EFFICIENT AND DYNAMIC HYBRID KEY CRYPTOGRAPHY FOR IDS MANAGEMENT SYSTEM IN MANETS

[1]Kavyashree J,[2]Bhaskar G
[1]Student,M.tech, CNE, [2]Assistant professor
Dept.of computer science, Siddaganga Institute of Technology
Tumakuru, Karnataka, India
E-mail: [1]kavya.charmi@gmail.com, [2]bhaskar_gopal@sit.ac.in

Abstract-- A group of freely migrating nodes called Mobile Ad hoc Network (MANET) is one of the most important and unique wireless network architecture. In recent decade migrating to Manet i.e. wireless adhoc network has became a global trend. Compared to contemporary wireless network Manet is preferred mainly for its mobility and scalable characteristics. In mantes each device is free to move independently in any direction and will therefore change its links to other devices frequently. These networks can change locations and configure itself on the fly they communicate via the radio waves. Each node in the Manet has a wireless interface to communicate with each other. However the open medium and wide distributions of nodes make to various types of malicious attacks. In the Existing system Enhanced adaptive acknowledgement approach (EAACK) Digital signature algorithm is used which causes the network overhead if more malicious node involves. Thus proposed system is used with AES and RSA algorithms as a Hybrid key cryptography to reduce the network overhead caused by digital signatures.

Index Terms—Adhoc, AES, IDS, Manet, RSA

I. INTRODUCTION

Manet is continuously self-configuring, infrastructure-less network of mobile devices that are connected without wires [1]. These have highly dynamic and autonomous topology. On the contrary to traditional Network architecture, Manet does not require a fixed network infrastructure, every single node works as both the transmitter and the receiver. Nodes communicate directly with each other when they are both within the communication range. The routing algorithm in MANET can be a single-hop or multi–hop. Single-hop communication is simpler in terms of structure and implementations but has lesser functions and applications compared to multi-hop communication. In multi-hop communication, the destination is beyond the transmission coverage of the source and hence the packets are forwarded via one or more intermediate nodes. Fig.1 shows a MANET network consisting of nodes and their transmission ranges. As shown in Fig.1, Node 2 and Node 3 are neighbours of Node 1 whilst Node 4 and Node 5 are not. Therefore, data transmission to Node 4 and Node 5 will have to be relayed by Node2.

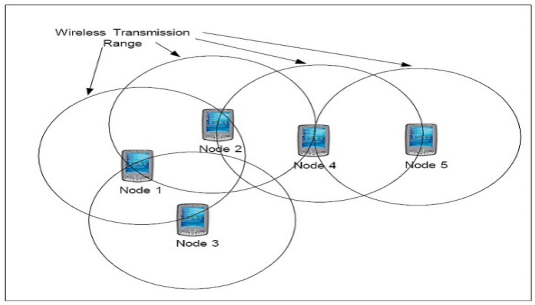

Fig 1. Representation of Manet

Manet is highly vulnerable to attacks because, node configuration and maintenance are done on

its own. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop efficient Intrusion detection mechanisms (IDS) to protect MANET from attacks.

II. LITERATURE SURVEY

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports in to a Management Station. Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs [2]. 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, Next section, mainly concentrate on discussing the background information required for understanding EAACK better.

Different IDS for MANET are:

A. Watch dog

Watchdog scheme is comprised of two sections, to be specific, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is in charge for detecting malicious node misbehaviours in the network. Watchdog detects malicious misbehaviours by indiscriminately hearing to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain time, it increases its failure counter. If node's failure counter exceeds a predefined threshold, the Watchdog node reports it misbehaving [3].

B. TWO ACK

In the Two-ACK, the rule is to let each three successive hub work in a group to find misbehaving nodes. For every three successive nodes in the route, the one which is the third hub has to send Two-ACK acknowledgment packet to the first node/hub [4]. The aim of presenting Two-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

C. AACK

It is similar as TWO-ACK IDS, AACK IDS is an acknowledgment based network layer IDS. It can be treated as a combination of an ID called TACK (identical to TWO-ACK) and an end-to-end acknowledgment IDS called Acknowledge (ACK). Compared to TWO-ACK IDS, AACK IDS reduced network overhead.

III. EXISTING SYSTEM

The existing system approach EAACK is intended to handle three of the six weaknesses of Watchdog scheme, specifically, false misbehaviour, limited transmission power and receiver collision.

EAACK is based on both DSA and RSA algorithm. The three important parts of the EAACK scheme are ACK, Secure ACK (S-ACK), and Misbehaviour Report Authentication (MRA)[5]. EAACK is an acknowledgement based IDS. This scheme utilizes the digital signature method to prevent the attacker from forging acknowledgment packets. Prior to the acknowledgement packets sent out EAACK needs all the acknowledgement packets to be digitally signed and verified by its receiver till they are accepted.

A. ACK

ACK is an end to end acknowledgement. It is the basic approach in EAACK, for reducing network overhead in times where there is no misbehaviour in network.

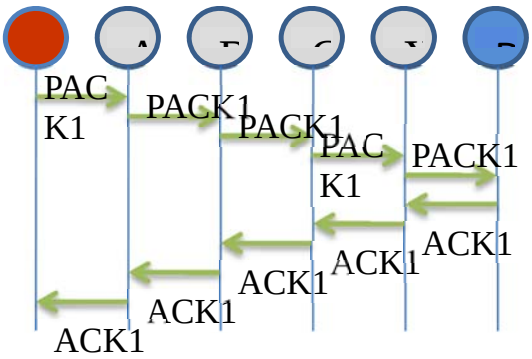

Fig.2. ACK Scheme

B. S-ACK

In S-ACK (Secure-ACK) mode the successive nodes like A, B, C work in group to find the misbehaving nodes in the MANETs

network. Node A sends the S-ACK packet i.e. Pack1 to C through the intermediate node B. The node C need to send back the S-ACK i.e., Ack1 acknowledgement packet to A. If in case node A has not received the S-ACK acknowledgement packet within certain predefined time both B and C are considered as malicious. The misbehaviour report will be produced by the node A and passes to the source node S. The source node immediately does not trust the misbehaviour report so EAACK requires the source node S to switch to MRA mode and confirm this misbehaviour report.

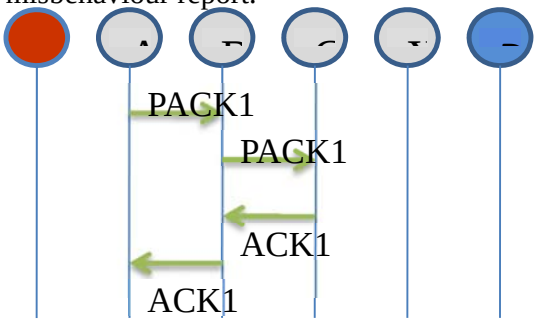

Fig.2. S-ACK scheme

C. MRA

The MRA (Misbehaviour Report Authentication) scheme is to verify whether the destination node got the reported missing packet through any alternate route. To begin the MRA mode, the source node searches its local base and looks for an alternate way to destination route. If no other route exists, the source node starts a DSR routing used to find another alternative path. When the destination node receives the MRA packet, it finds the local knowledge base and compares if the reported packet which was received. If the packet is already received then that is the false misbehaviour report and who ever made this report is announced as malicious. If not the misbehaviour report is trusted and accepted.

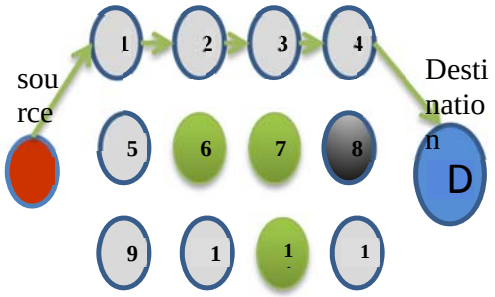

Fig.3. MRA Scheme

D. DIGITAL SIGNATURE

EAACK is an acknowledgement based IDS. All the parts of EAACK are acknowledgement based schemes. They are based on acknowledgement packets to detect the misbehaviour in the MANET [6]. It is extremely vital to ensure that acknowledgement packets in EAACK are authentic and confidential. If the attackers smart enough to forge acknowledgement packets, these three schemes will be vulnerable. So we incorporated digital signature in our existing system. To bring the integrity of the IDS, EAACK needs all the packets to be digitally signed before they encrypted and verified.

IV. PROPOSED SYSTEM

Here we propose a hybrid cryptography technique to reduce the network overhead caused by digital signature. In Some cases when more malicious nodes are present in the network more acknowledgement packets are required. Around then the ratio of digital signature in the whole network overhead increases. Hence used AES and RSA for data encryption and decryption SHA1 for hashing [7].

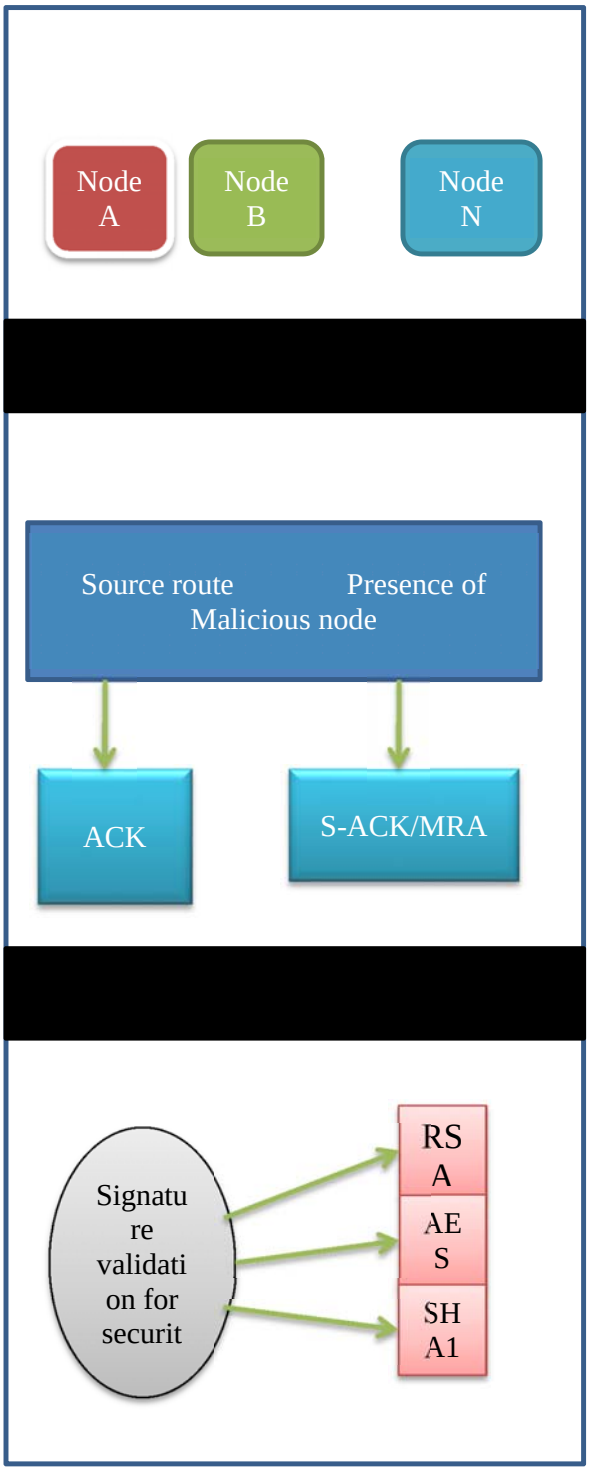

Fig.4. System Architecture

In Hybrid encryption and decryption we make use of RSA, AES and SHA1. The purpose behind selecting these algorithms is

1. AES-Rijndael algorithm: AES is symmetric secure cipher cryptography offers a very high performance and security. Not a single successful brute-force attack on AES has been found till date, it is the only possible known attack against AES [8].

2. RSA: It is a public key cryptography can be used for encryption. The key management is an essential feature of RSA algorithm.

3. SHA1: SHA-1 a message digest function with a block size of 512- bit generates 160-bit message digest. It has a very conservative design.

The advantages of combining an asymmetrical with a symmetrical cryptosystem to hybrid cryptography are:

- It increases speed
- This scheme is vulnerable for collision attacks.
- 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.

A. Encryption Process

Step1: An AES key 'K' of 128-bit, 192-bit or 256-bit is chosen.

Step2: Encrypt message (M) using AES algorithm and above selected key K.

eM = AES-encryption (M)

Step3: AES key K is encrypted by making use of RSA algorithm.

eK = RSA-encryption (K)

Step4: The cipher text (eM) is fed to SHA1 algorithm which generates a message digest of 160-bit.

mD = SHA1 (eM)

Step5: The message digest is signed by RSA algorithm using private key of sender.

DS = RSA-sign (mD)

Step6: The encrypted message (eM), digital signature (DS) and AES encrypted key (eK) is transmitted to the user over a network

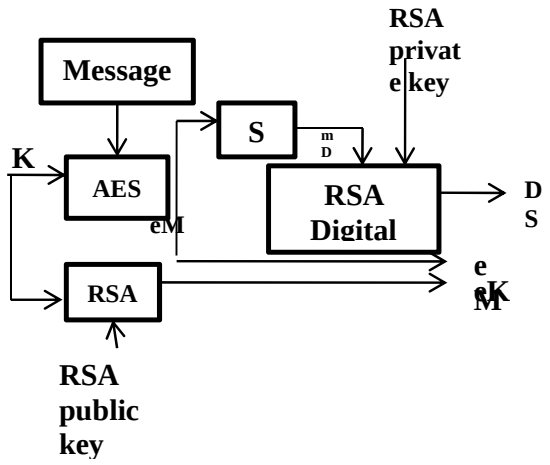

Fig.5. Encyption process

B. Decryption Process

This process is the reverse of encryption process and is having following steps:

Step1: The encrypted AES key (eK) is decrypted with RSA algorithm.

K = RSA-decryption (eK)

Step2: Similarly the encrypted message (eM) is decrypted by AES algorithm using key K.

M = AES-decryption (eM)

Step3: The message digest of encrypted message (eM) is computed using SHA1.

mD = SHA1 (eM)

Step4: The digital signature is verified by RSA algorithm by employing use of public key of sender. DS = RSA-verify (mD)

Step5: Thus we get message (M) of sender in step-2 which is verified by digital signature DS.

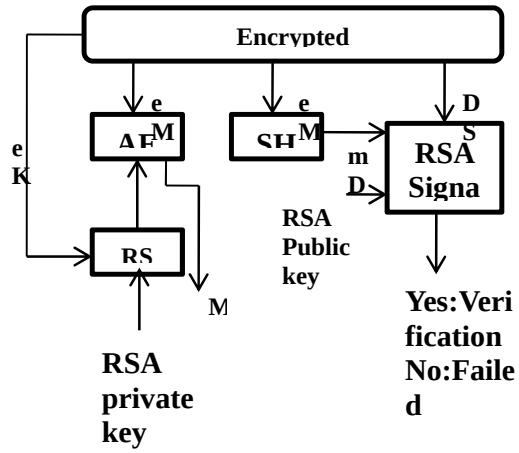

Fig.6. Decryption process

First the secure route for data transmission should be found. The source sends a data to the destination for route identification to the destination. Route identification based on AODV (Ad hoc On-demand Distance Vector routing protocol) protocol model. AODV protocol (Ad hoc On Demand Vector) protocol is implemented for finding routes in the MANET. The routing protocol is designed for use in mobile ad-hoc network of that even contains huge number of nodes. AODV refers to the class of Distance Vector Routing Protocol (DV). In a DV every node known its neighbours and the costs to reach them. The node contains its own routing table, storing all nodes in the network, distance and the next hop to them. If the node is not reachable the distance to it is set to infinity. After getting a secure route, the data send securely to the destination by using hybrid encryption cryptographic techniques. The data that send from the source node will be encrypted with RSA and AES techniques before its travelling to the destination node. The received data will be decrypted with RSA and AES in the destination node. After receiving the data at destination, the destination node required to send an acknowledgement packet to the source. In presence of malicious node, sender node cannot be defined the route. So that routing overhead is reduced in hybrid technique compared with DSA in EAACK.

V.CONCLUSION

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.

References

[1] T.Anantvalee J.Wu “A Survey on Intrusion Detection in Mobile Ad-hoc Networks in wireless/mobile security”, provides survey of various Intrusion Detection implementation in mobile ad-hoc networks.

[2] B. Sun, “Intrusion detection in mobile ad hoc networks,” Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[3] 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.
[4] 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.
[5] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE
"A Secure Intrusion-Detection System for MANETs" IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.
[6] Nat. Inst. Std. Technol., "Digital Signature Standard (DSS)" Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).
[7] Amudha Bharathi.B, Dr.S.Usha "FORTIFY MANETs FROM INVASION USING HYBRID CRYPTOGRAPHIC TECHNIQUES" International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.3, No5, October 2013.
[8] Jan Mohammad Najar Shahid Bashir Dar b " A New Design Of A Hybrid Encryption Algorithm" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 11 November, 2014 Page No. 9169-9171.