International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.8, pp : 1094-1099 1 Aug 2014

Performance Analysis and Special Security Issues of Secure Routing Protocols in Ad-Hoc Networks

[1]Dr. P. Rajamohan [2]Mr. Wong Chee Kong
[1]Senior Lecturer, [2]Head of School - School of IT, SEGi University, Kota Damansara, PJU 5, PJ, Malaysia.
parthasarathy_rajamohan@yahoo.com & rajamohanp@segi.edu.my, ckwong@segi.edu.my

Abstract: ***An ad-hoc wireless network is a collection of wireless mobile nodes that self-configure to construct a network without the need for any established infrastructure or backbone. Ad hoc networks use mobile nodes to enable communication outside wireless transmission range. 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. Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. The analysis of the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. This paper presents the performance analysis and comparison of all the secure routing protocols principles with theirs characteristics, functionality, merits, demerits and security issues.***

Keywords: Ad-Hoc Networks, Routing, Security Attacks, MANETs- Mobile Ad-Hoc Wireless NETworks.

I. INTRODUCTION

There are two different types of wireless networks. Infrastructured network: A network with fixed and wired gateways. When a mobile unit goes out of range of one base station, it connects with new base station. Infrastructureless (ad hoc) networks: All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes. A MANET is an interconnected system of wireless nodes that communicate over bandwidth constrained wireless links. A Mobile Ad-Hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. 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[1]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. 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 multi-hop routing [1][2].

A Mobile Ad-Hoc NETwork (MANET) 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.

Operating in ad-hoc mode allows all wireless devices within the range of each other to discover and communicate in peer-to-peer fashion without involving central access. An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage. Ad-hoc networks cannot bridge to wire Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. The wireless nature of communication and lack of any security infrastructure raises several security problems[1]-[3].

The mobile ad hoc network has the following typical features:

- Unreliability of wireless links between nodes.
- Constantly changing topology.
- Lack of incorporation of security features.

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 MANETAs 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[4][5].

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. 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[4]. In this paper, an attempt is made to expose the various issues in order to have a secured MANET.

II. SECURITY ISSUES IN AD-HOC NETWORK

Security is an important issue for wireless networks, especially for those security sensitive applications. Several security mechanism were provided for confidentiality, authentication, and access control. The following seven types of security parameters are considered.

- **Identity:** An essential element in any security system is reliable, robust non-malleable identity.
- **Access control:** Access control is the constraint that limits those who can utilize system resources. Two approaches are used, one is called access control list (ACL) and other as closed network.

- **Authentication:** It ensures that communication from one node to other is genuine. Only legitimate users can access the system and services. Two used systems are open system and shared key.
- **Availability:** Availability ensures the service offered by node will be available to its users when expected, in spite of attacks. Also only legitimate users can access data anytime.
- **Integrity:** It protects nodes from maliciously altered messages. The receiver wants to be sure that the source is genuine. It assures the data, system or platform has not been tampered with.
- **Non repudiation:** It ensures that the origin of the message cannot deny having sent the message.
- **Confidentiality:** It ensures that certain information is never disclosed to unauthorized entities. Personal or sensitive data is protected[4].

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[5].

- **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[6].

2.1 Security Issues

2.1.1 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.

- 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.
- 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[6][7].

2.1.2 Security Privacy Issue

The identification issue simultaneously leads to privacy issue for MANET. Mobile node uses various types of identities and that varies forms of 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 it is essential to provide security architecture to secure ad hoc networking [6].

2.2 Ad-Hoc Routing Protocols Security Issues

The occurring routing protocols for Ad-Hoc networks deal effectively with something difficulty well with dynamically changing topology but are not designed to accommodate defense against intending attackers. Today's routing algorithms are not able to prevent from common security threats. Threats and attacks against ad hoc routing under several areas of application and suggested solutions that could be used when secure protocols are designed.

2.2.1 Types of Ad-Hoc Routing Protocols

Ad hoc network is a multi hop wireless network, which consists of number of mobile nodes. These nodes generate traffic to be forwarded to some other nodes or a group of nodes. Due to a dynamic nature of ad hoc networks, traditional fixed network routing protocols are not viable.

In general there are two types of routing protocols: Proactive and Reactive routing protocols. In Proactive Routing Protocols, the nodes keep updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and the Topology Broadcast based on Reverse Path Forwarding Protocol (TBRPF)[21]. In Reactive or On Demand Routing Protocols the routes are created only when they are needed. The application of this protocol can be seen in the Dynamic Source Routing Protocol (DSR) and the Ad-hoc On-demand Distance Vector Routing Protocol (AODV)[18].

In today's world the most common ad-hoc protocols are the Ad-hoc On-demand Distance Vector routing protocol and the Destination-Sequenced Distance-Vector routing protocol and the Dynamic Source Routing. All these protocols are quite insecure because attackers can easily obtain information about the network topology[7]-[9].

2.2.2 Types of Attacks Faced by Routing Protocols

Attacks arising from malicious behavior can be divided in to those where packets are originated by the malicious node and those where a malicious node is an intermediate node and receives control packets for forwarding. When a malicious node is originating packets, it can send control packets using its own source address, an address which belongs to an existing node in the ad hoc network, or an arbitrary address which does not belong to any node. Malicious intermediate nodes can either modify or replay received packets.

The relevant attack methods are:

- Masquerading as an existing node,
- Masquerading as a previously connected node,
- Replay attacks,
- Byzantine behavior to attract traffic,
- Byzantine behavior to deflect traffic, and
- Misdirection using a wormhole.

Conventionally, origin authentication mechanisms are needed to prevent masquerade attacks. In this we first analyze the inherent security of proactive and reactive protocols when origin authentication is not used for internal nodes, or when a malicious node has found a way to circumvent the mechanisms used for origin authentication. This can be achieved by sending false control packets using an incorrect source address; this address could either belong to a node currently routing in the network, or it could be an address which is not currently being used, perhaps of a node which was previously connected to the ad hoc network. Such false control packets are also referred to as spoofed packets. Due to their underlined architecture, ad-hoc networks are more easily attacked than a wired network[4]-[7].

The attacks prevalent on ad-hoc routing protocols can be broadly classified into passive and active 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 vital routing information by sniffing about the network. An Active Attack, however, injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified.

2.2.3 Attacks Against Ad-Hoc Routing Networks

While a wireless network is more versatile than a wired one, it is also more vulnerable to attacks. This is due to the very nature of radio transmissions, which are made on the air. The most prominent (important) attacks prevalent against ad hoc networks, most of which are active attacks. Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding / delivery. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path.

The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack.

- Impersonating another node to spoof route message. Advertising a false route metric to misrepresent the topology.
- Sending a route message with wrong sequence number to suppress other legitimate route messages.
- Flooding Route Discover excessively as a DoS attack. Modifying a Route Reply message to inject a false route.
- Generating bogus Route Error to disrupt a working route. Suppressing Route Error to mislead others.

Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages. There are some more sophisticated routing attacks, which include Wormhole attacks, Rushing attacks and Sybil attacks.

The second category of attacks against routing is attacks on packet forwarding/delivery, which are not easy to detect and prevented.

There are two main attack strategies in this 10 type: one is selfishness, in which the malicious node selectively drops route messages that are assumed to forward in order to save it own battery power; the other is denial-of-service[5]-[9].

2.2.3.1. Attacks Based on Modification

This is the simplest way for a malicious node to disturb the operations of an ad-hoc network. The only task the malicious node needs to perform, is to announce better routes (to reach other nodes or just a specific one) than the ones presently existing. This kind of attack is based on the modification of the metric value for a route or by altering control message fields. There are 3 ways in which this can be achieved:

Redirection by Changing the Route Sequence Number: When deciding upon the best / optimum path to take through a network, the node always relies on a metric of values, such as hop count delays etc. The smaller that value, the more optimum the path. Hence, a simple way to attack a network is to change this value with a smaller number than the last "better" value.

Redirection by Altering the Hop Count: This attack is more specific to the AODV protocol wherein the optimum path is chosen by the hop count metric. In general, an attacker would use a value zero to ensure to the smallest hop count. Taking for example the 'wormhole' attack, an attacker records packet at one location in the network, tunnels them to another location, and retransmits them there into the network. This could potentially lead to a situation where, it would not be possible to find routes longer than one or two hops, probably disrupting communication.

Denial of Service by Altering Routing Information: Consider, in a bus topology, a scenario wherein a node A wants to communicate with node E. At node A the routing path in the header would be A-B-C-D-E. If B is a Compromised node, it can alter this routing detail to A-B-C-E. But since there exists no direct route from C to E, C will drop the packet. Thus, A will never be able to access any service / information from E. Another instance can be seen when considering a category of attacks called 'The Black Hole Attacks'. It can then choose to drop the packets thereby creating DoS[1]-[4].

2.2.3.2 Impersonation Attacks

More generally known as 'spoofing', since the malicious node hides its' IP and or MAC address and uses that of another node. Since current ad-hoc routing protocols like AODV[18] and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. Take for example a situation where in an attacker creates loops in the network to isolate a node from the remainder of the network. To do this, the attacker needs to spoof the IP address of the node he wants to isolate from the network and then announce new route to the others nodes. By doing this, he can easily modify the network topology as he wants[10][12].

2.2.3.3. Attacks by Fabrication of Information

There are basically 3 sub categories for fabrication attacks. In any of the 3 cases, detection is very difficult.

Falsification of Rote Error Messages: This attack is very prominent in AODV and DSR, because these two protocols use path maintenance to recover the optimum path when nodes move. The weakness of this architecture is that whenever a node moves, the closest node sends an "error" message to the other nodes so as to inform them that a route is no longer accessible. If an attacker can cause a DoS attack by spoofing any node and sending error messages to the all other nodes. Thus, the malicious node can isolate any node quite easily[18][19].

Corrupting Routing State-Route Cache Poisoning: A passive attack that can occur especially in DSR due to the promiscuous mode of updating routing tables which is employed. This occurs when information stored in routing tables is deleted, altered or injected with false information. A node overhearing any packet may add the routing information contained in that packet's header to its own route cache, even if that node is not on the path from source to destination. If enough routes are created, new routes can no longer be added due to an overwhelming pressure on the protocol. A good routing protocol should also be able to detect the malicious nodes and to react in consequence, by changing routes[19][20].

III. PERFORMANCE ANALYSIS OF SECURE ROUTING PROTOCOLS AND COMPARISON

The various secured routing protocols along with the features of strengths and weaknesses they posses in terms of its operations. The comparison of the secured routing protocols as ARAN, ARIADNE, SEAD, SRP, SAODV, SAR, SLSP[9]-[23].

ARAN[13] 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.

ARIADNE[14] 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.

SEAD[17] 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 to 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.

SRP (Secure Routing Protocol) [9][22] 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.

SAODV (Secure Ad hoc On Demand distance Vector) [18][23] 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.

SAR (Security-Aware Ad-Hoc Routing)[9][14][15] 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.

SLSP (Secure Link State Routing Protocol)[9][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.

All the above secured routing protocols analysis and its comparison table has been attached below such as:

Table 1: Comparison of Different Secure Routing Protocols.
Table 2: Ad-Hoc secure Routing Protocols Parameters.

IV. AD-HOC NETWORKS SECURITY ISSUES SOLUTION AND TECHNIQUES

In order to provide solutions to the security issues involved in ad-hoc networks, we must elaborate on the two of the most commonly used approaches in use today such as Prevention Detection and Reaction.

1. Prevention Using Asymmetric Cryptography
Using Symmetric Cryptography
Using One-Way Hash Chain
2. Detection and Reaction.

Prevention dictates solutions that are designed such that malicious nodes are thwarted from actively initiating attacks. Prevention mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. Among the existing preventive approaches, some proposals use symmetric algorithms, some use asymmetric algorithms, while the others use one-way hashing, each having different trade-offs and goals.

Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. A node may misbehave by agreeing o forward packets and then failing to do so, because it is overloaded, selfish or malicious. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets. A malicious node launches a denial of service attack by dropping packets. All protocols defined in this category detect and react to such misbehavior.

The broad classifications of security solutions techniques as implemented by the way of security mechanism and how to prevent the attacks through such ad-hoc secure routing protocols as given in table 3[3][4][24].

Table3: Shown below an Operational Requirements of the Surveyed Secure ad-Hoc Routing Protocols Solutions Techniques.

V. CONCLUSION

The lack of infrastructure and of an organizational environment of mobile ad-hoc networks offers special opportunities to attackers. Mobile ad-hoc networks have properties that increase their vulnerability to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application specific trade-offs between security and resource consumption of the device. A prevention only strategy will only work if the prevention mechanisms are perfect; otherwise, someone will find out how to get around them Mobile ad-hoc networks have properties that increase their vulnerability to attacks. 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. Most of the attacks and vulnerabilities have been the result of bypassing prevention mechanisms. In view of this reality, detection and response are essential.

VI. REFERENCES

i. C. Siva Ram Murthy and B. S. Manoj, "Ad hoc Wireless Networks: Architectures and Protocols," by Prentice Hall PTR in 2004, pp. 191-223, 299-359.

ii. C.-k. Toh, "Ad hoc Mobile Wireless Networks: Protocols and Systems," by Prentice Hall PTR in 2002, pp. 13-25, 27-37, 57-77.

iii. Shih-Lin and Yu-Chee Tseg, "Wireless Ad Hoc Networking: Personal-Area, Local-Area and the Sensory-Area Network," Auerbach Publications, 2007, ISBN: 0- 8493-9254-3, pp. 535-571

iv. 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.

v. J.-P. Hubaux, L. Buttyan, S. Capkun,"The quest for security in mobile ad hoc networks", In The 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing, October 2001.

vi. D. B. Johnson et al, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet Draft, IETF MANET Working Group, March 2nd 2001.

vii. Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields,"A Secure Routing Protocol for Ad-Hoc Networks", In Proceedings of the 10 Conference on Network Protocols (ICNP), November 2002.

viii. Miguel A. Ortuno Perez, Vicente Matellan Olivera and Luis Rodera Merino, "Abbreviated Dynamic Source Routing: Source Routing with Non-Unique Network Identifiers," at University of Rey Juan Carlos, Mostoles, Madrid, Spain.

ix. Jaspal Kumar, M. Kulkarni, Daya Gupta "Secure Routing Protocols In Ad Hoc Networks: A Review", Special Issue of IJCCT Vol. 2 Issue 2, 3, 4; 2010 for International Conference [ICCT-2010], 3rd-5th December 2010

x. Zulfiqar Ali, "Performance Comparison of Ad Hoc Routing Protocols," at Brunel University, School of Engineering & Design Electronics & Computer Engineering, February 2007.

xi. Tomoyuki Ohto, Munehiko Fujimoto, Shinji Inoue and Yoshiaki Kakuda, "Hi- Tora: A Hierarchical Routing Protocol in Ad Hoc Networks," at Hiroshima City University, Department of Computer Engineering, Hiroshima 731-3194, Japan.

xii. Masayuki Tauchi, Tetsuo Ideguchi and Takashi Okuda, "Ad-Hoc Routing Protocol Avoiding Route Breaks Based on AODV," at proceedings of 38th Hawaii International Conference on System Sciences, 2005

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

xiv. 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.

xv. IS.Venkata Lakshmi, IID. Kusumalatha, "Security Issues in Wireless Ad-Hoc Network Routing Protocols". International Journal of Advanced Research in Computer Science & Technology (IJARCST), Vol. 1 Issue 1 Oct-Dec 2013

xvi. C. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," ACM SIGCOMM,1994.

xvii. 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.

xviii.. Jin-Man Kim, Jong-Wook Jang, "AODV based Energy Efficient Routing Protocol for Maximum Lifetime in MANET," at Dong-Eui University, Department of Computer Engineering, 995 Eomgwangno, Busanjin-gu, Busan, Korea.

xix. David B. Johnson, David A. Maltz and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," at Carnegie Mellon University, Computer Science Department, Pittsburgh, PA 15213-3891

xx. Ana Cavalli, Cyril Grepet, Stephane Maag and Vincent Tortajada, "A Validation Model for the DSR Protocol," at Institute of National Telecommunications, 9 rue Charles Fourier F-91011 Evry Cedex, France.

xxi. Jean-Marie Orset and Ana Cavalli, "A Security Model for OLSR MANET Protocol," at Institute of National Telecommunications, 9 rue Charles Fourier, F- 91011 Every Cedex, France.

xxii. P. Papadimitratos, Z. J. Haas, and P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. draftpapadimitratos-secure-routing- protocol-00.txt, Dec. 2002.

xxiii. 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.

xxiv. 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.

Table 1: Comparison of Different Secure Routing Protocols

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

Table 2: Ad- Hoc Secure Routing Protocols 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	Optional	No
SEAD	Table-Driven	Yes	Distance	No	No
ARIADNE	On-demand	Yes	Distance	No	No
CONFIDANT	On-demand	Yes	Path Reliability	Depends	No

Table 3: Operational Requirements of the Surveyed Secure Ad- Hoc Routing Protocol Solutions Techniques.

Protocol	Requirements	Security Mechanis	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
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 Uncompromised 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 hop-count, 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 on repudiation.	Used with AODV, DSR - Heavy asymmetric cryptographic computation - Prone to wormhole attack if accurate time synchronization is not available.