IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 2, February 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202041 |

EAACK Based Detecting and Preventing Misbehavior Nodes Technique in MANET

Mr.R.Mohankumar, Naveen P

Assistant Professor, Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

ABSTRACT- Security has become an important part in Mobile Ad hoc Networks because of their dynamic mobility, scalability and shared resources. MANETs is a collection of mobile nodes and it does not require a fixed infrastructure. So it acts as a dynamic topology for many applications. MANETs are highly vulnerable for attacks because of their open medium, rapidly changing topology, lack of centralized monitoring. Both Watchdog and TWOACK methods are not sufficient for protect MANETs in the cases of receiver collision, limited transmission power and false misbehavior report. To overcome such attacks the proposed technique is a secure intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs.

KEYWORDS - Mobile Ad hoc NETwork, Intrusion Detection System, Watchdog, EAACK.

1. INTRODUCTION

One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring down the whole network. This problem has led to a growing interest among the research community in mobile ad hoc networks (MANETs), wireless networks comprised of mobile computing devices communicating without any fixed infrastructure.

MOBILE ADHOC NETWORK

Wireless network has become very popular in the computing industry. Wireless network are adapted to enable mobility. In a mobile ad hoc network (MANET), a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [1].

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202041 |

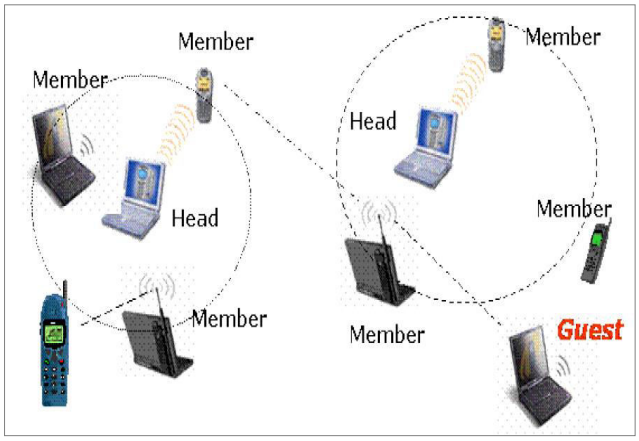

Fig.1.1. Mobile Ad-hoc NETwork(MANET)

This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. The above problem can be solved by two different types of networks. There are single-hop and multi-hop network infrastructure. In single-hop network the mobile nodes are communicate directly with each other. But in a multi-hop network, nodes are communicated using other intermediate nodes to transmit if the destination node is out of their radio range.

In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [2]; attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. In such case, it is essential to develop an intrusion-detection system (IDS) specially designed for MANETs.

II. NETWORK MODEL

INTRUSION DETECTION SYSTEM (IDS)

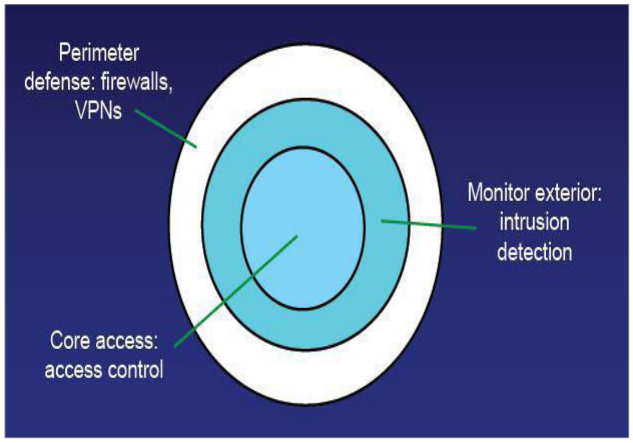

Fig.2.1. Intrusion Detection System (IDS)

Compare to fixed networks the mobile Ad Hoc networks needs more security mechanisms. MANET has features such as an open medium, dynamic changing topology, and the lack of a centralized monitoring and management point, many of the intrusion detection techniques developed for a fixed wired network are not applicable in MANET. Zhang [3] gives a specific design of intrusion detection and response mechanisms for MANET. Marti [4] proposes two mechanisms: watchdog and path rater, which improve throughput in MANET in the presence of nodes that agree to forward packets but fail to do so. Intrusion Detection Techniques for Node Cooperation in MANETs:

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202041 |

Since there is no infrastructure in mobile ad hoc networks, each node must rely on other nodes for cooperation in routing and forwarding packets to the destination. Intermediate nodes might agree to forward the packets but actually drop or modify them because they are misbehaving. There are several proposed techniques and protocols to detect such misbehavior in order to avoid those nodes, and some schemes also propose punishment as well [5, 6].

III. EXISTING WORK

If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches. In this section, we mainly describe two existing approaches, namely,

1. Watchdog [7],
2. TWOACK [8].

3.1 WATCHDOG

The Watchdog is basically point-to-point acknowledgement scheme. Watchdog used to increase the throughput of the network. This contains the failure counter and pathrater. These two parts are very important to handle misbehavior nodes. Sender can send data packet to destination means destination wants to send back acknowledgement to source node. Source node cannot get acknowledgement within certain period of time it will reported as misbehaving and increase the failure counter. Next the pathrater can find another route by using reliable data [2]. Watchdog cannot detect misbehavior nodes in the following situation: Receiver collision, Limited transmission power, false misbehavior report, and Partial dropping.

3.2 TWOACK

The TWOACK scheme can be implemented on top of any source routing protocol such as DSR. This follows from the fact that a TWOACK packet derives its route from the source route established for the corresponding data packet. The TWOACK scheme uses a special type of acknowledgment packets called TWOACK packets, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that of data packets.

TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination.

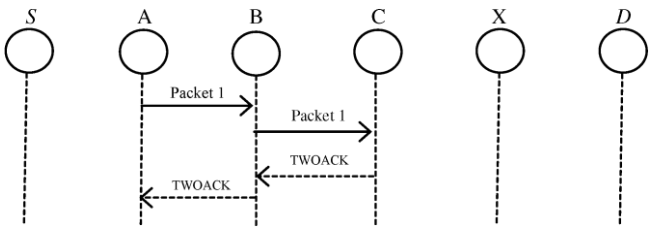

Fig.3.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocol s such as Dynamic Source Routing (DSR) [9]. The working process of TWOACK is shown in Fig.3.1. Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202041 |

The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route.

IV. PROPOSED SYSTEM

The proposed approach EAACK is designed to tackle three of the four weaknesses of Watchdog scheme, namely receiver collision, limited transmission power and false misbehavior.

The MANET uses the EAACK [3] technique for handling three of the previous four failures of watchdog. And also provide high performance of the network. This uses four main parts to handle the failures. These are summaries below.

4.1 ACK

ACK is essentially an End-to-End Acknowledgement scheme rather than watchdog. So the intermediate nodes cannot get other packets from any other nodes at the same time. So receiver collision cannot be occurs.

In ACK, the source node first sends out data packet to destination node. If destination is successfully receives packet, it required to send back an Acknowledgement to source node. Within the certain period of time, if source node receives Acknowledgement means transmission is successful. Otherwise source node will connected to S-ACK to detect misbehavior nodes in the route.

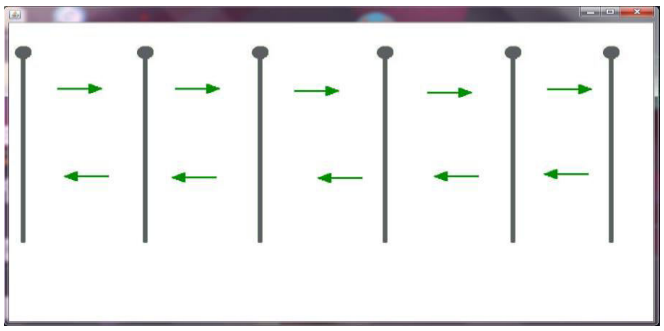

Fig.4.1. ACK Acknowledgement scheme

4.2 Secure-ACK

In Secure-ACK (S-ACK) scheme, at a time either data packet or acknowledgement packet only will be send, so limited transmission power will be managed. For every three successive nodes in the route, the third node is required to send an acknowledgement packet to first node.

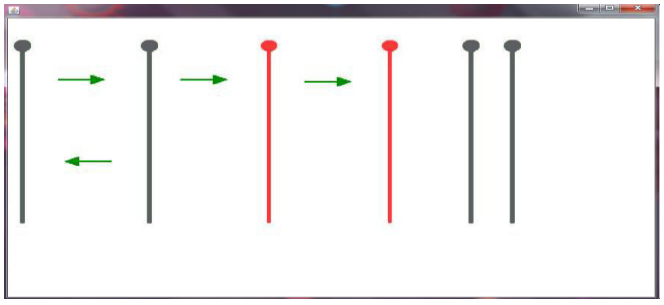

Fig.4.2. S-ACK scheme

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202041 |

The first node doesn't receive acknowledgement packet within predefined time period both second and third nodes are reported as malicious then it is switched to MRA scheme.

4.3 Misbehavior Report Authentication

Source node is starts to find out alternative routes to destination i.e. third node and send the data packet. This third node is send back acknowledgement means; the second node is misbehavior otherwise third node conclude as misbehaving. This can also identify the false misbehavior report.

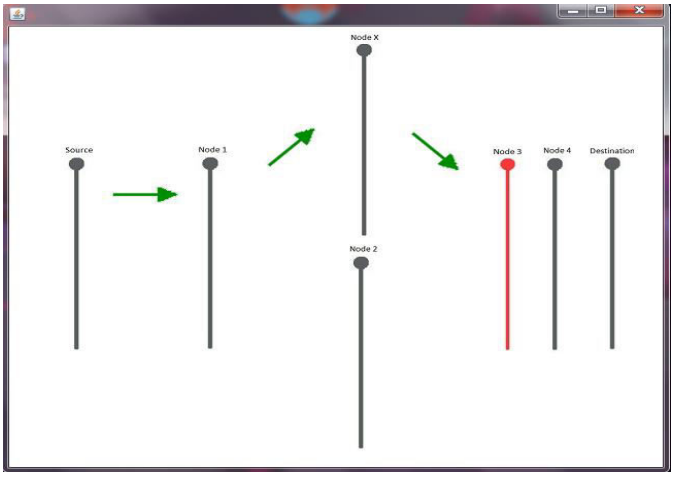

Fig.4.3. MRA scheme

4.4 Digital Signature

Fig.4.4. Encryption process

Digital signature is important to ensure that all packets in EAACK are authenticated. In case any malicious attackers get the data packet, it is impossible to access them. This uses either Digital Signature Algorithm (DSA) [10] or AES algorithm for encryption and decryption.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202041 |

The above four schemes are only detect the attacker. The prevention is also important part to prevent the data packets.

Packet filtering is another important mechanism for preventing data from attackers. This can find out alternative route and filter the data then finally send out in that selected route.

V. PERFORMANCE EVALUATION

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performance result comparison with Watchdog, TWOACK, and EAACK schemes.

The below Fig.5.1 shows the performance of EAACK based on packet delivery ratio in Mobile Ad hoc Networks.

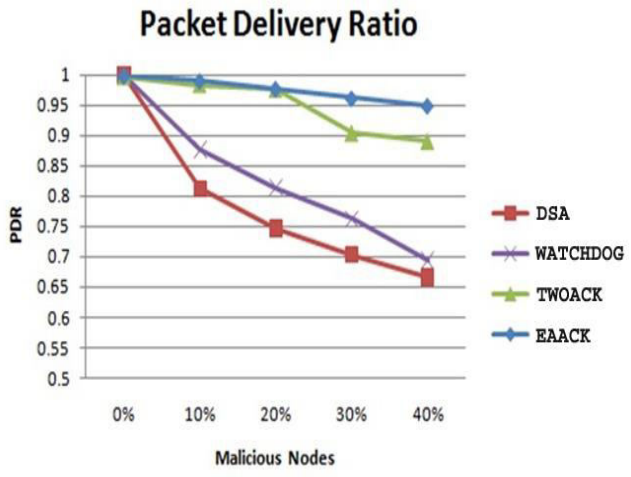

Fig.5.1. Performance results of all methodology

VI. CONCLUSION AND FUTURE WORK

Attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol specially designed for MANETs. The results demonstrated positive performances against Watchdog, and TWOACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Digital signature technique is also used for the preventing forged acknowledge attacks which also provide more security to the network.

In future work, we research to evade or minimize partial dropping in communication of mobile nodes.

REFERENCES

[1] 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.

[2] L. Buttyan and J. P. Hubaux, "*Security and Cooperation in Wireless Networks*," Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[3] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[4] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p.57.1, January 2003.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202041 |

[5] S. Buchegger and J. Le Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)," Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp.226-336, June 2002.
[6] P. Michiardi and R. Molva, \Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," Communication and Multimedia Security Conference (CMS'02), September 2002.
[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp.255–265.
[8] 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.
[9] D. Johnson and D. Maltz, “Dynamic Source Routing in ad hoc wireless networks,” in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.
[10] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details