Enhanced Security Framework for Mobile Ad hoc Networks

[1]Pavankumar Naik, [2] Avinash M, [3]Kalmeshwar G,[4]Somesh A,[5]Parishave
[1]Assistant Professor, [2,3,4,5] Students
[1]Computer Science and Engineering Department,
[1]SKSVMACET, Laxmeshwar,India

Abstract— Ad hoc networks are the new wireless technology for mobile nodes. Unlike other wireless networks, it does not rely on a pre-existing infrastructure such as routers in wired network. Instead each node act as routers to form a network and communicate with each other. The military tactical and search and rescue operations are the main application of the ad hoc networks. Main challenge in design of these networks is to robust and attack resistant trust management for the future. This paper mainly focuses on secure routing and thrust key management communication. We identify the new challenges and opportunities posed by this new network and explore new opportunities to secure its communication. In particular, we take advantages of the inherent redundancy in ad hoc network multiple routes between nodes and make it to choose best possible shortest path to communicate between the nodes and provide the secure communication by the attacks (DOS). We also use new cryptographic algorithm that is Advanced Encryption Standard (AES) to build a highly secure modes of transmission which forms the core of our security framework.

I. INTRODUCTION

Ad hoc is a Latin phrase which means "for this [purpose]". Ad hoc means an autonomous system of mobile nodes connected by wireless links form a network, often called as Mobile Ad hoc NETworks (MANET's).

A mobile ad-hoc network (MANET) is an autonomous system of mobile nodes, which is kind of a wireless network where the mobile nodes dynamically form a network to exchange information without any fixed infrastructure. For a MANET to be constructed, all needed is a node must send the data to a node, which wants to accept the data. Each mobile node of an ad-hoc network act as a host as well as a router, forwarding packets for other mobile nodes in the network that may not be within the transmission range of the source mobile node. Each node participates in an ad-hoc routing protocol that allows it to discover multi-hop paths through the network to any other node.

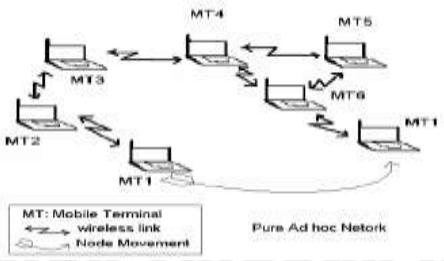

Fig -1 Ad hoc Network

MANET is the infrastructure less network. In this mobiles are self-configuring network of nodes and routers connected by wireless links, which in synchronization form a dynamic topology. These mobile Ad hoc networks operate in independent manner where routers and nodes are free to move randomly, causing a rapidly changing topology. This is why, these networks are very elastic and suitable for several types of applications, as they allow the constitution of temporary communication without any existing infrastructure.

The transmission range of a cellular node inside the community is constrained to a circular region around the node, whose radius depends at the transmitted strength, receiver sensitivity and propagation loss model. If the destination node is not in

the transmission range of the source node, then the mobile ad hoc network works like a multi hop network with one or more node acting as routing node.

Due to the constrained wireless transmission variety of every node, data packets then can be forwarded along multi-hops. The three types of traffic in MANETS are

1) Peer –to Peer: Communication between two nodes with one hop

2) Remote to Remote: Communication beyond one hop but existence of stable route

3) Dynamic Traffic: Nodes are dynamic and routes are reconstructed frequently

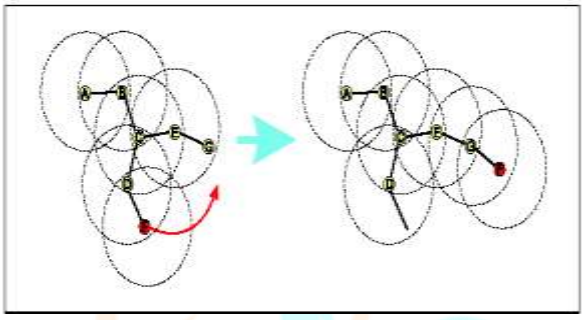

FIG -2 AD HOC NETWORK TOPOLOGY

II. WIRED V/S WIRELESS NETWORKS

The different types of networks available today are Wired and Wireless networks. Wired are differentiated from wireless as being wired from point to point.

WIRED NETWORKS

These networks are generally connected with the help of wires and cables. Generally the cables being used in this type of networks are CAT5 or CAT6 cables. The connection is usually established with the help of physical devices like Switches and Hubs in between to increase the strength of the connection. These networks are usually more efficient, less expensive and much faster than wireless networks. Once the connection is set there is a very little chance of getting disconnected.

ADVANTAGES

- A wired network offer connection speeds of 100Mbps to 1000Mbps
- Physical, fixed wired connections are not prone to interference and fluctuations in
- Available bandwidth, which can affect some wireless networking connections.

DISADVANTAGES OVER WIRELESS NETWORKS

- Expensive to maintain the network due to many cables between computer systems and even if a failure in the cables occur then it will be very hard to replace that particular cable as it involved more and more costs.
- When using a laptop which is required to be connected to the network, a wired network will limit the logical reason of purchasing a laptop in the first place.

WIRELESS NETWORKS

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminate the need for laying out expensive cables and maintenance costs.

ADVANTAGES OF WIRELESS NETWORKS

- Mobile users are provided with access to real-time information even when they are away from their home or office.
- Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.
- Network can be extended to places which cannot be wired.

DISADVANTAGES OF WIRELESS NETWORKS

- Interference due to weather, other radio frequency devices , or obstructions like walls.
- The total Throughput is affected when multiple connections exists.

PROBLEMS IN WIRELESS COMMUNICATION

A number of the issues related to wireless conversation are multipath propagation, path loss, interference, and limited frequency spectrum. Multipath Propagation is, when a signal travels from its source to destination, in between there are obstacles which make the signal propagate in paths beyond the direct line of sight due to reflections, refraction and diffraction and scattering. Path loss is the attenuation of the transmitted signal strength as it propagates away from the sender. Path loss can be determined as the ratio between the powers of the transmitted signal to the receiver signal. his is in particular depending on a range of factors together with radio frequency and the character of the terrain. it's far on occasion critical to estimate the direction loss in wireless conversation networks. Due to the radio frequency and the nature of the terrain are not same everywhere, it is hard to estimate the path loss during communication. During communication a number of signals in the atmosphere may interfere with each other resulting in the destruction of
the original signal. Limited Frequency Spectrum is where, frequency bands are shared by many wireless technologies and not by one single wireless technology.

III. CHARACTERISTICS

Dynamic Topologies

Bandwidth-constrained, variable capacity links

Power-constrained operations

Limited physical security

DYNAMIC TOPOLOGIES

Nodes are free to move arbitrarily; thus network topology which is typically multihop may change randomly and rapidly at unpredictable times. Adjustment of transmission and reception parameters such as power may also impact the topology.

BANDWIDTH-CONSTRAINED, VARIABLE CAPACITY LINKS

Wireless links will continue to have significantly lower capacity than their hard-wired counterparts. One effect of this relatively low to moderate link capacities is that congestion is typically the norm rather than the exception; i.e. aggregate application demand is likely to exceed network capacity frequently.

POWER-CONSTRAINED OPERATIONS

Some or all of the nodes in a MANET rely on batteries for their strength. for this reason, for those nodes, the maximum essential layout standards can be that of electricity conservation.

LIMITED PHYSICAL SECURITY

Mobile wireless networks are generally more vulnerable to bodily security threats than constant, tough-stressed out networks. current link security strategies are often implemented within wireless networks to reduce protection threats.

IV. PROBLEMS IN MANET

SECURITY

Because the signal is diffused in the air, everybody is able to receive it. This is a major problem for security. If people have the correct equipment for a specific signal, they are able to use it (i.e. radio, TV…). Using a wireless communication is equivalent to shouting information from the top of a roof. One of the most effective ways for securing a wireless signal is to encrypt it (encrypting data or even the signal).

BANDWIDTH

Wireless networks suffer from low and unreliable bandwidth. This problem is due to the radio media. Many parameters can affect a radio liaison: interferences, obstacles, mobility…etc As the number of frequencies is limited, and as the bandwidth is proportional to the frequency, the radio frequency space is cut in channels. For Wifi, there are two main frequency spaces, 2.4 GHz (802.11b/g) and 5 GHz (802.11a). 2.4 GHz is also the operating frequency of microwaves, so, using both of these in a close space affects the link quality of the wifi connection, and sometimes, the link is lost. Obstacles also affect radio waves. It first reduces the power of the signal, and then, it can also reflect the signal, and destroy it in the same way. In a mobile environment, radio waves are subject to the Doppler Effect, causing a frequency distortion. In addition, bandwidth on a radio link is shared between every device using it. Access methods must be designed for avoiding collisions and improve communication, but, these access methods also reduce the availability of the bandwidth. It has been proved that on a wifi link, in practice, only 50% of the theoretical bandwidth is available, and tests showed that latency is more important than on wired networks.

ENERGY

A known problem of radio links is the amount of energy they require, not only for the amount of calculation needed for modulation, but mainly for the power needed for the antenna. When a device wants to communicate with a wire, it concentrates all the energy on this wire. For wireless communication, antennas are usually omni-directional, as they need much more energy.

ASYMMETRIC CONNECTIONS

An asymmetric connection is a common problem in wireless telecommunications. There are many causes for that. The radio propagation model is the main cause. In theory, connections are symmetric, signal power reduces proportionally to the distance between the emitter and the receptor. In practice, the antenna design and the environment can cause the device to be able to receive from another device, but will not be able to send to this device. This problem can also appear depending on the chipset design. Some chipsets can restore a low-power signal but will not be able to provide enough power to the antenna for responding to this signal.

DYNAMIC TOPOLOGY

This is also the major problem with ad-hoc routing since the topology is not constant. The mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30sec. This updating frequency might be very low for ad-hoc networks.

ROUTING OVERHEAD

In wireless ad-hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

V. ROUTING IN MANET

DEFINITION

Routing is the mechanism used in communications to find a path between two entities. This is represented in the OSI model as the third layer (called Network). The role of routing a network is similar to the role of a road map for a post office, in both cases; we need to locate the destination, and more importantly, the best way to reach it. It especially has an important role, as the Internet was first designed for military communications. Americans wanted a communication infrastructure able to handle the fact that some part of a network core may be down. In this case, a mechanism should redirect data to its destination. As an OSI layer, this mechanism receives data "ready to send" from the upper layer, then calculates the best path for the destination, and forwards it to layer 2. In the real world, this layer has a very limited role for computers, but, it is the main role for routers, in a network core. For other kinds of network, there are similar mechanisms. For mobile phones, a database centralises the base station where each mobile is connected. This database is used for every call to a mobile phone, providing the end destination to the network core.

ROUTING IN AD HOC NETWORKS

In infrastructure mode, the routing part is handled by the access point and the distribution system; every wireless device just has to forward all its traffic to this access point. But, in Ad Hoc networks, there is no "referee" for connections, and, every device acts as a router. This scenario is totally new. Adding to this, devices are not fixed, they can be mobile, contrary to the Internet where every router has "fixed" neighbors (excepts if a link goes down).

For solving this problem, the IETF (Internet Engineering Task Force), powerful standardization authority in the communication world, created the MANET work group. This group has a mission to create and discuss routing protocols for Ad Hoc networks. This task is very important, due to the complexity of routing on Ad Hoc networks. The work started in January 1999, with the publication of the informational RFC 2501. This document presents the 4 main constraints for routing on Ad Hoc networks, such as dynamics topology, bandwidth constraints, energy constraints and low physical security. The group has then to comply with these constraints in order to build an efficient algorithm of route calculation.

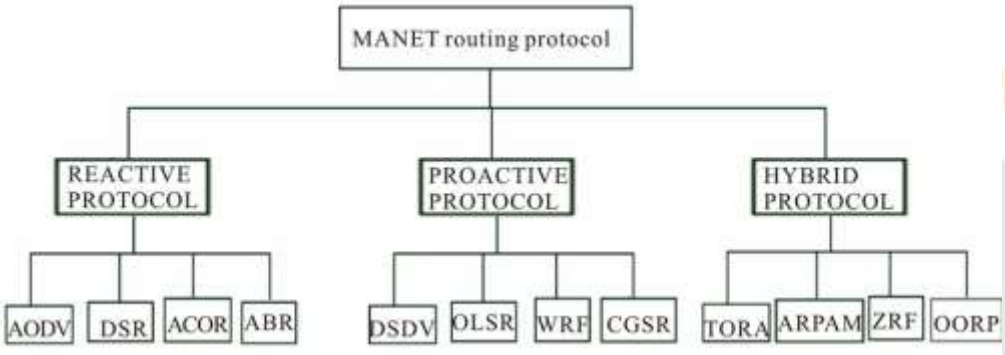

Fig 5.1 Routing Protocol in MANET's

AD-HOC ROUTING PROTOCOLS

There were different approaches, and then, different solutions. The three mains approaches are proactive protocols, reactive protocols and hybrids.

PROACTIVE

Proactive protocols are close to wired routing protocols in the manner that the routing table is built before the data has to be sent. That means these protocols are constantly making requests to their neighbours (if any) in order to draw a network topology, and then, build the routing table. The disadvantage of this principle is to not be reactive to topology changes, as the tables are pre-established. At the time the data has to be sent, it is not certain that the gateway designed by the routing table will still be there to forward the data.

REACTIVE

Reactive protocols are more specific to Ad Hoc networks. Contrary to the proactive algorithm, they ask their neighbours for a route when they have data to send. If the neighbours do not have any known route, they broadcast the request, and so on. Once the final destination has been reached by these broadcasts, an answer is built and forwarded back to the source. This source can then transmit the data on the newly discovered route. Each device used for forwarding the routing packets has learned the route at the same time. The disadvantage of this design is the amount of routing traffic exchanged between devices. In the case of a large topology, the traffic will be spread on each link until the end node is found. It also can result in a high latency.

HYBRIDS

A Hybrid protocol will use the two above algorithms. The main goal is to reduce broadcasts and latency, but improve the dynamism impact. The whole network will be separated into logical zones, and each zone will have a gateway. Inside each zone, a reactive protocol will be used. For inter-zone routing, a proactive protocol will be used.

VI. PRO-ACTIVE PROTOCOLS

As proactive protocols are constantly updating their routing tables in order to be ready when data has to be sent, they are called table-driven protocols. This type of protocol is close to wired networks where the same mechanisms are used in order to take routing decisions. These mechanisms are used for finding the shortest path across the network topology; it can be the "Link state" method or the "Distance Vector" method. With the "Link State" method, each node has its own view of the network, including the states of its own channels. When an event on the channel occurs, the node floods the network topology with its own new view of the topology. Other nodes which receive this information use algorithms to reflect changes on the network table. With the "Distance Vector" routing approach, each node transmits to its close nodes its vision of the distance which separate it from all the hosts of the network. Based on the information received by the neighbourhood, each node performs a calculation in order to define routing tables with the shortest path to all destinations available in the network.

DESTINATION SEQUENCED DISTANCE VECTOR (DSDV)

DSDV was one of the first proactive routing protocols available for Ad Hoc networks. It was developed by C. Perkins in 1994, 5 years before the informational RFC of the MANET group. It has not been standardized by any regulation authorities but is still a reference.

ALGORITHM

DSDV is based on the Bellman-Ford algorithm. First designed for graph search applications, this algorithm is also used for routing since it is the one used by RIP. With DSDV, each routing table will contain all available destinations, with the associated next hop, the associated metric (numbers of hops), and a sequence number originated by the destination node.

Tables are updated in the topology per exchange between nodes. Each node will broadcast to its neighbours entries in its table. This exchange of entries can be made by dumping the whole routing table, or by performing an incremental update, that means exchanging just recently updated routes. Nodes who receive this data can then update their tables if they received a better route, or a new one. Updates are performed on a regular basis, and are instantly scheduled if a new event is detected in the topology. If there are frequent changes in topology, full table exchange will be preferred whereas in a stable topology, incremental updates will cause less traffic. The route selection is performed on the metric and sequence number criteria. The sequence number is a time indication sent by the destination node. It allows the table update process, as if two identical routes are known, the one with the best sequence number is kept and used, while the other is destroyed (considered as a stale entry).

ILLUSTRATION

Let us consider the two following topologies (fig -4 and fig -5). At t=0, the network is organized as shows fig -4. We suppose at this time the network is stable, each node has a correct routing table of all destinations.

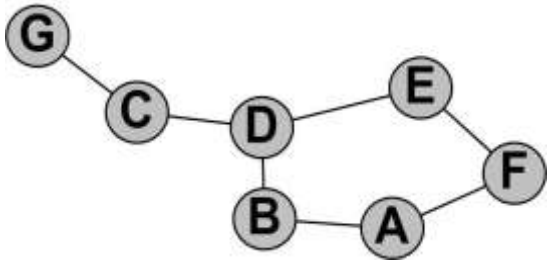

Fig -4 Topology 1

Then, we suppose G is moving, and at t+1, the topology is as shown in fig -5.

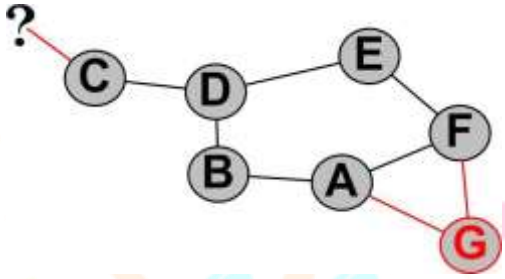

Fig -5 Topology 2

At this stage, the following events are detected, and actions are taken:

- On node C: Link with G is broken, the route entry is deleted, and updates are sent to node D.
- On node A and F: A new link is detected, the new entry is added to the routing table and updates are sent to neighbours.
- On node G: Two new links are detected (to A and F), and one is broken (to C), the routing table is updated and a full dump is sent to neighbours (as the routing table is entirely changed, a full dump equals an incremental update).

PERFORMANCE

As with every table-driven protocol, DSDV reduces the latency by having a route when the data has to be sent. But, DSDV presents a few problems, mainly in the route table update process. One of the major problems is that data is exchanged only between neighbours, and then, a change in the topology can take time to be spread in the whole topology. That introduces the notion of route fluctuation. When a node disappears, it takes time for this change to be reflected in the whole topology. So, if the topology is dynamic, the routing layer will be unstable until changes are reflected everywhere. Updates are sent after events, links broken and new links. At t+1, the routing protocol will transmit routing table updates according to the newly detected events . But, once these updates are processed by nodes D, B and E, nodes C and D still have no routes for G, and it will take two more updates until the entire topology will be updated on all nodes.

VII. SECURITY CRITERIA IN MANET

In this section, we have discussed different security criteria with reference to mobile ad-hoc networks.

- **Availability:** It refers to the property of the network to continue provide services regardless of the state of the network. A denial of service attacks is based to attack this property [9].
- **Integrity:** Integrity guarantees that no modification, addition, deletion is done in the message, the altering of message can be done malicious or accidental [9]. It assures that the data received are exactly same as sent by an authorized entity.
- **Confidentiality:** It allowed that the message cannot be even viewed in its original form by any unauthorized person. The transmitted message must make sense to only the intended receiver.

- **Authenticity:** With the help of this property, the sender and receiver prove their identities. This property ensures that the parties are genuine not impersonators or intruders.
- **Non-repudiation:** With the help of this property the sender and receiver cannot be able to deny about sending and receiving the message [10].
- **Authorization:** This property assigns different access rights to the different types of the users. For example, a network management can be performed by network administrator only.

ATTACKS ON LAYER

Table 1 Attacks on Network layers

Protocol layer	Layer Attacks
Physical Layer	Jamming; PUEA;OFA;CCDA
Link Layer	SSDF; Control channel saturation DoS attacks; SCN
Network Layer	Sink hole attack; hello flood attack
Transport Layer	Lion attacks; jellyfish attack
Application Layer	Attacks corresponding to all the layers have an advance effect on the application layer.

ATTACKS ON MANET's

There are two types of attacks in the MANET. First is the internal attack and second is the external attack. An external attack causes congestion, sends false routing information or causes unavailability of services. In an internal attack, the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities [13].

Denial of Service attack: This attack prevents the normal use or management of communications facilities. This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available to the actual recipients. The attacker generally uses the radio signal jamming and the battery exhaustion method [10].

Impersonation: Impersonation attack is a severe threat to the security of mobile ad hoc network. If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information of the users.

Eavesdropping: In [13], eavesdropping is another kind of attack that usually happens in the mobile ad-hoc networks. This is the passive attack. The node simply observes the confidential or personal information. This information can be later used or misuse by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized or attacker access.

Routing Attacks: Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad-hoc networks, attacks against routing are generally classified into the two categories: attacks on routing protocols and attacks on packet forwarding/delivery [4]. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on the packets forwarding try to disturb the packet delivery along a predefined path.

SECURITY SOLUTION IN MANET's

Providing security within MANETs suggests encrypting the message before sending it i.e. Cryptography [1]. Cryptography enables the user to transmit confidential information across any insecure network so that it cannot be used by an intruder. Cryptography is the process that involves encryption and decryption of text using various mechanisms or algorithms. There are two general categories of cryptographic algorithms. The first one is named Symmetric Key Cryptography which defines a shared key between each pair of nodes. If all shared keys are the same, the method will be

called Shared Key Cryptography. Examples include DES and AES. But symmetric-key cryptography has some limitations. One major limitation is the key distribution problem. In this method, compromising each node results in destroying security in the whole network. The second cryptographic algorithm is called Asymmetric Cryptography. In this kind of cryptography each node has two keys, public key and private key. The public key of each node is public for any node and the private key is known only by the owner of the key. Here, if a node wants to send a message to another one, it should encrypt the message by the destination node's public key. The encrypted message will not be decrypted other than with the private key that is known just by the destination node. In different networks that use asymmetric cryptography, there exists a third party or a group of distributed third parties that produces an infrastructure. As discussed before, MANETs do not have any infrastructure or server, so there is no third party. Using asymmetric cryptography in MANETs without third party or any other infrastructure, leads to store the public keys of all nodes in everyone.

VIII. ADVANCED ENCRYPTION STANDARD

AES [8] can process the 128 bit data blocks and uses key lengths of 128, 192, or 256 bits. For the key length of 128,192 and 256 bits, AES may be known to as AES-128, AES-192 and AES256 respectively. Unlike DES, AES is not a fiestel structure. Number of rounds in AES depends on key length i.e. for a key length of 128, number of rounds is 10 and similarly for 192 and 256 bit keys, it is 12 and 14 respectively. AES provides security against all known attacks, simple in the design and good speed of computation.

SALIENT FEATURES OF AES

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical. To appreciate the processing steps used in a single round, it is best to think of a 128-bit block as consisting of a 4×4 matrix of bytes, arranged as follows:

$$\begin{pmatrix} byte0 & byte4 & byte8 & byte12 \\ byte1 & byte5 & byte9 & byte13 \\ byte2 & byte6 & byte10 & byte14 \\ byte3 & byte7 & byte11 & byte15 \end{pmatrix}$$

Therefore, the first four bytes of a 128-bit input block occupy the first column in the 4 × 4 matrix of bytes. The next four bytes occupy the second column, and so on.

THE ENCRYPTION KEY AND ITS EXPANSION

Assuming a 128-bit key, the key is also arranged in the form of a matrix of 4 × 4 bytes. As with the input block, the first word from the key fills the first column of the matrix, and so on. The four column words of the key matrix are expanded into a schedule of 44 words. Each round consumes four words from the key schedule. Figure 12 on the next page depicts the arrangement of the encryption key in the form of 4-byte words and the expansion of the key into a key schedule consisting of 44 4-byte words.

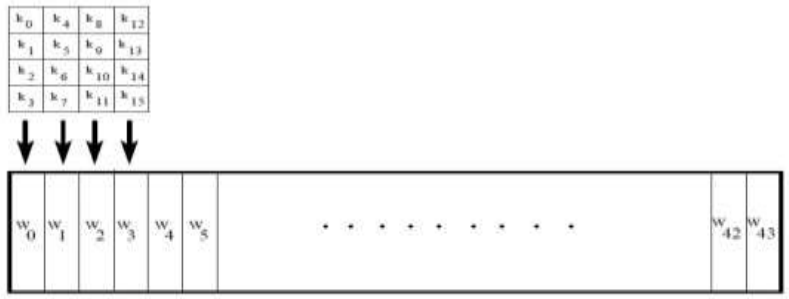

Fig -7 This figure shows the four words of the original 128-bit key being expanded into a key schedule consisting of 44 words.

THE OVERALL STRUCTURE OF AES

The overall structure of AES encryption/decryption[2] is shown in Figure 2. The number of rounds shown in Figure 2, 10, is for the case when the encryption key is 128 bit long. (As mentioned earlier, the number of rounds is 12 when the key is 192 bits, and 14 when the key is 256.) Before any round-based processing for encryption can begin, the input state array is XORed with the first four words of the key schedule. The same thing happens during decryption — except that now we XOR the ciphertext state array with the last four words of the key schedule.

For encryption, each round consists of the following four steps: 1) Substitute bytes, 2) Shift rows, 3) Mix columns, and 4) A dd round key. The last step consists of XORing the output of the previous three steps with four words from the key schedule.

For decryption, each round consists of the following four steps: 1) Inverse shift rows, 2) Inverse substitute bytes, 3) Add round key, and 4) Inverse mix columns. The third step consists of XORing the output of the previous two steps with four words from the key schedule. Note the differences between the order in which substitution and shifting operations are carried out in a decryption round vis-a-vis the order in which similar operations are carried out in an encryption round.

The last round for encryption does not involve the "Mix columns" step. The last round for decryption does not involve the "Inverse mix columns" step.

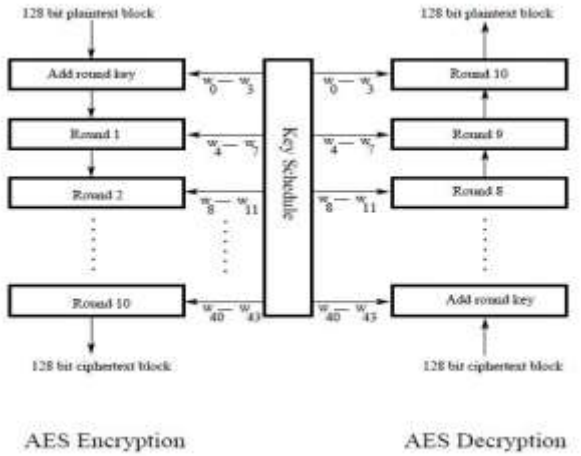

Fig -8 The overall structure of AES for the case of 128bit encryption key.

CONCLUSION

In this paper, We have analyzed the security threats an ad hoc network faces and presented the security objectives that need to be achieved. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. The idiosyncrasy of ad hoc networks poses both challenges and opportunities for these mechanisms.

We discovered during this report the problems associated with Ad Hoc networks, more specifically routing on Ad Hoc networks. We also discovered solutions for these problems. Five routing protocols were covered. First, proactive protocols; table-

driven as their peers in the wired world, they have the disadvantage of not being really reactive to topology changes. DSDV in particular is subject to route fluctuation, and brings a lot of instability

This focuses on how to secure routing and how to establish a secure key management service in an ad hoc networking environment. These two issues are essential to achieving our security goals. Besides the standard security mechanisms, we take advantage of the redundancies in ad hoc network topology and use diversity coding on multiple routes to tolerate both benign and Byzantine failures. To build a highly available and highly secure key management service, we propose to use threshold cryptography to distribute trust among a set of servers. Furthermore, our key management service employs share refreshing to achieve proactive security and to adapt to changes in the network in a scalable way. Finally, by relaxing the consistency requirement on the servers, our service does not rely on synchrony assumptions. Such assumptions could lead to vulnerability. A prototype of the key management service has been implemented, which shows its feasibility.

REFERENCES

[1] http://www.crhc.uiuc.edu/~nhv/

[2] http://www.adhoc.6ants.net/~paul/

[3] Securing Ad Hoc Networks∗ Lidong Zhou Department of Computer Science Zygmunt J. School of Electrical Engineering Cornell University Ithaca, NY 14853.

[4] M. Zapata, and N. Asokan, "Securing Ad Hoc Routing Protocols," ACM WiSe, 2002.

[5] Computer Networks by Tanenbaum

[6] S.Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.

[7] R. Li et al., "On Demand Public-Key Management for Mobile Ad Hoc Networks," Wiley's J. Wireless Commun. and Mobile Comp., vol. 6, no. 3, May, 2006, pp. 295–306.

[8] Khushdeep Kaur, Er. Seema, "Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices", International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012

[9] Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, "DSAB – A Hybrid Approach for Providing Security in MANET", INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, Vol.1, No.3

[10] Jayashree.A.Patil,Nandini Sidnal, "Survey - Secure Routing Protocols of MANET", International Journal of Applied Information Systems (IJAIS),Volume 5– No.4, March 2013

[11] Amol Bhosle, Yogadhar Pandey, "Review of authentication and digital signature methods in Mobile ad hoc network", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),Volume 2, Issue 3, March 2013

[12] Rashid Sheikhl, Mahakal Singh Chandee, Durgesh Kumar Mishra, "Security Issues in MANET:A Review",IEEE,2010

[13]Wenjia Li,Anupam Joshi, "Security Issues in Mobile Adhoc Networks:A Survey"