Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Secure Intrusion Detection System for MANET

Ms Priyanka P Kulkarni
Prof G.M.Bhandari Dept of Computer,
BSIOTR, Wagholi, India

Abstract— Mobile Ad hoc Network is a collection of wireless mobile nodes forming a network without using any existing infrastructure. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly. A new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs. EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report and compared it against other popular mechanisms in different scenarios through simulation. The results will demonstrate positive performances against Watchdog, TWOACK and AACK in the cases of receiver collision, limited transmission power and false misbehavior report. EAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances.

Keywords—ACK,EAACK,MANETetc

I. INTRODUCTION

MANET (Mobile Ad hoc network) is an IEEE 802.11 framework which is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links. Fig 1 shows

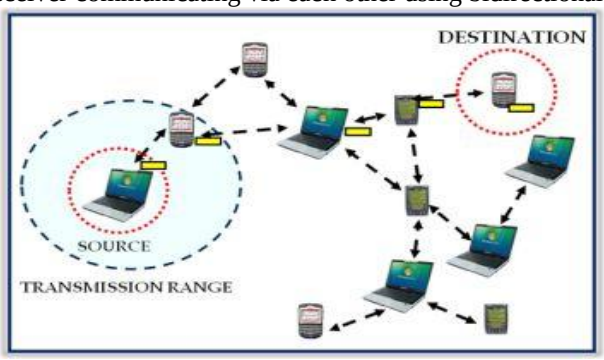


Fig 1 MANET Architecture

This type of peer to peer system infers that each node or user in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. MANETs are self-forming, self maintained and self-healing allowing for extreme network flexibility, which is often used in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances. MANETs are an appealing technology for many applications such as rescue and tactical operations due to the flexibility provided by their infrastructure. However, this flexibility comes at a price and introduces new security threats. Furthermore, many
conventional security solutions used are ineffective and inefficient for the highly dynamic and resource constrained environments where MANETs use might be expected. Unfortunately, the remote distribution and open medium of MANET makes them susceptible to various attacks. For example, due to lack of protection for nodes, malicious attackers can easily capture and compromise the mobile nodes to achieve attacks. Particularly, considering the fact – that most routing protocols in MANETs assume that every node in the network behave cooperatively with other nodes and presumably not a malicious one attackers can easily compromise MANETs by inserting malicious or non-cooperative node into the network. Due to MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. Hence, it is crucial to develop an intrusion detection system in MANETs. In this paper, we aim to develop such an efficient and reliable intrusion
detection system (IDS).

II. LITERATURE SURVEY

N. Kang, E. Shakshuki and T. Sheltami proposed a scheme called Enhanced Adaptive ACKnowledgement (EAACK). This scheme aims to overcome four of the weaknesses in traditional Watchdog mechanism, namely, ambiguous collisions, receiver collisions, limited transmission power and

false misbehavior. But there is no authentication for acknowledgements. The functions of detection scheme largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. So this scheme is not much efficient. Although the
simulation result showed that the proposed scheme outputs higher packet delivery ratio, it also has a higher overhead ratio with the increase of malicious nodes in the network. This is due to the introduction of MRA scheme. Elhadi M. Shakshuki proposed EAACK which was designed with the implementation of RSA and DSA digital signatures using DSR routing protocol. Performance evaluation was done and results were obtained. But this EAACK has no provision for handling link breakage and malicious source node scenario. Later the introduction of digital signature to prevent the attacker from forging acknowledgment packets was proposed. It used a new protocol for better security using hybrid cryptographic technique to reduce the overhead caused by digital signature. Prof. Anushka K. Rajyalakshmi G. V. [2], A Mobile Ad-hoc network (MANET) is an infrastructure-less network consisting of self-configuring mobile nodes associated by wireless links. Every single node works both as a transmitter and a receiver. Nodes correspond directly with each other when they are both within the same communication range. If not, they rely on their neighbors to relay messages. Furthermore, MANETs are highly vulnerable for passive and active attacks because of their rapidly changing topology, open medium and lack of centralized monitoring.
MANETs into industrial application. So it is vital to address its security issues. Such existing IDSs in MANETs are 1) Watchdog 2) TWOACK and 3) AACK.

Watchdog

Watchdog improves the throughput of the network even in the presence of attackers. It has two parts namely Watchdog and Path rater. It detects malicious nodes by overhearing next hop's transmission. A failure counter is initiated if the next node fails to forward the data packet. When the counter value
exceeds a predefined threshold, the node is marked malicious. The major drawbacks are 1) ambiguous collisions 2) receiver collisions 3) limited transmission power 4) false misbehavior report 5) partial dropping 6) collusion.

TWOACK

TWOACK overcomes the receiver collision and limited transmitted power limitation of Watchdog. Here acknowledgment of every data packet over every three consecutive nodes is sent from source to destination. If ACK is not received in a predefined time, the other two nodes are marked malicious. The major drawbacks are 1) Increased overhead 2) Limited battery power 3) Degrades the life span of entire network fig 2 shows.

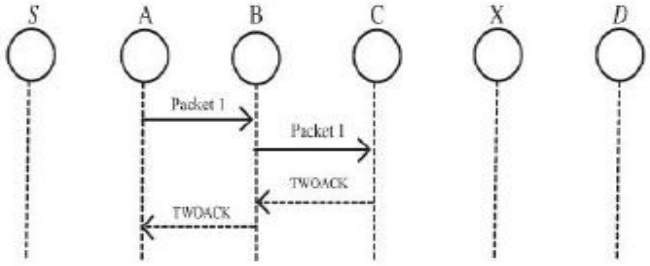


Fig: 2 TWO ACK IDS FOR MANETs

AACK

Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme. The major drawbacks is that it suffers from 1) False misbehavior report2) Forged acknowledgment packets.

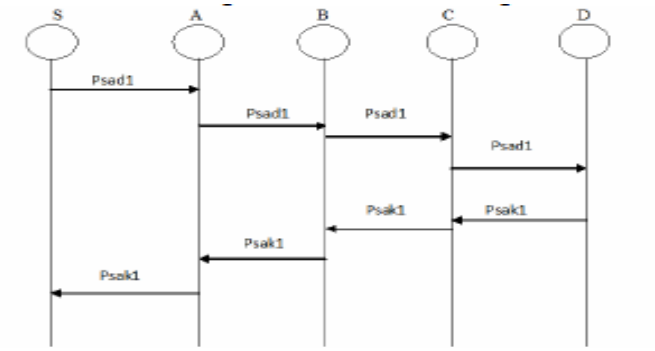


Fig: 3 END-END ACK for MANETs

Digital signature

Digital signature is a widely adopted approach to ensure the authentication, integrity, and no repudiation of MANETs. All algorithms except watchdog are based on acknowledgment. Hence, it should be authenticated through digital signature

Disadvantages:
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 misbehaviour 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.

EAACK
Enhanced Adaptive ACKnowledgment is designed to tackle false misbehavior, limited transmission power and receiver collision limitations of watchdog. It involves three parts namely ACK, SACK (Secure ACK), MRA (misbehavior report authentication). Digital signature is used in EAACK to prevent the nodes from forged acknowledgement attacks. This scheme is explained in detail later.

IDS
Intrusion detection can be classified based on audit data as either host based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as follows [2].
• **Anomaly detection systems**: The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.
• **Misuse detection systems:** The system keeps patterns (or signatures) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.
• **Specification-based detection**: The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

III. MANET ATTACKS

There are many kinds of intrusions or attacks known for MANETs. Like all the attacks, here also the first classification can be done as passive and active attacks as shown in figure 4.

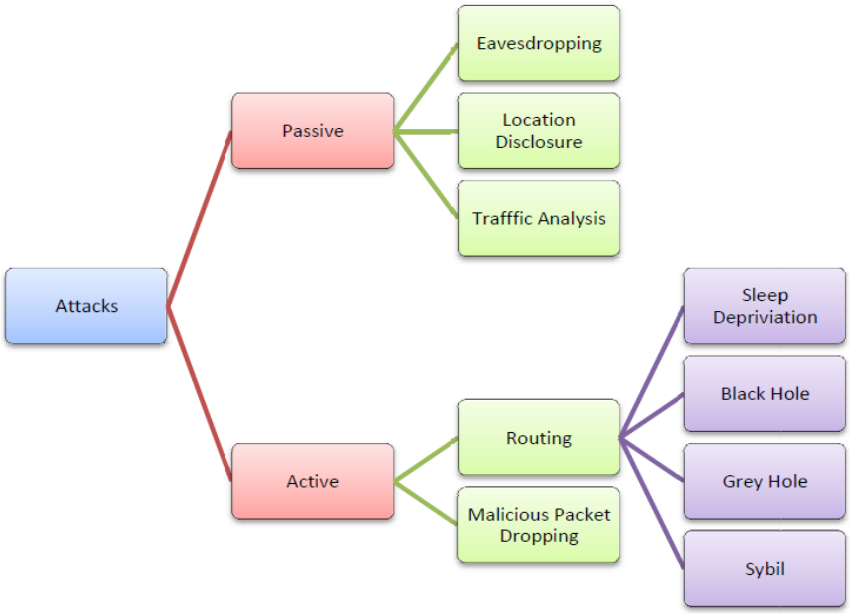


Figure 4. Classification of attacks in the network layer in MANETs.

Passive Attacks
The working of routing protocols is not at all disturbed during a passive attack but instead aims to collect handy information by analyzing the traffic. The information that comes handy includes the topology of the network, identity, location and other details about the nodes in the network.
1. Eavesdropping: A major disadvantage of wireless communication attacks. A communication can be inter received by any other device which has a transceiver
and is located within the transmission range. Sometimes encryption will prevent the attackers from getting use of get the needed information very easily.
2. Traffic Analysis and Location Disclosure: Similar to the eavesdropping approach, the locations of nodes are identified by thorough analysis of the traffic amount of transmissions between the nodes. For example in a situation which involves a commanding centre, that centre will be receiving and sending more number of communications. Thus an attacker can easily find the commanding the communication or traffic pattern.

Active Attack

1. Malicious Packet Dropping: The route discovery process establishes a route between the source and destination node. To ensure the successful transmission of packets after that, the intermediate nodes in the route must forward the packets. But some malicious nodes may decide to drop the packets. They are also called data packet dropping attack or data forwarding misbehavior.

2. Routing Attacks: Some malicious nodes will utilize the loop holes in the routing algorithms and the distributive or cooperative nature of the algorithms to attack. For e.g., AODV (Ad Hoc On Demand Distance Vector Routing) and DSR (Dynamic Source Routing) [4]. Four main types of routing attacks are discussed below.

a) Sleep Deprivation Attack: Here a node interacts with other nodes but the interaction is to keep the victim busy.

b) Black Hole Attack: If the malicious node is chosen as an intermediate node in the route, they may drop the packets instead of forwarding them.

c) Grey Hole Attack: It is similar to black hole attack. The difference lies in the fact
that here the packets are dropped selectively.

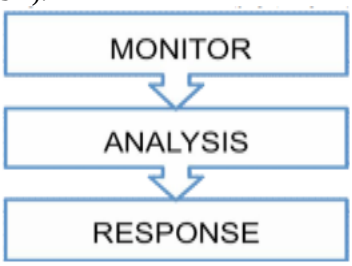
d) Sybil Attack: An attacker node may send control packets using different identities and may create chaos in the routing process.

DSA and RSA

Digital signature is a widely adopted approach to ensure the authentication, integrity, and non-repudiation of MOBILE AD-HOC NETWORKs. Digital signature schemes can be mainly divided into the following two categories.

1) Digital signature with appendix: The original message is required in the signature verification algorithm (digital signature algorithm (DSA)).

2) Digital signature with message recovery: This type of scheme does not require any other information besides the signature itself in the verification process (RSA).



ARCHITECTURE FOR DIGITAL SIGNATURE

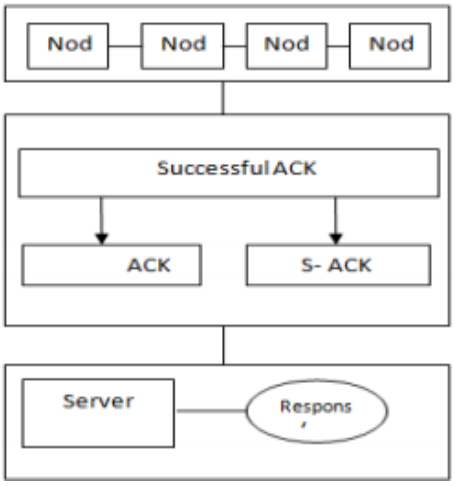


Fig 5 Architecture of DSA

DIGITAL SIGNATURE VALIDATION:

All three parts of EAACK, namely, ACK, SACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. This scheme ensures that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. V. Digital Signature Algorithm: The general flow of data communication with digital signature is shown in above diagram.

Step1: A fixed-length message digest is computed through a pre agreed hash function H for every message m. This process can be described as,

$$H(m) = d$$

Step2: The sender Vishwa needs to apply its own private key Pr− Vishwa on the computed message digest d. The result is a signature Vishwa, which is attached to message m and Vishwa's secret private key,

$$SP\ r{-}Vishwa(d) = Sig\ Vishwa$$

Step3: To ensure the validity of the digital signature, the sender Vishwa is obliged to always keep her private key Pr−Vishwa as a secret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Vishwa's signature and send them to Tamil. As these malicious messages are digitally signed by Vishwa, Tamil sees them as legit and authentic messages from Vishwa. Next, Vishwa can send a message m along with the signature Vishwa to Tamil via an unsecured channel. Tamil then computes the received message m against the pre agreed hash function H to get the message digest d. This process can be generalized as,

$$H(m') = d'$$

Tamil can verify the signature by applying Vishwa's public key Pk−Vishwa on SigAlice, by using SP k−Vishwa (SigVishwa) = d If d == d, then it is safe to claim that the message m_ transmitted through an unsecured channel is indeed sent from Vishwa and the messages itself are intact.

DIGITAL SIGATURE PROCESS:

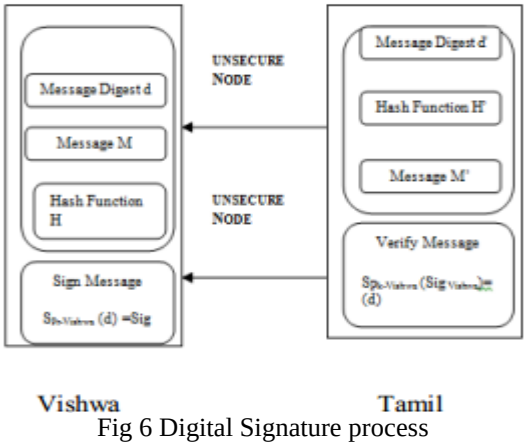


Fig 6 Digital Signature process

The Security of RIVEST-SHAMIR-ADLEMAN

Four possible approaches to attacking the RSA algorithm are:

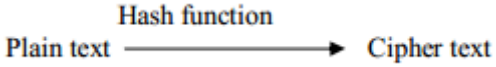
• Brute force: This involves trying all possible private keys.

• Mathematical attacks: There are several approaches, all equivalent in effort to factoring the product of two primes.

• Timing attacks: These depend on the running time of the decryption algorithm.

• Chosen cipher text attacks: This type of attack exploits properties of the RSA algorithm. The defense against the bruteforce approach is the same for RSA as for other cryptosystems, namely, to use a large key space. Thus, the larger the number of bitsin d, the better. However, because the calculations involved, both in key generation and in encryption/ decryption, are complex, the larger the size of the key, the slower the system will run.

Hash Function using Cryptography: Plain text not recoverable from cipher text.



In hash function it will inserting the

- nodes into budgets. The process should be in correct way
- After finishing the process it send the
- node to proper channel

Plain Text: The text should be clean and clear understand of the sender the it will encrypt after sending the plain text. Cipher text: This text will change our information to secret code then it will convert to bytes and send to destination, when it reach destination it will convert to cipher text to plain text.

IV. CONCLUSION

In this research paper, we have study a novel INTRUSION-DETECTION SYSTEM named EAACK protocol specially designed for MOBILE AD-HOC NETWORKs and compared it against other popular mechanisms in different scenarios through simulations. The demonstrated positive performances against Watchdog, TWOACK, and AACK.We also surveyed some intrusion detection systems that deals with various attacks. Attacker may find some new way to attack the system. Therefore system need to much robust so that it prevents new vulnerabilities and themselves. It is important to develop network security policies and deploy into MANET, this can be good research area. There should be system that learns from the knowledge of previous attacks and able to infer and detect new attacks; this can be potential research area.

REFERENCES

[1] E. M. Shakshuki , N. Kang and T. R. Sheltami "EAACK—A secure intrusion detection system for MANETs", IEEE Trans. Ind. Electron., vol. 60, no. 3, pp.1089 -1098 2013

[2] G.F.Cretu, J.Parekh, K.Wang and S.J.Stolfo, "Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks", Proc. IEEE Consumer Communication and Networking Conference, 2006.

[3] Huang, Yi-an, and Wenke Lee. "A cooperative intrusion detection system for ad hoc networks." Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. ACM, 2003.

[4] Aikaterini Mitrokotsa, Christos Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", Ad Hoc Networks, Volume 11, Issue 1, January 2013, Pages 226-237

[5] Wang, Shiau-Huey, Chinyang Henry Tseng, Karl Levitt, and Matthew Bishop. "Cost-sensitive intrusion responses for mobile ad hoc networks." In Recent Advances in Intrusion Detection, pp. 127-145. Springer Berlin Heidelberg, 2007.

[6] Lee J.S. 2008 A Petri net design of command filters for semiautonomous mobile sensor networks in *IEEE Trans. Ind. Electron*.

[7] Liu, K. Deng, J P. Varshney, K and Balakrishnan, K.2007 An acknowledgment-based approach for the detection of routing misbehavior in MANETs in *IEEE Trans. Mobile Compute*r.

[8] Marti,S., Giuli,T.J.,Lai,K and Baker,M.2000 Mitigating routing misbehavior in mobile ad hoc networks In Proceedings of the *6th Annu. Int. Conf. Mobile Compute. Newt*, Boston.

[9] Nasser, N and Chen, Y.2007 Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network In Proceedings of the *IEEE Int.Conf. Communication*, Glasgow, Scotland.

[10] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78. [11]T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[12] Charlie Obimbo#1, Liliana Maria Arboleda-Cobo*2 An Intrusion Detection System for MANET Communications in Information Science and Management Engineering(CISME) Vol.2 No.3 2012 PP.1-5 www.jcisme.org 2011-2012 World Academic Publishing.

[13] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Mo- biCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 255_265, New York, NY, USA, 2000. ACM.

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

