Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 07, July -2018

A NOVEL APPROACH TO ENSURE SECURITY FOR DYNAMIC ADDRESS ALLOCATION SCHEME IN MOBILE AD-HOC NETWORKS

Dr.S.Pariselvam#1, S.Shrilekha*2, M.Shobana*3, G.Preethika*4

1 Head of Department, Computer Science Department, ManakulaVinayagar Institute of Technology, Pondicherry
2,3,4 Department of Computer Science, ManakulaVinayagar Institute of Technology, Pondicherry

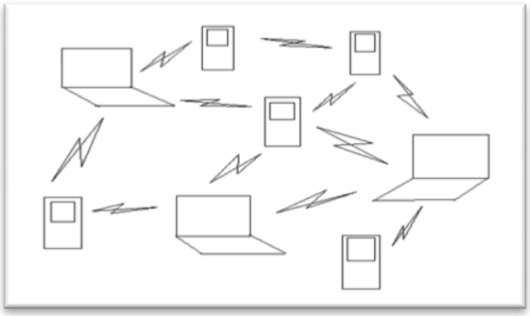
ABSTRACT *This project mainly deals with the allocation of address on the receiver side that in turn ensures secure transmission and reception of data. To serve that purpose, a secure distributed dynamic IP configuration (IPv6) protocol for address allocation in a managed MANET is proposed where authentication of nodes is very important. Any existing node in the network will be able to generate unique IP addresses from its own IP address for new authorized nodes using this protocol. Therefore, a new node can obtain an IP address from its neighbor nodes without broadcasting any message over the entire MANET during address allocation process. However, this scheme was not suitable incase of messages that intended more privacy. In order to solve this problem, a dynamic address allocation scheme is proposed that assigns dynamic addresses on the receiver side. For security purposes on transmitting the data, we use Advanced Encryption Standard algorithm (AES) to ensure more security and throughput while relaying the data. Simulation results indicate that the added security mechanisms is highly robust and scalable in a large network.*

INTRODUCTION:

There are two disparate types of networks in mobile wireless networks, they are infrastructure networks and Infrastructure less networks. The infrastructure networks, which was also known as Cellular network, have fixed and wired base gateways and They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. Each of the mobile nodes constituted in the cell is connected with each node and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example of this type includes office wireless local area networks (WLANs).

Then the other type is infrastructure less network, which is also known as Mobile AdHoc Networks (MANETs).These networks does not contain any fixed routers. In this network, all the nodes have the capability to move around anywhere in the network dynamically in arbitrary manner. The role and responsibilities of the MANET are all done within the terminals itself. There is no specific server in the network, since all the nodes are dynamic in nature, every nodes acts as a proxy server. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.

ADHOC NETWORKS



Ad-hoc networks were mainly used for military applications. Since then, they have become increasingly more popular within the computing industry. Applications include emergency search and rescue operations, deployment of sensors, conferences, exhibitions, virtual classrooms and operations in environments where construction of infrastructure is difficult or expensive. Ad-hoc networks can be rapidly deployed because of the lack of infrastructure.

Characteristics of MANET

Dynamic Topologies: Since nodes are free to move arbitrarily, the network topology may change randomly and rapidly at unpredictable times. The links may be unidirectional bidirectional.

Bandwidth constrained, variable capacity links: Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput.

Energy constrained operation: Some or all of the nodes in a MANET may rely on batteries. In this scenario, the most important system design criteria for optimization may be energy conservation.

Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANET provides additional robustness against the single points of failure of more centralized approaches.

Routing in Ad-hoc Network

Routing support for mobile hosts is presently being formulated as mobile IP technology when the mobile agent moves from its home network to a foreign (visited) network, the mobile agent tells a home agent on the home network to which foreign agent their packets should be forwarded .In contrast, the goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes, which may be combined routers and hosts, themselves form the network routing infrastructure in an ad hoc fashion. Routing protocols for mobile ad-hoc networks have to face the challenge of frequently changing topology, low transmission power and asymmetric links.

Ad Hoc Routing Protocols

A number of routing protocols have been suggested for ad-hoc networks. These protocols can be classified into two main categories:

- Table driven routing protocols
- Source initiated on demand routing protocols

LITERATURE SURVEY

Title: An Efficient and Robust Addressing Protocol for Node Auto configuration in Ad Hoc Networks
Authors: Natalia Castro Fernandes, Marcelo DufflesDonato Moreira and Otto Carlos Muniz Bandeira Duarte
Introduction
In this paper, the authors propose and analyze an efficient approach called Filter-based Addressing Protocol (FAP). The proposed protocol maintains a distributed database stored in filters containing the currently allocated addresses in a compact fashion. We consider both the Bloom filter and a proposed filter, called Sequence filter, to design a filter-based protocol that assures both the univocal address configuration of the nodes joining the network and the detection of address collisions after merging partitions. [7]Our filter-based approach simplifies the univocal address allocation and the detection of address collisions because every node can easily check whether an address is already assigned or not. We also propose to use the hash of this filter as a partition identifier, providing an important feature for an easy detection of network partitions.

Hence, we introduce the filters to store the allocated addresses without incurring in high storage overhead. The filters are distributed maintained by exchanging the hash of the filters among neighbors. This allows nodes to detect with a small control overhead neighbors using different filters, which could cause address collisions. Hence, our proposal is a robust addressing scheme because it guarantees that all nodes share the same allocated list.

Title: Dynamic and hierarchical IPv6 address configuration for a mobile ad hoc network
Authors: Xiaonan Wang and HuanyanQian
Introduction
This paper proposes a dynamic and hierarchical IPv6 address configuration scheme for a MANET, and it has the following contributions:

- The paper proposes the cluster generation algorithm that adopts the total number of potential cluster members as a measurement unit in order to minimize the total number of cluster heads. Because a central node is elected from cluster heads, the control cost for electing a central node is minimized. As a result, the address configuration cost is reduced.
- The paper proposes the hierarchical architecture and combines the advantages of distributed and centralized address configuration approaches. [8]A central node uses the centralized approach to assign IPv6 addresses for cluster heads, and a cluster head adopts the distributed approach to assign IPv6 addresses for the cluster members in the same cluster.
- A central node/cluster head uses the unicast communication mode to achieve the real time address reclamation, which ensures that it has enough address resources for assignment.
- The paper proposes the MANET merging and partitioning algorithms that guarantee that no address collision happens during the MANET merging and partitioning process and effectively reduce the number of MANET merging.

Title: A secure IPv6 address configuration scheme for a MANET
Authors: Xiaonan Wang and Yi Mu
Introduction
This scheme proposes the architecture for a MANET. In the architecture, a new node acquires a unique IPv6 address from a proxy node within one-hop scope without performing a DAD process, and the address resources occupied by failed nodes can be recovered automatically for reuse. In this way, the dynamic address configuration is achieved, the address configuration cost is reduced, and the address configuration delay is shortened.

This scheme proposes the hierarchical IPv6 address structure for a MANET. [9]On the basis of the hierarchical address structure, each proxy node can acquire a unique address scope for assignment and can assign a unique node Identifier (ID) for new nodes, so the address configuration task is distributed around proxy nodes, that is, multiple proxy nodes can perform the address configuration in parallel. In this way, the uniqueness of an assigned IPv6 address is ensured without a DAD process, and the configuration delay is shortened. Because the node ID is only a part of an IPv6 address and its size can be adjusted according to the size of a MANET, the memory and processing costs of the IPv6 address configuration is independent of the size of an IPv6 address.

The transmission scope of the control packets for the address configuration is controlled within one-hop scope, and the identification of a new node/proxy node is confirmed through authentication. Therefore, both the scalability and the security are accomplished, the address configuration cost is reduced, and the address configuration delay is shortened.

RELATED WORK

Location based Energy Efficient Scheme for Maximizing Routing Capability of AODV Protocol in MANET

The number of nodes in MANET considered dependent on batteries for their energy. So the most important parameter for optimization is energy conservation. It has been further concluded that due to the dynamically changing topology and infrastructure less, decentralized characteristics, location information and power awareness is hard to achieve in MANET. [2]Hence, location awareness and power awareness mechanisms should be built-in features for all sorts of applications based on ad hoc network. In this paper the LAR has fulfill the scarcity of location unawareness by that the power consumption or energy consumption of nodes are more utilizes in routing packets instead of retransmission of data due to link breakage. The proposed AODV with LAR and Energy approach is reduces the flooding of routing packets and provides the performance as equal to AODV with LAR. The proposed approach is improving the capability of AODV routing protocol and prolog the network life time.

An effective strategy of merging & partioning of network of nodes by incurring in mobile adhoc networks

The protocol doesn't need flooding of messages within the entire MANET throughout the address allocation process saving considerable bandwidth and. Within this paper, we've presented an ID based secure address allocation protocol named SD-RAC for handled mobile random systems. [3]SD-RAC makes each node within the network behave as proxy that may assign addresses with approved new nodes within the network. Performance analysis and simulation results reveal that SD-RAC has low addressing latency and fewer overhead in comparison with popular existing methods for MANET. The addressing latency and overhead doesn't increase much with rise in the amount of nodes within the network. Further, it may withstand network partitioning and merging that may take place in a MANET atmosphere. Thus the suggested SD-RAC protocol is robust and scalable.

Dynamic Address Allocation Protocols for Mobile Ad Hoc Networks Based on genetic algorithm

This paper addresses the problem of dynamic allocation of a unique IP address to a joining node in mobile adhoc networks and detection of duplicated addresses. In this 1000 1500 2000 2500 3000 3500 0.05 0.1 0.15 0.2 0.25 0.3 0.35 0.4 mobile network area (in m*m) latency (in secs) basic protocol GA protocol Fig. 4. Latency Vs Mobile Network Area paper,

[4] we present a distributed address assignment protocol to manage IP addresses in MANET. The protocol guarantees the uniqueness of the IP address when a node joins, leaves, and also when a MANET parts and merges. Our solution, Dynamic Address Allocation Protocol, is based on a node's MAC address based on genetic algorithm (GA), hence it significantly reduces the probability of duplicated addresses. The main idea of the protocol is based on using leaders, in the MANET to allocate and manage the IP addresses. The protocol works effectively in these processes, especially, in the process of MANETs merger.

IPv6 Addressing Technique based Dynamic Host Configuration Protocol in Mobile Ad-hoc Network

In radio communications, each vulnerable communications calling that relationship is affected by the position, the distances and angles between nodes form a relationship of mutual relations calls, as well as external interference to ongoing communications.[1] But as long as the conditions of lineof-sight from each of the nodes communicate with each other they will be, the effect is not too significant disorders influence end-to-end delay. End-to-end delay affected if the mechanism of inter nodeclient access in simultaneously, where the current channel load is to be increased; and consequently takes time to serve each request and service calls. This condition is linear to the number of node-client increasing to request to join the network. Besides, also with the addition of obstacle between the nodes communicate with each other will also affect end-to-end delay. Implemention of the method of IPv6 and Dynamic Host Configuration Protocol (DHCP) proved to be possible on the Mobile Ad-hoc Network (MANET), and thus the MANET method can be used as an alternative future network for the dynamic topology and breakthrough in radio communications. The position of a node in a wireless network can be classified into the angle position and distance position; and both these variables play a role in the effect of the transmit/received signal strength at the nodes in the network

Secure Intrusion Detection System in mobile ad hoc networks using RSA algorithm

Mobile Ad hoc networks are easily affected by various types of network layer attacks. These attacks affect the performance of MANETs drastically.[5] Secure Intrusion Detection technique using RSA algorithm successfully identifies the intruders. Results shows that our proposed secure IDS method gives better packet deliver ratio in presence of intruders. Even though routing overhead is on the higher side it is acceptable when we need to identify intruders.

Improve the security of CGA using adjustable key block cipher based AES, to prevent attack on AES in IPV6 over MANET

The proposed algorithm is based on AES as a modern symmetric-key block cipher to generate different sub keys the Symmetric real key and using each sub key to encrypt one AES block and details technique of sub keys generation and prove the security of this generator to prevent prediction or getting another sub key from available one.[6] Alternative use of Mix Columns transform step of original 128-bit AES algorithm may help to reduce the time complexity of the same. To reduce the hardware requirement, S-box and Inv. S-box in the original AES are replaced by one simple S-box used for encryption and decryption in the proposed method.

EXISTED WORK

A secure distributed dynamic IP configuration (IPv6)[10] protocol for address allocation in a managed MANET used for military communications, ncZ disaster management, outdoor conferences in remote areas, critical area surveillance, sensitive task monitoring, health care and many such related applications where authentication of nodes is very important. Using this protocol any existing node in the network will be able to generate unique IP addresses from its own IP address for new authorized nodes. Therefore, a new node can obtain an IP address from its neighbor nodes without broadcasting any message over the entire MANET during address allocation process. The protocol is also highly robust and scalable in a large network. Moreover, it is capable of handling the problems that may arise due to node failures, message losses, mobility of the hosts and network partitioning or merging.

This presents the algorithm for secure distributed address configuration where IP addresses are allocated to the network nodes dynamically. We call this proposed technique Secure and Distributed Robust Address Configuration (SDRAC) algorithm. Here all the existing network nodes (which are also set as proxies) are eligible to assign addresses and a new node N_n can acquire an address simply from its neighbors. Each proxy will compute a unique IP address for a new host N_n from its own IP address and as a result DAD is not a requirement. The SD RAC algorithm is divided into two parts, one for a new node (N_n) and the other for a proxy node.

The SD-RAC Address Allocation

When an authorized new node N_n wants to join the network, it periodically issues a signed (σN_n) DISCOVER(ID_{Nn}, r_3) broadcast message to its neighbors till it either receives an OFFER message or a DENY message. In case no messages are received within a specified time period, the new node $N_n$configures itself as a root node with an IP address and generates its digital certificate and a unique network ID (NID) as its network identifier. The DISCOVER(ID_{Nn}, r_3) message contains its hardware address as an identifier of the node (ID_{Nn}). The neighbor nodes on receiving the signed DISCOVER message

(Algorithm 2) start serving as proxies by sending the message (OFFER(IP_O, ID_P, r_4, DIG_CERT_P) + δ_P) to the new node N_n. Where, ID_P is the hardware address of the proxy; IP_O is the offered IP address to the new node, r_4 is a random number; and DIG_CERT_P is the digital certificate of the proxy and δ_P is the authentication tag. This tag is generated using a keyed-hashing for message authentication (HMAC) as the MAC algorithm and SHA- 3 as the hash function (H). When N_n receives the OFFER(IP_O, ID_P, r_4, DIG_CERT_P) messages from its neighbors, it chooses an IP address from among those offered by using Function select-ip() of Algorithm 1. This IP address is then unicasted in a (SELECT (ID_{Nn}) + δ_{Nn}) message back to the same proxy offering it. The other OFFER messages sent by neighboring proxies are ignored by N_n. Thereafter, the proxy on receiving the SELECT message, sends a message ACK(ID_P, DIG_CERT_{Nn}) + δ_P the new node N_n. After receiving the ACK message from the selected proxy, N_n performs the authentication process and a final check on the configuration parameters. The configuration parameters are default mask, Address Resolution Parameters (ARP) for the allocated network address and gateway addresses, if any. In Figures below (a) and below (b) the timing diagrams of a node joining and leaving a network is shown respectively.

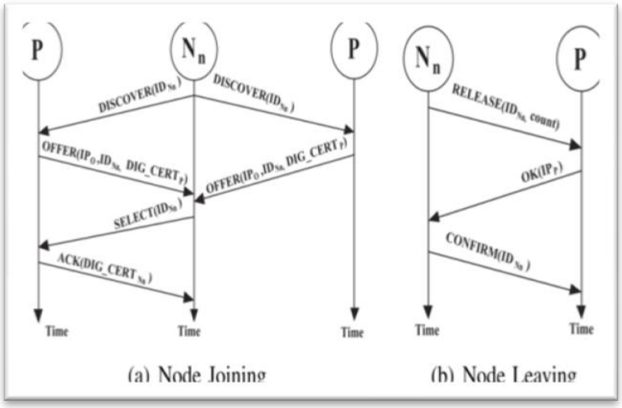


Fig. Timing Diagram of a Node Joining and Leaving a MANET

During the address allocation process, the proxy and a new node (N_n) may sometimes lose synchronization due to a channel error or because of their high mobility. In such a situation the concerned IP address may get wasted or it may be assigned to one or more nodes if proper steps are not taken. SD-RAC uses a timer to solve this problem. The timer sends a time-out signal in case acknowledgement is not received by a node, which triggers the concerned node to resend a packet.

Authentication

In Section above, only authorized nodes having a valid ID are allowed to enter the network. It was also stated that every node in the network carries a list of all the node IDs which have been distributed before the deployment of a network. At the time of address allocation, SD-RAC verifies the authentication of a new node N_n and the proxy node as follows: Either the signature scheme (σ) proposed in or the Message Authentication Code (MAC) scheme (δ) is used for message authentication.

PROPOSED WORK

Advance Encryption Standard (AES) is a symmetric-key block cipher, which the block and key can in fact be chosen independently form 128, 160, 192, 224, 256. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. The algorithm begins with an Add round Key stage followed by 9 rounds of four stages and a tenth round of three stages, The following processes are carried out under the AES algorithm to ensure the efficiency of the system, End to end authentication and Data integrity.

End to end authentication

Authentication is basically sending a request for transmission or reception which is bidirectional in nature sender to receiver. In this case this process is carried out that the transmission reaches the desired recipients without any loss

Data integrity

It is the process of ensuring that the data transmitted reaches the receiver without any interruption. We extend this process to make sure that the data reaches the destined receiver by monitoring the status of the data at all levels. The input is a single 128 bit block both for decryption and encryption and is known as the in matrix (figure 1). This block is copied into a state array which is modified at each stage of the algorithm and then copied to an output matrix (see figure 2). Both the plaintext and key are depicted as a 128 bit square matrix of bytes. This key is then expanded into an array of key schedule words (the w matrix). Ordering of bytes within the in matrix is by column. The same applies to the w matrix.

HIGH-LEVEL DESCRIPTION OF R-ROUND AES

Given a plaintext X, initialize state to be X and perform an operation Add round key, which X -ORs the round key with state. For each of the first r − 1 rounds, perform a substitution operation called Sub Bytes on state using an S-box; perform a permutation Shift Rows on state; perform an operation Mix Columns on state; and perform Add Round Key. Perform Sub Bytes; perform Shift Rows; and perform Add Round Key. Define the cipher text Y to be state. From this high-level description, we can see that structure of the AES is very similar in many respect to the SPN discussed earlier. In every round of both these cryptosystems, we have sub key mixing, a substitution step and a permutation step. AES is “larger,” and it also includes an additional linear transformation (Mix Columns) in each round. All operations in AES are byte-oriented operations, and all variables used are considered to be formed from an appropriate number of bytes. The plaintext X consists of 16 bytes. state is represented as a four by four array of bytes. We will often use hexadecimal notation to represent the contents of a byte. Each byte therefore consists of two hexadecimal digits.

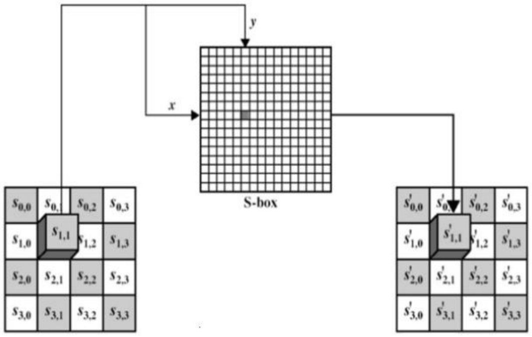
Inner Workings of a Round

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows Substitute bytes, Shift rows, Mix Columns and Add Round Key The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following Inverse Shift rows, Inverse Substitute bytes, Inverse Add Round Key, Inverse Mix Columns.

Again, the tenth round simply leaves out the Inverse Mix Columns stage. Each of these stages will now be considered in more detail.

Substitute Bytes

This stage (known as Sub Bytes) is simply a table lookup using a 16 × 16 matrix of byte values called an s-box. This matrix consists of all the possible combinations of an 8 bit sequence (28 = 16 × 16 = 256). However, the s-box is not just a random permutation of these values and there is a well defined method for creating the s-box tables. The designers of Rijndael showed how this was done unlike the s-boxes in DES for which no rationale was given. Our concern will be how state is effected in each round. For this particular round each byte is mapped into a new byte in the following way: the leftmost nibble of the byte is used to specify a particular row of the s-box and the rightmost nibble specifies a column. For example, the byte {95} (curly brackets represent hex values in FIPS PUB 197) selects row 9 column 5 which turns out to contain the value {2A}. This is then used to update the state matrix. Figure 3 depicts this idea.


y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Substitute byte stage of AES algorithm

The Inverse substitute byte transformation (known as Inv Sub Bytes) makes use of an inverse s-box. In this case what is desired is to select the value {2A} and get the value {95}. Table 4 shows the two s-boxes and it can be verified that this is in fact the case. The s-box is designed to be resistant to known cryptanalytic attacks. Specifically, the Rijndael developers sought a design that has a low correlation between input bits and output bits, and the property that the output cannot be described as a simple mathematical function of the input. In addition, the s-box has no fixed points (s-box(a) = a) and no opposite fixed points (s-box(a) =− a) where − a is the bitwise compliment of a. The s-box must be invertible if decryption is to be possible (Is-box[s-box(a)]= a) however it should not be its self inverse i.e. s-box(a) 6= Is-box(a)

Algebraic formulation of AES S-box

In contrast to the S-boxes in DES, which are apparently “random” substitution, the AES S-box can be defined algebraically. AES S-box involves operations in the finite field: F2 8 = Z2[x]/(x 8 + x 4 + x 3 + x + 1). Let FieldInv denote the multiplicative inverse of a field element. Let Binary To Field convert a byte to a field element; and Field To Binary perform the inverse conversion.

The field element X 7 i=0 aix i corresponds to the byte: a7a6a5a4a3a2a1a0, where ai∈ Z2 = {0, 1} for $0 \leq i \leq 7$. We now discuss Sub Bytes algorithm where eight input bits a7a6a5a4a3a2a1a0 are replaced by the eight output bits b7b6b5b4b3b2b1b0.

Algorithm

```
SubBytes(a7a6a5a4a3a2a1a0)
external: FieldInv, BinaryToField, FieldToBinary
z ← BinaryToField(a7a6a5a4a3a2a1a0)
if z 6= 0 then z ← FieldInv(z)
(a7a6a5a4a3a2a1a0) ← FieldToBinary(z)
 (c7c6c5c4c3c2c1c0) ← (01100011)
comment: all subscripts are to be reduced modulo 8
for i ← 0 to 7
do bi ← (ai + ai+4 + ai+5 + ai+6 + ai+7 + ci) mod 2
return (b7b6b5b4b3b2b1b0)
```

Algorithm

```
InvSubBytes(b7b6b5b4b3b2b1b0)
external: FieldInv, BinaryToField, FieldToBinary
(d7d6d5d4d3d2d1d0) ← (00000101)
comment: all subscripts are to be reduced modulo 8
for i ← 0 to 7
do b ′ i ← (bi+2 + bi+5 + bi+7 + di) mod 2
z ← BinaryToField(b ′ 7 b ′ 6 b ′ 5 b ′ 4 b ′ 3 b ′ 2 b ′ 1 b ′ 0 )
if z 6= 0 then z ← FieldInv(z)
(a7a6a5a4a3a2a1a0) ← FieldToBinary(z)
return (a7a6a5a4a3a2a1a0)
```

Shift Row Transformation

This stage (known as Shift Rows) is shown in figure 5. Simple permutation an nothing more. It works as follow the first row of state is not altered. The second row is shifted 1 bytes to the left in a circular manner. The third row is shifted 2 bytes to the left in a circular manner. The fourth row is shifted 3 bytes to the left in a circular manner.

The Inverse Shift Rows transformation (known as Inv Shift Rows) performs these circular shifts in the opposite direction for each of the last three rows (the first row was unaltered to begin with). This operation may not appear to do much but if you think about how the bytes are ordered within state then it can be seen to have far more of an impact. Remember that state is treated as an array of four byte columns, i.e. the first column actually represents bytes 1, 2, 3 and 4. A one byte shift is therefore a linear distance of four bytes. The transformation also ensures that the four bytes of one column are spread out to four different columns.

Mix Column Transformation

This stage (known as Mix Column) is basically a substitution but it makes use of arithmetic of GF(28). Each column is operated on individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column. The transformation can be determined by the following matrix multiplication on state .

Each element of the product matrix is the sum of products of elements of one row and one column. In this case the individual additions and multiplications are performed in GF(28). The Mix Columns transformation of a single column j ($0 \leq j \leq 3$) of state can be expressed as:

$s'0,j = (2 \bullet s0,j) \oplus (3 \bullet s1,j) \oplus s2,j \oplus s3,j$
$s'1,j = s0,j \oplus (2 \bullet s1,j) \oplus (3 \bullet s2,j) \oplus s3,j$
$s'2,j = s0,j \oplus s1,j \oplus (2 \bullet s2,j) \oplus (3 \bullet s3,j)$ (1)
$s'3,j = (3 \bullet s0,j) \oplus s1,j \oplus s2,j \oplus (2 \bullet s3,j)$

Algorithm MixColumn(c)

```
external: FieldMult, BinaryToField, FieldToBinary
for i ← 0 to 3
doti ← BinaryToField(si,c)
```

```
u0 ← FieldMult(x,t0) ⊕FieldMult(x + 1,t1) ⊕ t2 ⊕ t3
u1 ← FieldMult(x,t1) ⊕FieldMult(x + 1,t2) ⊕ t3 ⊕ t0
u2 ← FieldMult(x,t2) ⊕FieldMult(x + 1,t3) ⊕ t0 ⊕ t1
u3 ← FieldMult(x,t3) ⊕FieldMult(x + 1,t0) ⊕ t1 ⊕ t2
for i ← 0 to 3
dosi,c ← FieldToBinary(ui)
```

The InvMixColumns is defined by the following matrix multiplication

This first matrix of equation can be shown to be the inverse of the first matrix in equation. If we label these A and A−1 respectively and we label state before the mix columns operation as S and after as S ′, we can see that:

$AS = S'$

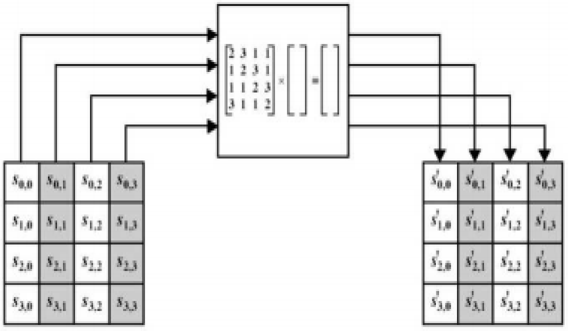
Therefore

$A-1S'$

$= A-1\ \ AS = S$

Add Round Key Transformation

In this stage (known as Add Round Key) the 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a column wise operation between the 4 bytes of a state column and one word of the round key. This transformation is as simple as possible which helps in efficiency but it also effects every bit of state. The AES key expansion algorithm takes as input a 4-word key and produces a linear array of 44 words. Each round uses 4 of these words as shown in figure 2. Each word contains 32 bytes which means each subkey is 128 bits long. Figure 7 show pseudocode for generating the expanded key from the actual key.


2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2
×
=
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

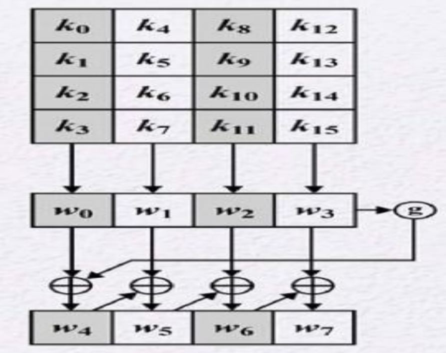
Key expansion pseudocode.

Algorithm KeyExpansion(key)

```
external: RotWord, SubWord
Rcon[1] ← 01000000
Rcon[2] ← 02000000
Rcon[3] ← 04000000
Rcon[4] ← 08000000
Rcon[5] ← 10000000
Rcon[6] ← 20000000
Rcon[7] ← 40000000;
Rcon[8] ← 80000000
Rcon[9] ← 1B000000;
Rcon[10] ← 36000000
for i ← 0 to 3
do w[i] ← (key[4i],key[4i + 1], key[4i +
2],key[4i + 3])
for i ← 4 to 43
do temp ← w[i − 1] if i ≡ 0 (mod 4)
then temp ← SubWord(RotWord(temp)) ⊕Rcon[i/4]
w[i] ← w[i − 4] ⊕ temp
end do
return (w[0],w[1], · · · , w[43])
```

. The function g consists of the following subfunctions: 1. RotWord performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2,b3] is transformed into [b1,b2,b3, b0]. 2. SubWord performs a byte substitution on each byte of its input word, using the s-box described earlier. 3. The result of steps 1 and 2 is XORed with round constant, Rcon[j]. The round constant is a word in which the three rightmost bytes are always 0. Thus the effect of an XOR of a word with Rcon is to only perform an XOR on the leftmost byte of the word. The round constant is different for each round and is defined as Rcon[j] = (RC[J], 0,0,0), with RC[1]= 1, RC[j]= 2. RC[j − 1] and with multiplication defined over the field GF(28).

The inclusion of a round-dependent round constant eliminates the symmetry, or similarity, between the way in which round keys are generated in different rounds. Figure 9 give a summary of each of the rounds. The Shift Rows column is depicted here as a linear shift which gives a better idea how this section helps in the encryption.



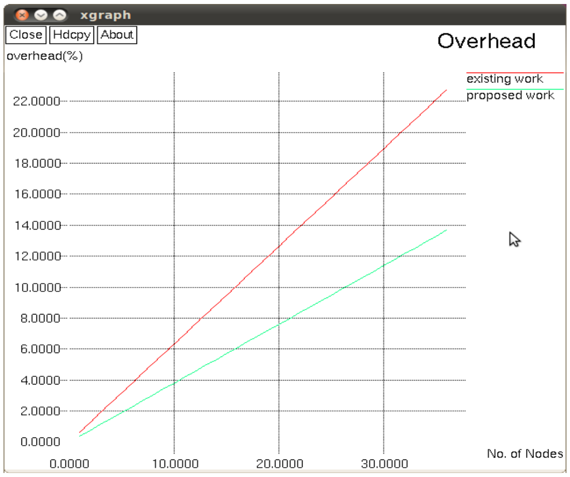
AES key expansion

PERFORMANCE ANALYSIS

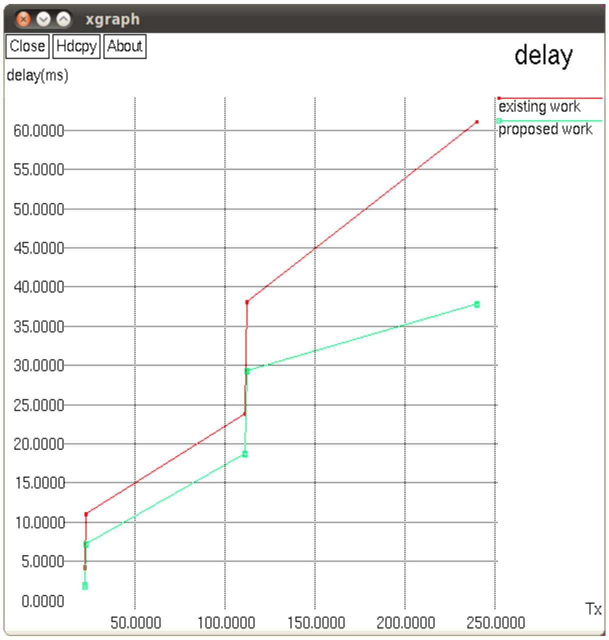
RSA works with two different keys: A public and a private one. Both work complementary to each other, which means that a message encrypted with one of them can only be decrypted by its counterpart. Since the private key cannot be calculated from the public key, the latter is generally available to the public.

Those properties enable asymmetric cryptosystems to be used in a wide array of functions, such as digital signatures. In the process of signing a document, a fingerprint encrypted with RSA, is attached to the file, and enables the receiver to verify both the sender and the integrity of the document. The security of RSA itself is mainly based on the mathematical problem of integer factorization. A message that is about to be encrypted is treated as one large number. When encrypting the message, it is raised to the power of the key, and divided with remainder by a fixed product of two primes. By repeating the process with the other key, the plaintext can be retrieved again. The best currently known method to break the encryption requires factorizing the product used in the division. Currently, it is not possible to calculate these factors for numbers greater than 768 bits. That is why modern cryptosystems use a minimum key length of 3072 bits.

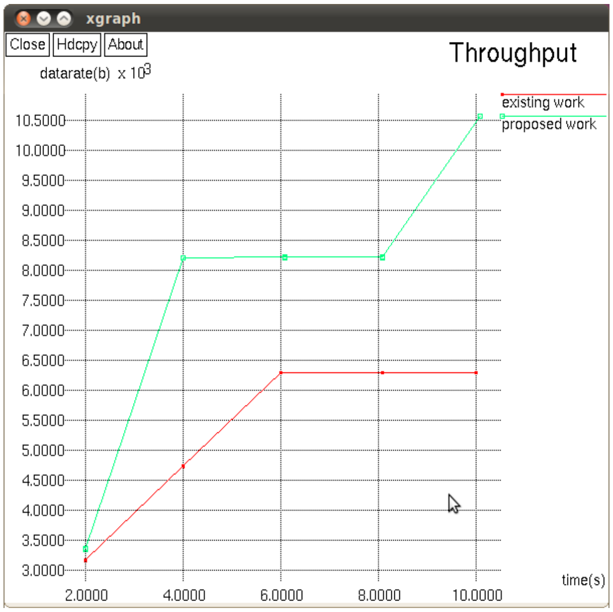
1) **Overhead ratio:** overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to perform a specific task. It is a special case of engineering overhead. The below graph shows that the memory, bandwidth and time required are high in RSA. By using AES algorithm all the above mentioned things have been reduced. So that the overall system performance have increased



2) **Delay ratio** : The graph shows that the Delay increased simultaneously with the encryption/decryption of RSA algothirm and by using AES algorithm the delay decreases simultaneously with the encryption and decryption of data



3) **Throughput ratio:** Throughput is the amount of work that a computer can do in a given time period. Throughput has been a measure of the comparative effectiveness of large commercial computers that run many programs concurrently. Comparing to the throughput of RSA and AES. Throuput is high by using AES algorithm as shown in below graph



CONCLUSION

In this paper we have used a secure distributed dynamic IP configuration (IPv6) protocol for address allocation in a managed MANET where authentication of nodes is very important. Any existing node in the network will be able to generate unique IP addresses from its own IP address for new authorized nodes using this protocol. Therefore, a new node can obtain an IP address from its neighbor nodes without broadcasting any message over the entire MANET during address allocation process. For security purposes on transmitting the data, we use Advanced Encryption Standard algorithm (AES) to ensure more security and throughput while relaying the data.

REFERENCES

[1]. IPv6 Addressing Technique based Dynamic Host Configuration Protocol in Mobile Ad-hoc Network S.N.M.P. Simamora

[2]. Location based Energy Efficient Scheme for Maximizing Routing Capability of AODV Protocol in MANET Sudhir Goswamia , Chetan Agrawalb , Anurag Jainc

[3]. An effective strategy of merging & partioning of network of nodes by incurring in mobile adhoc networks 1bethamsetti srilatha, 2a.v.raghava rao

[4]. Dynamic Address Allocation Protocols for Mobile Ad Hoc Networks Based on genetic algorithm Liu Yong

[5]. secure intrusion detection system in mobile ad hoc networks using rsa algorithm Sankaranarayanan.S

[6]. Improve the Security of CGA using Adjustable Key Block Cipher based AES, to Prevent Attack on AES in IPV6 over MANET Kavita T.Patil M

[7]. An Efficient and Robust Addressing Protocol forNode Autoconfiguration in Ad Hoc Networks Natalia Castro Fernandes, Marcelo DufflesDonato Moreira and Otto Carlos Muniz Bandeira Duarte

[8]. Dynamic and hierarchical IPv6 address configuration for a mobilead hoc network Xiaonan Wang and HuanyanQian

[9]. A secure IPv6 address configuration scheme for a MANET Xiaonan Wang and Yi Mu

[10]. A Secure Addressing Scheme for Large Scale Managed MANETs Uttam Ghosh and Raja Datta