International Journal of communication and computer Technologies, ISSN: 2278-9723
Available at http://www.ijccts.org

Secure Data Transmission In AODV Routing Protocol

Kartik Kumar Srivastava, Avinash Tripathi, Anjnesh Kumar Tiwari
B-Tech Final Year
Computer Science & Engineering
Institute of Technology & Management
GIDA, Gorakhpur

Received: 13-02-2013, **Revised:** 01-04-2013, **Accepted:** 04-05-2013, **Published online:** 29-05-2013

Abstract- Secure Information exchange in a network of mobile and wireless nodes without any infrastructure support such networks are called as adhoc networks. A Mobile adhoc network (MANET) is multi-hop, mobile, infrastructure less wireless network which is capable of independent operation. In this paper we have been discussing some of the basic routing protocols in MANET like Destination Sequenced Distance Vector(DSDV), Dynamic Source Routing(DSR), Ad-hoc On Demand Distance Vector(AODV) and Zone Routing Protocol(ZRP).

Security is one of the principal issue in MANETs as they are infrastructure-less and independent. Therefore, in manet having security needs, there must be two considerations kept in mind: one to make a data transmission. Our endeavour in this paper would focus on achieving the routing and secure data exchange. In this course, we have designed the Ad Hoc on Demand Routing Protocol (AODV) using asymmetric cryptographic algorithm such as RSA . Which is more efficient as well as we have implemented the security technique so that we can prevent the data loss at the time of transmission.

Keywords- Adhoc network, key management, mobile adhoc network, routing protocol, security.

1. Introduction

An ad-hoc network is a set of wireless mobile hosts forming a impermanent network without the assistance of any separate infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks. Each and every node in mobile ad hoc networks is set up with a wireless transmitter and receiver, which permits it to communicate with other nodes in its communication area only. Nodes communicating with each other usually share the similar physical media; they transmit and get signals at the same frequency band, following the same hopping sequence or spreading code. If the destination node is not inside the transmission area of the source node, the source node takes help of the intermediate nodes in between in order to communicate with the destination node by transmitting the messages hop by hop. Fig1. illustrates the Mobile ad-hoc network. In order to transmit a message from a node to a node that is out of its radio range, the collaboration of other nodes in the network is required; this is commonly called as multi-hop communication. Therefore, each node at the particular time must act both as a host and as a router as well.

Mobile wireless networks are commonly open to various attacks, such as information and physical security attacks than fixed wired networks. Securing wireless ad hoc networks is prone to more difficulty such as: vulnerability of channels and nodes, absence of infrastructure, dynamically changing topology and etc. The wireless channel is available to both legitimate network users and malicious attackers. The abstract of centralized management makes the standard security solutions reliable on certification authorities and on-line servers not applicable. A malicious attacker can quickly become a router and break network operations by deliberately not following the protocol specifications.

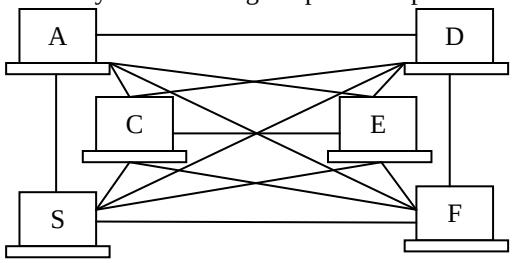

Figure-1 A mobile Ad-hoc Network

All the nodes in the network are free to move in any direction and organize themselves arbitrarily. They can join or leave the network whenever they want. Due to the repeatedly change in the network topology there is a significant change in the status of trust among different nodes which adds the difficulty to routing among the various mobile nodes. The self-organization of nodes in mobile ad hoc networks may tend to refuse providing services for the advantage of other nodes in order to keep their own resources acquaint new security that are not concentrated in the infrastructure-based networks.

2. Exploring AODV

AODV is an efficient as well as a reactive routing protocol which has been designed for a mobile ad-hoc networks. AODV is a advanced routing protocol that implements a purely *reactive* approach. At the starting time of a communication session it establishes a route on-demand, and uses it till it breaks, after that a

new route setup is started. In AODV protocol, when a source node S wants to send a packet to its destination node D and does not having any route to D, it begins its route discovery phase by broadcasting a route request message (RREQ) to its neighbour nodes. The route discovery phase of this protocol is shown in Figure.1.

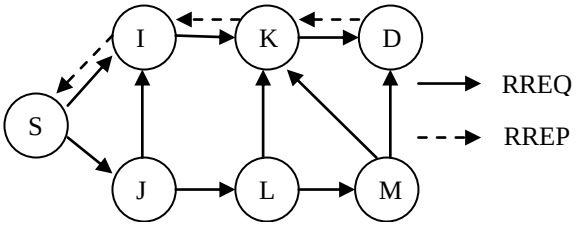

Figure 3: Route Discovery Process of AODV Routing Protocol

The RREQ message is of the following format:
<s_addr, id, s_seq, d_addr, d_seq, hop_count>
where, s_addr=IP address of source node,
d_addr= IP address of destination node,
id=broadcast ID,
s_seq= the sequence number of source node,
d_seq= the sequence number of destination node,
hop_count= number of nodes this message have passed.

On receiving the RREQ message, the intermediate node i.e I, J, K, L and M which have no route to the destination node would increment the hop_count by 1, rebroadcast this RREQ message to its neighbours and launching a Reverse Path Pointer for the node from which it receives the RREQ message. This process is recurred until the RREQ message reaches the destination node. Upon receiving the first RREQ message, the destination node unicasts a Route Reply message (RREP) to the source node through the reverse path from where the RREQ message arrived. The RREP message is of the following format:
<s_addr, d_addr, d_seq, hop_count, lifetime>
where, s_addr=IP address of source node,
d_addr= IP address of destination node,
hop_count can be reset to zero and counted again,

The intermediate node will increase the hop_count by 1 and transmit it according to its Reverse Path Pointer. The same RREQ that arrives later will be discarded by the destination node.

Additionally, AODV allows intermediate nodes that have sufficiently fresh routes to generate and send an RREP message to the source node having destination sequence number equal or greater than one in the RREQ. For example, if the intermediate node K has the fresh route with highest sequence number to the destination D, upon receiving the RREQ message, it sends the RREP message to the source S. This condition is shown in Figure 2.

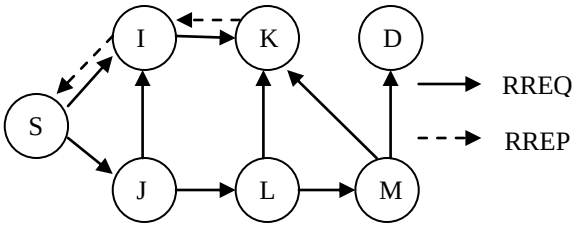

Figure 4: Route Reply Process Of AODV Routing Protocol

Once the source node receives the correct RREP message ,the data transmission starts. With the intention of speeding up the Route Discovery process, AODV also allows the intermediate nodes which have the route to the targeted destination node to generate a RREP message and send it back to source node again. It is to be noted that only those nodes which are adjacent to the active route or Reverse Path, store necessary information in their route tables and the other intermediate nodes will reject the routing information like Reverse Path pointer.

3. Proposed work

3.1 Introduction

Encryption is the act of encoding text so that others cannot understand the content of the text. Encryption has long been the field of spies and diplomats, but recently it has moved into the public interest with the concern of the protection of electronic transmissions data and digitally stored data. Standard encryption techniques usually have two basic defects: A secure channel must be established at some point so that the sender may exchange the decrypting key with the receiver; and there is no assurance who sent a given message. Public key cryptography has rapidly grown in popularity (and controversy, see, for example, discussions of the Clipper chip on the archives given below) because it offers a very secure and reliable encryption method that addresses these concerns. In a traditional cryptosystem in order to make sure that nobody, except the intended recipient, decrypts the message, the people involved had to endeavor to keep the key secret. In a public-key cryptography, it solves one of the most annoying problems of all prior cryptography i.e., the necessity of establishing a secure channel for the exchange of the key.
In asymmetric cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. RSA is the first algorithm known to be appropriate for signing as well as encryption, and was one of the first great progress in public key cryptography. RSA is broadly used in electronic commerce protocols, and is supposed to be secure given

sufficiently long keys and the use of up-to-date implementations.

3.2 Operation

The RSA algorithm involves three basic steps i.e., key generation, encryption and decryption.

3.2.1 Key Generation

RSA involves a public and a private key**.** The public key is known to everyone and is used for encryption of messages. Messages encrypted with the public key can only be decrypted using the private key of the user only i.e., confidential. The public and private keys for the RSA algorithm can be generated in the following way:
Choose two distinct prime numbers p and q. Note that the integers p and q should be chosen unvaryingly at random and should be of similar bit-length. Prime integers can be efficiently selected using a primality test.

1. Compute $n = pq$ where n is used as the modulus for both the public and private keys
2. Compute $\varphi(pq) = (p - 1)(q - 1)$ where φ is Euler's totient function.
3. Choose an integer e such that $1 < e < \varphi(pq)$, and e and $\varphi(pq)$ share no divisors other than 1 i.e. e and $\varphi(pq)$ are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption. However, small values of e (such as $e = 3$) have been shown to be less secure in some settings.
4. Determine d (using modular arithmetic) which satisfies the congruence relation.

$$\boldsymbol{de \equiv 1 (mod \varphi(pq))}$$

   - Stated differently, $ed - 1$ can be evenly divided by the quotient $(p - 1)(q - 1)$
   - This is often computed using the extended Euclidean algo-rithm.
   - d is kept as the private key exponent

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the private (or decryption) exponent d which must be kept secret..

3.2.2 Encryption

Destination node broadcasts its public key (n,e) to Source node and keeps the private key secret. then source **S** wants to send message **M** to Destination **D**
It first converts **M** into an integer $0 < m < n$ by using an agreed-upon reversible protocol known as a padding scheme. It then computes the cipher text c corresponding to:

$$\boldsymbol{c = m^e mod\ n} \qquad \text{.....(1)}$$

This can be done rapidly using the method of exponentiation by squaring. Source **S** then transmits c to Destination **D**.

3.2.3 Decryption

Destination can decrypt $\boldsymbol{M}$ from c by using his private key exponent d by the following computation:

$$\boldsymbol{c^d \equiv m (mod\ n)} \qquad \text{.....(2)}$$

Given $\boldsymbol{M}$, Destination can recover the original message **M** by reversing the padding scheme.

Example of RSA Algorithm

Example of RSA with small numbers:
$p = 47$, $q = 71$, compute $n = pq = 3337$
Compute phi = 46 * 70 = 3220
Let e be 79, compute d = $79\text{-}1 \bmod 3220 = 1019$
Public key is n and e, private key d, discard p and q.
Encrypt message $m = 688$, $68879 \bmod 3337 = 1570 = c$.
Decrypt message c = 1570, $15701019 \bmod 3337 = 688 = m$.
Thus RSA is very practical algorithm in order to obtain the security aware AODV protocol as it uses both the public key as well as the private key.

4. Conclusion

In the proposed paper, we design a security to the protocol to provide reliable and efficient data transmission. Here we employ the Ad hoc On Demand Distance Vector protocol and provide the security by using Asymmetric cryptographic technique. The AODV network protocol set up at the time of broadcasting. To prevent the data from losses and misuses,we have implemented the security using Asymmetric technique. The encoding and decoding are used for the security in AODV protocol. The Asymmetric technique uses the RSA algorithm for the encryption and decryption of the data. Thus with the use of propagation methods of AODV the network is established and data packets are sent from the source to the destination nodes.

References

[1] Kartik Kumar Srivastava,Avinash Tripathi Anjnesh Kumar Tiwari,"Secure Data Transmission in MANET routing protocol" , Vol 3 (6), 1915-1921,Nov-Dec 2012.
[2] IEEE Computer Society, "IEEE 802.11 Standard, IEEE Standard for Information Technology", 1999.http://standards.ieee.org/catalog/olis/lanman.html.
[3] S Corson and J. Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. Internet Request for comment RFC 2501, Jan 1999.
[4] P. Papadimitratos ,Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks"in Proceedings of the *SCS Communication Networks and Distributed System*.
[5] Gustav J. Simmons. Symmetric and Assymetric encryption. ACM Computing surveys (CSUR). Volume 11, Issue 4 pp 305-330, Dec 1979.
[6] Bruce Schneir: Applied Cryptography. John Wiley and sons inc, 1996