# A Review of Secure Routing Protocol in Mobile Ad Hoc Network

Rajender Nath[1], Pankaj Kumar Sehgal[2]
[1]Deptt. of Computer Science and Applications, Kurukshetra University, Kurukshetra, Haryana, India.
[2]Department of Information Technology, MM University,Mullana(Ambala), Haryana, India
email: rnath_2k3@rediffmail.com, pankajkumar.sehgal@gmail.com

***Abstract:*** Mobile ad hoc networks (MANETs) is an emerging research area with commercial and military applications. The fundamental characteristics such as dynamic topology, open medium and distributed cooperation are combined with security threats. The routing protocols plays important and essential role in secure data transmission for entire network. This paper presents the review of some secure routing protocols for MANETs. The paper gives a comparative study of these protocols with respect to various security parameters and attacks.

*Keywords*: routing protocol, security attacks, security threats.

## 1. Introduction

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any established infrastructure or centralized authority. Until now, the main research focus has been on improving the protocols for multi-hop routing, performance and scalability of the ad hoc networks [20]. Though, the performance and scalability have their place in wireless network research, the current and future applications of the ad hoc networks has forced the research community to look at dependability and security aspects of ad hoc networks. Security in an ad hoc network is essential even for basic network functions like routing and packet forwarding, since such network functions are carried out by the nodes themselves rather than specialized routers. Hence, the nodes of an ad hoc network must be trusted for the proper execution of basic network functions. The intruder in the ad hoc network can come from anywhere, along any direction and target any communication channel in the network. Compare this with a wired network where the intruder gains physical access to the wired link or pass through security holes at firewalls and routers. Since the infrastructure-free mobile ad hoc network does not have a clear line of defense, every node must be prepared for the adversary. Hence a centralized or hierarchical network security solution for the existing wired and infrastructure-based cellular wireless networks will not work properly for mobile ad hoc networks. Securing the ad hoc networks, like any other field of computers, is based on the principle of confidentiality and integrity. These principles exist in every field, but the presence of malicious nodes, covert channels and eavesdroppers in the mobile ad hoc network makes this an extremely important and challenging problem [21]. In past several years, there has been a surge of network security research in the field of information assurance that has focused on protecting the data using techniques such as authentication and encryption. These techniques are applicable in a wired and infrastructure based cellular network. In the case of infrastructure-free mobile ad hoc networks these techniques are not applicable [20]. In the infrastructure-free networks, the nodes themselves perform basic network functions like routing and packet forwarding. Therefore, mobile ad hoc network security is a pressing issue which needs immediate research attention [22, 23, 24, 25].

Rest of the paper is structured as follow: Section 2 provides a brief of security mechanism available for secure routing protocols. Section 3 gives a brief summary of some secure routing protocols. Section 4 presents a comparative study of secure routing protocols described in Section 3. Section 5 gives concluding remarks.

## 2. Security Mechanism for Routing Protocols

Message encryption and digital signatures are two important mechanisms for data integrity and user authentication. There are two types of data encryption mechanisms, symmetric and asymmetric (or public key) mechanisms. Symmetric cryptosystems use the same key (the secret key) for encryption and decryption of a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and another key (the private key) to decrypt it. Public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used for decryption purpose. Even if attacker comprises a public key, it is virtually impossible to deduce the private key. Any code attached to an electronically transmitted message that uniquely identifies the sender is known as digital code. Digital signatures are key component of most authentication schemes. To be effective, digital signatures must be non-forgeable. Hash functions are used in creation and verification of a digital signature. It is an algorithm which creates a digital representation or fingerprint in the form of a hash value (or hash result) of a standard length which is usually much smaller than the message and unique to it. Any change to the message will produce a different hash result even when the same hash function is used. In the case of a secure hash function, also known as a one-way hash function, it is computationally infeasible to derive the original message from knowledge of its hash value. In mobile ad hoc networks, the secrecy of the key does not ensure the integrity of the message. For this purpose, message Authentication Code (MAC) [26] is used. It is a hashed representation of a message and even if MAC is known, it is impractical to compute the message that generated it. A MAC, which is a cryptographic checksum, is computed by the message initiator as a function of the secret key and the message being transmitted and it is appended to the message. The recipient re-computes the MAC in the similar fashion upon receiving the message. If the MAC computed by the receiver matches the MAC received with the message then the recipient is assured that the message was not modified. The next section provides some secure routing protocols based on above security mechanism.

# 3. Secure Routing Protocols

### 3.1 Secure efficient ad hoc distance vector routing

The Secure Efficient Ad hoc Distance vector routing (SEAD) [7] protocol is a secure ad hoc network routing protocol which is based on the design of the Destination-Sequenced Distance-Vector (DSDV) [19] routing protocol. In this protocol for the limited CPU processing capability, and to guard against Denial of- Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we can use one-way hash function but we can not use the asymmetric cryptographic operations. The key feature of proposed security protocol is the use one- way hash chains, using an one way hash function H. Each node computes a list of hash values $h_o,h_1,\ldots\ldots h_n$, where $h_i = H(h_i\text{-}1)$ and $0<i<=n$, based on an initial random value ho. The paper assumes the existence of a mechanism for distributing hn to all intended receivers. If a node knows H and trusted value $h_n$, then it can authenticate any other value hi, $o<i<=n$ by successively applying the hash function H and then computing the result with $h_n$. This protocol provides a robust protocol against attackers trying to create in correct routing state in other node by modifying the sequence number or the routing metric. SEAD does not provide a way to prevent an attacker to use the same metric and sequence number learned from some recent update message, for sending a new routing update to a different destination.

### 3.2 A Secure on demand routing protocol

A Secure OnDemand Routing Protocol for Ad Hoc Networks (ARIADNE) [8] provides security against arbitrary active attackers and relies only on efficient symmetric cryptography This paper present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne is more general, more efficient or more secure. Ariadne does not require a trusted hardware and does not require powerful processors. This protocol prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks. In case of using only highly efficient symmetric cryptographic primitives Ariadne is efficient. This protocol can authenticate routing messages using one of three schemes: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures. The performance of ad hoc network routing protocol has been evaluating by ns-2 simulator.

### 3.3 ENDAIRA

endairA[1] is designed by the inspiration of Ariadne with digital signature. The name endairA is just reverse of Ariadne. The protocol endiarA is based on the various possible attacks on the Ariadne[8]. The protocol focus on the route discovery process of on-demand source routing protocols. The result is based on the simulation paradigm and actual implementation is still pending.

### 3.4 Cooperation of nodes fairness in dynamic ad-hoc networks

Cooperation of nodes fairness in dynamic ad-hoc networks CONFIDANT [6] protocol is designed as an extension to reactive source-routing protocol such as DSR. It is a collection of components which interact with each other for monitoring, reporting, and establishing routes by avoiding misbehaving nodes. CONFIDANT components in each node include a network monitor, reputation system, trust manager, and a path manager. When DSR is fortified with the CONFIDANT protocol extensions, it is very scalable in terms of the total number of nodes in the network and it performs well even if more than 60% of the nodes are misbehaving. The overhead for incorporating different security components is manageable for ad hoc environment. However, detection based reputation system has few limitations and routes are still vulnerable to spoofing and Sybil attacks.

### 3.5 Security-Aware Routing

A Security-Aware Routing (SAR) [14] Protocol is an on demand routing protocol based on AODV. This protocol integrates the trust level of a node and the security attributes of a route to provide the integrated security metric for the requested route. A Quality of Protection (QoP) vector used is a combination of security level and available cryptographic techniques. SAR uses the timestamps and sequence numbers to stop the replay attacks. Interception and subversion threats can be prevented by trust level key authentication. Attacks like modification and fabrication can be stopped by verifying the digital signatures of the transmitted packet. The main drawbacks of using SAR are the excessive encrypting and decrypting required at each hop during the path discovery. By using SAR route discovered may not be the shortest route in the terms of hop-count, but it is secure.

### 3.6 Secure routing protocol

The Secure Routing Protocol (SRP) [15] is extension that can be applied to many of the on demand routing protocols. SRP provide protection against attacks that disrupt the route discovery process and identify the correct topological information. The main purpose of SRP is to provide the security association (SA) between a source and destination node without need of cryptographic validation of the communication data by the intermediate node. This protocol assumes that security association can be achieved though a shared key $K_{st}$ between the source s and target t. The source node s initiates the route discovery by sending a route request packet to the destination t. This protocol uses the additional header called the SRP header. The SRP header contains the following information: the query sequence number $Q_{sec}$, query identifier number $Q_{id}$, and a 96 bit MAC field. If SRP header is missing intermediate nodes discard a route request message otherwise they forward the request towards destination after extracting $Q_{id}$ , Source, and destination address.

# 4. Comparative Study

We summarize the various secure routing protocols that have been explained in section 3. We consider several attributes and comment on these attributes with respect the each of the

protocol discussed above. Table 1 presents the comparative study on various security parameters and security attacks.

**Table 1.** Comparative study of various protocols

| **Performance parameters** | **SEAD** | **ARIADNE** | **ENDAIRE** | **CONFIDANT** | **SRP** | **SAR** |
|---|---|---|---|---|---|---|
| Base Protocol | DSDV | DSR | DSR | DSR | DSR/ ZRP | AODV |
| Encryption Algorithm | Symmetric | Symmetric | Symmetric | Symmetric | Symmetric | Symmetric/ Asymmetric |
| Synchronization | Yes | Yes | Yes | No | No | No |
| Integrity | **No** | **Yes** | **Yes** | **Yes** | **Yes** | Yes |
| Nonrepudiation | **No** | **No** | **No** | **Yes** | **No** | Yes |
| Authentication | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** | Yes |
| Confidentiality | **No** | **No** | **Yes** | **No** | **No** | Yes |
| DoS Attacks | Yes | Yes | Yes | Yes | Yes | No |

## 5. Conclusion

The paper discussed six different secure routing protocols and gives a comparative study based on characteristics of these protocols. The comparative study made in this paper shown the different types of approaches in respect to various security parameters and security attacks. The comparative study will help the researcher to focus on specialized methods for making routing protocols more secure for mobile ad hoc networks.

## References

[1] Gergely Acs, Levente Buttyan and Istvan Vajda, " Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks", IEEE transactions on Mobile Computing, Vol.5, No.11, November 2006, pp. 1533-1546.

[2] Jaier Gomez, Andrew T. Campbell, "Variable –Range Transmission Power Control in Wireless Ad Hoc Networks", IEEE transactions on Mobile Computing, Vol.6, No.1, January, 2007, Pg. 87-99.

[3] Ting-Yao Jiang, Qing-hua Li, "A Secure Routing Protocol for Mobile Ad-Hoc Network " Proceeding of the third International conference on Machine Learning and Cybernetics, 26-29 Augest 2004, Pg. 2825-2829.

[4] Rendong Bai and Mukesh Singhal, "DOA: DSR over AODV routing for mobile ad hoc network", IEEE transactions on Mobile Computing, Vol 5, No 10, October 2006, Pg. 1403-1416.

[5] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network", ACM Wireless Networks, Vol 8, No 2, Mar. 2002, pp. 153-167.

[6] S. Buchegger and J. L. Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks", In Proc. Of IEEE/ACM Symposium on Mobile Ad Hoc Net- working and Computing (MobiHOC), Jun. 2002.

[7] Y. –C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Fourth IEEE Workshop on Mobile

[8] Y. –C. Hu, D. B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Mobicom'02, 2002.

[9] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol, RSA Cryptobytes (RSA Laboratories)", Vol 5, No 2, Summer/Fall 2002, pp. 2-13.

[10] C. S. R. Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", Prentice Hall PTR, 2004.

[11] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) Specifications," 1997.

[12] Y. Zhang, Wenjing Lou and Yuguang Fang, " Securing Mobile Ad Hoc Networks with Certificate less Public Keys", IEEE transactions on Dependable and Secure Computing, Vol.3, No. 4, Octuber-December 2006, pp. 386-399.

[13] Williams, B. and Camp, T.: "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks", In: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MOBIHOC '02). pp. 194–205. Lausanne, Switzerland. June 9-11 2002.

[14] R. Kravets, S. Yi, and P. Naldurg, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks", In ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001.

[15] P. Papadimitratos and Z. J. Haas,"Secure Routing for Mobile Ad hoc Networks", In Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan. 2002.

[16] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", Proc. of the 3rd Intl. Symp. on Information Processing in Sensor Networks, 2004.

[17] Charles E. Perkins and Elizabeth M. Royer. "Ad Hoc OnDemand Distance Vector (AODV) algorithm", In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), New Orleans, Louisiana, USA, February 1999.

[18] Y. -C. Hu, D. B. Johnson, and A. Perrig, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", WiSe 2003, 2003.

[19] C Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers", ACM SIGCOMM, (October 1994).
[20] Hubaux. J., Buttyan, L., and Capkun, S. , "The Quest for Security in Mobile Ad Hoc Networks," MobiHw 2001.
[21] Stajjano, F. and Anderson, R., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," Proceedings of Security Protocols Workshop, 1999.
[22] Vinayakraj-Jani, P., "Security within Ad hoc Networks," PAMPAS Workshop, London, Sept. 16/17 2002.
[23] Wrona, K., "Distributed Security: Ad Hoc Networks & Beyond," PAMPAS Workshop, London, Sept. 16/17 2002.
[24] Buttyan, L., and Hubaux, J.,"Repn on a Working Session on Security," Wiretess Ad Hoc Networks Mobile Computing and Communications Review, Vol. 6, Number 4,2002.
[25] Michiardi, P., Molva, R., "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks," European Wireless Conference, 2002.
[26] Zapata, M., "Secure Ad hoc On-Demand Distance Vector Routing.," ACM Mobile Computing and Communications Review (MCZR), Vol. 6. No. 3, July 2002, pp. 106-107. pp. 1516-1521