International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
Volume 4 Issue 2 May 2013

SURVEY ON SECURE ROUTING PROTOCOLS FOR AODV

Nitya Jain
Department of CSE
Sharda University, Greater Noida, India

Aparajita Naiwal
Department of CSE
Sharda University, Greater Noida, India

Abstract:

A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Most of the protocols in this category are not incorporating proper security features. The ad hoc environment is accessible to both legitimate network users and malicious attackers. It has been observed that different protocols need different strategies for security. An attempt has been made to review some of the existing protocols. The objective is to make observations about how the performance of these protocols can be improved.

1. Introduction

Ad hoc network [1] is a wireless network without having any fixed infrastructure. Each mobile node in an ad hoc network moves arbitrarily and acts as both a router and a host. A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio

range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks.

Although security [2] has long been an active research topic in wired networks, the unique characteristics of Ad Hoc networks present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic topology. Some of the main security attributes [2,3] that are used to inspect the security state of the mobile adhoc network are : Availability, Integrity, Confidentiality, Authenticity, Non repudiation, Authorization, Anonymity.

2 .0 Security Aspects

Security services include the functionality required to provide a secure networking environment. The main security services can be summarized as follows:

- **Authentication:** This service [4,5] verifies a user's identity and assures the recipient that the message is from the source that it claims to be from. Firstly, at the time of communication initiation, the service assures that the two parties are authentic, that each is the entity it claims to be. Secondly, it must assure that a third party does not interfere by impersonating one of the two legitimate parties for the purpose of authorized transmission and reception. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures [6] and certificates. Details of the construction and operation of digital signatures can be found in RFC2560 [7].
- **Confidentiality:** This service ensures that the data/information transmitted over the network is not disclosed to unauthorized users. Confidentiality can be achieved by using different encryption techniques such as only legitimate users can analyze and understand the transmission.
- **Integrity:** The function of integrity control is to assure that the data is received in verbatim as sent by authorized party. The data received contains no modification, insertion or deletion.

- **Access Control:** This service limits and controls the access of such a resource, which can be a host system or an application.
- **Availability:** This involves making the network services or resources available to the legitimate users. It ensures the survivability of the network despite malicious incidences.

3.0 Attacks on MANET

The attacks based on the domain of MANET, classified into two categories namely internal attacks and external attacks. These classifications are shown in Figure 1.

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
Volume 4 Issue 2 May 2013

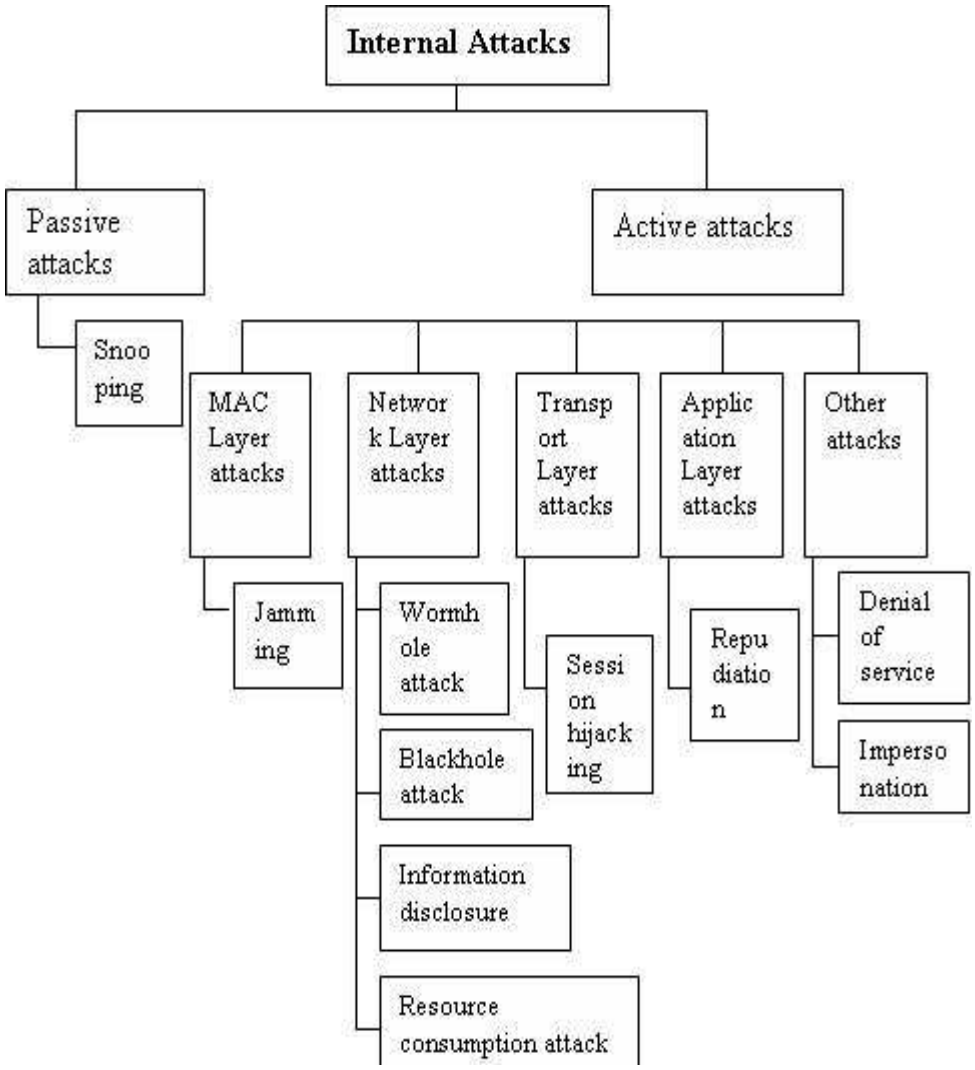

Figure 1: Classification of Internal attacks

3.1 External Attack: - External attacks are attacks, launched by nodes that do not possess a valid certificates, means these nodes do not have authorized member of the MANET. For instance, in a military setting each authorized soldier might possess a signed certificate from a trusted party granting him membership in the MANET. Such a node is an insider node. Any node not possessing such a certificate is considered an outsider node. The outsider attacks have the capability to spoof its identity, such as spoofing its IP and MAC addresses to impersonate an insider node. Outsider attacks have the capability to access the wireless channel so it can eavesdrop on legitimate traffic.

3.2 Internal Attack: - Internal attacks are attacks, launched by one or more compromised nodes that possess a valid certificate, means these nodes are authorized member of the MANET. Internal attacks are more severe comparatively to outsider attacks since the insider knows valuable and secret information, and possesses privileged access right. Internal attacks can be classified as shown in figure 1 according to network protocol stacks.

3.2.1 Passive Attacks: - A Passive Attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Passive attacks basically involve obtaining crucial routing information by sniffing about the network. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks. These attacks do not disturb the operation of communication i.e. do not degrade the performance of the MANET. These type of attack read the network node position, bandwidth used, traffic pattern etc.

3.2.2 Active Attacks: **-** An active attack involves information interruption, modification, or fabrication, thereby to degrade the performance of the MANET. An Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the threat. These attacks can be classified into further following types.

- **Impersonation:** Since current ad hoc routing protocols do not *authenticate* routing packets a malicious node can launch many attacks in a network by masquerading as another node

(known as *spoofing*). Spoofing occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather.

- **Modification:** Existing routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Malicious nodes can easily cause traffic subversion and denial of service by simply altering the fields of the packet: such attacks compromise the *integrity* of routing computations.
- **Fabrication:** The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted.
- **Wormhole Attack**: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, say node A, captures routing traffic at one point of the network and tunnels them to another point in the network, say to node B, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers.
- **Denial of Service:** This active attack aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in resistance to Denial of Service attacks, compared to fixed networks.
- **Black hole attack:** The black hole attack is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets.

4. Secured Protocols:

Various security protocols have been analysed based on certain common metrics. Some of the most common have been highlighted here are:

(i) ARAN [8]

The Analyzing security of Authenticated Routing Protocol (ARAN) secure routing protocol is an on-demand routing protocol that detects and protects against malicious actions carried out by third parties and peers in the ad hoc environment. ARAN introduces authentication, message integrity and non-repudiation as part of minimal security policy for the ad hoc environment and consists of a preliminary certification process, a mandatory end to-end authentication stage and an optional second stage that provides secure shortest paths.

Characteristics of ARAN are:

i. The ARAN protocol protects against exploits using modification, fabrication and impersonation

ii. The ARAN protocol uses of asymmetric cryptography makes it a very costly protocol to use in terms of CPU and energy usage.

iii. Against ARAN is not immune to the wormhole attack.

(ii) SAODV [9]

The Secure Ad hoc On Demand distance Vector (SAODV) protocol is an extension of the AODV protocol. The Secure AODV scheme is based on the assumption that each node possesses certified public keys of all network nodes.

Characteristics of SAODV are:

i. Ownership of certified public keys enables intermediate nodes to authenticate all in-transit routing packets.

ii. The protocol operates mainly by using the new extension message with the AODV protocol.

iii. The SAODV can be used to protect the route discovery mechanism of the AODV by providing security features like integrity, authentication and nonrepudiation.

(iii) SAR [10]

Security-Aware Ad-Hoc Routing (SAR) is the generalized framework for any ondemand ad-hoc routing protocol. SAR requires that nodes having same trust level must share a secret key. SAR augments the routing process using hash digests and symmetric encryption mechanisms. The signed hash digests provide message integrity while the encryption of packets ensures their confidentiality.

Characteristics of SAR are:

i. SAR uses security information to dynamically control the choice of routes installed in the routing table.

ii. SAR enables applications to selectively implement a subset of security services based on the cost-benefit analysis.

iii. The routes discovered by SAR may not always be the shortest between any two communicating entities in terms of hopcount. However these routes have quantifiable guarantee of the security.

iv. SAR will find the optimal route if all the nodes on the shortest path satisfy the security requirements.

v. SAR may fail to find the route if the ad hoc network does not have a path on which all nodes on the path satisfy the security requirements in spite of being connected.

4. A-SAODV [11]

Adaptive-SAODV (A-SAODV) secure routing prototype is proposed for securing AODV. Mobile ad hocnetworks create new type of security issues, resulted by their characteristics of collaborative and open systems and by restricted accessibility of resources. In this paper, the author considers a Wi-Fi connectivity data link layer as a basis and deals with routing security. The author elaborates the implementation of the secure AODV protocol extension that includes tuning approach which is intended at enhancing its performance. The author provides an adaptive method that enhances SAODV behavior. In addition, the author examines the adaptive strategy and another method which delays the confirmation of digital signatures.

Characteristics of A-SAODV are:

i. Ownership of certified public keys enables intermediate nodes to authenticate all in-transit routing packets.

ii. loop free.

iii. adaptive as per security attack mentioed in the algorithm.

iv. uses trust party arrangements.

Table 1: Comparison and summery of different routing security mechnism.

Protocols	Attacks Prevented	Security Mechanisms	Comments
ARAN [8]	Provides network services like authentication and non-repudiation	Secure certifictae server	- Used with AODV, DSR - Heavy asymmetric cryptographic computation - Prone to wormhole attack if accurate time synchronization is not available
SAODV [9]	Provides integrity, authentication and non-repudiation	Certified public keys	- Used with AODV - operates mainly by using the new extension message with the AODV - protects the route discovery mechanism of the AODV
SAR [10]	Uses sequence numbers and timestamps to stop replay attacks in routing update packets	Quality of protection (QoP) metric	- Used with AODV - Rute discovered may not be the shortest route in terms of hop-count but it is always secured - Defends against modification and fabrication attacks

A-SAODV [11]	Uses trust party arrangements	Certified public keys	- Used with AODV - loop free - Adaptive as per security attack

Acknowledgements: Thanks to Dr Ashwani kush, Head , Dept of computer science, University College, Kurukshetra University India for his valuable suggestions in completing this work

5. Conclusion:

Analytical review of various protocols have been done. All efforts have been made to be biasless and provide all characteristics on the same scale. It has been observed that most schemes are attack oriented and whenever there is some new attack, that scheme actually collapses. Next part of the work will concentrate on simulating the scheme using some simulator and designing a new scheme that will be more robust and secured.

Ad hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. Several protocols for secured routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The current security mechanisms, each defeats one or few routing attacks. It is still a challenging task to design routing protocols resistant to multiple attacks.

References

[1] Poongothai T. and Jayarajan K., “A non-cooperative game approach for intrusion detection in Mobile Adhoc networks”, International Conference of Computing, Communication and Networking (ICCC), 18-20 Dec 2008, St. Thomas, VI, pp 1-4

[2] Kush, Ashwani June 2009 Security and Reputation Schemes in Ad-Hoc Networks Routing, International Journal of Information Technology and Knowledge Management, Volume 2, No. 1, pp. 185-189.

[3] Kush, A. March 2009 Security Aspects in AD hoc Routing, Computer Society of India Communications, Vol. no 32 Issue 11, pp. 29-33.

[4] A. Perrig, R. Canetti, D. Song and J. D. Tygar, "Efficient and Secure Source Authentication for Multicast," *In Proc. of NDSS 2001.*

[5] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *In Proc. of IEEE Symposium on Security and Privacy,* 2000.

[6] W. Mehuron, "Digital Signature Standard (DSS)," U.S. Department of commerce, *National Institute of Standards and Technology (NIST)*, Information Technology Laboratory (ITL). FIPS PEB 186,1994

[7] RFC 2560 www.ietf.org/rfc/rfc2560.txt, last accessed on March 25,2007.

[8] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, 978-0-7695-4336-9/11 $26.00 © 2011 IEEE DOI 10.1109/ISMS.2011.58

[9] B. Dahill, B. N. Levine, E. Royer, C. Shields, 2002,"ARAN: A secure Routing Protocol for Ad Hoc Networks", UMass Tech Report 02-32.

[10] Zapata,M.G.,"Secure ad-hoc on-demand distance vector (SAODV) routing ," IETF MANET ,internetdraft (Work in progress),draft -guerrero-manet-saodv-00.txt,2001.- accessed 10/10/2006.

[11] Yi,S., Naldurg ,P., Kravets ,R.,"Security aware ad-hoc routing for wireless networks," Proc. Of the 2nd ACM international Symposium on Mobile Adhoc networking and Computing (Mobi - Hoc'01), pp.299-302, 2001.

[12] Davide Cerri, Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE Communication Magazine, Pp. 120-125, 2008.