International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:4, 2008

Addressing Security Concerns of Data Exchange in AODV Protocol

Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam

***Abstract*—**The Ad Hoc on demand distance vector (AODV) routing protocol is designed for mobile ad hoc networks (MANETs). AODV offers quick adaptation to dynamic link conditions; it is characterized by low memory overhead and low network utilization. The security issues related to the protocol remain challenging for the wireless network designers. Numerous schemes have been proposed for establishing secure communication between end users, these schemes identify that the secure operation of AODV is a bi tier task (routing and secure exchange of information at separate levels). Our endeavor in this paper would focus on achieving the routing and secure data exchange in a single step. This will facilitate the user nodes to perform routing, mutual authentications, generation and secure exchange of session key in one step thus ensuring confidentiality, integrity and authentication of data exchange in a more suitable way.

***Keywords*—**AODV, key management, security, wireless networks.

I. Introduction

IEEE 802.11 is a widely used wireless network standard [1]. Users in the wireless networks are either connected in an infrastructure or ad hoc mode. Ad hoc wireless networks of mobile nodes MANETs [2] are dynamic in nature. MANETs are characterized by bandwidth constrains, low physical security and power limitations. These networks comprise of a dynamic set of cooperating peers, which share their wireless capabilities with other similar devices to enable communication with devices not in direct radio - range of each other [3]. Due to their versatile characteristics, ad hoc networks operate on special routing protocols. There are two major classes of routing protocols associated with ad hoc networks, proactive routing protocol and reactive routing protocol [4]. Proactive protocol focus on maintaining consistent overview of the network, each node is responsible for broadcasting topology information at regular interval of time (eg DSDV) [5].

Reactive protocols are on demand protocols that discover the route once needed (eg AODV [6]). The reactive protocols display considerable bandwidth and overhead advantages over proactive protocols. AODV routing protocol offers quick adaptation to dynamic link conditions, low processing, low memory overheads, and low network utilization [6]. AODV protocol is susceptible to security threats and any malicious intention may compromise its overall performance.

The ultimate goal of the security solutions for AODV protocol is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users. In order to achieve these goals, the security solution should provide complete protection spanning the entire protocol stack. Table I identifies the security issues in each layer [7]. In this article we would concentrate in addressing security concerns related to data exchange. A modified protocol will be proposed that accumulate the routing, authentication, generation and secure exchange of session key in a single step. This would facilitate the users to establish parameters during the routing session and these parameters would subsequently be used to ensure confidentiality and integrity of data exchange.

TABLE I
Security Issues Related to Each Layer in Protocol Stack

Layer	Security Issues
Application Layer	Prevention, detection of viruses, worms, malicious codes, application abuses
Transport Layer	Authentication and end to end data security through encryption techniques
Network Layer	Security of ad hoc routing protocols and associated parameters.
Physical layer	Preventing signal jamming, denial of service attacks and other active attacks.

The paper has been organized in sections. Section 2 deals with attacks against AODV, Section 3 & 4 discuss security attributes and security mechanisms associated with data exchange. Section 5 comprises of current security techniques associated with AODV and a brief discussion on conventional security protocols. Finally in Section 6 we have proposed a protocol that will address the title issue of this paper.

Manuscript received September 1, 2006. This work was presented to the College of Signals, National University of Sciences and Technology, Rawalpindi, Pakistan as thesis work for completing MS in Information Security.

Monis Akhlaq is with College of Signals, National University of Science and Technology, Rawalpindi, Pakistan (phone: 92-321-5263923, e-mail: monisakhlaq@yahoo.com).

M N Jafri is Prof of Electrical Engineering with College of Signals, National University of Science and Technology, Rawalpindi, Pakistan (phone: 92-51-9272473, e-mail: mnjafri@mcs.edu.pk).

Muzammil A Khan is with College of Signals, National University of Science and Technology, Rawalpindi, Pakistan (Tel No. 92-321-5186897, email: muzammilahmedkhan@gmail.com).

Babar Aslam is with College of Signals, National University of Science and Technology, Rawalpindi, Pakistan (Tel No. 92-321-5818580, email: ababer@gmail.com).

II. Attacks Against AODV

AODV implemented networks are subjected to two main kinds of attacks, passive attacks and active attacks. The passive attacks only intercept the message transmitted in the network without disturbing the transmission. By doing this, the attacker will be able to analyze the valuable information like network topology etc. Eavesdropping and subsequent analysis of the intercepted data may also jeopardize the entire network security. These kinds of attacks in ad hoc networks are difficult to detect. The other type of attacks, active attacks are carried out by malicious nodes with aim to disrupt transmission among other nodes [8]. Our efforts here would focus on passive attacks only and would propose a solution that may contribute in security of data exchange.

To adopt a systematic way to counter the passive attacks against AODV, a better understanding of security attributes and security mechanisms are required.

III. Security Attributes

Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation [4], [9],[19].

A. Confidentiality

It is to keep the information sent unreadable to unauthorized users or nodes. MANETs uses an open medium, so usually all nodes within the direct transmission range can obtain the data.

B. Authentication

It enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

C. Integrity

It ensures to keep the message sent from being illegally altered or destroyed in the transmission. When the data is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The malicious attackers can also resend it, which is called a replay attack.

D. Non Repudiation

It is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it.

(Our discussion in this paper would be restricted to ensure first three attributes only).

IV. Security Mechanisms

A variety of security mechanisms are being used to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of defense. The first line of defense would be considered as the defense against the passive attacks. As a second line of defense, we have intrusion detection systems and cooperation enforcement mechanisms implemented in MANETs. These help to defend against active attacks and enforce cooperation i.e, reducing selfish node behavior.

- *Preventive Mechanism*

The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography [10]. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in transmission [11]. Threshold cryptography can be used to hide data by dividing it into a number of shares [11]. Digital signatures can be used to achieve data integrity and authentication services [11]. It is also necessary to consider the physical safety of mobile devices, since the hosts are normally small devices, which are physically vulnerable. For example, a device could easily be stolen, lost, or damaged. In the battlefield they are at risk of being captured. The protection of the sensitive data on a physical device can be enforced by some security modules, such as tokens or a smart card that is accessible through PIN, pass phrases, or biometrics. Although in theory, these cryptographic primitives combined can prevent most attacks but in reality, due to the design, implementation selection of protocols and physical device restrictions, there are still a number of malicious attacks bypassing prevention mechanisms. Our effort in this paper would be related to the design the parameters that would efficiently ensure the security of data exchange.

V. Current Security Techniques used in AODV

A. SAODV

The Secure Ad hoc On-Demand Distance Vector (SAODV) [12] addresses the problem of securing a MANET network. SAODV is an extension of the AODV [6] routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation. SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. Achieving this is the job of the key management scheme. Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). This is because for the non-mutable information, authentication can be performed in a point-to-point manner, but the same kind of techniques cannot be applied to the mutable information. Route error messages are protected in a different manner because they have a big amount of mutable information. In addition, it is not relevant which node started the route error and which nodes are just forwarding it. The only relevant information is that a neighbor node is informing to another node that it is not going to be able to route messages to certain destinations anymore. Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole message and that any neighbor that receives verifies the signature [12].

SAODV implementation ensures the security of routing messages only whereas; the similar requirement of data exchange remains unaddressed.

B. SAR (Security Aware Ad Hoc Routing)

SAR [13] embeds security metric into the RREQ packet itself, and change the forwarding behavior of the protocol with respect to RREQs. Intermediate nodes receive an RREQ packet with a particular security metric or trust level. SAR ensures that this node can only process the packet or forward it if the node itself can provide the required security or has the required authorization or trust level. If the node cannot provide the required security, the RREQ is dropped. If an end to end path with the required security attributes can be found, a suitably modified RREP is sent from an intermediate node or the eventual destination. The operation of SAR addresses the security of both routing and data exchange. However, the concept of trust level hierarchy and secure routing metrics may affect the overall efficiency of the network in which the entire reliance would be focused on the availability of trust worthy node. Our designed work would be considered more efficient than SAR as no reliance is needed on trustworthiness of the participating nodes.

C. Conventional Security Protocols

1) SSL/TLS

Secure Socket Layer (SSL) and Transport Layer Security (TLS) were designed for secure communications and are based on public key cryptography [14]. TLS/SSL can help secure data transmission. It can also help to protect against masquerade attacks, man-in-the-middle (or bucket brigade) attacks, rollback attacks, and replay attacks. These protocols used cryptographic techniques [11] which are considered as CPU-intensive and requires comprehensive administrative configuration [15]. Therefore, the application of these schemes in MANETs using AODV is restricted. TLS/SSL has to be modified in order to address the special needs of MANETs.

2) Interaction with IPSec

The fundamental differences between ad hoc networks and standard IP networks [16] necessitate the development of new security services. In particular, the measures proposed for IPSec [17] help only in end-to-end authentication and security between two network entities that already have routing between them; IPSec does not secure the routing protocol.

The conventional security protocol function is independent of routing protocol and thus they need their own setup for provision of data security; whereas our proposed protocol performs routing and data security setup in one phase.

VI. Proposed CAODV

AODV protocol would be the basis of our proposed work. Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs) are the message types defined by AODV [6]. Our proposed protocol Classified AODV (CAODV) would be implemented at network layer. The designed protocol encompasses the routing mechanism and exchange of security parameters in a single step. This would be considered as major change from the current security techniques used in AODV and conventional security protocols affiliated with the network and transport layer. In general the overall concept of operation would base on the utility of digital certificates issued by trusted CA (Certification Authority). It is assumed that a trust relationship exists between CA and all participating nodes.

A. Basic Idea

Our proposed work encompasses following idea.

1) The concept of asymmetric cryptography (public key and private key cryptography) will be used for exchange of session key [11].

2) Certificates will be used to bind asymmetric keys (public and private keys) to the nodes.

3) Certificates of sender and receiver are attached with RREQ and RREP messages.

4) Asymmetric cryptography is resource intensive and could be considered as unsuitable choice for MANETs. Our proposal limits the use of said technique for exchange of session key only.

5) We propose use of symmetric cryptographic techniques [11] such as Advanced Encryption Standard (AES) [18] for data encryption.

6) Certificates can be issued to all participating nodes in relation to their MAC address or IP address, personal credentials or on any agreed pattern. The mechanism of issuing certificates by CA is considered out of the scope of this paper. It is also assumed that procedure for verification of certificates is known by all participating nodes.

There are two options available in our proposed protocol with varying advantages and disadvantages.

Following symbols will be used in the proposed options, source (S), destination (D), session key (K_S), encrypted session 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 K, D_K decryption using key K.

B. Option 1

A source generates RREQ, attaches its certificate and sends it for route discovery of destination. In addition source also requests for a session key from the destination node. The intermediate nodes rebroadcast the RREQ packet in accordance with the operation of AODV protocol [6]. On receipt of RREQ, the destination node verifies the certificate of source and on confirmation generates a session key. The destination also encrypt the session key with the public key of the source ($K_E = E_{KAS} (K_S)$). The destination finally sends RREP including encrypted session key to the source. On receipt source decrypts the encrypted session key by its private key and obtain the session key ($K_S = D_{KBS} (K_E)$). The obtained session key will finally be used for secure data exchange (Fig. 1).

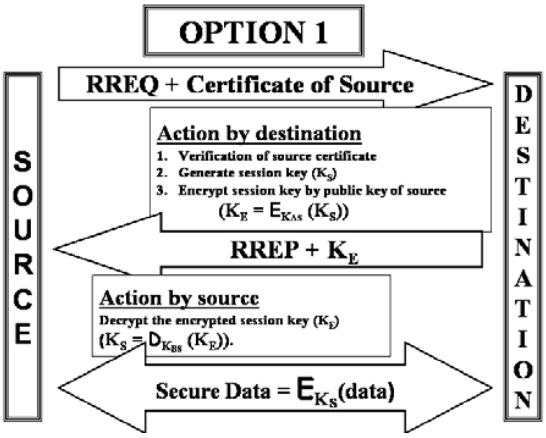

Fig. 1 Routing, generation of session key and encryption of session key in Option 1

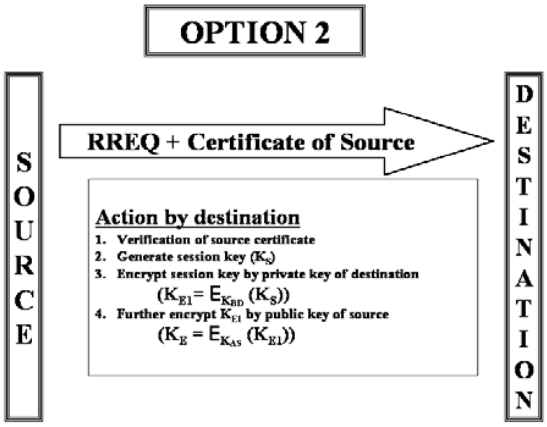

Fig. 2 Generation of RREQ, session key and encryption of session key

C. Option 2

Source generates RREQ, attaches its certificate and sends it for route discovery of destination. Source also attaches a request for a session key from the destination node. The intermediate nodes rebroadcast the RREQ packet in accordance with the operation of AODV protocol [6]. On receipt of RREQ, the destination node verifies the certificate of source and on confirmation generates a session key. Destination encrypts the session key with its private key as ($K_{E1} = E_{KBD}(K_S)$) and further encrypts K_{E1} with the public key of the source as ($K_E = E_{KAS}(K_{E1})$). Destination respond with RREP attach its certificate and encrypted session key K_E. On receipt, source confirms the authenticity of destination from its certificate, decrypts the session key first through its private key and then through public key of destination as ($K_{E1} = D_{KBS}(K_E)$) and ($K_S = D_{KAD}(K_{E1})$) respectively. Finally session key is obtained that will subsequently be used for secure data exchange (Fig 2 & 3).

D. Comparison of Proposed Options

The analysis of both options identify that option 1 has a limitation. That is, if any intermediate node sends a forged reply, the sender would not be able to distinguish it and would be easily deceived. This is due to lack of mutual authentication.

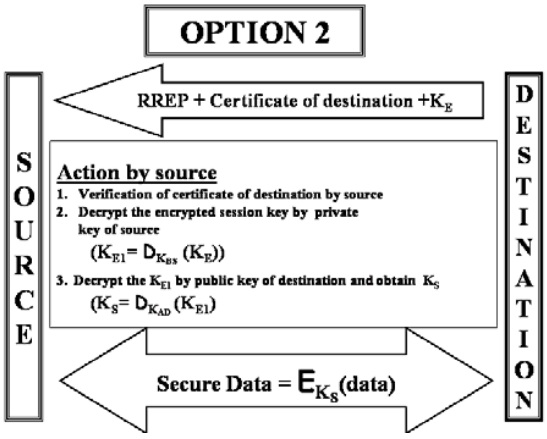

Fig. 3 RREP, decryption of session key and exchange of secure data in Option 2

Fig. 4 also identifies the same problem associated with option 1. However, the option 1 has inbuilt advantages of low computation and less memory requirements. The option 2 has uses mutual authentication in which both sender and receiver authenticate each other with respective certificates and the recipient also encrypts the generated session key with its private key (ensuring its authentication for the sender) and further encrypts the session key with the public key of the sender thus confirming the authentication of the sender.

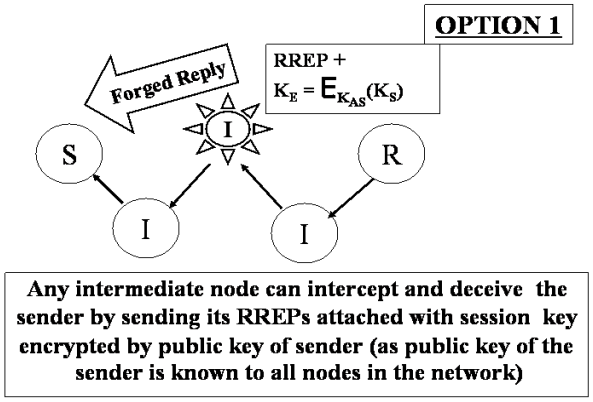

Fig. 4 Forged RREP from an intermediate node

The session key is bound to the sender – receiver pair due to double encryption and cannot be used by any other source for same destination. Thus, there is no requirement of storing the session key in routing tables of intermediate nodes. If data encryption is not needed then sender will initiate normal RREQ without its certificate and request for session key.

The concept of gratuitous RREPs in AODV facilitates the routing process by allowing intermediate nodes to respond to RREQ of the messages if the route to the required destination is known. The privilege of gratuitous RREPs is not applicable in our proposed design It can only be used if session key is not requested by the sender node. Relevant modifications in messages types defined by AODV [6] would also be necessary in the proposed work.

VII. Simulation Result

The proposed modifications in existing AODV protocol have been successfully implemented in NS2 Simulator. The added parameters in the RREQ message include:

- Request for session key/ session key status.
- Certificate of sender.
- Public key of sender.

On receipt of RREQ, the destination responds with RREP having additional parameters include:

- Request for session key/ session key status.
- Certificate of destination.
- Public key of destination.
- Session key

The session key received by the source will be passed to the application layer and the same will be used in AES [18] or any symmetric encryption technique. Thus routing and exchange of session key have been ensured in a single step

VIII. Conclusion

AODV does not specify any special security measures. The proposed protocol, CAODV would be considered as an endeavor to enhance the security requirements of AODV operated MANETs. In the proposed protocol authentication is achieved by double encryption of session key using asymmetric cryptography (using public and private keys of source and destination respectively). Data confidentiality and integrity can be achieved by data encryption using strong symmetric key algorithm such as AES.

Thus the proposed protocol which is implemented in a single step will inherent added advantages over other security conscious protocols designed for AODV.

References

[1] IEEE Computer Society, "IEEE 802.11 Standard, IEEE Standard for Information Technology", 1999. http://standards.ieee.org/catalog/olis/lanman.html.
[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] Michael Jarrett, Paul Ward, "Trusted Computing for Protecting Ad-hoc Routing," cnsr, pp. 61-68, 4th Annual Communication Networks and Services Research Conference (CNSR'06), 2006.
[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] C. Perkins and P Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing DSDV for mobile computers". In ACM SIGCOMM'94 Conference on Communication Architectures, protocols and applications, 1994, pp. 234-244.
[6] C.E. Perkins, E. Belding Royer, and S.R. Das, "Ad hoc On demand distance vector (AODV) routing", IETF RFC 3561, July 2003.
[7] Hao Yang, Haiyun Loo, Fan Ye, Sogwu Lu and Lixia Zhog: Security in mobile ad hoc networks, challenges solution, Wireless Communication, IEEE Volume I, issue I publication date Feb 2004.
[8] Bingwen He, Joakin Hagglund, QingGu: Security in Ad hoc Network. http://www.cse.fau.edu/~jie/research/publications/Publication_files/SecureRouting.pdf
[9] T Friiso, T Brekne, P Haaland, M Radziwill. Security challenges in self organizing wireless networks. Telenor No ISBN 82-423-0581-1, ISSN 1500-2616, project No TFPFAN programme peer to peer computing security Gr, Dec 2003.09.08.
[10] Gustav J. Simmons. Symmetric and Assymetric encryption. ACM Computing surveys (CSUR). Volume 11, Issue 4 pp 305-330, Dec 1979.
[11] Bruce Schneir: Applied Cryptography. John Wiley and sons inc, 1996.
[12] M. G. Zapata, `Secure Ad hoc On-Demand Distance Vector (SAODV) Routing', INERNET DRAFT, draft-guerrero-manet-saodv-00.txt, Aug. 2001.
[13] 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.
[14] T. Dierks and C. Allen. The TLS protocol version 1.0 , RFC 2246, Jan 1999.
[15] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei: A survey of attacks and counter measures in mobile ad hoc networks, Department of Computer Science and Engg, Florida, Atlanta university. http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf
[16] S. Kent and R. Atkinson. Security architecture for the Internet Protocol. Internet Request for comment RFC 2401, Internet Engineering Task Force, Nov.1998.
[17] C. R. Davis. IPSec: Securing VPNs. McGraw-Hill, New York, 2000.
[18] "Advanced Encryption Standard (AES) (FIPS PUB 197). "National Institute of Standards and Technology (NIST)". Nov 2001.
[19] Project No: IST-507102, Project full title: My Personal Adaptive Global NET (MAGNET).http://www.istmagnet.org/GetAsset.action?contentId=942902&assetId=943011