ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Security Enhancements of AODV Protocol: A Comparative Study

A.Ranichitra, V.Lakshmi Praba

Dept of MCA, Sri S.R.N.M.College, Sattur, India

Rani Anna Govt College for Women, Tirunelveli, India

ABSTRACT: Ad hoc networks are a new-fangled wireless networking paradigm for mobile nodes. Unlike traditional wireless networks, ad-hoc networks do not rely on any fixed infrastructure. Instead, the mobile nodes rely on each other to share the information. The main dispute in designing these networks is their susceptibility to security attacks. The increase in number of applications of ad-hoc networks depends on a large number of factors, with reliability being one of the key challenges to be met. Ad-hoc On-Demand Distance Vector (AODV) is one of the extensively used protocols which do not satisfy the various security requirements like availability, confidentiality and integrity. This paper discusses the various security requirements for the ad-hoc networks and the various security enhancements of AODV protocol.

KEYWORDS: MANET, ad-hoc, security, security services, AODV, Digital Signatures, hash chains

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a wireless network which is an autonomous collection of wireless mobile nodes that are self configured to form a network environment without any infrastructure establishment (Figure 1). Ad-hoc network can form a spontaneous network at will momentarily. The information transmitted by a mobile node will be received by all the other nodes within its transmission range due to its wireless connectivity and Omni-directional antennae based on predefined protocol. Thus each node in the network can act both as a host and as a router. Due to the limited transmission capability of the network, the nodes cannot directly communicate with those which are not one hop neighbours. This weakness is overcome through multi hop communication. They transmit the packets to other nodes across the network without any access points and any infrastructure establishment.

The mobile nodes in MANET are generally closed in communication and not connected to the Internet. But, if one of the mobile nodes has a connection to a public or private network, this connection can be shared among other members of the ad-hoc network. This will allow other mobile nodes in the ad-hoc network to connect to the Internet as well. The network topology of MANET may often change rapidly and it is not predictable. The decision making with respect to route, is autonomous by the nodes themselves.

Characteristics of Mobile ad-hoc networks

Like other network, MANET possess the following characteristics

- No need for elaborate physical back bone connectivity for network establishment.
- Dynamic topology enabling demand based capacity addition or removal.
- Self-Organizing and Self Healing.
- Network Scalability.
- Chances of frequent Link Failure.
- Multi-hop Communication.
- Highly Scalable as individual networks or network of networks.

10.15680/ijircce.2014.0212020

Figure 1.1: Mobile Ad-hoc Network

The traditional routing protocols may lead to untrusted environment due to misbehaving nodes in the network environment. Therefore, the use of routing protocols with security features is essential to ensure data reliability for the end users. However, many technological challenges are to be overcome in designing and securing wireless ad-hoc networks. The paper presented here considers the existing reactive routing protocol AODV (Ad-hoc On Demand Vector). This protocol has been enhanced with added security feature using various cryptographic techniques. Hence, the security enhancement of AODV has been studied and compared in this paper.

This paper is organized as follows; Section II describes the literature survey, Section III describes the security services. Section IV describes security in ad-hoc networks. In Section V the various security enhancement of AODV is studied and compared. Section VI presents the conclusion.

II. LIREATURE SURVEY

Unlike the wired networks, the Ad-hoc Network poses some unique characteristics and includes a number of nontrivial disputes in designing architecture. MANET includes issue such as multicast routing, clustering, mobility pattern management, QoS and Security. At present, Routing, QoS and Security are the hot topics of Research. This paper focuses only on the security aspects of the networks. It is vital to protect the network from different kinds of security threats. This is primarily due to the high dynamic nature of the ad-hoc network and due to the need to operate efficiently with limited resources. The overall goal of the security solutions for ad-hoc networks is to provide security services to the users.

A number of routing protocols with security features have been developed which employ a variety of cryptographic tools for protecting the vulnerabilities in different routing protocols. However, these protocols have been developed to specific problems that arose due to the attacks on routing protocols. One of the most important protuberant communication protocols in Ad-hoc Network is AODV protocol. However this protocol still has many weaknesses, which attracted many researchers to develop new protocols based on the existing traditional protocol AODV. In this paper, [7 - 16] shows the enhancement of AODV with added security features.

III. SECURITY SERVICES

Potential security services should include a way of assuring that the packet/data was generated by a trusted source as well as a way of assuring that the packet/data was not tampered with or altered after it was generated. The ad-hoc networks should satisfy the following requirements [1, 2, and 3] to establish secure communication between mobile nodes:

1. Authentication - Assures that the communicating entity is the one that claims to be.
2. Access Control - Prevention of unauthorised use of resources.
3. Data Confidentiality - Protection of data from unauthorized disclosure.
4. Data Integrity - Assures that the data received are exactly as they were sent by the sender.
5. Non-Repudiation - Provides protection against denial by any one of the communicating entities.
6. Privacy - Users of networks may be monitored or tracked. Hence, the privacy of drivers or vehicles against unauthorized users should be protected.
7. Revocation: Tracing and disabling malicious On Board Units or Road Side Units by the trusted authority.

IV. SECURITY IN AD-HOC NETWORKS

Unlike the wired networks, the Ad-hoc Network poses some unique characteristics and includes a number of nontrivial disputes in designing architecture. MANET includes issue such as multicast routing, clustering, mobility pattern management, QoS and Security. At present, Routing, QoS and Security are the hot topics of Research. This study focuses only on the security aspects of the networks. It is vital to protect the network from different kinds of security threats. This is primarily due to the high dynamic nature of the ad-hoc network and due to the need to operate efficiently with limited resources. The overall goal of the security solutions for ad-hoc networks is to provide security services to the users.

The characteristics of MANETs make them susceptible to many new attacks. To protect an ad-hoc network from various assaults the routing protocol should guarantee that the revealed path between the source to destination functions correctly even in the presence of misbehaving nodes so that

1. Only authorised nodes will be able perform route discovery and route maintenance.
2. Detection of Fabricated / Modified / Spoofed messages.
3. Identification and elimination of loop formation in routing the control messages.
4. Revocation of malicious nodes from the network.

A number of routing protocols with security features have been developed which employ a variety of cryptographic tools for protecting the vulnerabilities in different routing protocols. However, these protocols have been developed to specific problems that arose due to the attacks on routing protocols. One of the most important protuberant communication protocols in Ad-hoc Network is AODV protocol [4, 5, 6]. However this protocol still has many weaknesses, which attracted many researchers to develop new protocols based on the existing traditional protocol AODV.

V. SECURITY ENHANCEMENT IN AODV

Securing the AODV protocol can be achieved using the various Security Mechanisms like digital signature, trust mechanisms, hash chains, etc. or by creating an additional table to store the malicious nodes or by creating an additional module to detect the misbehaving nodes. Some of them are discussed below.

a. Digital Signature and Hash chains

Zapata et al in 2002, [7] used Digital Signature and hash chains as the security measures to authenticate the control messages in the secured version of AODV called Secure AODV (SAODV) which provides integrity, authentication and non-repudiation of routing information. Two mechanisms are used to secure the AODV messages, digital signatures to authenticate the non-mutable fields of the RREQ and RREP messages so that they sign every message, and hash chains to secure the hop count information of RREQ and RREP messages in such a way that allows every node that receives the message to verify that the hop count has not been decremented by an attacker. SAODV

10.15680/ijircce.2014.0212020

does not require additional messages with respect to AODV. Nevertheless, SAODV messages are significantly bigger mostly because of digital signatures. Moreover, SAODV requires heavyweight asymmetric cryptographic operations: every time a node generates a routing message, it must generate a signature, and every time it receives a routing message (also as an intermediate node), it must verify a signature. This gets worse when the double signature mechanism is used because this may require the generation or verification of two signatures for a single message. In the SAODV operations, SAODV allows to authenticate the AODV routing data.

Wadbude et al [8] proposed an efficient secure AODV routing protocol which uses improved security mechanisms that satisfy the main security requirement and guarantees the discovery of a correct and secure path. This protocol uses Hash Chain, Digital Signature and Protocol Enforcement Mechanism. Hash chains are used to authenticate the hop count of the routing messages. All the messages are appended by the digital signature, and the receiving node verifies the signature and stores the route with signature, life time and the originator IP address of the RREP. This proposed method shows better performance in route discovering with acceptable delays with increase in number of nodes.

b. Trust Mechanism

Cerri et al [9] proposed an Adaptive mechanism over SAODV called A-SAODV which optimizes the routing performance of secured protocols with the help of a threshold mechanism. ASAODV is a multithreaded application. This protocol performs the cryptographic operations by a dedicated thread to avoid blocking the processing of other messages and other threads to all other functions. Every node has a queue of routing messages to be signed or verified and the length of the queue implies the load state of the routing thread. Whenever a node processes a route request and has enough information to generate a RREP on behalf of destination, it first checks its routing message queue length. If the length of the queue is below a threshold, then it replies, otherwise, it forwards the RREQ without replying. The value of threshold can be changed during execution. The A-SAODV also maintains a cache of latest signed and verified messages in order to avoid signing and verifying the same message twice. This adaptive reply decision has a significant improvement on the performance of SAODV and as A-SAODV prototype caches the latest signed and verified messages, which avoids signing or verifying the same message twice.

Mishra et al [10] proposed an extension to adaptive SAODV which includes further filtering to improve the performance of the protocol. This protocol optimizes the routing performance of secured protocols by choosing a small value as TTL-threshold field. The intermediate nodes are allowed to reply a route request only if the TTL field of RREQ packet is larger than the TTL-threshold value; otherwise the request packet is simply forwarded to all neighbouring nodes that either the destination is within TTL-threshold hop neighbourhood of it or packet is to be dropped after TTL hops. This may significantly reduce the queue length of any intermediate node in the path to destination. Moreover, an intermediate node having a route to destination simply forwards a route request for the same without sending reply if it finds that its current routing message queue length is more than threshold queue length. If an intermediate node has a valid path to destination, then among all the copy of forwarded packets to all neighbouring nodes, the packet which has been forwarded to the next hop node of route entry for destination will follow the optimal path to destination. This model performs an additional checking to verify whether the next hop to the destination’s load factor is less than the threshold level. If yes, then the request packet is simply forwarded to the next hop node instead of forwarding to all neighbouring nodes which reduce the load of the nodes which are not active members of the optimal path to the destination.

Jassim et al [11] incorporated a trust mechanism to enhance the reliability of the AODV protocol. When request and reply messages are generated and forwarded by the nodes in the network, each node appends its own trust value to the trust accumulator and updates its routing table with all the information in the control messages. The trust value is associated with the possibility of the node to perform a packet drop. The use of R-AODV provides a higher percentage of successful data delivery and the impact of routing overload, and end-to-end delay is very minimal.

Sharma et al.[12] designed trusted routing protocols using trust frameworks and intrusion detection system which extended the routing table and the routing messages of AODV with trust information. This information is updated directly through the monitoring neighbourhood. When performing trusted routing discovery, the recommended opinions are combined to make a routing judgment based on each element of the new opinion which reduces the

10.15680/ijircce.2014.0212020

computation overhead, and the trustworthiness of the routing procedures is guaranteed. This model shows that the malicious nodes are separated from the trusted nodes. Moreover, this model thwarts more malicious attacks.

c. *Malicious node detection*

Raj et al [13] proposed a Detection, Prevention and Reactive AODV (DPRAODV) to prevent security threats of black hole by notifying other nodes in the network of the incident. This model does an additional check to find whether the RREP_seq_no is higher than the threshold value which is updated dynamically in every time interval. If the value of RREP_seq_no is higher than threshold value, then the node is suspected to be malicious and adds the node to the black hole list. After detection, a new control packet, ALARM with the black list node as parameter is sent to its neighbours so that the RREP packet from the malicious node is discarded and no processing is done. Malicious nodes in the network are isolated by the ALARM packet and the continuous replies from them are blocked, which lead to decrease in routing overhead. The threshold value is the average of the difference of dest_seq_no in each time slot between the sequence number in the routing table and the RREP packet. DPRAODV increases PDR with minimum increase in average End-to end Delay and normalized routing overhead.

Sharma et al [14] analyzed the effect of the black hole attack in an AODV protocol and proposed a solution that attempted to reduce the black hole attacks. Two modules: self fish module and IDS module are created. The IDS module checks which node has updated the routing table and sends higher sequence number to the sender node and eliminates the path where black hole is present and searches for a new route. This module provides only protection of misbehaving and provides trust communication between sender and destination. This model shows 99% of Packet delivery fraction with 0.14% of black hole nodes. The proposed model tries to eliminate the black hole effect by making an entry of secure route so that each node is known to the rest of the nodes present in the network. When a new node joins the network, the authenticity will be tested and black hole will be detected which takes place after the route determination mechanism.

d. *Additional table*

Mistry et al [15] focused on analyzing and improving the security of AODV routing protocol for mobile networks based on black hole attacks. This scheme is designed to prevent ant alterations in the default operations of either intermediate nodes or that of the destination nodes. The reply messages are stored in a table and the destination sequence number of the stored messages is compared. The RREP message is discarded which has high destination sequence number and the node is defined as malicious. This system ignores the control messages from the defined malicious nodes, and the control messages are not forwarded to the malicious nodes. Since no control messages are added to the existing AODV, it need not regenerate any control messages, which does not increase the routing overhead on either intermediate nodes or the destination nodes. This proposed solution achieves a very good rise in Packet Delivery Ratio (PDR) and acceptable rise in end-to-end delay.

e. *Additional Module*

Aggarwal et al [16] proposed a novel approach to secure AODV protocol which is named as AODV Security Extension (AODVSEC) against the insider attacks like Resource Consumption (RC) attack, Route Disturb (RD) attack, Route Invasion (RI) attack and Black Hole (BH) attack launched through active forging of its Route Reply (RREP) control message. Upon receiving that particular message, a node will always check its routing table for probable updates. This proposed model maintains a cache containing the important information to validate any incoming RREP packet. If RREQ is duplicated, then the node is supposed to compare its identity with “Previous Node IP Address” field in RREQ if valid; the information is stored in the RREQ-ACK cache followed by the normal processing. If RREP is to be generated, then RREQ_ACK is sent back before sending the RREP to the same node. On receiving RREQ-ACK, the Information from the message is stored in the RREQ-ACK Cache. Upon receiving RREP after Validation through RREQ-ACK Cache, RREP is accepted followed by the normal processing. The performance of AODVSEC is no less than that of SAODV, but the same is achieved with lower processing requirement which leads to save computational power.

The summary of the various security enhancement in AODV protocol are listed in Table A with the security mechanisms, security attacks addressed and their purpose.

10.15680/ijircce.2014.0212020

Table A Summary of Various Security enhancements of AODV

S.No	Protocols	Security Mechanisms	Attacks	Central Authority	Additional Control Messages	Purpose
1.	[7]	Digital Signatures Hash Chains	Replay Attack Affecting the Route table	Yes	No	Malicious Node Detection
2.	[8]	Hash Chain Digital Signatures	Control Message attack	No	No	Improving the Routing
3.	[9]	Incorporates Trust Mechanism	Unreliable Routing	No	No	Secure Routing to improve the performance
4.	[10]	Incorporates Trust Mechanism	Unreliable Routing	No	No	Optimize the Routing
5.	[11]	Incorporates Trust Mechanism	Unreliable Routing	No	No	Best Path Selection
6.	[12]	Incorporates Trust Mechanism	Control Message attack	No	No	Trust Routing Malicious Node Detection & Intrusion Detection
7.	[13]	Incorporates Trust Mechanism	Black Hole Attack	No	Yes (ALARM Packets)	Malicious Node Detection
8.	[14]	Additional Module to provide trust communication between source and destination	Black Hole Attack	No	No	Intrusion Detection Prevention
9.	[15]	Additional table to maintain freshness of the route	Black Hole Attack	No	Yes	Malicious Node Detection
10.	[16]	Validating with RREP messages	Insider Attack	No	Yes RREQ-ACK	Secure Routing to improve the performance

VI. CONCLUSION

Security and secure routing in ad-hoc networks have been of interest for quite a long time among the research community. The information that is communicated between the ad-hoc nodes is very vital so that they should not be altered by an attacker. The attacker that exists in the network has to be identified and isolated from the network.

This paper considers the traditional routing protocol AODV which is one of the most protuberant communication protocols in ad-hoc network. AODV is best suited for public mobile ad-hoc networks as it consumes less bandwidth and lower overhead. However, this protocol still has many weaknesses, which attract many researchers to develop new variants by enhancing the AODV protocol to improve its performance and to add security features to it. Hence the various secure routing protocols created based on various security mechanisms are discussed in this paper. Each and every scheme has its own advantages and disadvantages.

10.15680/ijircce.2014.0212020

REFERENCES

[1] US Dept. Transportation, “Vehicle Safety Communications Project Task 3 Final Report” http://www.its.dot.gov/research_docs/pdf/59vehicle-safety.pdf, 2005.

[2] Raya, M., Hubaux, J.-P, ”Securing Vehicular Ad Hoc Networks”, J. Computer Security, Special Issue on Secu- rity, Ad Hoc and Sensor Networks 15(1), 39–68 (2007)

[3] Parno, B., & Perrig, A., “Challenges in securing vehicular networks”, In *Workshop on hot topics in networks (HotNets-IV)* (pp. 1-6). 2005.

[4] S.Bhimla,N.Yadav,”Comparison between AODV protocol and DSR protocol in MANET”,IJAERS, Vol 2,issue 1,2012.

[5] Ali, Asar, and Zeeshan Akbar. "Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications” , Electrical Engineering and Telecommunication, Kalskrona ,2009.

[6] Azad, M. S., Uddin, M. M., Anwar, F., & Rahman, M. A.. “Performance Evaluation of Wireless Routing Protocols in Mobile WiMAX Environment”, In Proceedings of the international multiconference of engineers and computer scientists (Vol. 2), 2008

[7] Zapata, M. G., & Asokan, N. “Securing ad-hoc routing protocols”, In Proceedings of the 1st ACM workshop on Wireless security (pp. 1-10), 2002

[8] Wadbude, D., & Richariya, V. “An Efficient Secure AODV Routing Protocol in MANET”. International Journal of Engineering and Innovative Technology (IJEIT) Volume, 1.issue 4, 2012.

[9] Cerri, D., & Ghioni, A. “Securing AODV: the A-SAODV secure routing prototype”. Communications Magazine, IEEE, 46(2), 120-125,2008.

[10] Mishra, A. K., & Sahoo, B. “A modified Adaptive-SAODV prototype for performance enhancement in MANET”, International Journal of Computer Applications in Engineering, Technology and Sciences. Vol 1,issue 2,pp 443-447, 2009.

[11] Jassim, H. S. H., Tiong, S. K., Yussof, S., Koh, S. P., & Ismail, R. “Scenario based performance analysis of reliant ad-hoc on-demand distance vector routing (R-AODV) for mobile ad-hoc network”, Journal of Engineering and Computer Innovations Vol, 2(5), 78-89, 2011.

[12] Sharma, P, Jain .Y.K.,“Trust based secure aodv in manet”, Journal of Global Research in Computer Science, 3(6), 107-114, 2012.

[13] Raj, P. N., & Swadas, P. B.” Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet”, Internaltional Journal of Computer Science Issues,Vol 2,pp 54-59, 2009.

[14] Sharma, A., Singh, R., & Pandey, G.. “Detection and Prevention from Black Hole attack in AODV protocol for MANET”, International Journal of Computer Applications, 50(5), 1-4, 2012.

[15] Mistry, N., Jinwala, D. C., & Zaveri, M. “Improving AODV Protocol against Blackhole Attacks”, In Proceedings of the International MultiConference of Engineers and Computer Scientists ,Vol. 2, pp. 17-19, 2010

[16] Aggarwal, A., Gandhi, S., Chaubey, N., Shah, P., & Sadhwani, M. “AODVSEC: A novel approach to secure Ad-hoc on-Demand Distance Vector (AODV) routing protocol from insider attacks in MANETs”, Vol 4, No 4 pp191-210, 2012.

10.15680/ijircce.2014.0212020