INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1072-1076
RECEIVED : 05/06/2016. PUBLISHED : 21/06/2016
June 21, 2016

AN ACKNOWLEDGMENT BASED APPROACH FOR THE DETECTION OF ROUTING MISBEHAVIOR IN MANETS

[1]S.Syeda Naheeda Tasneem, [2]A.Sudakar M.E.,(Ph.D).,
[1]PG Scholar, Computer Science & Engineering, Bharathidasan Engineering College, Nattrampalli,
[2]Head Of Department, Bharathidasan Engineering College, Nattrampalli.

Abstract:

In the modernization world the usage of wireless network is more because of their scalability and mobility. MANET is most preferred by many applications because of its infra-structure less network model. The nodes in the network are self configurable. When two nodes come in a range they communicate each other otherwise the communication is established through the neighbor nodes. This type of open medium of communication has high level of threats and attacks. To avoid this, the intrusion-detection-system mechanism has to be introduced to protect MANET from attackers. To improve the security, use MANET system into various industrial applications and in emergency situations. This approach mainly focuses on the Intrusion Detection System.

Keywords—MANET,ACK,S-ACK,MRA,AACK,EAACK.

1. INTRODUCTION

The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, they are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, it is vital to address its potential security issues. A new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs are implemented. Compared to contemporary approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly affect the network performances.

2. RELATED WORK

The security problem and the misbehaviour problem of wireless networks including MANETs have been studied by many researchers. Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: Credit-based schemes and Reputation-based schemes. In this approach, the packet does not carry beans, but it is traded for beans by intermediate terminal nodes. Each intermediary buys it from the previous one for some beans, and sells it to the next one (or to the destination) for more beans. In this way, each intermediary that provided a service by

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1072-1076
RECEIVED : 05/06/2016. PUBLISHED : 21/06/2016
June 21, 2016

forwarding the packetincreases its number of beans, and the total cost of forwarding the packet is covered by the destination of the packet.In this model, the originator of charge is distributed among the forwarding terminal nodes in the following way: When sending the packet, the originator loads it with a number of beans sufficient to reach the destination Each forwarding terminal node acquires one or several beans from the packet and thus, increases the stock of its beans, The number of beans depends on the direct connection on which the packet is forwarded (long distance requires more beans). If a packet does not have enough beans to be forwarded, then it is discarded. Packet forwarding in the Packet Purse Model is illustrated in Figure 1. The basic problem with this approach is that it might be difficult to estimate the number of beans that are required to reach a given destination. If the originator underestimates this number, then the packet will be discarded, and the originator loses its investment in this packet. If the originator over-estimates the number, then the packet will arrive, but the originator still loses the remaining beans in the packet3.

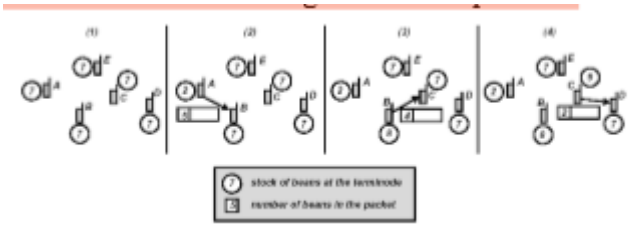

Fig.1. The Packet Trade Model

In this approach, the packet does not carry beans, but it is traded for beans by intermediate terminal nodes. Each intermediary buys it from the previous one for some beans, and sells it to the next one (or to the destination) for more beans. In this way, each intermediary that provided a service by forwarding the packet increases its number of beans, and the total cost of forwarding the packet is covered by the destination of the packet.

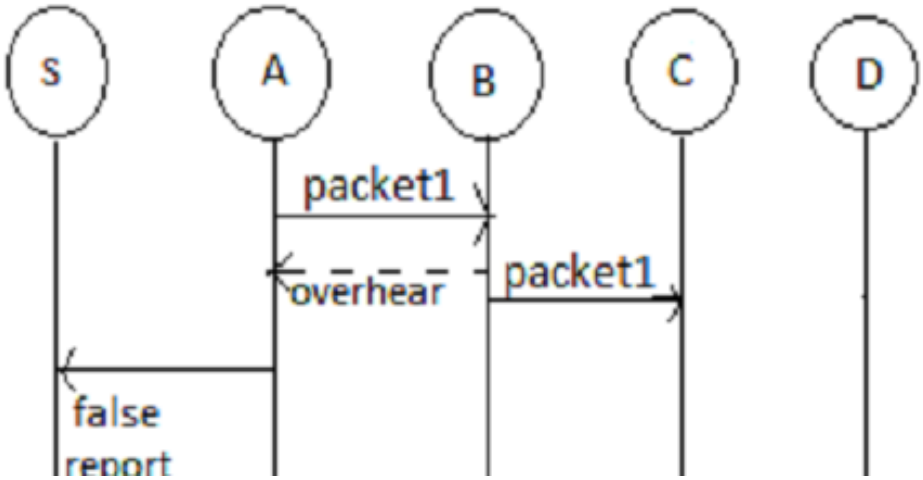

Fig.2. False misbehaviour report-send by node A to source S that node B is malicious though B forwards packet1 to node C.

In order to overcome the drawbacks in watchdog, a new scheme is proposed that is TWOACK, to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination.

3. PROPOSED SYSTEM

Existing schemes are largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic but they suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets. Another drawback of most previous schemes is the significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such overhead can easily degrade the life span of the entire network.

This routing protocol is an on demand protocol.In order to identify the most recent routes it employs the destination sequence numbers.The main difference between the Dynamic Source Routing and AODV is that DSR uses source routing in which a data packet carries the complete path to be traversed and in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission.

Later, a new technique called Enhanced Adaptive Acknowledgment is introduced. It solves all the three above

issues. This technique depends on acknowledged packets. So it also includes Digital Signatures to prevent the attackers from attacking the packets.EAACK consists of three parts:

1.ACK

2.Secure ACK (S-ack)

3.Misbehavior Report Authentication

4.Digital Signature

In ACK scheme, source node should get the acknowledgment packet within the predefined time period, it implies that destination node receives the packet and no malicious node exists in the route, otherwise send secure ACK packet. The intention of introducing S-ACK mode is to find malicious node by forming every three nodes into one group. First node sends packet to next node, third node is required to send back S-ACK packet to first node otherwise second and third nodes are malicious.

Then MRA scheme is to check whether misbehavior report is authentic by checking that reported missing packet is received by receiver via some other route. If destination node already receives this packet then node which generates this report is marked as malicious. Otherwise false misbehavior report is trusted and destination node is marked as malicious.

4. RESULT ANALYSIS

Digital Signature is used to digitally sign the packets both at the sender and receiver side to prevent the forging of packets. Thus required resources need to be incorporated for implementing digital signature and both DSA and RSA can be used. Also this project proposes a detection scheme called the cooperative bait detection scheme, which aims at detecting and preventing malicious nodes launching gray hole/collaborative black hole attacks in MANETs.

The CBDS scheme comprises three steps:
1) The initial bait step
2) The initial reverse tracing step and
3) The shifted to reactive defense step.

The first two steps are initial proactive defense steps, whereas the third step is a reactive defense step.

The watchdog detection mechanism has a very low overhead. Unfortunately, the watchdog technique suffers from several problems such as ambiguous collisions; receive collisions, and limited transmission power. The main issue is that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link. A misbehaving node can either be the sender or the receiver of the next-hop link, we focus on the problem of detecting misbehaving links instead of misbehaving nodes. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet: It will not be forwarded further. The result is that this link will be tagged. Our approach discussed here significantly simplifies the detection mechanism.

CONCLUSION

In this survey paper, a comparative study of Intrusion-Detection Systems (IDS) for discovering malicious nodes and attacks on MANETs is presented. Due to some special characteristics of MANETs, prevention mechanisms alone are not adequate to manage the secure networks. In this case detection should be focused as another part before an attacker can damage the structure of thesystem. we study about secure IDS named EAACK protocol specially designed for MANETs and in future it is required to compare against other popular mechanisms. Security is major part in MANETS, hybrid cryptography architecture will tackle the issue in an efficient manner. This way we can better preserve battery and memory space of mobile nodes.

REFERENCES

[1] D. Johnson and D. Maltz, "Dynamic Source Routing in *adhoc* wireless networks," in *Mobile computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[2] Hoang Lan Nguyen, Uyen Trang Nguyen, Elsevier "A study of different types of attacks on multicast in mobile ad hoc networks" AdHoc Networks(2008) 32-46.

[3] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[4] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[5] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[6] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[7] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[8] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[9] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 747–752.