Data Security Key Establishment in AODV

MONIS AKHLAQ[1], M NOMAN JAFRI[2], MUZAMMIL A KHAN[3], BABER ASLAM[4]
Information Security Department, College of Signals
National University of Science & Technology
Tamizuddin Road, Rawalpindi
PAKISTAN

Abstract: - The adhoc on demand distance vector (AODV) protocol enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an adhoc network. The use of AODV remains a concerned in the situations where security/ trust are the major requirements. The use of AODV is also restricted in the networks characterized by large processing, heavy data flow and uncontrolled overheads. The mechanism proposed in [1] addresses the issues related to overheads and processing in AODV but its use is restricted to network layer only. An endeavor has been made in this paper to propose a more versatile and secure AODV which can be used at network and upper layers.

Key-Words: - AODV, data security, MANET, secure routing, session key, trust relationship.

1 Introduction

A mobile adhoc network (MANET) is a collection of mobile nodes establishing communication in the absence of fixed infrastructure [2]. Adhoc networks may be different from each other depending on their area of application: For example in a classroom an adhoc network could be formed between students' PDAs and teachers' workstation. In an another scenario the group of soldiers using communication devices while operating inside enemy territory also forms an adhoc network. These two scenarios are different from each other as the former operates in a friendly environment therefore no special security requirements are needed whereas the later operates in an extreme hostile conditions thus demand fool proof security.

The adhoc networks are subject to versatile security threats as heavy reliance has been made on availability of trustworthy nodes and secure environment. However, the secure operation remains challenging as wireless communication is accessible to anyone operating within the communication range irrespective of friendliness or hostility.

The adhoc on demand distance vector (AODV) algorithm enables dynamic, self starting, multi hop routing between participating mobile nodes wishing to establish and maintain an adhoc network [3]. AODV is an example of reactive and stateless protocol [4] that establishes routes only as desired by a source node using route request (RREQ) and route reply (RREP) messages. AODV protocol is also susceptible to security threats and any malicious intrusion may compromise its overall performance. In relation to the security concerns of AODV, various schemes have been proposed [5], [6] etc. The analysis of these schemes identify that major stress has been laid on ensuring secure routing only whereas, security of data exchange has been left to other security protocols like IPSec etc [7].

The ultimate goal of any security solution for AODV should be to provide security services, such as authentication, confidentiality, integrity and non repudiation [8]. In order to achieve these goals, the security solution must give complete protection against the attacks designed for each layer. Table 1 identifies some security attacks [6].

Table 1: Security Attacks

Layer	**Attacks**
Application Layer	Repudiation, data corruption.
Transport Layer	Session hijacking.
Network Layer	Wormhole, location disclosure attacks.
Data Link Layer	Traffic analysis, monitoring.
Physical Layer	Jamming, interception, eavesdropping.
Multi- Layer Attacks	DoS, impersonation, replay, man in the middle attack.

The mechanism proposed in [1] ensures integration of routing and data security key establishment in a single phase. However, its use is restricted to the network layer only (since it provided only one key which could be used to protect a single session only). The proposed method will enhance the utility of [1] by making it usable for all upper layers. This work has introduced session key generation mechanism .which makes it more versatile. The enhancement makes the solution applicable to network and all upper layers and also makes it independent of number of concurrent protected sessions.

The paper has been organized into sections, section 2 deals with the characteristics of adhoc networks, section 3 deals with the analysis of current security techniques used in AODV. Section 4 describes the proposed method of Data Security Key Establishment (DSKE) and section 6 describes simulation of proposed method.

2 Characteristics of Adhoc Networks

The adhoc networks comprise of free to move mobile nodes. These nodes may be of same or variable type devices like laptops, PDAs, palmtops etc. These nodes operate in wireless modes thus inherit all the characteristics and limitations of wireless networks. The nodes in an adhoc network share a common bandwidth. The mobile nodes in adhoc networks also have dual tasks to perform (routing and own independent functions). These requirements have forced certain peculiarities on adhoc networks, they are:

- Adhoc networks are subject to bandwidth constrain, the bandwidth is shared for routing and data transfer (self and others).
- The dual function causes the networks to perform slower in comparison with traditional routers based networks.
- They have limited power (battery packs) and varied processing capability.
- High degree of security/ trust mechanism is required as the mobile nodes are free to join and leave the network without any laid down policy/ rule.

These peculiarities identify that any protocol / techniques designed for mobile adhoc networks must obey certain characteristics which include:

- Minimum overheads to be involved in order to address bandwidth limitation.
- Minimal processing to be involved (encryption/ decryption at source and destination only) to conserve processing and power requirements.
- Routing need not to be processing intensive as some times routing becomes secondary task and majority of node's processing power is unavailable for routing.
- Ensuring security requirements related to wireless communication, routing and exchange of data.

3 Analysis of Current Security Techniques

3.1 SAODV

The SAODV routing protocol proposed in [5] is used to protect the routing messages of the original AODV. SAODV uses digital signatures [8] to authenticate non-mutable fields and hash chains [8] to authenticate the hop-count field (only mutable field) in both RREQ and RREP messages.

The SAODV uses cryptographic extensions [8] to provide authenticity and integrity of routing messages and prevent the manipulation of the hop count information. However, exchange of key and other classified information for secure data exchange can be made only after identifying the route by using other protocols such as IPSec etc [5].

3.2 SAR

SAR is an extension framework to existing on demand ad hoc routing protocols [6]. The framework gives nodes different level of security by assigning them trust values. This means that when a packet is sent, it is assigned a trust value and certain security attributes, this is done by the user. The packet can only be routed through nodes with equal or greater trust value. If a node has lower security level it simply discards the packet. In case if there isn't a node in the network with the right level of security, then the packet can't be send, unless the packet's level of security is lowered.

SAR operates on the principle of sending classified data through trustworthy nodes and exchange of key has not been ensured for secure data exchange. The entire reliance on the availability of trustworthy nodes may jeopardize the overall efficiency of the network.

3.3 Conventional Security Protocols

SSL is the Internet security protocol for point to point connections [9]. It provides protection against eavesdropping, tampering, and forgery. Clients and servers are able to authenticate each other and establish a secure link or "pipe" across the internet or intranet that protects the transmitted information.

Transport Layer Security (TLS), the enhancement of SSL provides privacy for transmissions between two applications. TLS is partitioned into two layers, labeled the TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol provides encryption and message authentication for each message. The TLS Handshake Protocol operates on top of the TLS Record protocol. A TLS Handshake supplies authentication and key exchange operations for TLS protocol. The security state agreed upon in the handshake is then used by the TLS Record protocol to provide session security [7], [10].

The IPSec protocol [11] can be deployed in two basic modes: transport and tunnel. In tunnel mode, on which we focus here, cryptographic protection is provided for entire IP datagram. In essence, a whole datagram plus security fields are treated as the new payload of an outer IP datagram, with its own header, called the outer header. The original, or inner, IP datagram is said to be encapsulated within the outer IP datagram. In tunnel mode, IPSec processing is typically performed at security gateways on behalf of endpoint hosts. The gateways could be perimeter firewalls or routers. IPSec provides authentication and integrity protection and/or confidentiality services for network layer data through the AH and ESP protocols [12].

The operation of these conventional security protocols demands the establishment of communication path between source and destination before their application. Authors of AODV have also identified the phenomena used in IPSec for security implementation [3] however, following are few observations in relation to the use of IPSec with AODV and other Secure AODVs.

- Increased overheads due to AODV based routing and subsequently applying SSL/ IPSec technique for data protection.
- Bandwidth constrain on account of two separate mechanisms (routing and secure data exchange).
- Increased complexity and processing time as Secure AODV routing techniques have their inbuilt cryptographic parameters/ mechanisms. Any subsequent implementation of conventional security protocols for data security may duplicate the desired authentication and integrity checks

4 Data Security Key Establishment (DSKE)

4.1 Assumptions.

It is assumed that trust relationship exists only between source and destination nodes. Intermediate nodes participating in routing are out of trust relationship bondage.

4.2 Basic Idea

- Integrating routing and exchange of Master Key in the routing phase.
- Use of certificates [8] by source and destination for mutual authentication.
- Master Key request from source, Master key generation from destination.
- Use of asymmetric cryptography [8] for the exchange of Master Key.
- Use of Symmetric Cryptography (AES) [13] for data encryption by using session key derived from exchanged Master Key.
- Necessary modifications in message types (RREQ, RREP) defined by AODV.

4.3 Implementation Technique

Symbols used are source (S), destination (D), Master Key (K_M), encrypted Master Key (K_E). K_{AX} public key of x, K_{BX} private key of x, where x is either source or destination. E_K encryption using key session key K_S, D_K decryption using session key K_S.

Source generates a Route Request (RREQ), attaches its certificate alongwith a request for Master Key and sends it to the destination. It is assumed that a trust relationship exists only between the source and destination nodes. The intermediate nodes rebroadcast the route request in accordance with operation of AODV protocol. On receipt of the Route Request (RREQ), destination confirms the authenticity of source by its certificate and generates a Master Key. The destination encrypts the Master Key using its private key and further encrypt it with the public key of source.

$K_{E1} = E_{K_{BD}} (K_M)$…….(1)

$K_E = E_{K_{AS}} (K_{E1})$……..……(2)

The encrypted Master Key and certificate of destination node are returned with RREP to the source. The source confirms the authenticity of destination by its certificate, decrypts the encrypted Master Key by its private key first and then by the public key of destination to obtain the Master Key.

$K_{E1} = D_{K_{BS}} (K_E)$……...(3)

$K_M = D_{K_{AD}} (K_{E1})$…….....(4)

The Master Key thus obtained will be used for generating session keys as required. Fig 1 also explains the same procedure.

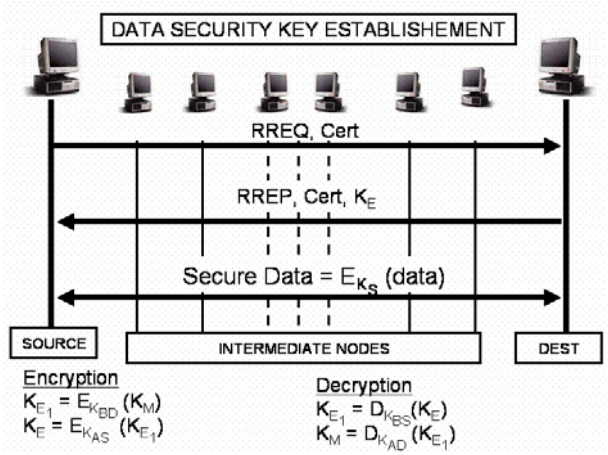

Fig 1: Data Security Key Establishment

Similar technique can also be used in scenarios where low grade security is required. This may be achieved by replacing double encryption with the single encryption .

The Master Key can be used for encryption at network layer. However, in situations where encryption is to be done at application layer and at each application, then this key will be used for generating session keys [6] for each application.

4.4 Generation of Session Key

The basic idea is to use Pseudo Random Function (PRF) already defined in [14] for generation of session keys from Master Key. The details are as follows:

S_{Kx} = {PRF(X) (K_M, "Data Security Key Establishment", SA, DA)}

Where:

K_M: Master Key

S_{Kx}: K1 || K2 || K3|| K4 || ------||Kn (Concatenation of required keys)

SA: Source Address

DA: Destination Address

$$X = \sum_{i=1}^{n} K_{Li}$$

Where K_{Li} - Length of key i,

n – total number of session keys required

4.5 Analysis

- The technique uses mutual authentication in which both sender and receiver authenticate each other with respective certificates. In addition mutual authentication is further enhanced by double encryption and decryption at destination and source respectively.
- Data Security Key Management uses asymmetric cryptography for exchange of Master Key and symmetric cryptography for data encryption.
- The mechanism ensures the confidentiality of data exchange once route to destination has been established thus total reliance has been made on route discovery which has been protected by the use of mutual authentication. Finding a route means secure exchange of data.
- Malicious intrusions such as forged route reply, wrong routing information and interception are countered by the proposed technique. Forged reply is detected/ protected by the process of mutual authentication, false routing information and interception becomes meaningless when data is encrypted.
- The single phase operation of routing and key exchange ensures limited overheads, low processing complexity and low bandwidth usage thus improving the efficiency.
- The reliance of trust relationship between source and destination seems not exaggerated as nodes intending exchange of classified information must have some mutually agreed parameters.
- The privilege of Gratuitous RREPs are not applicable in Data Security Key Establishment. It can only be used if session key is not requested by the sender node.

5 Simulation

NS2 [15] has been selected for simulation of proposed technique as [3] has already been implemented in it.

5.1 Modifications

The technique involves integration of routing and data security key exchange. This demands modifications of RREQ and RREP messages to include additional fields along with necessary changes in the protocol to modify handling of these messages at source and destination nodes. In addition the privilege of gratuitous reply needs to be deactivated because the Key can only be generated by destination.

5.1.1 Source Node

Following modifications have been made in handling of messages at source node.

- **RREQ Message**

Generate RREQ with request for Master Key alongwith its certificate and sends it for the route discovery of destination.

- **RREP Message**

Verify the certificate of destination, decrypt the encrypted Master Key by using public Key of destination and own private Key (Equation 3, 4).

5.1.2 Destination Node

Following modifications have been made in handling of messages at destination node.

- **RREQ Message**

Verify the certificate of source.

- **RREP Message**

Generate Master Key, encrypt Master Key with public Key of destination and own private key (Equation 1, 2). Send RREP alongwith its certificate and encrypted Master Key to the source.

5.1.3 Intermediate Nodes

The intermediate nodes rebroadcast the RREQ and RREP messages in accordance with AODV protocol. The privilege of gratuitous reply has been de activated.

5.2 Scenario

The studied scenario consists of 16 mobile nodes exchanging TCP traffic. The topology was a rectangular area with 1600 m length and 1300 m width. A rectangular area was chosen in order to force the use of longer routes between nodes. Nodes were distributed randomly within the mobile ad hoc network.. The scenario has also shown in Fig 6.

5.3 Simulation Conducted

A node was selected as the source node and all remaining nodes were used one by one as the destination node. The procedure was repeated for all nodes as a source node in different time periods. TCP source was attached with the source node and sink was attached with the destination node. The simulation results identified the successful integration of routing and exchange of data security key exchange which includes:

- Generation of Master Key by destination.
- Encryption of Master Key by destination.
- Broadcast of RREQ and Transmission of encrypted Master Key by intermediate nodes to the source.
- Decryption of Master Key by source.
- Exchange of encrypted data by using exchanged Master Key.

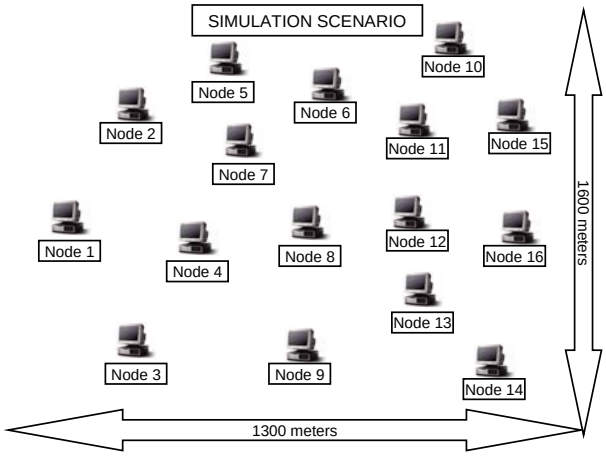

Fig 6: Simulation scenario of 16 mobile nodes in ad hoc mode.

6 Conclusion

AODV does not specify any special security measures. Various efforts have been made to counter security challenges affiliated with the protocol. The current trends of providing security cover to AODV adopted networks ensure secure routing and secure data in separate phases. The suggested mechanism has integrated routing and exchange of Master Key in a single phase. It will improve the credibility of AODV and enhance its security

References:

[1] Monis Akhlaq, M Noman Jafri, Muzammil A Khan, Baber Aslam, Addressing Security Concerns of Data Exchange in AODV. *Transactions on Engineering, Computing and Technology*, Volume 16 November 2006 ISSN 1305-5313, pp. 29-33.

[2] 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.

[3] C.E. Perkins, E. Belding Royer, and S.R. Das, Ad hoc On demand distance vector (AODV) Routing, *IETF RFC 3561,* July 2003.

[4] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu, Routing Security in Ad hoc Wireless Networks, *Department of Computer Science and*

Engg, Florida Atlantic University, Boca Raton, FL 33431.

[5] M. G. Zapata, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, *INERNET DRAFT,draft-guerrero-manet-saodv-00.t*xt, Aug. 2001.

[6] Seung Yi, Prasad Naldrug, Robin Kravets, A Security Aware Routing Protocol for Wireless Ad hoc Networks, *In the proceedings of 3rd ACM international of mobile ad hoc networking and computing* pp 226-236, 2002.

[7] Alec Yasinac, Justin Childs: Analysing Internet Security Protocols, i*n the proceedings on High Assurance System Engineering, 2001*. Sixth IEEE International -.Symposium, ISBN – 0-7615-12.

[8] Bruce Schneir: *Applied Cryptography*. John Wiley and Sons inc, 1996.

[9] *Introduction to Secure Socket Layer*, Cisco System Inc. (http://www.cisco.com).

[10] T. Dierks and C. Allen., The TLS protocol version 1.0, *RFC 2246*, Jan 1999.

[11] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, *Internet Request for Comment RFC 2401*, Internet Engineering Task Force, Nov.1998.

[12] C. R. Davis. *IPSec: Securing VPNs*. McGraw-Hill, New York, 2000.

[13] *Advanced Encryption Standard (AES) (FIPS PUB 197).* National Institute of Standards and Technology (NIST)". Nov 2001.

[14] IEEE P802.11i – 2004. IEEE standard for information Technology – Telecommunication and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[15] The Network Simulator. ns-2. http:// nsnam.isi.edu/nsnam/ns.