SECURE EAACK TO DETECT DoS ATTACKS IN MANET

P.Madhavan, Asst Professor,
Department of CSE,
Sri Krishna College of Technology,
Coimbatore, India.

R.Anandakumar, Avinash Premanath
Fadle Ahmed (UG Scholar)
Department of CSE,
Sri Krishna College of Technology,
Coimbatore, India.

Dr.P.Malathi
Principal,
Bharathiyar Institute of Engineering for Women,
Salem, India

ABSTRACT

Wireless allows data communication between different parties and still maintains their mobility but this communication is limited to the range of transmitters. MANET solves this problem by allowing intermediate parties to relay data transmissions by dividing MANET into two types of networks, namely, single-hop and multi-hop. MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious. Attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. MANET's distributed architecture and changing topology makes traditional centralized monitoring technique no longer feasible in MANETs. EAACK is an intrusion-detection system (IDS) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behaviour-detection rates while does not greatly affect the network performances. But EAACK does not provide encryption to the data packets and the digital signature causes higher overhead in the presence of more malicious nodes. Hence we go for a hybrid encryption scheme using symmetric cipher AES - Rijndael and public key cryptography RSA with hash function SHA-512. The AES - Rijndael algorithm provides confidentiality, the hash function provides the integrity and RSA will ensure the authentication.

Index Terms- **MANET, EAACK, AES Rijndael algorithm, RSA, SHA-512.**

I. INTRODUCTION

WIRELESS ADHOC NETWORK

A wireless ad hoc network is a decentralized type of wireless network. The network is adhoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

MOBILE ADHOC NETWORK (MANET)

A mobile ad hoc network is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

SECURITY GOALS OF MANET

In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

- Availability
- Confidentiality
- Integrity
- Authentication
- Non repudiation
- Anonymity
- Authorization

VULNERABILITIES IN MANET

Vulnerability is a weakness in security system. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

- Lack of centralized management.
- Resource availability.
- Scalability.
- Cooperativeness.
- Limited power supply.
- Bandwidth constraint.
- Adversary inside the Network.
- No predefined Boundary.

ATTACKS IN MANET

Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET.

- Denial of Service attack.
- Impersonation.
- Eavesdropping.
- Routing Attacks.
- Black hole Attack.
- Wormhole Attack.
- Replay Attack.
- Jamming.
- Man-in-the-middle
- Gray-hole attack.

II. RELATED WORKS

EAACK is consisted of three major parts, namely, ACK, secure ACK (SACK), misbehavior report authentication (MRA) and digital signature [1]. In this paper, they proposed and implemented a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behaviour-detection rates in certain circumstances while does not greatly affect the network performances.

Drawbacks

- No encryption is done for packets at sender side.
- Keys are pre-distributed.

TWOACK detects misbehaving nodes by acknowledging every data packet over every three consecutive nodes from source to destination [2]. In this paper, they proposed the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehaviour and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Analytical and simulation results are presented to evaluate the performance of the proposed scheme.

Drawbacks

- Adds unwanted network overhead.
- False misbehaviour report.

AACK - a combination of TACK (identical to TWOACK) and end-to-end acknowledgement scheme called ACKnowledgement (ACK) [3]. AACK overcomes the unwanted routing overhead caused by TWOACK.

Drawbacks

- False misbehaviour report.

III. PROPOSED WORK

Beginning with ACK mode, end-to-end acknowledgement scheme, is used in this hybrid scheme to reduce network overhead. Source node (S) sends data packet to destination node (D) and if it receives the data packet, it sends an ACK back to node A in the reverse order. Within a predefined time period, if node S receives the ACK, then the packet transmission from node S to node D is successful. Otherwise it switches to S-ACK mode. In S-ACK mode, for every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. If first node does not receive this acknowledgment packet within a predefined time period, both nodes second and third are reported as malicious. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. The MRA scheme is designed detect misbehaving nodes with the presence of false misbehaviour report. In MRA mode the source node tries to find an alternate path to the destination node and it sends an MRA packet along this route to circumvent the misbehaviour reporter node. When the destination node receives the MRA packet it checks whether it has received the reported packet. If it is already received, then it is a false misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be encrypted using the hybrid encryption scheme (AES - Rijndael and RSA) before they are sent out and verified for their integrity until they are accepted

SYSTEM OVERVIEW

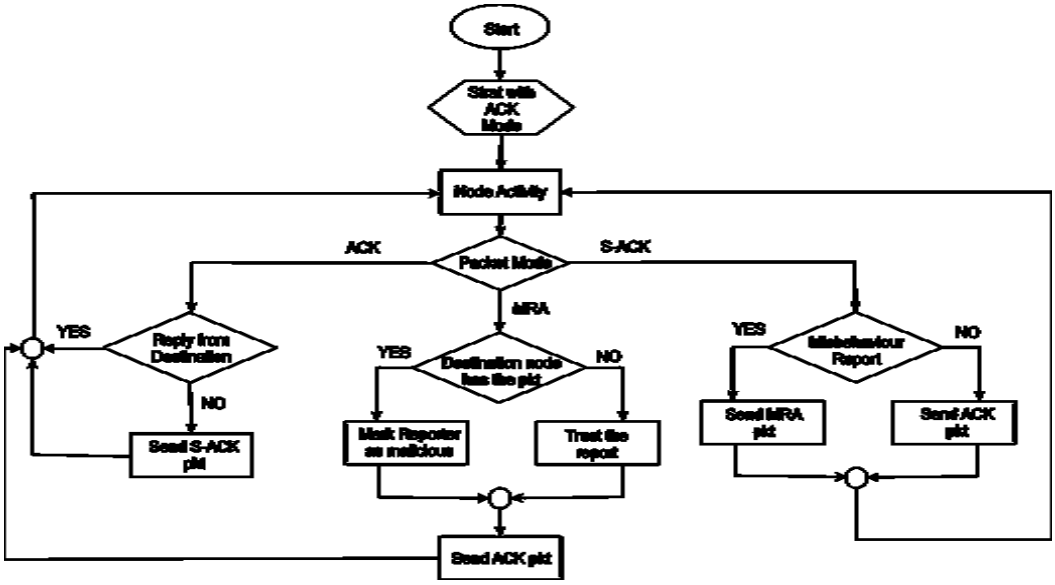

Fig 1 EAACK System

Here all the data packets and the acknowledgement packets are encrypted using the Hybrid Encryption technique using AES - Rijndael and RSA.

IV. PROPOSED WORK

The proposed system comprises the following modules:

- EAACK
  - Acknowledgement (ACK).
  - S-Acknowledgement (S-ACK).
  - Misbehavior Report Authentication (MRA).
- HYBRID ENCRYPTION
  - AES – Rijndael.
  - RSA.

EAACK

Acknowledgement (ACK)

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. For example, in ACK mode, node S (Source) first sends out an ACK data packet *Pad*1 to the destination node D (Destination). If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives *Pad*1, node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order. Within a predefined time period, if node S receives *Pak*1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

S-Acknowledgement (S-ACK)

The S-ACK scheme is an improved version of the TWOACK scheme. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. In S-ACK mode, the three consecutive nodes (i.e., N1, N2, and N3) work in a group to detect misbehaving nodes in the network. Node N1 first sends out S-ACK data packet *Psad*1 to node N2. Then, node N2 forwards this packet to node N3. When node N3 receives *Psad*1, as it is the third node in this three-node group, node N3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node N2. Node N2 forwards *Psak*1 back to node N1. If node N1 does not receive this acknowledgment packet within a predefined time period, both nodes N2 and N3 are reported as malicious. Moreover, a misbehavior report will be generated by node N1 and sent to the source node S. Nevertheless, unlike

the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

Misbehavior Report Authentication (MRA)

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts an AODV routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

HYBRID ENCRYPTION

In this hybrid encryption approach, sender side using 128-bit session key value with AES-Rijndael [5] to encrypt the message. The hash value of message was encrypted using RSA [4] algorithm with 1028 bit public key of the receiver. In the receiver side the decryption done for the encrypted message using AES-Rijndael with 128-bit session key value. To calculate the hash value using hash function SHA-512 for the original message. Using RSA with 1028 bit private key of the receiver to decrypt the encrypted hash value. To ensure the integrity the comparison performed between calculated and decrypted hash values.

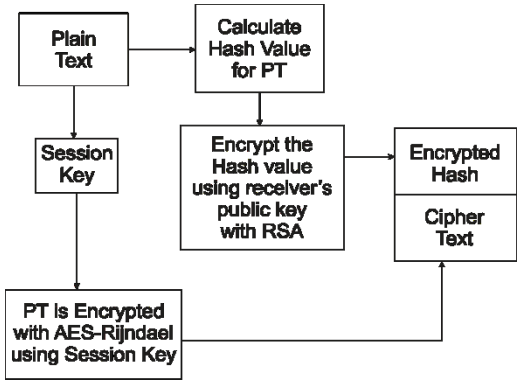

Fig.2 Hybrid Encryption

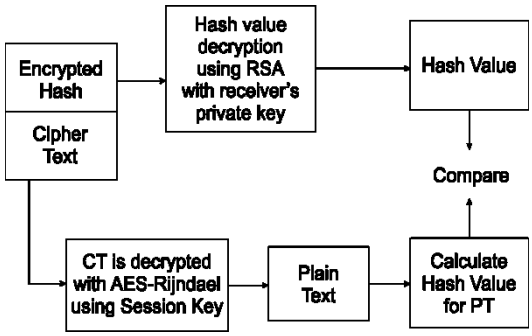

Fig.3 Hybrid Decryption

AES-Rijndael

The Rijndael proposal for AES [5] defined a cipher in which the block length and the key length can be independently specified to be 128, 192 and 256 bits. A use of three key size alternatives but limits the block length to 128 bits

In AES, four different stages are used

i. Substitution bytes: Use S-box to perform byte-to-byte substitution of the block.

ii. Shift rows: A simple permutation.

iii. Mix columns: A substitution that makes use of arithmetic.

iv. Add round key: A simple bit wise XOR of the current block with the portion of the expanded key.

In add round key stage makes use of the key. Any other stage applied at the beginning or end is reversible without knowledge of the key, this scheme is more efficient and secure. Each stage is easily reversible. For the substitute byte, shift row, mix column stages, as inverse function used in the decryption algorithm. For add round key stage, the inverse is achieved by XOR the same round key to the block. The decryption algorithm is not identical for the encryption algorithm. This is a consequence of the particular structure of the AES.

RSA

The RSA [4] scheme is a block cipher in which the plain text and cipher texts are integers between 0 and n-1 for some n. The plain text is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is 2k bits, where $2k < n <= 2k+1$. Encryption and decryption are of the following form, for some plain text block M and cipher text block C.

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, the public key encryption algorithm with a public key of KU = {e, n} and private key of KR = {d, n}. For this algorithm to be satisfactory for public key encryption, the following requirements must be met:

1. It is possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all $M < n$.

2. It is relatively easy to calculate M^e and C^d for all values of $M < n$.

3. It is infeasible to determine d given e and n.

V. IMPLEMENTATION

The Simulation of the proposed system has been carried out in Network Simulator 2 (NS2) with GCC 4.4.3 in Ubuntu 13.10.

Fig.4 Neighbour discovery and routing.

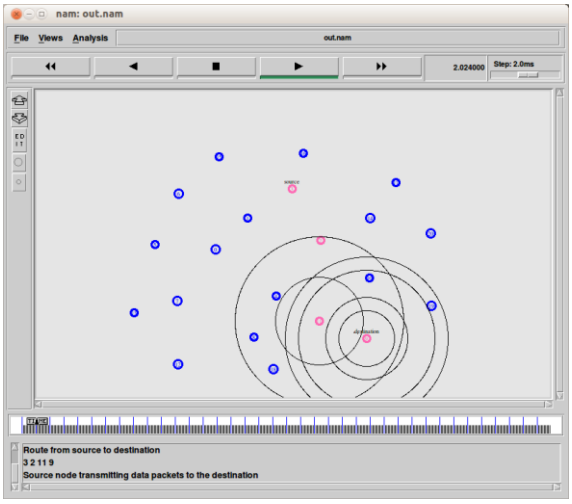

Fig.5 Data packet transmission

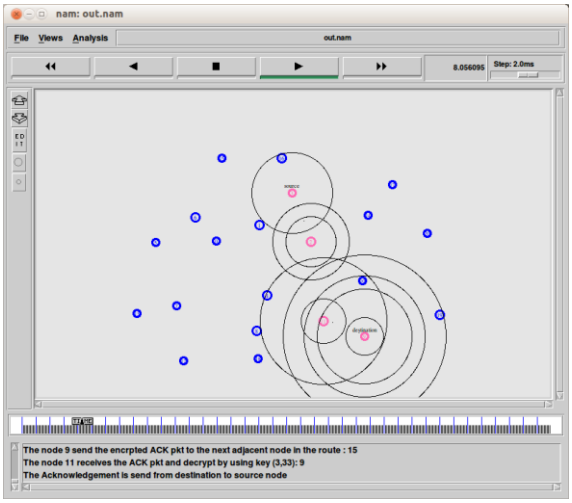

Fig.6 ACK mode

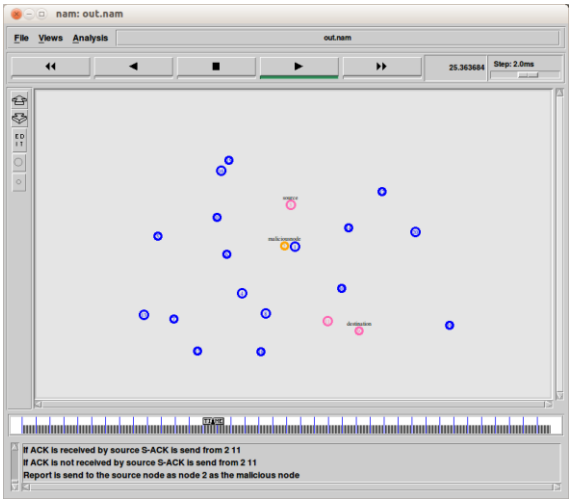

Fig.7 S-ACK mode

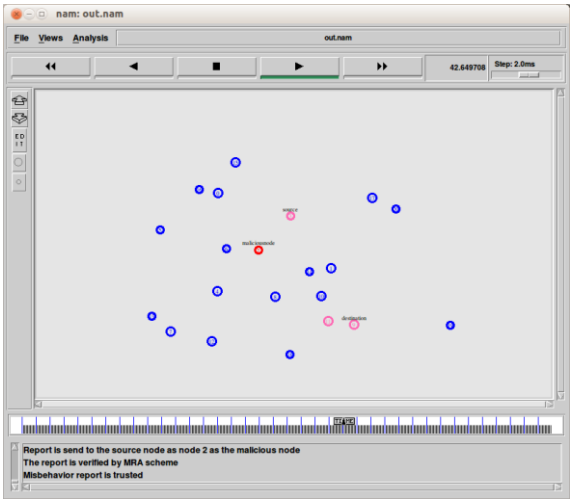

Fig.7 MRA mode

VI. RESULTS

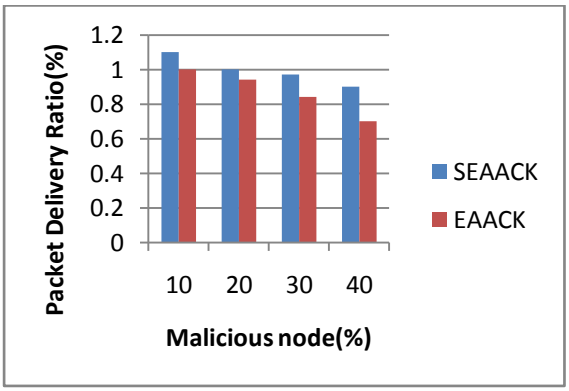

Fig.8 Packet Delivery Ratio Graph

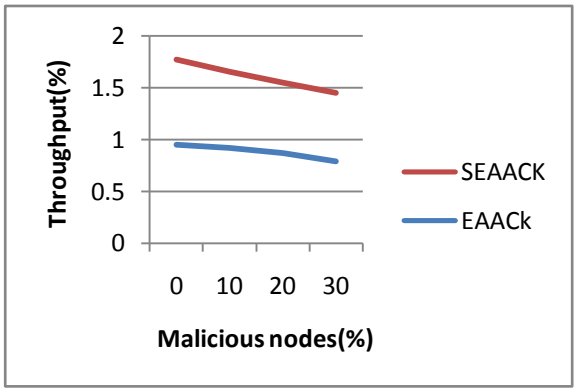

Fig.8 Throughput Graph

VII. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. EAACK protocol is specially designed for MANETs which outperforms Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Using AES – Rijndael and RSA algorithm as a hybrid encryption scheme we can improve confidentiality, availability and integrity of the system. So our proposed system ensures more security to the network and also improves throughput.

VIII. REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami " EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No 3, March 2013.

[2] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, May 2007.

[3] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud "Video transmission enhancement in the presence of misbehaving nodes in MANETs", Int. J. Multimedia System, Oct. 2009.

[4] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2,Feb. 1983, pp. 120–126.

[5] Joan Daemen and Vincent Rijmen, "AES Proposal: Rijndael," April 2003.

