Secure Routing with the DSR Protocol

Asad A. Pirzada and Chris McDonald

School of Computer Science and Software Engineering
The University of Western Australia
35 Stirling Highway, Crawley, WA 6009, Australia

Abstract. An ad-hoc network is a spontaneous network that emerges when two or more wireless nodes pledge to help each other. As the wireless range of these nodes is usually limited so each node commits to forward the packets on behalf of its neighbours in accordance with a predefined routing protocol. Dynamic Source Routing (DSR) is one of the widely used routing protocols that is currently undergoing extensive research and development. DSR is based on source routing, but the routes are discovered not on a periodic basis but on an as per requirement basis. The control and data packets traverse the network in accordance with the list of IP addresses held by each packet. As this list is mutable, it creates a potential vulnerability that is frequently exploited by malicious nodes. By adding, deleting or modifying IP addresses in the list, malicious nodes can control and monitor the flow of network traffic. Similarly, transmission of routing packets in clear text, also discloses vital information about the network topology, which is again a potential security hazard. This necessitates that the routing and data packets must be obscured and authenticated prior to usage. In this paper we present a novel and pragmatic scheme for securing the Dynamic Source Routing protocol that protects against a number of attacks carried out against mobile ad-hoc wireless networks.

1 Introduction

Present ad-hoc wireless networks make use of the Internet Protocol (IP) at the network layer primarily due to standardization and compatibility reasons. This also facilitates to integrate ad-hoc networks with wired networks and a multitude of other hardware devices using IP in the protocol stack. Each node of the ad-hoc network acts similar to a mobile IP router [1] and endeavours to uphold a reliable flow of network traffic. Due to a variety of factors including dynamic topology, energy constraints and uni-directionality of the links, standard intra-router protocols cannot be directly applied to mobile ad-hoc wireless networks. In addition, as the routers are moving majority of the time, the network is void of any single traffic concentration point, a basic requirement of all standard routing protocols. Several types of routing protocols have been specially developed for ad-hoc networks and have been classified into two categories as Reactive and Proactive [2]. In Reactive Routing Protocols, in order to conserve a node's

A. Pirzada A. and McDonald C. (2004).
Secure Routing with the DSR Protocol.
In *Proceedings of the 3rd International Workshop on Wireless Information Systems*, pages 24-33
DOI: 10.5220/0002676200240033

battery, routes are only discovered when required, while in Proactive Routing Protocols routes are established prior to use and hence avoid the latency delays incurred while discovering new routes. For effective operation, routing protocols for ad-hoc networks require that all participating nodes display benevolent behaviour. This is more than often difficult to achieve in open networks and requires some out-of-band mechanism for establishing and maintaining trust in the network [3]. Cryptographic mechanisms are still a major tool enforcing mutual trust relationships among the wireless nodes for the protection of routing protocols.

Security in mobile ad-hoc wireless networks is a two-fold problem. One is the security of the routing protocols that enable the nodes to communicate with each other and the second is the protection of the data that traverses the network on routes established by the routing protocols. In this paper after Introduction, in Section 2 we describe some recent secure routing protocols for ad-hoc networks, which were developed to counter known attacks. In Section 3 we recommend a scheme for securing the Dynamic Source Routing protocol. A security analysis of the proposed scheme is presented in Section 4 and Section 5 offers some concluding remarks.

2 Previous Work

To protect an ad-hoc network from modification, impersonation and fabrication attacks [4] a routing protocol must fulfil a set of requirements [5] to ensure that the discovered path from source to destination functions properly in the presence of malicious nodes. A number of secure routing protocols have been recently developed that conform to most of the requirements. A comparison of these protocols [6] revealed that the secure routing protocols employ a variety of cryptographic tools to protect the underlying routing protocol. However, these protocols have been developed as a practical response to specific problems that arose due to attacks on ad-hoc network routing protocols. Consequently, these protocols only cover a subset of all possible threats and are not flexible enough to be integrated with each other. Some of the recent secure routing protocols are explained in the following sub-sections.

2.1 ARIADNE

ARIADNE [4] is an on-demand secure ad-hoc routing protocol based on the Dynamic Source Routing (DSR) protocol that protects against node compromise and relies only on extremely efficient symmetric cryptography. The security of ARIADNE is based upon the secrecy and authenticity of keys that are kept at the nodes. ARIADNE prevents a large number of Denial-of-Service attacks from malicious or compromised nodes. ARIADNE provides assurance that the target node of a route discovery process can verify the initiator, that the initiator can verify each transitional node that is on the path to the destination present in the `ROUTE REPLY` message and that no intermediate node can reduce the

node list in the ROUTE REQUEST or ROUTE REPLY messages. Route Discovery is performed in two stages: the Initiator floods the network with a ROUTE REQUEST that solicits a ROUTE REPLY from the Target. During route discovery the Target authenticates each node in the node list of the ROUTE REQUEST and the Initiator authenticates each individual node in the node list of the ROUTE REPLY. For node authentication, ARIADNE has three alternative techniques i.e. TESLA (Timed Efficient Stream Loss tolerant Authentication) [7], Digital Signatures, or pair-wise shared secret keys.

2.2 ARAN

The Authenticated Routing for Ad-hoc Networks (ARAN) [5] secure routing protocol is an on-demand routing protocol that identifies and shields against malevolent actions by malicious nodes in ad-hoc networks executing the DSR protocol. ARAN relies on the use of digital certificates and can successfully operate in the managed-open scenario where no network infrastructure is pre-deployed, but a small amount of prior security coordination is expected. ARAN provides authentication, message integrity and non-repudiation in ad-hoc networks by using a preliminary certification process that is followed by a route instantiation process that guarantees end-to-end provisioning of security services. ARAN requires the use of a trusted certificate server. All nodes are supposed to keep fresh certificates with the trusted server and should know the server's public key. Prior to entering the ad-hoc network, each node has to apply for a certificate that is signed by the certificate server. The certificate contains the IP address of the node, its public key, a timestamp of when the certificate was generated and a time at which the certificate expires, along with the signature by the certificate server. ARAN accomplishes the discovery of routes by a broadcast route discovery message from a source node, which is replied to in a unicast manner by the destination node. All the routing messages are authenticated at every hop from the source to the destination, as well as on the reverse path from destination to source

3 Securing the DSR Protocol

3.1 DSR Protocol

The DSR protocol [8] is an on-demand routing protocol. Its most interesting feature is that all data packets sent using the DSR protocol have absolutely no dependency on intermediate nodes regarding routing decisions, as each carries the complete route it traverses. When a node requires a route to a particular destination, it broadcasts a ROUTE REQUEST packet. Each recipient node that has not seen this specific ROUTE REQUEST and has no knowledge about the required destination rebroadcasts this ROUTE REQUEST after appending its own address to it. If this ROUTE REQUEST reaches the destination or an intermediate node that has a route to the destination in its ROUTE CACHE, it sends a ROUTE REPLY

packet containing the complete route from the source to the destination. The source node may receive a number of such route replies and may decide to select a particular route based upon the number of hops, delay or other such criteria. All nodes forwarding or overhearing any packets must add all usable routing information from that packet to their own `ROUTE CACHE`. For route maintenance, intermediate nodes that find any route broken, returns a `ROUTE ERROR` packet to each node that had sent a packet over that particular route. The major vulnerabilities present in the DSR protocol are:

Deceptive alteration of IP addresses. During propagation of the `ROUTE REQUEST` packet, intermediate nodes add their IP addressees to it for route creation. However, any malicious node may modify, delete or add IP addressees to create routes as per its own requirement. Doing so enables malicious nodes to launch a variety of attacks in the network including creation of worm-holes and black-holes.

Deceptive alteration of Hop Count. The hop count field of the IP packet usually informs the recipient of the total number of hops that the packet has traversed so far. So malicious nodes may increase this number so as to portray longer routes or decrease it for shorter routes. By doing so a malicious node is able to degrade or upgrade routes, thereby creating a topology that is most favourable to it.

3.2 Secure DSR Protocol

Securing the DSR protocol can be divided into the following three broad categories:

1. Key Exchange
2. Secure Routing
3. Data Protection

Key Exchange. Most of the current key exchange protocols are dependent upon a central trust authority for initial authentication. A variant of the central trust authority is the Distributed Public-Key Model [9] that makes use of threshold cryptography to distribute the private key of the Certification Authority (CA) over a number of servers. Whatever the case may be, the requirement of a central trust authority in such a dynamic environment is considered both impractical and unsafe, as such an entity may not always be accessible and it also creates a single point of failure. Similarly, key exchange using a Key Distribution Server [10] creates a similar set of problems. We suggest that all nodes, before entering a network, procure a one-time public and private key pair from the CA along with the CA's public key. After this, the nodes can negotiate session keys among each other, without any reliance on the CA, using any suitable key exchange protocol for ad-hoc networks [11]. These session keys are used for

securing the routing process and subsequently the data flow. To avoid multiple peer-to-peer encryptions during broadcast or multicast operations, a group session key may be established between immediate neighbours using a suitable Group Keying Protocol [11]. This mechanism absolves the ad-hoc network of superfluous requirements and provides necessary elements to secure both routing and data in presence of malicious nodes by providing security services like authentication, non-repudiation, confidentiality and integrity.

Secure Routing. The Dynamic Source Routing protocol operates at the second layer of the TCP/IP protocol suite. The source node that requires a route to a destination broadcasts a `ROUTE REQUEST` packet, each intermediate recipient node retransmits the packet, if not a duplicate, and the final destination unicasts a `ROUTE REPLY` packet back to the original sender. For route maintenance it uses `ROUTE ERROR` packets that inform active users of route failures. The `ROUTE REQUEST` and `ROUTE REPLY` packets are usually modified by the intermediate nodes so as to add necessary routing information to these packets. The core security related problems linked to ad-hoc networks originate due to the route development by the intermediate nodes. It is therefore, imperative that only authorized nodes are allowed to update routing packets and malicious nodes be avoided at all costs. To restrict modification of routing packets by intermediate nodes, we recommend peer-to-peer symmetric encryption of all routing information. All routing control packets between nodes are first encrypted and then transmitted. The sequence of steps for route discovery and route maintenance is as follows:

Route Request

1. Any Node 'x' desiring to establish communication with another Node 'y' first establishes a group session key K_x with its immediate neighbours (nodes that are a single hop away) as shown in Fig. 1.
2. It then creates the `ROUTE REQUEST` packet as per the routing protocol specifications.
3. The `ROUTE REQUEST` packet is then encrypted using the group session key K_x and broadcasted.
4. All intermediate recipient nodes that share the same group session key decrypt the `ROUTE REQUEST` packet and, if required, modify it according to the routing protocol specifications.
5. The intermediate nodes that do not possess group session keys with their immediate neighbours, initiate the group session key exchange protocol.
6. After establishing the group session key, the intermediate nodes encrypt the `ROUTE REQUEST` packet using the new session key and rebroadcast the packet.
7. Steps 4 to 6 are followed until the final destination Node 'y' receives the packet.

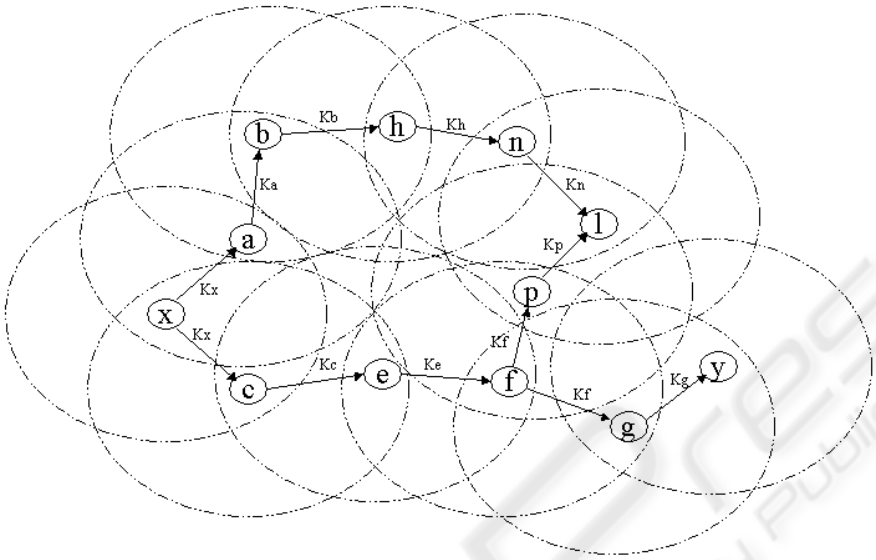

Fig. 1. Point-to-Point Establishment of Secure Routes

Route Reply

1. In response to the `ROUTE REPLY` packet Node 'y' creates a `ROUTE REPLY` packet as per the routing protocol specifications.
2. The `ROUTE REPLY` packet is encrypted using the last group session key (K_g in this case) that was used to decrypt the received `ROUTE REQUEST` packet and is unicast back to the original sender.
3. If any of the intermediate nodes has moved out of the wireless range a new group session key is established.
4. All recipient nodes that share the forward group session key decrypt the `ROUTE REPLY` packet and, if required, modify it according to the routing protocol specifications.
5. The `ROUTE REPLY` packet is then again encrypted using the backward group session key and unicast towards Node 'x'.
6. Steps 4 and 5 are repeated until the packet is received by Node 'x'.

To avoid key synchronization problems it is recommended that each node maintain a table indexed by Node ID as the primary key along with associated group members and session keys as shown in Fig. 2. The table also helps establish secure routes with other nodes with which a chain can be established using the available session keys. A secure chain is highlighted in the figure between Node 'x' and 'y'.

Route Maintenance. In a mobile ad-hoc network, established routes may be broken due to a variety of reasons. However, the underlying routing protocol

		Destination											
Source	ID	a	b	c	e	f	g	h	l	n	p	x	y
	a		K_a									K_x	
	b	K_a						K_b					
	c				K_c							K_x	
	e			K_c		K_e							
	f				K_e		K_f				K_f		
	g					K_f							K_g
	h		K_b							K_h			
	l									K_n	K_p		
	n							K_h	K_n				
	p					K_f			K_p				
	x	K_x		K_x									
	y						K_g						

Fig. 2. Session Key Table

takes care of such events by either gratuitously repairing them or sending a `ROUTE ERROR` packet to inform the nodes currently using the route. All messages associated with route maintenance also need to be authenticated and protected from eavesdropping. If a packet is received for an inoperative route the recipient node takes the following steps:

1. The node detecting the broken link creates a `ROUTE ERROR` packet as per the routing protocol specifications.
2. This packet is then encrypted using a group session key in the direction of the recipient node using the Session Key Table and is multicast back to the recipients.
3. If any of the intermediate nodes has moved out of the wireless range a new group session key is established.
4. All recipient nodes that share the group session key decrypt the `ROUTE ERROR` packet, and if required, modify it according to the routing protocol specifications.
5. The `ROUTE ERROR` packet is then again encrypted using the group session key and is multicast back to the recipients.
6. Steps 4 and 5 are repeated until the intended recipients receive the `ROUTE ERROR` packet.

Data Protection. Once protected routes have been established, secure data transfer is relatively straightforward. To ensure connection confidentiality a source node adopts the following steps:

1. Any node 'x' desiring to establish an end-to-end secure data channel, first establishes a session key K_{xy} with the intended node 'y' using the key exchange protocol as shown in Fig. 3.
2. It then symmetrically encrypts the data packet using the session key K_{xy} and transmits it over the secure route.
3. The intermediate nodes simply forward the packet in the intended direction.
4. When the encrypted data packet reaches the destination it is decrypted using the session key K_{xy}.
5. Steps 2 to 4 are followed for all further data communication.

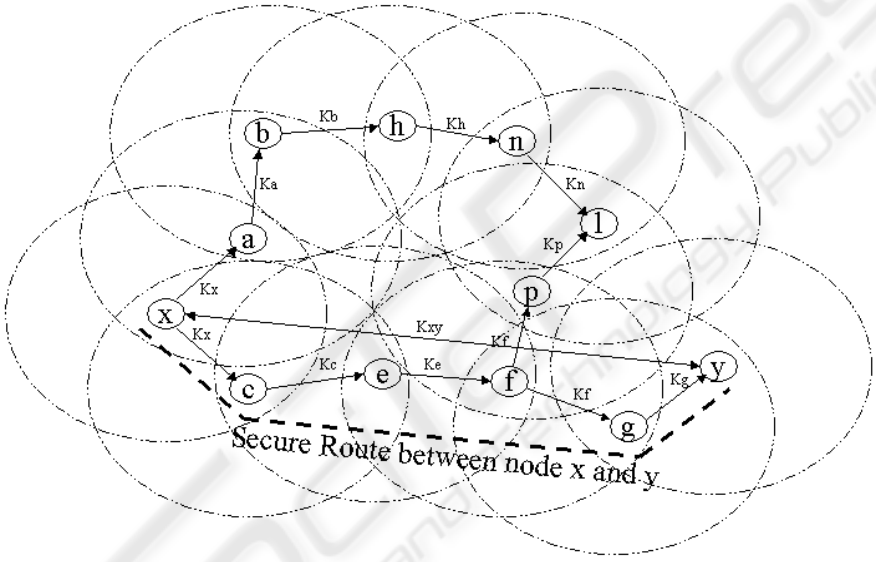

Fig. 3. End-to-End Establishment of Secure Routes

4 Security Analysis

In this section we discuss how the presented security scheme defies possible attacks in an ad-hoc network. As discussed earlier, the basis of a security infrastructure is primarily dependent on the initial key exchange providing authentication. Other security services like confidentiality, integrity and non-repudiation all rely on the accuracy of the authentication service. Key revocation, being an important issue has not been addressed in the scope of this paper, primarily because it requires the presence of an omnipresent, and often omniscient, trust authority, which we have already deemed inappropriate for such a dynamic environment. We now discuss how this scheme satisfies the seven requirements of any secure routing protocol:

4.1 Authorized nodes to perform route computation and discovery

The authentication and key exchange protocol ensures that only authorised nodes are able to perform the route discovery. As the routing control packets are encrypted and authenticated by each forwarding node, malicious nodes will not be able to create fallacious routing packets.

4.2 Minimal exposure of network topology

As all routing information is encrypted between nodes, an adversary will gain no information regarding the network topology from passive eavesdropping.

4.3 Detection of spoofed routing messages

Spoofing of either the MAC or IP addresses does not provide any benefit to the adversary until the time the authentication protocol is assumed to be secure. As the initial authentication links a number of identities to each node's private key, the spoofing node will have to create a similar private key prior to launching any attack.

4.4 Detection of fabricated routing messages

Malicious nodes cannot inject fabricated routing messages into the network as each routing packet is secured through an encryption key, which provides the benefit of confidentiality, authentication and integrity at the same time. To fabricate a routing message the session key needs to be compromised, which is not possible until the time the key exchange protocol is assumed to be secure.

4.5 Detection of altered routing messages

Routing messages are relayed between the nodes in an unintelligible format. If the symmetric cipher also provides the integrity then the alteration of routing messages is virtually impossible. Addition of a keyed hash for better integrity checking may be considered only after a cost-benefit analysis.

4.6 Avoiding formation of routing loops

The proposed scheme ensures that routing loops cannot be formed through malicious action. Routing loops usually occur if a malicious node is able to spoof, alter or fabricate legitimate routing packets.

4.7 Prevent redirection of routes from shortest paths

Shortest paths are created usually by decrementing the number of addresses in the source routing protocol. The scheme is designed in such a manner that routing packets are only accepted from authenticated immediate neighbours. This ensures that an adversary cannot inject such routing packets unless an authorised node first authenticates it.

5 Conclusion

In this paper we have presented a scheme for securing the Dynamic Source Routing protocol used in mobile ad-hoc wireless networks. The secure DSR protocol provides requisite measures for protection of route discovery and transfer of data. These measures can be exercised independently without a central trust authority with nodes negotiating session keys independently. Nodes are, however, required to register themselves once with a Certification Authority, prior to joining a network. The scheme is based upon point-to-point and end-to-end encryption using symmetric key-based mechanisms. Nodes desiring secure communication, execute any standard authentication and key exchange protocol to acquire session keys. These keys are subsequently used in point-to-point encryption for route discovery and end-to-end encryption for data packets. Malicious nodes trying to launch passive or active attacks against the network are thwarted through efficient key verification mechanisms and a multi-layered enciphering scheme. To highlight its viability we have discussed its resistance to a number of attacks specific to ad-hoc networks.

References

1. Corson, S., Macker, J.: Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETF RFC 2501 (1999)
2. Royer, E.M., Toh, C.-K.: A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. IEEE Personal Communications Magazine, Vol. 16(2) (1999) 46–55
3. Pirzada, A.A., McDonald, C.: Establishing Trust In Pure Ad-hoc Networks. Proc. of 27th Australasian Computer Science Conference (ACSC04) Vol. 26(1) (2004) 47–54
4. Hu, Y-C., Perrig, A., Johnson, D.B.: Ariadne - A Secure On-Demand Routing Protocol for Ad Hoc Networks. Proc. of MOBICOM (2002) 12–23
5. Dahill, B., Levine, B.N., Royer, E., Shields, C.: ARAN - A Secure Routing Protocol for Ad Hoc Networks. Proc. of ICNP (2002) 78–87
6. Pirzada, A.A., McDonald, C.: A Review of Secure Routing Protocols for Ad hoc Mobile Wireless Networks. Proc. of 7th International Symposium on DSP for Communication Systems (DSPCS03) and 2nd Workshop on the Internet, Telecommunications and Signal Processing (WITSP03) (2003) 118–123
7. Perrig, R., Canetti, D., Tygar, Song, D.: The TESLA Broadcast Authentication Protocol. RSA CryptoBytes (2002) 2–13
8. Johnson, D.B., Maltz, D.A., Hu, Y.: The Dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR). IETF MANET, Internet Draft (2003)
9. Zhou, L, Haas, Z.J.: Securing Ad Hoc Networks. IEEE Network Magazine Vol. 13(6) (1999)
10. Pirzada, A.A., McDonald, C.: Kerberos Assisted Authentication in Mobile Ad-hoc Networks. Proc. of 27th Australasian Computer Science Conference (ACSC04) Vol. 26(1) (2004) 41–46
11. Carman, D.W., Kruus, P.S., Matt, B.J.: Constraints and approaches for distributed sensor network security. Technical Report #00-010, NAI Labs (2000)