has to redirect S-ACK packet to n1. Node n1 is assured that there is no misbehavior till now. But n3 instead of forwarding Packet1 further it drops the packet which n2 knows but it hides the misbehavior of n3 and does not generate any misbehavior report. So it is found that n2 and n3 performs malicious activity in collusion. But this goes undetected by node S. Misbehavior in collusion is severe in MANET because it may drop packets or forges the packet if no encryption is there.

V. CONCLUSION

The main drawback of EAACK is that it is not able to detect misbehavior if nodes misbehave in collusion. In future a new scheme may be proposed which will be able to detect misbehavior even if nodes misbehave in collusion whose performances will be measured by the following parameters [13]:

A. *Packet delivery ratio (PDR):* PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

B. *Routing overhead (RO):* RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

REFERENCES

[1] Trupti G. Ghongade1, Prof. Avinash P.Wadhe2 ,G. H. Raisoni College of Engineering & Management, SGBAU, Amravati, Maharashtra, *Review on Enhanced & Adaptive Intrusion Detection System for Manet,* International Journal of Futuristic Machine Intelligence & Application (IJFMIA) Vol. 1 Issue 1.

[2] A.Janani Department of IT, St.Joseph's College of Engineering Chennai, Tamil Nadu, India, A.Sivasubramanian Department of ECE, St.Joseph's College of Engineering Chennai, Tamil Nadu, India, S*urvey of packet dropping attack in manet* A.Janani et.al / Indian Journal of Computer Science and Engineering (IJCSE) Vol. 5 No.1 Feb-Mar 2014

[3] S. Djahel, F.N. Abdesselam, Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks : Proposals and Challenges, IEEE Communications Surveys & Tutorials, Vol.13, No.4, Fourth Quarter 2011.

[4] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad,2003."Chapter 30:Security in wireless adhoc networks, the handbook of Ad hoc wireless network". CRC PRESS Publisher

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000.

[6] E. Hernandez, M.D. Serrat, Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog, IEEE Communications Letters, Vol.16, No.5, May 2012.

[7] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A Review,"J. Comput. Sci., vol. 3, no. 8.

[8] L. Zhou and Z. Haas, "Securing ad-hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999

[9] E. Hernandez, M.D. Serrat, Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog, IEEE Communications Letters, Vol.16, No.5, May 2012.

[10] D.Johnson and D.Maltz, "Dynamic Source Routing in ad hoc wireless networks," in mobile computing. Norwell, MA: Kluwer, 1996, ch. 5.

[11] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010.

[12] Treesa Nice P. A."A Survey on Intrusion Detection Systems in Mobile Ad Hoc Networks" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 5, May 2013

[13] IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013 1089 EAACK—A Secure Intrusion-Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE