ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

A Novel Node Security Mechanism For Mobile Ad-Hoc Network

Mr.D.Saravanan[1], Mr.I.Anbumuthu[2]

Associate Professor, Dept. of CSE, Pavendar Bharathidasan College of Engineering and Technology (PACET), Tiruchirappalli, Tamil Nadu[1]

PG Scholar, Dept. of CSE, Pavendar Bharathidasan College of Engineering and Technology (PACET), Tiruchirappalli, Tamil Nadu[2]

Abstract – In Mobile Ad-Hoc Networks (MANETs) Security is an important issue in order to provide protected communication between mobile nodes in hostile environment. The unique characteristics of (MANETs) pose a number of nontrivial challenges to security design such as open peer-to-peer network architecture, shared wireless medium, stringent resources constraints, and highly dynamic network topology these challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. Here proposed an efficient Symmetric-key algorithm (AES) that provides complete security solution and encompass all three security components of prevention, detection, and reaction.

Keywords-Mobile ad-hoc network (MANET), ad-hoc on-demand distance vector routing (AODV), advanced encryption standard (AES), confidentiality.

I. INTRODUCTION

A Mobile Ad-hoc NETwork (MANET) is one that comes together as needed, not necessarily with any support from existing Internet infrastructure or any other kind of fixed stations. We can formularize this statement by defining an ad hoc network as an autonomous system of mobile hosts (also serving as routers) connected by wireless links, the union of which forms a communication network model that supports the needs of wireless communication by installing base stations as access point. In these cellular networks, communications between two mobile nodes completely rely on the wired backbone and the fixed base stations. In a MANET, no such infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move. The mode of operation, in ad hoc networks are basically peer-to-peer multi-hop mobile wireless networks where information packets are transmitted in a store-and-forward manner from a source to an arbitrary destination, via intermediate nodes as shown in the figure 1.

As the nodes move, the resulting change in network topology must be made known to other nodes so the outdated topology information can be updated or removed. Figure 1 raises another issue of symmetric (bi-directional) and asymmetric (unidirectional) links with associative radio range

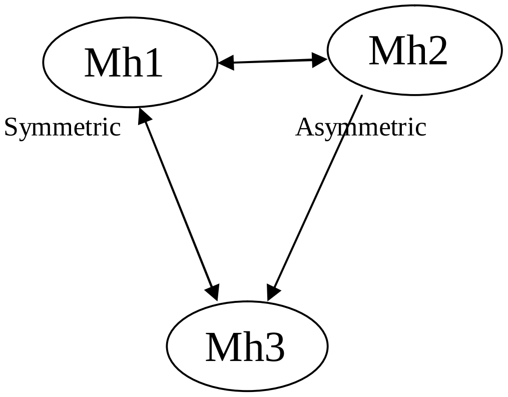

Figure 1 --- A Mobile Ad-hoc Network

Applications

- Personal area networking
  – Cell phone, laptop, ear phone, wrist watch
- Military environments
  – Soldiers, tanks, planes
- Civilian environments
  – Taxi cab network
  – Meeting rooms
  – Sports stadiums
  – Boats, small aircraft
- Emergency operations
  – Search-and-rescue
  – Policing and fire fighting

II. ROUTING IN MANET

It has become clear that routing in a MANET is intrinsically different from traditional routing found on infrastructure networks. Routing in a MANET depends on many factors including topology, selection of routers, initiation of request and specific underlying characteristic that could serve as a heuristic in finding the path quickly and efficiently.

One of the major challenge in designing a routing protocol for ad-hoc network stems from the fact that, on one hand, a node needs to know at least the reachability information to its neighbors for determining a packet route and, on the other hand, the network topology can change quite often in ad hoc network. Ad-hoc routing protocols can be broadly classified as being Proactive (or table-driven) or Reactive (on-demand).Proactive protocols mandates that nodes in a MANET should keep track of routes to all possible destinations so that when a packet needs to be forwarded, the route is already known and can be immediately used. On the other hand reactive protocols employ a lazy approach whereby nodes only discover routes to destinations on demand i.e., a node does not need a route to a destination until that destination is to be the sink of data packets sent by the node.

a. REACTIVE ROUTING APPROACH

In this section, we describe some of the most cited reactive routing protocols

Ad Hoc On-Demand Distance Vector Protocol

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is basically a combination of Destination Sequence Distance Vector (DSDV) and Dynamic Source Routing (DSR). It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR. Plus the use of hop-by-hop routing, sequence numbers and periodic beacons from (DSDV).AODV minimizes the number of required broadcasts by creating route on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. AODV classified as a pure on-demand route acquisition system since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges .It supports only symmetric links with two different phases:

- Route Discovery, Route Maintenance and
- Data forwarding

At first all the nodes send hello message on its interface and receive hello message from its neighbors. This process is repeated periodically to determine to determine neighbor connectivity and to update routing table entry. When a route is needed to some destination, the protocols start route discovery. It uses two term route request & route reply.

Route Request Message RREQ:
Source node that needs to communicate with another node in the network transmits RREQ message. AODV sends RREQ message. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

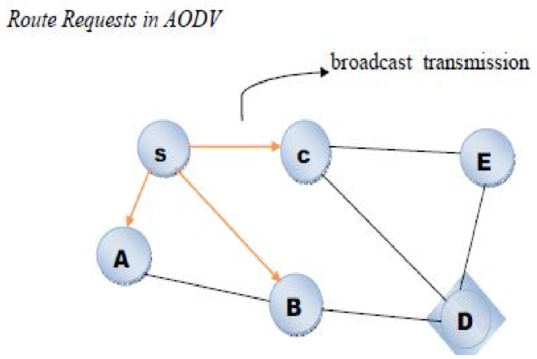

Figure 2 Route request in AODV

Route Reply Message RREP:
A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

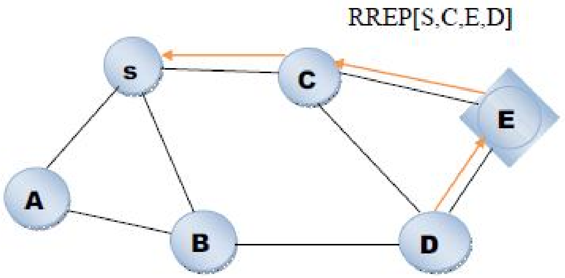

Figure 3 Route reply in AODV

III. PROBLEM

Encryption is the process of transforming information to make it unintelligible to all unauthorized parties except the intended recipient and forms the basis of data integrity and privacy which is necessary for the authenticated users. Among all the encryption methods transposition ciphers is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a bijective function is used on the characters positions to encrypt and an inverse function to decrypt.

Transposition can be broken by statistical methods because the pairs of successive characters in a normal language have typical likelihood. Other pairs do occur much less often. If the messages are short, some characters may not appear thus it is possible to say which words do not exist in the text. An improvement on this cryptographically method is to put the cipher text through a second transposition cipher. There are a lot of even more complicated transposition ciphers disadvantage of transposition is the high demand for memory, therefore substitution is far more common.

IV.CONTRIBUTION

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. It is based on the Rijndael cipher, Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

High-Level Description of the Algorithm

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round -AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds

SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

Apart which add round key also play a vital role as we mentioned in above initial round.

4. Final Round (no MixColumns)

□ SubBytes
□ ShiftRows
□ AddRoundKey.

System architecture:

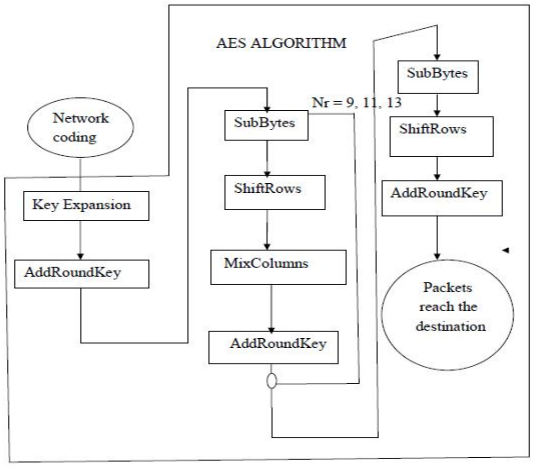

Figure 4 System Architecture

V. SYSTEM IMPLEMENTATION

1. MODULES DESCRIPTION:
2. Performance of AODV protocol
3. Analysis of AODV protocol
4. Performance of proposed AES Algorithm
5. Throughput Calculation

Performance of AODV protocol

Normal Network with AODV protocol is been used for creating nodes and transfer packets with less amount of queue length in order to obtain Drop.

Analysis of AODV protocol

Topology of wireless networks with more no of nodes , transmission of packets between the nodes is done using Normal Network with AODV protocol, parameters such as end to end delay, throughput, packet delivery ratio is calculated and the output is shown using graphs.

Performance of proposed AES Algorithm

Topology of wireless networks with more no of nodes , transmission of packets between the nodes is done using AES Encryption Scheme to avoid attacks, parameters such as end to end delay, throughput, packet delivery ratio, is calculated and the output is been compared with node insertion .

VI.CONCLUSION

The security issues in MANETs based on the technique symmetric cryptographic is performed. Using AES, an lightweight encryption scheme on top of network coding is been implemented and it reduces energy consumption in MANETs by cutting the security cost. Genetic algorithm is effective to break transposition ciphers on the passage choosen, Then experiment it with AES to encrypt a given plain text with length up to 1K bytes and measure the time they use. The experiment setting is followed by a 192 bit key for AES, Results with less encryption time means larger throughput. As the plaintext length increases, the per-byte energy consumption of AES converges. Hence it shows that AES is efficient in computation, and incurs less energy consumption for encryptions/decryptions.

REFERENCES

[1] Aoki K. and Lipmaa H. (2000) "Fast Implementations of AES Candidates".
[2] Benjie Chen, Kyle Jamieson, Hari Balakrishnan. and Robert Morris,Span. (2002) " An Energy - Efficient Coordination Algorithm for Topology.
Maintenance in Ad Hoc Wireless Networks " 8,481-494,2002
[3] Bhattad K . and Narayanan K R. (2005) " Weakly secure network coding" in Proceedings of NetCod, Apr.2005.
[4] Cagalj M.,Hubaux J. and Enz C. (2002) "Minimum-energy broadcast in all-wireless networks:Np- completeness and distribution issues".
[5] Dimovski A. and Gligoroski D. (2003) "Attacks on the Transposition Cipher Using Optimization Heuristics.
[6] Fragouli C.,Widmer J. and Boudec J. (2006) "A network coding approach of energy efficient broadcasting,from theory to practice".
[7] Ho T., M´edard M., Koetter R., Karger D R., Effros M.,Shi J.,Leong B. (2006) "A random linear network coding approach to Multicast", vol. 52,no. 10, pp.4413–4430,Oct.2006,

[8] Li L., Ramjee R., Buddhikot M. and Miller S. (2007)"Network coding based broadcast in mobile ad-hoc Networks in Proceedings of IEEE INFOCOM, 2007.

[9] Lima L., M´edard M. and Barros J. (2007) " Random linear network coding: A free cipher" in Proceedings of IEEE ISIT

[10] Potlapally N R.,Ravi S.,Raghunathan A. and Jha N K. (2006) "A study of The energy consumption characteristics of cryptographic algorithms and Security protocols" vol. 5, no.2, pp.128 143,2006,

[11] Saravanan D., Chandrasekaran RM.,Sarma Dhulipala V R.,Vishnu Prabha B. (2011) " Trust Worthy Architecture for Mobile Ad Hoc Network Environment".

[12] Vilela J P.,Lima L. and Barros J. (2008) " Lightweight security for network coding".

[13] Wang J.,Lu K., Xiao B. and Gu N. (2010) "Optimal linear network coding design for secure unicast with multiple streams "

[14] Wu Y., Chou P. and Kung S. (2005) " Minimum-energy multicast in mobile ad hoc networks using network coding"Vol :53 Issue:11

[15] Xiao Y.and Shen X. (2006) " A Survey on Intrusion Detection in Mobile Ad Hoc Networks" pp. 170 – 196.