International Journal of scientific research and management (IJSRM)
\||Volume||3||Issue||3||Pages|| 2470-2473||2015||
Website: www.ijsrm.in ISSN (e): 2321-3418

Prevention and Detection of Attacks in MANET Using Hybrid Approach

Ms.Apurva Kulkarni[1], Mr.Prashant Rewagad [2], Mr. Mayur Agrawal [3]

[1]Student, M.E. Computer Science and Engg Department, North Maharashtra University Jalgaon,India
apurvakulkarni152@gmail.com
[2]Hod of Computer Science and Engg. Department, North Maharashtra University Jalgaon,India
Prashant.rewagad@raisoni.net
[3]Faculty of Computer Science and Engg Department, North Maharashtra University Jalgaon,India
mayur.agrawal@raisoni.net

Abstract: *These MANET Stands for Mobile Ad-hoc network is an autonomous system of mobile routers and its associated hosts connected by wireless links. Because MANETS are mobile, they use wireless connections to connect to various networks Mobile Ad-hoc Network are formed dynamically by an Autonomous system of mobile nodes that are connected via wireless links. Nodes in MANET Communicate directly with each other when they are in same communication range otherwise they rely on their neighbors to send messages.MANET is a unique application. MANET is prone to various types of attacks due to its increased use. So Todays urgent need is to develop efficient intrusion-detection system to protect MANET from malicious attacks.This paper focuses on Enhanced Adaptive Acknowledgment (EAACK) which is an IDS Specially designed for MANET which will detect malicious nodes very efficiently and in addition to that EAACK can be extended further by adopting hybrid encryption as a preventive measure which will enhance security of messages in MANET.*

Keywords: EAACK , MANET , Hybrid Encryption

1. Introduction

MANET has natural mobility and scalability feature of wireless network so they are mostly preferred. Wireless networks have gained much more preferences over wired networks in the past few decades due to improvement in technology and objective of reducing costs. In a single-hop network, all nodes communicate directly with each other if they are within the same radio range. On the other hand, in a multi hop network, nodes depend on other intermediate nodes to transmit the data if the destination node is out of their radiorange. MANET does not have centralized and fixed network infrastructure thus, all nodes are free to move. There are many applications of MANET like it is used in critical mission applications like military conflict or emergency recovery, Disaster relief, Economic and commercial applications like mesh networks, Personal area network, Ad-hoc Gaming etc. It requires Minimal Configuration and it is easy to deploy. In wireless network security is of great importance. MANET is open medium so it makes node prone to various types of attacks. Nodes in MANET behave co-operatively with each other they rely on each other. In such scenario attackers can take advantage by inserting malicious or non-cooperative nodes into the network. Traditional Monitoring technique is no longer safe to protect nodes in MANET from attacks due to changing topology, open medium and its wide distribution so it is crucial todevelop an intrusion-detection system (IDS) specially designed for MANETs. Set of actions that attempt to identify and compromise the integrity, confidentiality, or availability of a resource is known as Intrusion Detection. Next section, mainly concentrate on discussing the background information required for understanding EAACK better. Diagram Fig. 1 showing MANET mobile nodes.

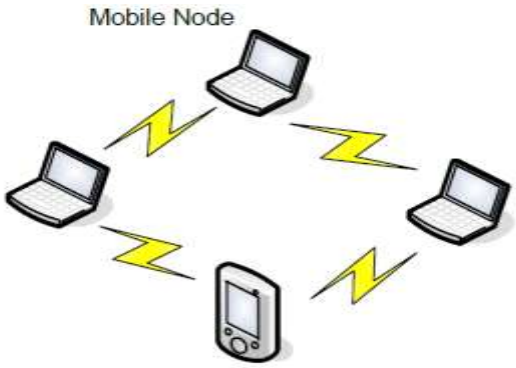


Figure 1. MANET

2. Literature Survey

Different IDS for MANET are:

A. Watchdog Scheme: The main idea of Watchdog scheme is Monitoring of nodes. Once a node is believe to be misbehaving the source would choose a new route with the aid of pathrater such Watchdog Mechanism do not perform well in presence of adverse channel conditions and interference allowing the misbehaving node to corrupt a single packet while being undetected with high probability. Watchdog detects malicious misbehaviours by listening to its next hop's transmission. When next node fails to forward the packet within a certain period of time and if watchdog node overhears that failure

counter is increased. Whenever a counter of node's failure exceeds a predefined threshold the Watchdog node reports it as misbehaving.The Watchdog scheme fails to detect malicious misbehaviours with the presence of the following that is partial dropping,ambiguous collisions, limited transmission power, collusion, receiver collisions and false misbehaviour report [1]. Figure 2, figure 3, figure 4 shows a receiver collision, Limited Transmission power, false misbehaviour report.

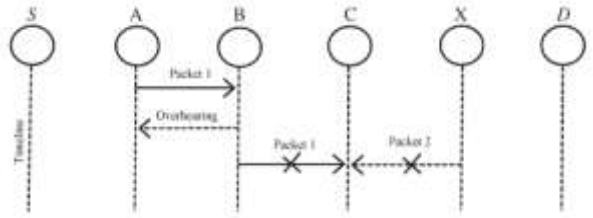


Figure 2. Receiver Collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

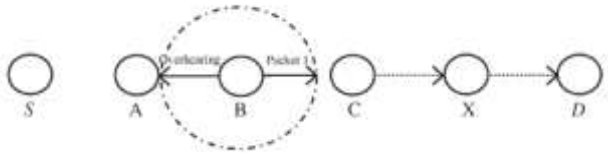


Figure 3. Limited Transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

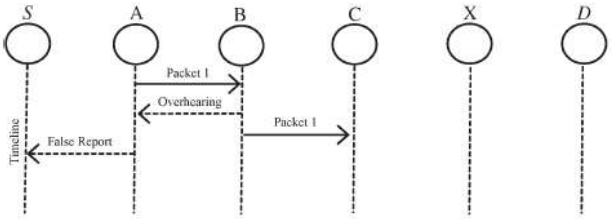
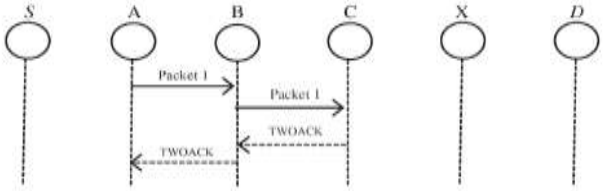


Figure 4. False Misbehaviour Report: Node A sends back a misbehaviour report even though node B forwarded the packet to node C.

B. TWOACK: It is use to resolve the receiver collision andlimited transmission power problems of Watchdog, it is neither an enhancement nor a Watchdogbased scheme. TWOACK detects misbehaving links by giving acknowledgement of each and every data packets transmitted from the source to the destination over each three consecutive nodes along the pathUpon receiving packet , each node is required to send back an acknowledgement packet along the route to the node that is two hops away from it down the route.Fig. 5. Showing TWOACK scheme where each node is required to send back an acknowledgement packet that is two hop away[1][17].



3. Misbehaviorreport authentication(MRA)

For Hybrid Encryption

1. AES Rjindael Algorithm

2. RSA

Figure 5. TWOACK Scheme

Problems posed by Watchdog such as receiver collision and limited transmission power is successfully solved by TWOACK scheme. However, significant amount of unwanted network overhead is caused by the acknowledgment process required in every packet transmission process.

C. AACK: AACK is Proposed by Sheltami et al.This Scheme is Based on the combination of TWOACK or TACK and ACK(end-to-end ACKnowledgement). Same network throughput is maintained and it also significantly reduces network overhead. In AACK Source node s sends packet 1 to destination node. This packet 1 is received by destination node after it is forwarded by all intermediate nodes. Once the packet is received by destination it is required to send back an acknowledgement packet to source node within predetermined time.If it fails to send back acknowledgement in predetermined time than source node switch to TACK scheme by sending out TACK packets.Fig. 6. Shows transmission of packet 1 from source to destination and receiving an Acknowledgement back.

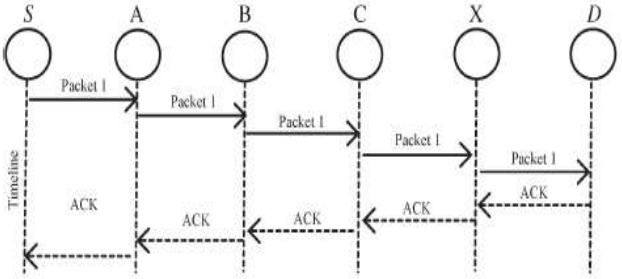


Figure 6. AACK Scheme

3. Problem Definition

TWOACK and AACK both of them are prone to the false misbehavior attack even though it solves two weaknesses, namely, receiver collision and limited transmission power. So Proposed IDS EAACK Enhanced Acknowledgement specially designed for MANET is designed to solve three of the six weaknesses of watchdog scheme namely limited transmission power, receiver collision and false misbehavior. To enhance the security of the network Hybrid Encryption scheme is used. In this way Proposed EAACK is used to avoid attacks and enhance security.

4. Scheme Description

In this section, we describe EAACK scheme in detail. In addition to that it can be made more secure with the introduction of Hybrid Encryption technique to enhance its security.EAACK is consisted of three major parts namely

1. ACK

2. Secure ACK (S-ACK),

ACK: As discussed before, end-to-end acknowledgment scheme is ACK. In Figure 7, source node S first sends out an ACK data packet Pad1 to the destination node D. If all the intermediate nodes are cooperative along the route between the nodes S and D then node D successfully receives packet

Pad1,now node D destination node is required to send an ACK acknowledgment packet Pak1 back in a reverse order along the same route to source. If node S receives Pak1 Within a predefined time period, then the transmission of packet from node S to node D is successful. Otherwise, sender node S will switch to S-ACK mode to detect the misbehaving nodes in the route by sending out an S-ACK data packet.

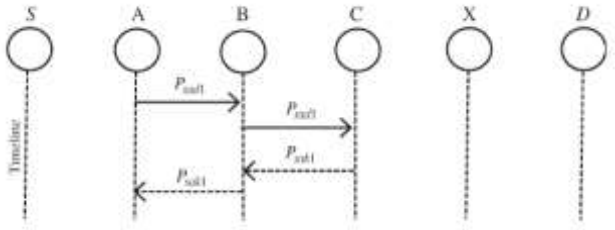


Figure 7 . ACK Scheme

SACK: The S-ACK scheme reduces extra traffic caused by TWO-ACK. It is derived from TWOACK Scheme but an

improved approach. The S-ACK principle is to let every three nodes which are consecutive to work in a group to detect nature of nodes weather they are misbehaving or not. In this the third node in consecutive group is required to send an S-ACK acknowledgment packet to the first node. The S-ACK mode intention is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. It also suffers from network overhead.

MRA Scheme:

Malicious Attackers generate false misbehavior report to falsely report innocent nodes as malicious. Now it's very difficult weather to trust it or not so MRA scheme is used to ensure. The MRA scheme is used to authenticate whether the destination node has received the reported missing packet through a different route. In MRA mode, Firstly local knowledge base of source node is searched and alternative route to the destination node exists or not is checked. The source node starts a DSR routing request if there is no other that exists to find another route. We circumvent the misbehavior reporter node by adopting an alternative route to the destination node. After receiving MRA packet by destination node it searches its local knowledge base and checks and compares if the reported packet was received. If it is received already, then misbehavior report is false and it is safe to conclude and the node that generated this report is marked as malicious. Otherwise misbehavior report is trusted and accepted. Figure 8, shows flow of execution of EAACK [1].

HYBRID Encryption: In Hybrid encryption and decryption AES-Rijndael algorithm with 128-bit session key value is used to encrypt the message. Hash value of the same message is calculated which is again encrypted using RSA algorithm with 1028 bit public key of the receiver. On the receiver side decryption is done using 128-bit session key value of AES-Rijndael of encrypted message and hash value which was encrypted is decrypted with RSA 1028 bit private key of the receiver. To ensure the integrity of message weather it has arrived intact or not is checked by calculating hash value of received message and then it is compared with the hash value which is received. Thus in this way we can enhance the security of messages and better increase the performance of network. This hybrid encryption will protect data in the packets and will provide better security.

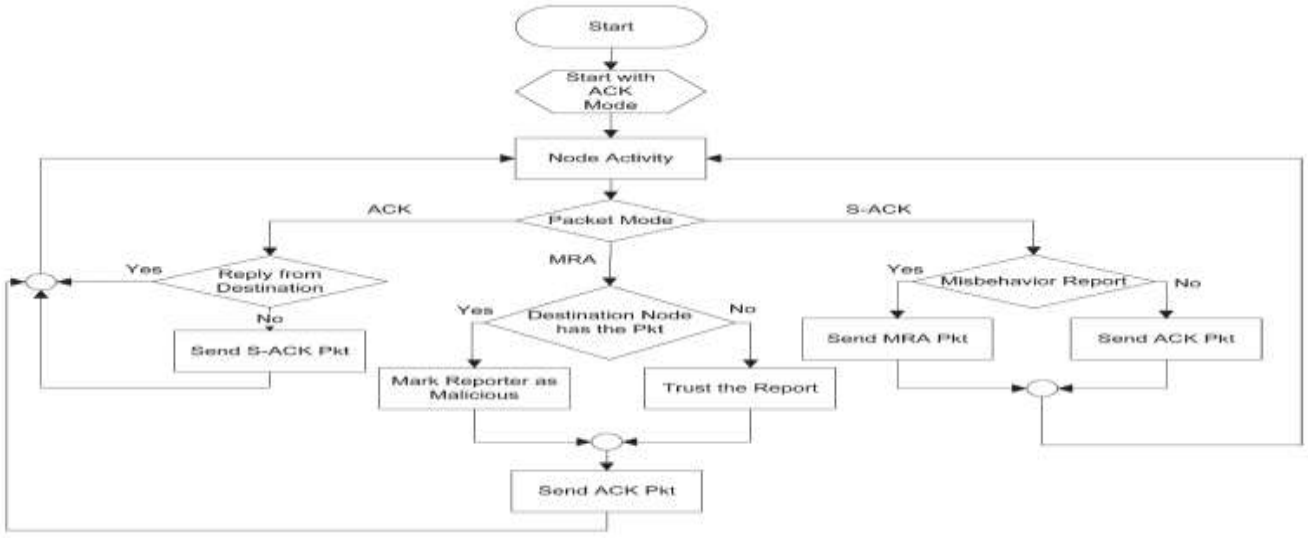


Figure 8. EAACK System

5. Conclusion and Future Work

Mobile Ad Hoc Network has always been prone to security attacks packet dropping has always been a major threat. EAACK Methods are concentrating only on detection of malicious nodes.So it can be further extended to include hybrid encryption to strengthen the security of nodes. Detection of malicious nodes can be done by using EAACK and Prevention of messages, nodes and reducing network overhead caused by EAACK can be taken care by hybrid encryption using AES-Rijandel and RSA Algorithm. In future security can be further enhanced by improving Hash algorithms.

6. References

[1] Elhadi M. Shakshuki, *Senior Member, IEEE*, Nan Kang, and Tarek R. Sheltami, *Member, IEEE* EAACK—A Secure Intrusion-Detection

System for MANETs IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013
[2] K. Al Agha, M.-H.Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and
J.-B. Viollet, "Which wireless technology for industrial wireless sensor
networks The development of OCARI technol," *IEEE Trans. Ind. Electron.*,
vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
[3] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network
Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.
[4] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.
[5] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile
Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer- Verlag, 2008.
[6] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless
Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
[7] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7,Pp. 2759–2766, Jul. 2008.
[8] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks:
Challenges, design principles, and technical approach," *IEEE Trans. Ind.
Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
[9] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshopMobile Comput. Syst. Appl.*, 2002, pp. 3–13.
[10] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23.
[11] 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.
[12] 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.n AEC industry," *J. Inf. Technol. Const.*, vol. 9, pp. 313–323,2004.
[13] 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.
[14] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An
acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5,
pp. 536–550, May 2007.
[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu.Int. Conf. MobileComput.Netw.*, Boston, MA, 2000, pp. 255–265.
[16] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied
Cryptography*. Boca Raton, FL: CRC, 1996, T-37.
[17] 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.
[18] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in *Proc. IEEE Int. Conf.*