Applying Symmetric Key Cryptography for Security Issues in MANET's

Rakesh Kumar ER
Asst. Prof. & Head
Computer Science and Engineering,
SAMS College of Engineering and Technology, Chennai, INDIA
rakeshkumarer@gmail.com

Abstract- Mobile Ad-Hoc Network (MANET) is set of nodes consists of wireless-transmitter and receiver that communicate with each other through two way wireless links .Security is an important issue for MANET due to its unique features such as limited power, open nature, lack of infrastructure so it is necessary to design intrusion detection technique for MANET. Intrusion is defined as kind of unwanted activity happened in network which is affecting the integrity and confidentiality of network. The existing intrusion detection technique like Enhanced Adaptive Acknowledgement Scheme (EAACK) is used to find malicious nodes and based on Digital Signature Algorithm (DSA) and Ron Rivest, Adi Shamir, Leonard Adleman (RSA) asymmetric key cryptography. But RSA takes much longer time for encrypting data and signature size of RSA is large which creates network overhead. In proposed methodology intrusion detection technique is implemented by using Advanced Encryption Standard (AES) and routing through Ad-Hoc On Demand Distance Vector (AODV) protocol. The proposed technique maintains security along with improvement in performance of MANET like PDR and end to end delay. The proposed technique requires less time for encrypt and decrypt the data so it overcomes the problem of EAACK.

Keywords---- *AES, AODV, MANET, PDR*

I. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is collection of wireless mobile nodes that are free to move in any directions at any speed. Mobile nodes are equipped with a wireless transmitter and a receiver that communicate directly with each other. One of the major advantage of mobile networks is to allow different nodes for data communications and still maintain their mobility [1]. However, this communication is limited to the range of transmitters; it means that two node cannot communicate with each other when the distance between them beyond the communication range of their own. MANET solves this problem by allowing intermediate nodes to relay data transmissions. This is achieved by dividing MANET into two types of networks such as single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. But in a multihop network, nodes rely on other intermediate nodes to transmit data, if the end point node is out of their radio communication range [2]. Initially, MANET was designed for military applications, but, in recent years, has found new usage. For example, search and rescue mission, data collection, virtual classes and conferences where laptops, PDA or other mobile devices are in wireless communication. But, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System.[3]

II. RELATED WORKS

A. Cryptography Concept:

Cryptography is the art of achieving security by encoding messages to make them non-readable. It is a technique of hiding information from unwanted user. Cryptography is considered a branch of mathematics and computer science. It is closely affiliated with information theory, computer security and engineering. Applications of cryptography are security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography [4]. There are two types of cryptography symmetric key and asymmetric key cryptography.

Symmetric Cryptography: In the symmetric key cryptography, same key is used for both encryption and decryption process. Symmetric algorithms have the advantage of not consuming too much computing power and it works with high speed in encrypt them [5]. The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. Types of symmetric key cryptography are DES Algorithm, Triple DES algorithm, the AES algorithm and Blowfish algorithm.

Asymmetric Cryptography: Asymmetric key cryptography is the technique, in which the different keys are used for the encryption and the decryption process. One key is public and second is kept private. If the encryption key is first published then the system enables private communication from the public to the unlocking key's user .If the decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key. Public key methods are important

because they can be used for transmitting encryption keys even when the both the users have no opportunity to agree on a secret key in private Algorithm. Example of asymmetric cryptography Diffie-Hellman Algorithm, RSA Algorithm.

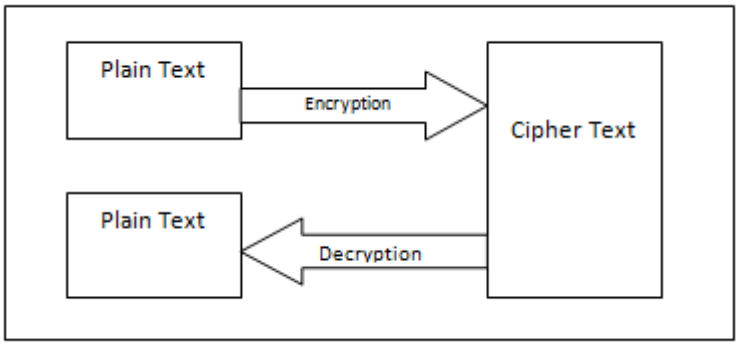

Fig 1: Overview of simple cryptosystem

B. Intrusion Detection System in MANETs Due to the limitation of most MANET routing protocol, 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 on the network with just one or two compromised nodes. To address this drawback, IDS should be added to enhance the security level of MANET [6]. If MANET can detect the attackers as soon as they enter the network, then it may be possible to completely eliminate the potential damages caused by compromised nodes at the first time.

III. EXISTING SYSTEM

Enhanced Adaptive Acknowledgement Scheme (EAACK) is consisted of three major parts.1.ACK, 2.Secure ACK (S-ACK), and 3.Misbehavior Report Authentication (MRA).Since these all are acknowledgement based scheme so they all relay on acknowledgement packet. Therefore it is necessary that all acknowledgement packets are authenticate and untrained otherwise if the attackers are smart enough then it is possible to forge the acknowledge packets. These all above mention schemes will fail in this condition. So because of this concern digital signature scheme is implemented. According to this scheme all the acknowledgement packets should be digitally signed. To achieve this extra resources are required.EAACK including DSA and RSA digital signature scheme.DSA and RSA are type of asymmetric key cryptography. To compare performances between DSA and RSA schemes, 1024-b DSA key and a 1024-b RSA key is used for every node in the network. It is assumed that both a public key and a private key are generated for each node and they were all distributed in advance. The typical sizes of public- and private-key files are 654 and 509 B with a 1024-b DSA key, respectively. On the other hand, the sizes of public-key and private-key files for 1024-b RSA are 272 and 916 B, respectively. The signature file sizes for DSA and RSA are 89 and 131 B, respectively [7]. But if there are more malicious nodes in network then it increases more networks overhead. It is clear that more malicious node required more acknowledgement packet and increase network overhead. Signature size required in RSA algorithm is more that is also one of the causes to increase network overhead.DSA algorithm required more computational power. So to overcome this problem new scheme is implemented which provides security to network as well as improves the performance of system.

IV. PROPOSED METHOD

The proposed method is divided into two parts that is security of system and enhancing the performance of the MANET

A. Implementation of AODV routing protocol.

- **Route Request Message (RREQ) :** Before source node starts to communicate with another node in MANET then it transmits RREQ message. AODV floods RREQ message within the network. Every RREQ message contains Time to Live (TTL) value which states the number of hops. It should be transmitted by RREQ.

- **Route Reply Message (RREP):** RREQ contains source node's IP address and current sequence number and broadcast ID, and also the most recent sequence number for the destination of which it is known by source node. Then either it is destination node or intermediate node which receive RREQ may sends RREP, if the corresponding sequence number of that node is greater than or equal to that carries in RREQ. It transmits a RREP back to the source. Or else, RREQ retransmitted .Then nodes maintained track of the RREQ's source IP address and broadcast ID. But if they receive a RREQ which they have already forwarded, then they discarded the RREQ and do not transmit it.

- **Route Error Message (RERR):** All nodes in the network continue monitoring the link status to its neighbor's nodes during active transmission of RREQ. When the node finds a link crack in an transmission route, RERR message is produced by the node in order to inform other nodes that the link is down.

Route Discovery in AODV:

• Source node S sends RREQ to its neighbors to starts communication with destination node.
• Neighbor node forwards the RREQ to destination.
• The destination node responds a RREP back to the source node.
• Nodes keeps routing table entries only for active routes, unused routes are deleted from the routing table after active route timeout.

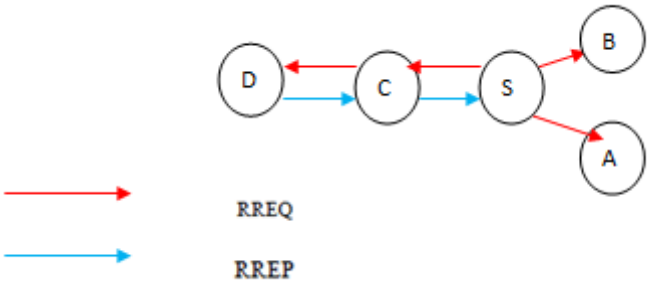

Fig. 2: Route Discovery

Route Maintenance in AODV:

• When there is a link between source and destinations is broken then links are unreachable from the source node. Then the RERR message is sent to the source node.
• RREQ message is transmitted from source node "S" to the neighbor's nodes, at destination node "D" the link is cracked between, so a route error RERR message is produced at node "D" and transmitted to the source node to inform that there route error.

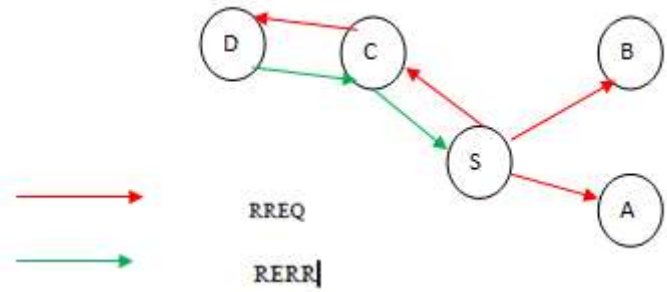

Fig. 3 Route Maintenance

B. Implementation of AES cryptography technique for encryption and decryption.

After routing through AODV protocol next step is to implement cryptography technique to secure the data. AES is block cipher with a fixed block size of 128 and a variable key length. The various types of transformations perform on the in-between results, called state. The state consists of rectangular array of bytes and therefore the block size is 128 bits, which is 16 bytes, the rectangular array is of 4x4 size. The cipher key is similar as a rectangular array with four rows. The number of columns of the cipher key, represented by **Nk**, is equal to the key length divided by 32. AES uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds. A key of size 192 has 12 rounds. A key of size 256 has 14 rounds. Following steps are applied to encrypt a 128-bit block:

• Obtained the set of round keys from the cipher key.
• Starts to initialize the state array with the plaintext.
• Proceed to add the initial round key to the starting state array.
• Execute nine rounds of state manipulation.
• Execute the tenth and final round of state manipulation.
• Do copy the final state array as the encrypted data (cipher text).

Every round of the encryption steps requires a series of steps to alter the state of array. These steps involve four types of operations.

Sub Bytes: The working of sub byte is a simple substitution that transforms every bite into a different value.
Shift Rows: Every row is rotated to the right by a certain number of bytes.
Mix Columns: Each column of the state array is operated differently to produce a new column. The new column provides substitute the old one.
XOR Round Key: Simple XOR operation performs in this round
Decryption: Decryption performs inverse operation of all the above steps which are using to encrypt the data like InvSubBytes , InvShiftRows , InvMixColumns This method is applied on AODV protocol for securing the data. And results are compared with the normal AODV and this secure.

V. FLOW CHART

As seen in flow chart it starts with start function. Nodes are initiated. First source node find the route for transmission of data. AODV protocol is used to find the route between source to destination. When a source node S desires a route to a destination D for which it does not already have a route, it transmits RREQ packet across the network. If the RREQ sequence number is less than or equal to sequence number of RREQ then that corresponding node sends RREP signal back to the source node, otherwise node increments hop count and retransmit the packet across network. After receiving RREP signal source node updates its routing information and encrypts the data by using AES encryption algorithm. If the destination node receive this encrypted data then that data is decrypted at the destination side by using AES decryption algorithm, otherwise its mark as malicious node and that node is discarded from the network. If the data is received successfully at destination side then packet transmission is successfully done. Plot the graph of PDR and end to end delay for better understanding of result.

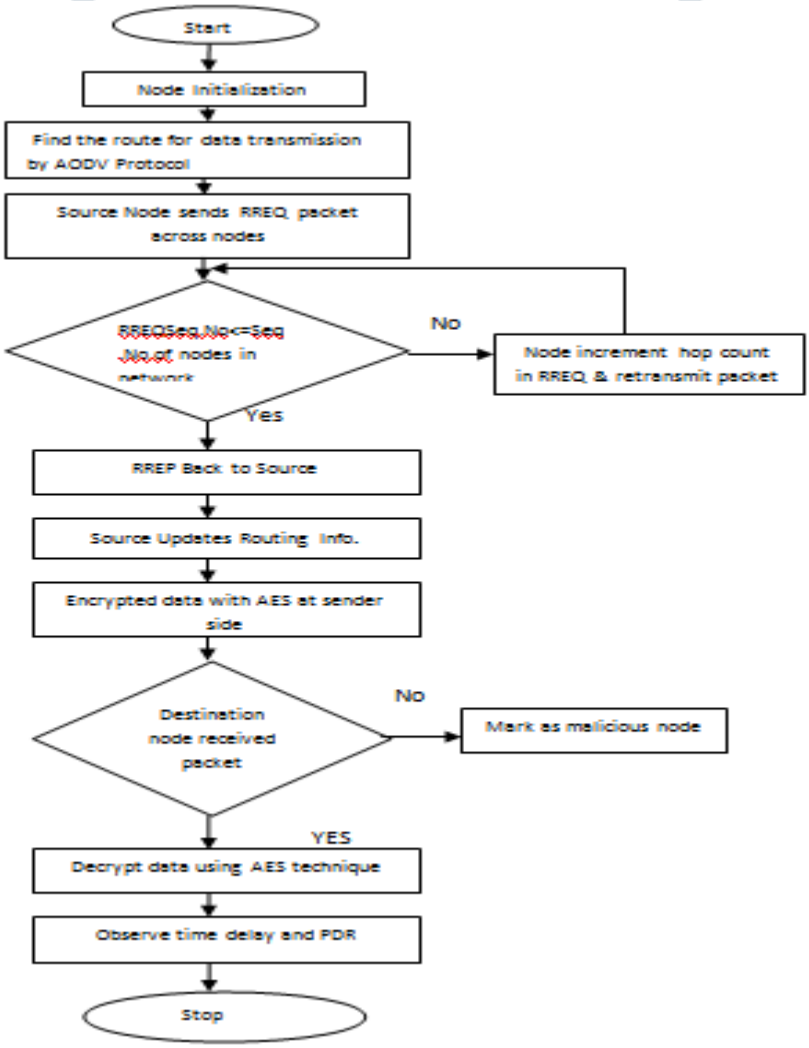

Fig.4: Flow Chart of Proposed Methodology

VI. Simulation Configuration

No.	General Parameters	Values
1	Simulator	NS 2.34
2	Topography Size	1800*1000
3	No. of mobile nodes	22
4	Traffic type	CBR,UDP
5	Antenna Type	Omani Directional Antenna
6	Packet Size	512 byte
7	Transmission Range	250 m
8	Simulation Time	5 sec
9	Pause Time	3.5 ms

Table. 1 Simulation parameters

VII. Comparison Graph of PDR and End to End Delay

Fig.5 shows the packet delivery ratio with time varying from 0 to 5 sec.Graph shows comparison of AES technique with normal working of AODV.PDR lies between 100% to 90% for all the time except at 3.5, it decreases to below 80% . PDR for without AES technique is varying frequently for all time. It is clear from the graph that MANET gives better PDR when transmission of packet is done with AES cryptography.

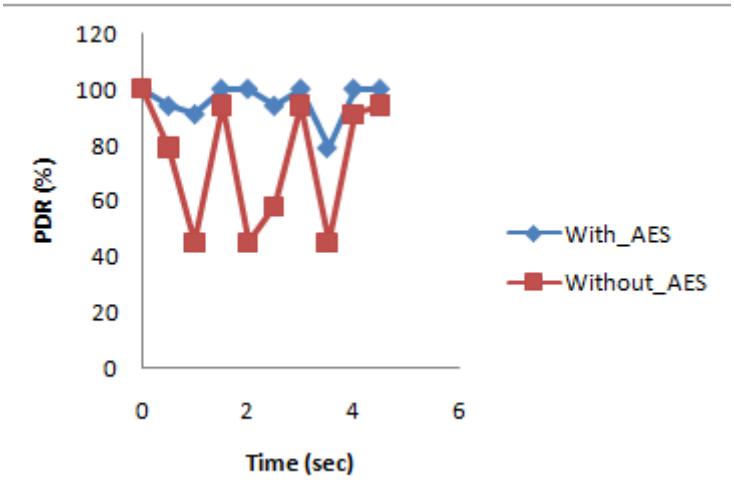

Fig.5: Comparison graph of PDR

Fig. 6 shows delay graph of end to end delay the with time varying from 0 to 5 sec on X axis and end to end delay for both the techniques is taken along Y axis. The end to end delay drastically is varying for normal working of AODV and its very high at time 3 and 5sec.On other hand end to end delay for intrusion detection with AES is varying nearly in constant range for all time and it has very less value.

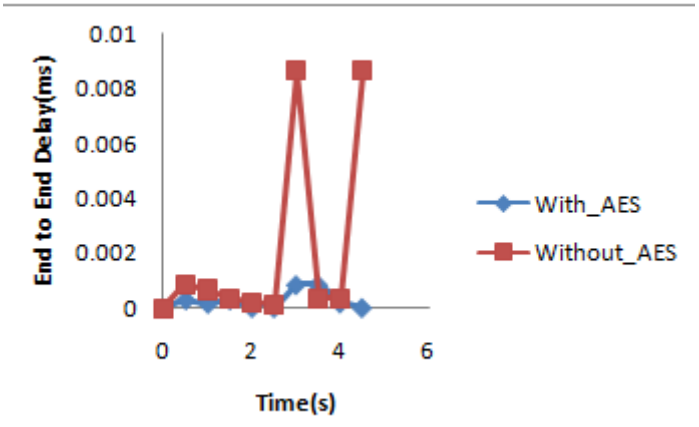

Fig.6: Comparison graph of end to end delay

VIII. RESULT

In proposed method performance comparison of two techniques is analyzed. MANET shows the better PDR for intrusion detection technique which is based on AES as compare to normal working of AODV routing protocol. The graph shows end to end delay is comparatively less for intrusion detection with AES. Since AES does not take long time to encrypt and decrypt the data so battery power consumption is also less. This is the most secure symmetric cryptography therefore it is popular among all others cryptography technique. It can improve the network's PDR when the attackers are smart to forge acknowledgement data packets. In MANET delay is an important parameter where challenging network environments are considered, either because of variations of node speed, and packet transmission rate or because of temporary disconnection. So AODV routing protocol provides quick adaptation to dynamic link conditions, less processing, overhead, and low network utilization. So proposed work improves the performance of MANET as well as maintains the security.

• The existing intrusion detection technique EAACK increases overhead in the network, so in future work will try to reduce the network overhead.
• Testing the performance of proposed work in real network environment instead of software simulation.

REFERENCES

[1] B.Patel, P.Shah, H.Jethva, N.Chavda, "Issues and Imperatives of Ad-Hoc Networks", International Journal of Computer Applications Volume 62 – No.13, pp.0975 – 8887, January 2013.

[2] P.Ghosekar, G.Katkar, P.Ghorpade, "Mobile Ad-Hoc Networking: Imperatives and Challenges", IJCA Special Issue on "Mobile Ad-Hoc Networks" MANETs, Feb2010.

[3] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222,March 2009 .

[4] Kofahi, N.A, Turki Al-Somani, Khalid Al-Zamil, "Performance evaluation of three Encryption/Decryption Algorithms", IEEE 46th Midwest Symposium on Circuits and Systems, Vol 2, Issue 1, pp. 790-793, Dec. 2003

[5] AL.Jeeva1, Dr.V.Palanisamy and K.Kanagaram, "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, pp.3033-3037, May-Jun 2012.

[6] Paul Brutch and Calvin Ko,‖ Challenges in Intrusion detection for wireless Ad hoc network‖,Proceedings of the Workshop on Security and Assurance in Ad hoc Networks in Orlando, pp. 368-373, Jan 2003.

[7] E.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

AUTHOR DETAILS

Rakesh Kumar ER was born in Kanyakumari District, Tamil Nadu, India in 1985. He obtained his B.Sc., M.Sc. M.E. M.Phil. Degrees in Computer Science in the years 2005, 2007, 2010 and 2012, M.B.A Degree in Human Resources in the year of 2013 respectively. He has more than 7 years of teaching experience. He has presented 5 research papers in various national and international conferences. He has also published more than 15 research papers in reputed national and international journals. He has guided several UG and PG students for their project work. His area of interest is Network Security and Wireless Sensor Networks. Currently, he is with SAMS College of Engg. & Tech, Chennai, India, as Asst. Prof and Head of the Department of Computer Science and Engineering.