International Journal of Computer and Communication Technology

Volume 3 | Issue 2 Article 6

April 2012

SECURE ROUTING PROTOCOLS IN AD HOC NETWORKS: A REVIEW

JASPAL KUMAR
Department of Electronics and Engineering Bhiwani Shanker Anangpuria Institute of Technology & Management, Faridabad, jaspalkumar@rediffmail.com

M. KULKARNI
Department of Electronics and Communication Engineering National Institute of Technogy karnataka, Surathkal,Mangalore-575025, mkuldce@gmail.com

DAYA GUPTA
Department of Computer Engineering Delhi College of Engineering, Delhi University, Delhi, daya_gupta2005@yahoo.co.in

SECURE ROUTING PROTOCOLS IN AD HOC NETWORKS: A REVIEW

JASPAL KUMAR
Department of Electronics and Engineering
Bhiwani Shanker Anangpuria Institute of Technology & Management, Faridabad
jaspalkumar@rediffmail.com

M. KULKARNI
Department of Electronics and Communication Engineering
National Institute of Technogy karnataka, Surathkal,Mangalore-575025
mkuldce@gmail.com

DAYA GUPTA
Department of Computer Engineering
Delhi College of Engineering, Delhi University, Delhi
daya_gupta2005@yahoo.co.in

Abstract

Mobile Ad hoc wireless networks (MANETs) assume no existing infrastructure is available for routing packets end-to-end in a network and instead rely on intermediary peers. The nodes in MANET are subject to various attacks that range from naïve eavesdropping to vicious battery draining attacks. Routing Protocols, data, bandwidth and battery power are the common target of theses attacks. This paper gives an overview of seven such secure routing protocols by presenting their characteristics and functionality along with their respective merits and drawbacks. A Comparison of these protocols is also presented based upon certain security parameters.

Keywords: *Routing, MANET , security*

1. INTRODUCTION

With the advancement in radio technologies like Bluetooth[1], IEEE 802.11[2] or Hiperlan [3] , a new concept of networking has emerged , known as ad hoc networks, In such a network potential mobile users arrive within the common perimeter of radio link and participate in setting up the network topology for communication. Nodes within radio range are mobile and they communicate with each through direct wireless links or multihop routing. A Mobile Ad hoc NETwork (MANET)[4] consists of a set of mobile hosts that carry out basic networking functions like- packet forwarding, routing, and service discovery without the help of an established infrastructure. Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each node's wireless transmissions.

A MANET is an interconnected system of wireless nodes that communicate over bandwidth-constrained wireless links. Each wireless node can function as a sender, a receiver or a router. When the node is a sender, it can send messages to any specified destination node through some route.

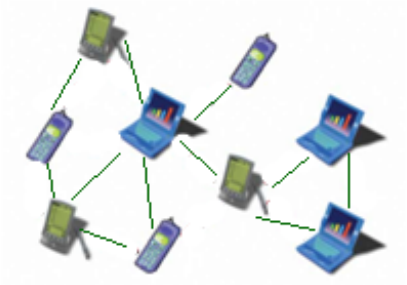

Figure1. MANET in Operation

As a receiver, it can receive messages from other nodes. When the node functions as a router, it can relay the packet to the destination or next router in the route. When necessary, each node can buffer packets awaiting transmission. MANET have several advantages over traditional wireless networks including ease of deployment, speed of deployment, and decreased dependence on a fixed infrastructure, thus giving rise to an emerging wireless networking technology for future mobile communications. In moving forward towards fulfilling this opportunity, the task of finding good solutions for these challenges will play a critical role in achieving the eventual success and potential of mobile ad-hoc network technology.

Security in MANET is an essential component for basic network functions like- packet forwarding, routing and network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. In this paper, an attempt is made to expose the various issues in order to have a secured MANET.

This paper is organized as follows. Section 2 presents an overview of various issues regarding the ad hoc networks, Section 3 compares different secure ad hoc routing protocol based on various parameters specified above and in the next section

various challenges are discussed and finally we conclude.

2. ISSUES IN SECURING

The build up of ad hoc network can be envisaged where support of wireless access or wired backbone is not feasible. Ad hoc wireless network does not have any predefined infrastructure and all network services are configured and created on the fly. Thus it is obvious that with lack of infrastructure support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness.

Achieving security within an MANET is challenging due to following reasons.

- *Dynamic Topologies and Membership*

A network topology of ad hoc network is very dynamic as mobility of nodes or membership of nodes is very random and rapid. This defines the need for secure solutions to be dynamic.

- *Vulnerable wireless link*

Passive/Active link attacks like eavesdropping, spoofing denial of service masquerading, impersonation are possible.

- *Roaming in dangerous environment*

Any malicious node or misbehaving node can create hostile attack or deprive all other nodes from providing any service.

Briefly discussed below are the main issues for providing security in MANET.

2.1 Identification issue

Nodes having access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate.

i. Before establishing secure communication link the node should be capable enough to identify another node. As a result node needs to provide his/her identity as well as associated credentials to another node.
ii. The delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node.

Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised.

2.2. Privacy Issue

The *identification* issue simultaneously leads to *privacy* issue for MANET. Mobile node uses various types of identities and that varies form link level to user/application level. Also in mobile environment very frequent mobile node is not ready to reveal his/her identity or credentials to another mobile node from privacy point of view. Any compromised identity leads attacker to create privacy threat to user device. Unfortunately the current mobile standards do not provide any location privacy and in many cases revealing identity is inevitable to generate communication link. Hence a seamless privacy protection is required to harness the usage of ad hoc networking.

Therefore by the issues discussed above it is essential to provide *security architecture* to secure ad hoc networking.

3. SECURED ROUTING PROTOCOLS REVIEW

Briefly discussed below are the various routing protocols along with the features in terms of strengths and weaknesses they posses.

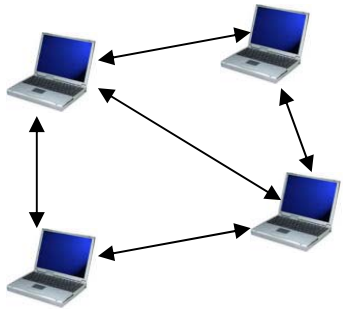

Figure 2. Routing Paths in MANET

3.1 ARAN

3.1.1 Introduction

The ARAN[5] 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.

3.1.2 Operation

ARAN requires the use of a trusted certificate server (T): before entering in the ad hoc network, each node has to request a certificate signed by T. The certificate contains the IP address of the node, its public key, a timestamp of when the certificate was created and a time at which the certificate expires along with the signature by T. All

nodes are supposed to maintain fresh certificates with the trusted server and must know T's public key.

The goal of the first stage of the ARAN protocol is for the source to verify that the intended destination was reached. As with any secure system based on cryptographic certificates, the key revocation issue has to be addressed in order to make sure that expired or revoked certificates do not allow the holder to access the network. In ARAN, when a certificate needs to be revoked, the trusted certificate server T sends a broadcast message to the ad hoc group that announces the revocation. Any node receiving this message re-broadcasts it to its neighbors. Revocation notices need to be stored until the revoked certificate would have expired normally. Any neighbor of the node with the revoked certificate needs to reform routing as necessary to avoid transmission through the now un-trusted node. This method is not failsafe.

In some cases, the un-trusted node that is having its certificate revoked may be the sole connection between two parts of the ad hoc network. In this case, the non- trusted node might not forward the notice of revocation for its certificate, resulting in a partition of the network, as nodes that have received the revocation notice will no longer forward messages through the un-trusted node, while all other nodes depend on it to reach the rest of the network. This only lasts as long as the un-trusted node's certificate would have otherwise been valid, or until the un-trusted node is no longer the sole connection between the two partitions. At the time that the revoked certificate should have expired, the un-trusted node is unable to renew the certificate, and routing across that node ceases. Additionally, to detect this situation and to hasten the propagation of revocation notices, when a node meets a new neighbor, it can exchange a summary of its revocation notices with that neighbor; if these summaries do not match, the actual signed notices can be forwarded and re-broadcasted to restart propagation of the notice.

3.1.3 In nutshell

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

3.2 ARIADNE

3.2.1 Introduction

ARIADNE[6] is an *on-demand* secure ad hoc routing protocol based on DSR that withstands node compromise and relies only on highly efficient *symmetric* cryptography. ARIADNE guarantees that the target node of a route discovery process can authenticate the initiator, that the initiator can authenticate each intermediate node on the path to the destination present in the RREP message and that no intermediate node can remove a previous node in the node list in the RREQ or RREP messages.

3.2.2 Brief Operation

As for the SRP[12] protocol, ARIADNE needs some mechanism to bootstrap authentic keys required by the protocol. In particular, each node needs a shared secret key ($K_{S, D}$) is the shared key between a source S and a destination D) with each node it communicates with at a higher layer, an authentic TESLA [11] key for each node in the network and an authentic "Route Discovery chain" element for each node for which this node will forward RREQ messages.

3.2.3 Features

i. ARIADNE provides point-to-point *authentication* of a routing message using a message authentication code (MAC) [10] and a shared key between the two parties.
ii. For authentication of a broadcast packet such as RREQ, ARIADNE uses the TESLA broadcast authentication protocol
iii. Selfish nodes are not taken into account.

3.2.4 Strengths

i. ARIADNE copes with attacks performed by *malicious* nodes that modify and fabricate routing information, with attacks using impersonation and, in an advanced version, with the wormhole attack
ii. ARIADNE is protected also from a flood of RREQ packets that could lead to the cache poisoning attack.
iii. ARIADNE is immune to the wormhole attack only in its advanced version: using an extension called TIK (TESLA with Instant Key disclosure) that requires tight clock synchronization between the nodes, it

is possible to detect anomalies caused by a wormhole based on timing discrepancies.

3.3 SEAD

3.3.1 Introduction

Hu, Perrig and Johnson presented a *proactive* secure routing protocol based on the Destination-Sequenced Distance Vector protocol (DSDV)[7]. In a proactive (or periodic) routing protocol nodes periodically exchange routing information with other nodes in attempt to have each node always know a current route to all destinations.

3.3.2 Basic Idea

SEAD[8] authenticates the sequence number and metric of a routing table update message using hash chains elements. In addition, the receiver of SEAD routing information also authenticates the sender, ensuring that the routing information originates form the correct node. The source of each routing update message in SEAD must also be authenticated, since otherwise, an attacker may be able to create routing loops through the *impersonation* attack.

3.3.2 Features

i. SEAD deals with attackers that *modify* routing information broadcasted during the update phase of the DSDV-SQ protocol: in particular, routing can be disrupted if the attacker modifies the sequence number and the metric field of a routing table update message.

ii. SEAD makes use of efficient one-way hash chains rather than relaying on expensive asymmetric cryptography operations.

iii. SEAD assumes some mechanism for a node to distribute an authentic element of the hash chain that can be used to authenticate all the other elements of the chain.

3.3.3 Weakness

i. SEAD does not cope with *wormhole* attacks.

3.4 SRP

3.4.1 Introduction

The Secure Routing Protocol (SRP)[12] was designed as an extension compatible with a variety of existing *reactive* routing protocols. SRP combats attacks that disrupt the route discovery process and guarantees the acquisition of correct topological information:

3.4.2 Operation

SRP allows the initiator of a route discovery to detect and discard bogus replies. SRP relies on the availability of a *security association* (SA) between the source node (S) and the destination node (T). The SA could be established using a hybrid key distribution based on the public keys of the communicating parties. S and T can exchange a secret symmetric key ($K_{S,T}$) using the public keys of one another to establish a secure channel. S and T can then further proceed to mutual authentication of one another and the authentication of routing messages.

3.4.3 Strengths

i. SRP copes with non-colluding *malicious* nodes that are able to modify (corrupt), replay and fabricate routing packets.

ii. Assuming that the neighbor discovery mechanism maintains information on the binding of the medium access control and the IP addresses of nodes, SRP is proven to be essentially immune to IP spoofing.

iii. In case of the Dynamic Source Routing (DSR) protocol [9], SRP requires including a 6-word header containing unique identifiers that tag the discovery process and a message authentication code (MAC) computed using a keyed hash algorithm.

3.4.4 Weaknesses

i. The basic version of SRP suffers from the route cache poisoning attack.

ii. SRP suffers from the lack of a validation mechanism for route maintenance messages

iii. SRP is not immune to the wormhole attack: two colluding malicious nodes can misroute the routing packets on a private network connection and alter the perception of the network topology by legitimate nodes.

3.5 SAODV

3.5.1 Introduction

The Secure Ad hoc On Demand distance Vector (SAODV)[13] 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.

3.5.2 Operation

The originator of the routing control packet appends its RSA signature and the last element of a hash chain to the routing packets. A

packet transverse the network, intermediate nodes cryptographically authenticates the signature and the hash value. The intermediate nodes generate the k^{th} element of the hash chain, with k being the number of transverse hops, and place it in packet.

The SAODV protocol gives two alternatives for ROUTE REQUEST and ROUTE REPLY messages. In the first case when a ROUTE REQUEST is sent, the sender creates a signature and appends it to packet. Intermediate nodes authenticate the signature before creating or updating the reverse route to the host. The reverse rout is stored only when the signature is verified. When the node reaches the destination, the node signs the ROUTE REPLY with its private key and sends it back. The intermediate nodes again verify the signature .The signature of the sender is again stored with the along with the route entry.

3.5.3 Features

i. Ownership of certified public keys enables intermediate enable 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 non-repudiation.

3.6 SAR

3.6.1 Introduction

Security-Aware Ad-Hoc Routing (SAR)[14] is the generalized framework for nay on-demand 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.

3.6.2 Operation

SAR when implemented on AODV protocol adds two additional fields to the ROUTE REQUEST packet and one additional to the ROUTE REPLY packet. The first field added to the ROUTE REQUESTPACKET is the security requirement field and is set by the sender .It indicates the preferred level of trust for the path to the destination. The Second field added to is the security guarantee that signifies the maximum level of security provided by the discovered paths. If the security requirement field has an integer representation then the security guarantee field will be minimum of all security levels of the participating nodes in the path. If the security requirement field is represented in vectors then the security guarantee field value id computed by ANDing the security requirement values of the participating nodes in the path. The value thus computed is copied into additional security guarantee field of the ROUTE REPLY packet and sent back to the sender. This value is also copied into the routing table of nodes in the reverse path, to preserve the security information with reference to cashed paths

3.6.3 Features

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 hop-count. 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.

3.7 SLSP

3.7.1 Introduction

Secure Link State Routing Protocol (SLSP)[15] provides secure proactive topology discovery and can be used as either as a stand-alone protocol or as a part of Hybrid routing framework when combined with a reactive protocol.

3.7.2 Operation

To function effectively without central key management authority, SLSP enables each node to periodically broadcast its public key to nodes within its zone. In addition each node also broadcasts signed HELLO messages containing its medium access control address and IP address pair to its neighbors. The distribution of medium access control address strengthens the scheme by forbidding nodes from spoofing at the data link layer.

To achieve theses goals a Neighbor Lookup Protocol (NLP) is made an integral part of SLSP. The NLP is responsible for the following tasks.

Maintaining a mapping of MAC and IP layer addresses of the node's neighbors.
Identify potential discrepancies, such as the use of multiple IP addresses by a single data-link interface.
Measuring the rates at which control packets are received from each neighbor by differentiating the traffic primarily based on MAC address.
This rate of incoming control packets helps in discarding nodes which maliciously seek to exhaust network resources.

3.7.3 Features

i. SLSP can operate in the networks of recurrently changing topology and memberships.
ii. SLSP is resilient against individual attackers and is capable of altering its range between local and network wide topology discovery.
iii. SLSP employs a round robin servicing mechanism to provide the assurance the benign control traffic will be relayed even under clogging DoS attacks.

The comparison of all secured routing protocols is given in table 1.

4. SECURITY SERVICES

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

i. Authentication: This service [11,18] 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 [20,21] and certificates. Details of the construction and operation of digital signatures can be found in RFC2560 [19].
ii. Confidentiality: This service ensures that the data/information transmitted over the network is not disclosed to unauthorized users [16, 17]. Confidentiality can be achieved by using different encryption techniques such as only legitimate users can analyze and understand the transmission.
iii. 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.
iv. Access Control: This service limits and controls the access of such a resource, which can be a host system or an application.
v. Availability: This involves making the network services or resources available to the legitimate users. It ensures the survivability of the network despite malicious incidences.

5. CONCLUSION

As the available wireless networking and mobile computing hardware is now capable of fulfilling the promise of this technology .It is the need of the hour to design and develop routing protocols which should support the performance with endurance. The correct execution of these routing protocols is mandatory for smooth functioning of a MANET. A variety of protocols have been proposed targeted at securing MANETs but no performance comparison between these protocols has previously been available. In the presented work we have compared these protocols by highlighting their features, differences and characteristics. It can be summed up that each protocol has definite advantages and disadvantages, and can be appropriate for a particular application environment.

REFERENCES

[1] An Overview of the Bluetooth wireless technology", VIEEE Communication Magazine, vol. 39, no.12,pp. 86-94.December 2001.
[2] Brian P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, "IEEE 802.11 Wireless Local Area Networks", IEEE Communication Magazine, Vol. 35,N. 9, September 1997, pp. 116-126.
[3] A. Doufexi et al., "A Study of the Performance of HiperLAN/2 and 802.11a Physical Layers," IEEEVTC'01 Spring.
[4] C. E. Perkins (Ed.), Ad Hoc Networking, Addison-Wesley Longman, 2000.

[5] B. Dahill, B. N. Levine, E. Royer, C. Shields, 2002,"ARAN: A secure Routing Protocol for Ad Hoc Networks", UMass Tech Report 02-32.
[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc. 8th ACM Int'l. Conf. Mobile Computing & Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.
[7] C. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," ACM SIGCOMM,1994.
[8] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD:Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.
[9] D. B. Johnson et al, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet Draft, IETF MANET Working Group, March 2nd 2001.
[10] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2003http://standards.ieee.org/getieee802/download/802.11-1999.pdf - accessed 10/10/2006.
[11] A. Perrig, R. Canetti, J. Tygar, and D. Song,"The TESLABroadcast Authentication Protocol," RSA CryptoBytes, vol. 5 (Summer), 2002.
[12] P. Papadimitratos, Z. J. Haas, and P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. draft-papadimitratos-secure-routing- protocol- 00.txt, Dec. 2002.
[13] 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.
[14] 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.
[15] Papadimitratos,P., and Haas,Z., "Secure link state routing for mobile ad-hoc networks ," Proc. Of Symposium on Applications and the internet Workshops (SAINT'03), pp. 379-383, 2003.
[16] Narula P. and Dhurandher S. K. and Mishra S. and Woungang I., "Security in Mobile Ad hoc Network Using Soft Encryption and Trust Based Multipath Routing", Journal on Computer Communication, Vol. 31(4), pp. 760-769, 2008.
[17] Marie E. G. and Helvik B. E. and Knapskog S. J., "TSR Trust Based secure MANET routing using HMMs", 4th ACM symposium on QoS and Security for wireless and mobile networks (ACM Q2S Winet'08), pp. 83-90, 2008.
[18] 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.
[19] RFC 2560 www.ietf.org/rfc/ rfc2560.txt, last accessed on March 25,2007.
[20] 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.
[21] A K Verma, Mayank Dave, R C Joshi," SANE-DNA- A Novel Secure routing Algorithm, J. of discrete mathematics and cryptography vol. 11, issue4 pp.393-404,2008.

Table 1: Comparison of different secure routing protocols

Performance Parameters	**ARAIDNE**	**ARAN**	**SEAD**	**SRP**	**SAODV**	**SAR**	**SLSP**	**SANE-DNA**
Type	Reactive	Reactive	Proactive	Reactive	Reactive	Reactive	Proactive	Reactive
MANET Protocol	DSR	AODV/ DSR	DSDV	DSR/ ZRP	AODV	AODV	ZHLS	DSR
Encryption	Sym	Asym	Sym	Sym	Asym	Sym/Asym	Asym	Sym
Synchronization	Yes	No	Yes	No	No	No	No	Yes
Trust Authority	KDC	CA	CA	CA	CA	CA/KDC	CA/KDC	No
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Confidentiality	No	Yes	No	No	No	Yes	No	Yes
Integrity	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Non-repudiation	No	Yes	No	No	Yes	Yes	Yes	Yes
Anti-Spoofing	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
DoS Attacks	Yes	No	Yes	Yes	No	No	Yes	Yes

Table2. Operational requirements of the surveyed secure ad hoc routing solutions

.

Protocol	Requirements	Security Mechanism	Attacks Prevented	Comments
SEAD	*Clock synchronization, or a shared secret between each pair of nodes*	*One-way hash chains*	*Prevents an attacker from forging better metrics or sequence numbers in routing update packets*	*Used with DSDV* *- Designed to protect routing update packets* *- Does not prevent an attacker from tampering other fields or from using the learned metric and sequence number for sending new routing updates*
ARIADNE	*Clock synchronization and the existence of a shared secret between each pair of nodes. Also, an authentic TESLA key for each node in the network and an authentic route discovery chain element for each node for which this node will forward route requests. TESLA keys are distributed to the participating nodes via an online key distribution center*	*One-way hash chains*	*Prevents attackers from tampering un compromised routes consisting of uncompromised nodes* *- Immune to wormhole attack*	*Used with DSR* *- Provides a strong defense against attacks that modify and fabricate routing information* *- Prone to selfish node attack*
SAR	*Key distribution or secret sharing mechanism*	*Quality of Protection (QoP) metric*	*Uses sequence numbers and timestamps to stop replay attacks in routing update packets*	*Used with AODV* *- Route discovered may not be the shortest route in terms of hopcount, but it is always secured* *- Defends against modification and fabrication attacks*
SRP	*Existence of a security association between each source and destination node. Malicious nodes do not collude within one step of the protocol process.*	*Secure certificate server*	*Defends against attacks that disrupt the route discovery process and guarantees to identify the correct topological information*	*Used with DSR, ZRP* *- Lack of validation mechanism for route maintenance messages* *- Prone to wormhole attacks and invisible node attacks*
ARAN	*Online trusted certification authority. Each node knows a priori the public key of the CA*	*Secure certificate server*	*Provides network services like authentication and non-repudiation*	*Used with AODV, DSR* *- Heavy asymmetric cryptographic computation* *- Prone to wormhole attack if accurate time synchronozation is not*

				available

Table 3. Ad hoc Routing Parameters

Proposed Solutions	**Routing Approaches**	**Loop Freedom**	**Routing Metric**	**Shortest Path Identification**	**Intermediate Nodes Allowed to Reply to Route Requests**
ARAN	*On-demand*	*Yes*	*None*	*Optional*	*No*
SAR	On-demand	Depends on the selected security requirement	A security requirement	No	No
SRP	On-demand	Yes	Distance	No	Optional
SEAD	Table-Driven	Yes	Distance	No	No
ARIADNE	On-demand	Yes	Distance	No	No
CONFIDANT	On-demand	Yes	Path Reliability	Depends	No

AUTHORS:

Jaspal Kumar is currently a Ph. D. candidate in the department of Electronics and Communication Engineering at Delhi College of Engineering, Delhi (India). He received his B.E. and MTech. in 1992 and 2006. At present he is working as Asstt.Prof with BSAITM, Alampur ,Faridabad and coordinating the various activities related to the electronics department. He has more than 16 years of rich experience in Industry as well as in Academics. He has been in the designing Microprocessor based Circuits in USA. He has been a visiting faculty to many institutions**.** His research interests include wireless networks, Digital electronics and communication systems

Muralidhar Kulkarni received his B.E.(Electronics Engineering) degree from University Visvesvaraya College of Engineering, Bangalore University, Bangalore, M. Tech (Satellite Communication and Remote Sensing) from Indian Institute of Technology, Kharagpur (IIT KGP) and PhD from JMI Central University, New

Delhi in the area of Optical Communication networks. He has held the positions of Scientist in Instrumentation Division at the Central Power research Institute, Bangalore, Aeronautical Engineer in Avionics group of Design and Development team of Advanced Light Helicopter(ALH) project at Helicopter Design Bureau at Hindustan Aeronautics Limited(HAL),Bangalore, Lecturer (Electronics Engineering) at the Electrical Engineering Department of University Visvesvaraya College of Engineering, Bangalore and Assistant Professor in Electronics and Communication Engineering (ECE) Department at the Delhi College of Engineering (DCE), Delhi. He has served as Head, Department of Information Technology and Head, Computer Center at DCE , Govt. of National Capital territory of Delhi, Delhi. Currently, he is a Professor in the Department of Electronics and Communication Engineering (ECE) Department, National Institute of Technology Karnataka (NITK), Surathkal, Karnataka, India.

Dr. Kulkarni's teaching and research interests are in the areas of Digital Communications, Fuzzy Digital Image Processing, Adhoc networks, Wireless Sensor networks and Optical Communication & Networks. He has published several research papers in the above areas, in national and international journals of repute. For various contributions his Biography has been listed in the Marquis, Who's Who in Science & Engineering (2008). He has also authored four very popular books in Microwave &Radar Engineering, Communication Systems, Digital Communications and Digital Signal Processing.

Daya Gupta completed her Ph. D. in Computer Science. She joined Department of Computer Engineering at Delhi College of Engineering.where she is continuing as professor of CSE department and currently guiding BTech and MTech projects and dissertations and PhDs. She has published several research papers in referred journals and conferences. Her research interests include Computer Networks and Database Systems and ad-hoc networks**.**