# Hash Chains at the Basis of a Secure Reactive Routing Protocol

Thouraya Bouabana-Tebibel

National School of Computer Science
Laboratory of Communication in Informatics Systems
Algiers, Algeria
t_tebibel@esi.dz

**Abstract.** Presently, the main concern of ad hoc routing protocols is no longer to find an optimal route to a given destination but to find the safe route free from malicious attackers. Several secure ad hoc routing protocols proposed, in the literature, are based on public key cryptography which drawback is to consume much more resources and decrease consequently network performances. In this paper, we propose a secure routing scheme for the DSR protocol. The proposed scheme combines the hash chains and digital signatures to provide a high level of security while reducing the costs of hop-by-hop signature generation and verification. The proposed protocol is analyzed using the NS-2 simulator.

**Keywords:** DSR, routing protocols, mobile ad hoc networks, hash chains, digital signature.

## 1 Introduction

MANET or Mobile Ad hoc Network is a set of wireless mobile nodes, forming a temporary network without the use of any fixed infrastructure. Each node acts as a router (relay) and data packets are forwarded from node-to-node towards their destination in a multi-hop fashion. Ad hoc routing protocols have been designed to be more and more efficient without keeping security in mind. This makes them vulnerable to a variety of attacks which affect the reliability of data transmission. So, the present question is no longer to find an optimal route to a given destination but to provide a safe route free from malicious attackers.

In fact, most of ad hoc routing schemes provide no security system. All entities can participate in routing and there are no barriers for a malicious node to cause traffic disruptions. The attacker wants essentially to affect the routing process, in order to control the network and destroy routing operations [19,21]. He achieves his objectives by: message alteration, message fabrication, message replay and impersonation. In [22] a classification of insider attacks against mobile ad-hoc routing protocols is presented. It includes route disruption, route invasion, node isolation, and resource consumption.

L. Chen, M. Yung, and L. Zhu (Eds.): INTRUST 2011, LNCS 7222, pp. 258–270, 2012.

Some solutions are proposed to secure the most important routing protocols against those attacks [4,6,7,11,13,17,18,28]. But they remain incomplete, blocking only a subset of attacks among all those well-known for the damage they cause to the networks. On the other hand, each secure scheme defines an appropriate environment of execution and presupposes a number of satisfied hypotheses to ensure its successful running. Indeed, protocols based on cryptography require a mechanism of key distribution and management [19]. Furthermore, when efficient, the used techniques are often too expensive in time calculation and memory space.

As a compromise, protocols based on reputation [9] integrate a new metric, the level of reliability of the route, to select the path towards destination. This reduces considerably the solution cost by diminishing calculation intensity.

As for intrusion detection systems, they can reduce the risks of intrusion but cannot completely eliminate them [23]. They also, sometimes fail with application of solutions as punishment of selfish nodes or location of malicious nodes which continuously change identity [29].

In terms of reliability, most of solutions rely on asymmetric cryptography and certificates delivered on line by authorities of certification. Message authentication and integrity are realized using digital signature [32]. When applied at each hop, they degrade the system performance.

DSR is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets. Another advantage of the DSR protocol is the very rapid recovery when routes change in the network. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes and is designed to work well even with very high rates of mobility.

The aim of our work is to protect the DSR protocol routing messages by using strong cryptographic functions and keeping in mind as main objective, minimization of complex calculation burden. This will be achieved by means of two essential mechanisms. The first one relies on hash chains which consume a little time for their generation and require a minimal storage space. The second one is digital signature that reinforces authentication and ensures integrity, and non-repudiation of messages. The latter is only applied on the source and destination nodes to reduce the latency.

The remainder of the paper starts with a brief description of the reactive routing protocol DSR. Section 3 deals with the core of our secure routing scheme SRS_DSR. We simulate in section 4 the performance of the proposed protocol using NS-2 simulator. In Section 5, we discuss works related to ours. We conclude by motivating our work and showing its novelty and relevance versus related works.

## 2 DSR Protocol

DSR (Dynamic Source Routing) is a routing protocol based on Distance-Vector routing algorithm [14,15]. It is reactive involving route construction only when data are available for transmission. The protocol is composed of the two main mechanisms

of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network.

When a source node needs to determine a route to a destination node, it broadcasts a request message RREQ (Route REQuest). Intermediate nodes add their address to the packet and then broadcast it. When the request reaches the destination, or an intermediate node with an active route towards the destination, it generates a reply message RREP (Route REPly).The answer is sent unicast to the source following the reverse path, already built by the intermediate nodes.

RREQ packet format is shown in fig. 1. Option Type specifies that the packet is a RREQ. Opt Data len gives the packet length. Identification is a sequence number generated for each Route Request. It allows a receiving node to discard the RREQ in the case it has recently seen a copy of this Request. Target Address is the destination node address. Address[i] is the address of the i-th node recorded in the Route Request option. Each node propagating the Route Request adds its own address to this list, increasing the Opt Data Len value by 4 octets.

| Option Type | Opt Data Len | Identification |
|---|---|---|
| Target Address | | |
| Address [1] | | |
| … | | |
| Address [n] | | |

**Fig. 1.** RREQ packet format

RREP packet format is shown in fig. 2. It is composed of the same fields as RREQ excluding the Target Address and including a Reserved field and the Last hop external field which indicates that the last hop given by the Route Reply (the link from Address[n-1] to Address[n]) is actually an arbitrary path in a network external to the DSR network.

| Option Type | Opt Data Len | Last hop ext | Reserved |
|---|---|---|---|
| Address [1] | | | |
| … | | | |
| Address [n] | | | |

**Fig. 2.** RREP packet format

Link breaks are detected according to two ways. The first one occurs during the unicast reverse routing when a node reveals to be unreachable. The second way is based on information directly received from the MAC sub-layer. If a link breaks within an active route, the node involved before the link break may choose to repair locally the link or deliver an error message RERR (Route ERRor) listing the unreachable destinations. Thus, a new route discovery phase should be established by the source node [25].

As basic DSR scheme provides no security mechanism, malicious nodes can disturb the routing process. Table 1 summarizes the consequences of attacks affecting DSR control packets.

**Table 1.** Attacks against dsr

| Target field | Attack |
|---|---|
| Target Address | The attacker creates routes to unavailable destinations in order to consume the network energy. |
| Identification | The attacker increments this field to invalidate any future requests from a legitimate node. He decrements it so as to the request will be considered as already processed. |
| Address [1..n] | The attacker modifies the addresses or alters their order. |

# 3 SRS_DSR Solution

## *3.1* Basic Assumptions

The protocol is based on the following assumptions:

- a packet sent from node A is received by the latter one hop neighbor B before a third node C replays the packet to B.
- a trusted Certification Authority performs the pre-distribution of both private key and X509v3 certificate [8] to each member of the network through a physical contact. The conventional certificate X509v3 contains the public key, the identity of the certificate owner and other fields. All these fields are encrypted by means of a digital signature integrated to the certificate.

## *3.2* Proposed Scheme

The solution which we propose integrates security mechanisms that take into account the limited resources of nodes. These mechanisms are not based on unrealistic assumptions such as availability of an always-online security infrastructure (trusted third-party).

Our approach is inspired from Lamport authentication algorithm [16] used in remotely accessed computer systems. Authentication described by Lamport was designed for a client/server architecture where the management is centralized. In Lamport authentication, a server randomly chooses a password $H_n$. Afterwards, he applies to $H_n$, n times, a one-way function h to get n passwords ($H_{n-1}$, $H_{n-2}$, …, $H_1$, $H_0$) called One Time Password sequence or OTP, for short.

$$H_n \rightarrow h(H_n) = H_{n-1} \quad \rightarrow h(H_{n-1}) = H_{n-2} \quad \rightarrow h(H_{n-2}) = H_{n-3} \quad \ldots \quad \rightarrow h(H_1) = H_0$$

We were attracted by the effectiveness of hash functions because they reduce the high costs caused by traditional cryptographic mechanisms. Thus, we combined the use of hash chains authentication with digital signatures to achieve a satisfying security level. We adopt the notations of table 2.

**Table 2.** Notations

| Symbol | Signification |
|---|---|
| $SK_A$, $PK_A$ | Private key. Public key of node A |
| $[d]SK_A$ | Signature of a message with the private key of A |
| $Cert_A$ | A certificate belonging to node A |
| $ID_A$ | Node A identifier |
| $H_j^A$ | The $j^{th}$ element of the hash chain of node A |

The security process we propose is divided into two phases: initialization phase and authentication phase.

### 3.2.1 Initialization Phase

As set in the basic assumptions, a trusted certification authority performs the pre-distribution of one certificate and one private key to each member of the network. Each entity A, identified by an $ID_A$, constructs its own OTP sequence and broadcasts the last value $H_0^A$ to its one-hop neighbors. In order to ensure the provenance authenticity of $H_0^A$, we propose what follows. Node A first signs $H_0^A$ using its private key and then transmits the clear $H_0^A$ and signature $[H_0^A]SK_A$ as well as its identity $ID_A$ and certificate $Cert_A$ to all one-hop neighbors, refer to (1). Each neighbor decrypts the encrypted $H_0^A$ using the public key of node A transmitted within $Cert_A$. To ensure that the decrypted value is authentic and so, effectively transmitted by node A, the receiver compares it with the unencrypted value $H_0^A$. If the comparison matches, node A identity and $H_0^A$ integrity are proved true. So, $H_0^A$ value is saved in a new entry of the Neighbors table which keeps the $H_0^A$ value of each neighbor. The comparison fails if either the sender authenticity or $H_0^A$ integrity is compromised. In both cases, the message is ignored.

The one-hop neighbors also send the last values of their own hash chain and certificates to node A, see (2). At the end of this step, each node knows the $H_0$ value of its one-hop neighbors.

$$A \rightarrow \text{Broadcast} \quad \text{PWD} : \{ID_A, H_0^A, [H_0^A]SK_A, Cert_A\} \tag{1}$$

$$V \rightarrow A \quad \text{PWDREP}: \{IDv, H_0^V, [H_0^V]SK_V, Cert_V\} \tag{2}$$

### 3.2.2 Authentication Phase

Control packets RREQ, RREP and RERR are used to construct and maintain routes from source to destination nodes. For each phase of the routing, we will explain how the values of the hash chain and private keys are used.

**Secure the route discovery.** When a node S needs to know a route to some destination D, and such a route is not available, it broadcasts a route request RREQ, see (3).

$$S \rightarrow \text{Broadcast RREQ: } \{ RREQ^S, [RREQ^S]SK_S, Cert_S, H_i^S \} \quad (3)$$

This request contains the same basic DSR protocol fields excluding the Opt Data Len, see figure 1. We add the source node certificate $Cert_s$ in case of large-scale networks where nodes have not necessarily the public keys of all the network members.

The RREQ fields transmitted by S are non-mutable. They are signed with the private key of S and accompanied by a hash value Hi ($1< i <n$). To not reuse a password already revealed, an index i is incremented within the node at every use.

The generated packet is then broadcasted on the channel. When a node receives it, it checks the $H_i^S$ value to ensure that the packet comes from a legitimate node. To do so, it applies i times the hash function on $H_i^S$ to obtain $H_0^S$, the password initially transmitted by the neighbor and stored in the Neighbors table. If the receiver does not reach $H_0^S$ after i iterations, it infers that the message is fabricated by a malicious node. So, it rejects it without any process. Otherwise the message is accepted. The intermediate node adds its address to the packet. It signs this address and the previous one using its private key. Such a signature, applied to two successive node addresses, protects against any attempt to alter the addresses order. It is added with the node certificate to the packet. The node also replaces the received $H_i$ by a new password of its own chain, and finally broadcasts the RREQ, see (4).

$$J \rightarrow \text{Broadcast RREQ: } \{RREQ^S, [RREQ^S]SK_S, Cert_S, \ldots, Address_J, [Address_{j-1}, Address_j]SK_j, Cert_j, H_i^J\} \quad (4)$$

Eventually, the message is received by the destination D which verifies the source signature, as well the intermediate node signatures, and then responds using a RREP. The source digital signature authenticates the source and destination nodes. This control is made on IDs and $ID_d$ fields. The intermediate encryptions authenticate the intermediate nodes. This authentication is reinforced by the check of the addresses order. Once decrypted, the obtained value is compared with the two previous node addresses.

In (5) J denotes the last intermediate node of the path, connecting S to D. The destination node sends the response to J according to the following formula (5):

$$D \rightarrow J \text{ RREP:} \{RREP, [RREP]SK_D, Cert_D, H_i^D\} \quad (5)$$

RREP fields are signed by the destination node and value $H_i^D$ is associated to the packet. Each node sending the response is authenticated along the path using $H_i$. The reverse route construction is exposed to the risk of a diversion launched by an attacker who responds instead of the destination node. This attack is detected thanks to the destination certificate which includes the destination identity. If the latter doesn't

match with the destination identity invoked by the source node, one can deduce an intrusion attempt. As for the digital signature, it authenticates the source and destination nodes and controls the message replay. Finally, once the destination signature checked, the source node updates its cache with the new path.

In [30] an approach comparable to ours, called a Zero Common Knowledge authentication was proposed. It differs from ours in the use of $h(H_i)$. In this approach, the receiver checks the value $H_i$ by calculating only $h(H_i)$ and testing the relationship $h(H_i) = H_i+1$. If checked then the node identity is proved true. This approach supposes the storage of the latest password which may put in check the control process in case of lost messages.

**Secure Route Maintenance.** When a link breaks within an active route, the precursor of the unreachable node does the following:

- Invalidates the routes including this node in its cache.
- Lists all receivers that are no longer reachable (Unreach_Address).
- Delivers an appropriate RERR to such receivers.

Let a node A discovering a link break, and a source node S using this path. A warns S about the topology changes by sending the following message RERR to it:

$$A \rightarrow S \quad RERR \quad : \{RERR_A, Cert_A , [RERR_A, Cert_A] SK_A\} \tag{6}$$

This packet is signed by A and verified by the intermediates nodes. Each node receiving the RERR message carries out the same operations and spreads it to different sources.

**Update the Hash Chain.** When the node depletes all its hash values, it should reset the passwords sequence to allow its authentication. The node chooses a new random value $H_N$_new, and then generates a new sequence, using the hash function and sends the final value $H_0^A$_new to the one-hop neighbors. To authenticate the update message, we use the last undisclosed hash value of the old sequence (instead of the certificate in PWD). Here is a simplified format of the update message:

$$A \rightarrow \text{Broadcast UPDATE} : \{ID_A , H_0^A\text{\_new} , (H_0^A\text{\_new}) SK_A, \quad H_n\} \tag{7}$$

## 4 Simulation and Test

In order to evaluate the routing protocol performance, one often uses simulation. In fact, it would be very costly, or even impossible, to establish a network for testing purposes. An ad hoc network simulation does not take much time, and it keeps us closer to the real use of the routing protocol. These two major advantages help us to better see the behavior of the protocol in different scenarios and evaluate its performance.

We carry out simulations using the NS-2 simulator [20]. We choose NS-2 because of its popularity among academic researchers [26]. In addition, it already supports a verified version of DSR. Simulations are held considering a network of size 670 m x 670 m, composed of 20 nodes. We define simulations with parameters defined in table 3

**Table 3.** Simulation Parameters

| Parameter | Value |
|---|---|
| Antenna | OmniAntinna |
| MAC layer type | IEEE 802.11 |
| Radio propagation model | Two Ray Ground |
| Bandwidth | 1Mb |
| CBR traffic | 4 packets/s |
| Packet size | 512 bit |
| Pause time | 30 ms |
| Transmission range | 250 m |
| Simulation time | 200s |

The nodes move according to the RWP mobility model (Random Waypoint Model). This model has become a standard in wireless networks research. It provides several scenarios where the mobile entities randomly move in the simulation area. For each experiment, we created several scenarios for traffic and mobility using the parameters set out above. Each time, we vary the speed between [0, 20m/s] and evaluate one of the following metrics:

1. *EED Average end to end delay:* it gives the average time required to transmit a data packet from the source to the destination node.
2. *APL Average path length:* is calculated using the hop count field. It is often used as a metric for choosing the best path to route data.
3. *RL Routing load (the routing overhead):* it gives us information about the number of control packets generated by the protocol for the path establishment and route maintenance.

To evaluate the SRS_DSR performances, we carry out our experimentations on three protocols: ARAN (Authenticated Routing for Ad-hoc Networks) [26] that has been chosen for its robustness and its high level of security, DSR and SRS_DSR.

ARAN is a secure protocol, implementing asymmetric cryptography. It uses a trusted Certification Authority called CA to generate certificates. Before entering the Ad-hoc network, each node requests a certificate from the CA. In ARAN, each node signs the discovery packets and route reply messages before retransmitting them. Each node verifies the previous node digital signature and then replaces it with its own. The cryptographic operations cause additional delays at each hop thus increasing the route acquisition latency. Only the destination can answer the Request packet. When the source receives the RREP, it verifies the destination signature. This allows an end-to-end authentication between the source and destination. However, the latency increases especially for long paths.

Fig. 3 shows that the increase in the movement speed leads to a rather large increase of the end-to-end delay. Indeed, the nodes movement involves frequent link failure in the established paths. Nodes are forced to rebuild invalid routes. Thus,

delivery of data packets is delayed. We note that the required delay for ARAN is much higher than that of DSR and SRS_DSR.

Indeed, SRS_DSR established routes faster than ARAN: the time spent to check the hash values in SRS_DSR is insignificant, compared to the time needed in a certificate checking or a digital signature. We can therefore say that the processing of digital signature using only the two path ends (source and destination) reduces the delay of packets transfer.

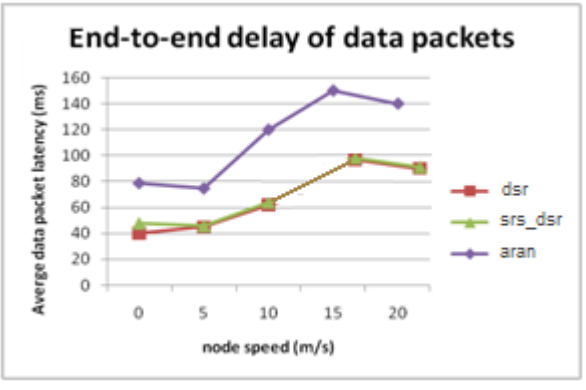


**Fig. 3.** End to End Delay (EED)

Fig. 4 shows the ratio of control packets relative to received packets. We note that the three protocols apply for the rule: the packets need increase with a higher speed. The space overhead caused by SRS_DSR is higher than the one of DSR and ARAN, because of the new control packets, namely PWD and UPDATE packets that we used to secure DSR.

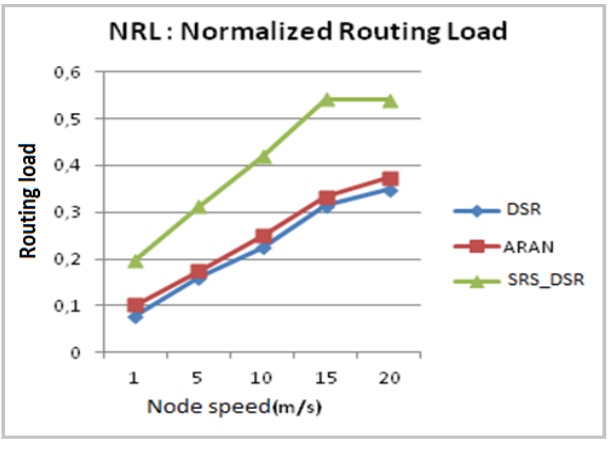


**Fig. 4.** Normalized routing Load

## 5 Related Work

The first works that deal with DSR security are those of Papadimitratos and Haas. They proposed SRP [24] in order to provide an end-to-end protection during the route discovery phase. They conducted tests on many known attacks and concluded that the proposed SRP proves to be secure in absence of grouped attacks. Their claim has never been formally proved.

Indeed, Buttyán and Vajda showed in [5] the weakness of the analysis presented in [24]. They presented an attack launched by a single hacker who succeeds to inject forged information during an SRP route construction.

Ariadne has been proposed by Hu et al. in [10,11] in order to improve the security mechanisms provided in SRP. It aims to secure all intermediate nodes by means of an appropriate authentication applied at each hop. They test their solution using different classes of attacks. But the solution was invalidated by Buttyán, Vajda and Ács in [5], [1] who succeed in launching several attacks.

To improve the weakness revealed in Ariadne, Buttyán and Vajda proposed a new version called enairA [5]. This solution remains insecure against an attack where two hackers encapsulate the control messages into data packets.

Other protocols have emerged as improvements to SRP, Ariadne, SAODV (Secure AODV) [33], FLSL (Adaptive Fuzzy Logic Based Security Level Routing Protocol) [12] and SAR (Security Aware Ad-hoc Routing) [21], for instance. In FLSL, a new attribute called security level is introduced in the format of the control messages to denote the reliability and dependability of certain mobile hosts or routes. The security level is used by source and destination nodes to determine the most secure and shortest route. As for SAR, it can discover a path with desired security attributes. The path found by the SAR protocol is not necessarily the shortest, but the safest of all the paths.

DSR and most of the on demand ad hoc routing protocols use single route reply along reverse path. Rapid change of topology causes that the route reply could not arrive to the source node. To avoid this, a new technique which tries multiple route replies is proposed in [27].

Latest researches in the area are conducted to secure ad hoc networks against grouped attacks. In [2] Awerbuch et al. propose ODSBR, the first on-demand routing protocol for ad hoc wireless networks that provides resilience to attacks caused by internal individual or colluding nodes. The protocol uses an adaptive probing technique that detects a malicious link after log n faults have occurred, where n is the length of the path. Problematic links are avoided by using a route discovery mechanism that relies on a new metric that captures adversarial behavior. Later, Awerbuch and Scheideler claim in [3] that the biggest threats appear to be join-leave attacks, used to isolate honest peers in the system, and against which no provably robust mechanisms are known so far. In this paper he showed that, on a high level, a scalable DHTcan be designed that is provably robust against adaptive adversarial join-leave attacks.

## 6 Conclusion

The purpose of this paper is to present a new scheme to secure the DSR protocol. We showed that the proposed scheme made of hash chains and end-to-end digital signature provides a high security level at a very low cost.

The initialization phase always raises the problem of secure distribution of keys and passwords, particularly on large scale systems when the by hand distribution becomes unrealizable. We proposed a remote pre-distribution carried out in an efficient and secure manner. We resorted afterwards to the use of one way hash chains to authenticate the control message senders during the route discovery. This authentication is principally useful while crossing the route from the source towards the destination. It guarantees the route drawing with legitimate nodes. Furthermore, the use of key-chain scheme is very well suited to pervasive computing devices since it requires nearly no computational power, very low bandwidth and memory storage.

At destination, the request message integrity is checked using a digital signature. This end-to-end checking ensures a fast source and destination authentication as well as a non message replay control.

The proposed solution can be extended to treat attacks. It will be also, interesting to validate this work by formalizing the specification and verification of the SRS_DSR protocol.

## References

1. Ács, G., Buttyán, L., Vajda, I.: Provably secure on-demand source routing in mobile ad hoc networks. IEEE Transactions on Mobile Computing 5(11), 1533–1546 (2006)
2. Awerbuch, B., Curtmola, R., Holmer, D., Nita-Rotaru, C., Rubens, H.: ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks. ACM Trans. Inf. Syst. Secur. 10(3) (2007)
3. Awerbuch, B., Scheideler, C.: Robust random number generation for peer-to-peer systems. Theoretical Computer Science 410(6-7), 453–466 (2009)
4. Burmester, M., De Medeiros, B.: On the Security of Route Discovery in MANETs. IEEE Transactions on Mobile Computing 8(9), 1180–1188 (2009)
5. Buttyán, L., Vajda, I.: Towards provable security for ad hoc routing protocols. In: Setia, S., Swarup, V. (eds.) SASN, pp. 94–105. ACM (2004)
6. Cerri, D., Ghioni, A.: Securing AODV: The A-SAODV Secure Routing Prototype. IEEE Communications Magazine (February 2008)
7. Curtmola, R., Nita-Rotaru, C.: BSMR: Byzantine-Resilient Secure Multicast Routing in Multihop Wireless Networks. IEEE Transactions on Mobile Computing 8(4), 445–459 (2009)
8. Eichler, S., Roman, C.: Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC. Technical Report: LKN-TR-2. Technische Universität München, Germany (2006)
9. Galice, S., Minier, M., Ubéda, S.: A Trust Protocol for Community Collaboration. In: Etalle, S., Marsh, S. (eds.) IFIPTM. IFIP, vol. 238, pp. 169–184. Springer, Boston (2007)

10. Hu, Y.-C., Perrig, A., Johnson, D.B.: Ariadne: a secure on-demand routing protocol for ad hoc networks. In: Akyildiz, I.F., Lin, J.Y.-B., Jain, R., Bharghavan, V., Campbell, A.T. (eds.) MOBICOM, pp. 12–23. ACM (2002)
11. Hu, Y.-C., Perrig, A., Johnson, D.B.: A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks 11(1-2), 21–38 (2005)
12. Jin, L., Zhang, Z., Zhou, H.: Performance comparison of AODV, SAODV and FLSL routing protocols in mobile ad hoc network. In: 4th IEEE Consumer Communications and Networking Conference, CCNC 2007, pp. 479–483 (January 2007)
13. Jung, S., Lee, B., Talipov, E., Ahn, M.W., Kim, C.: Effects of Valid Source-Destination Edges for Node-Disjoint Multipaths on AD HOC Networks. In: MSV 2008, Las Vegas, USA, pp. 308–313 (2008)
14. Johnson, D.B., Maltz, D.A.: Dynamic source routing in ad hoc wireless networks. Mobile Computing, 153–181 (1996)
15. Johnson, D.B., Maltz, D.A., Hu, Y.C.: IETF RFC4728: The dynamic source routing protocol (DSR) for mobile ad hoc networks (February 2007)
16. Lamport, L.: Password Authentication with Insecure Communication. Communication of the ACM 24, 770–772 (1981)
17. Luo, H., Kong, J., Zerfos, P., Lu, S., Zhang, L.: URSA: Ubiquitous and robust access control for mobile ad hoc networks. IEEE/ACM Transactions on Networking 12(6), 1049–1063 (2004)
18. Mallouli, W., Wehbi, B., Cavalli, A.R.: Distributed Monitoring in Ad Hoc Networks: Conformance and Security Checking. In: The 7th International Conference on AD-HOC Networks & Wireless, Sophia Antipolis, France, September 10-12 (2008)
19. Mishra, A.: Security and quality of service in ad hoc wireless network, pp. 3–106. Cambridge University Press, New York (2008)
20. NS Manual. VINT Project (2008), `http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf`
21. Naldurg, S., Yi, P., Kravets, R.: Security aware ad hoc routing for wireless networks. In: 2nd ACM Int. Symp. on Mobile Ad Hoc Networking & Computing, Long Beach, pp. 299–302. ACM Publisher, USA (2001)
22. Ning, P., Sun, K.: How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-Hoc Routing Protocols. Ad Hoc Networks 3(6), 795–819 (2005)
23. Orset, J.-M., Alcalde, B., Cavalli, A.: An EFSM-Based Intrusion Detection System for Ad Hoc Networks. In: Peled, D.A., Tsay, Y.-K. (eds.) ATVA 2005. LNCS, vol. 3707, pp. 400–413. Springer, Heidelberg (2005)
24. Papadimitratos, P., Haas, Z.J.: Secure Routing for Mobile Ad hoc Networks. In: Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, USA, pp. 193–204 (January 2002)
25. Pirzada, A., McDonald, C., Datta, A.: Performance Comparison of Trust-Based Reactive Routing Protocols. IEEE Transactions on Mobile Computing 5(6) (June 2006)
26. Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., Belding-Royer, E.M.: Authenticated routing for ad hoc networks. In: 10th IEEE International Conference on Network Protocols, Paris, France (2002)
27. Talipov, E., Jin, D., Jung, J., Ha, I., Choi, Y., Kim, C.: Path Hopping Based on Reverse AODV for Security. In: Kim, Y.-T., Takano, M. (eds.) APNOMS 2006. LNCS, vol. 4238, pp. 574–577. Springer, Heidelberg (2006)
28. Tsaur, W.-J., Pai, H.-T.: A New Security Scheme for On-Demand Source Routing in Mobile Ad Hoc Networks. In: IWCMC 2007, Honolulu, Hawaii, USA, August 12-16, pp. 577–582 (2007)

29. Tseng, C.-Y.H.: Distributed Intrusion Detection Models For Mobile Ad Hoc Networks. PhD Thesis, University of California (2006)
30. Weimerskirch, A., Westhoff, D.: Zero Common-Knowledge Authentication for Pervasive Networks. In: Matsui, M., Zuccherato, R. (eds.) SAC 2003. LNCS, vol. 3006, pp. 73–87. Springer, Heidelberg (2004)
31. Zapata, M.G.: Secure Ad hoc on Demand Distance Vector (SAODV) Routing. Mobile Ad Hoc Networking Working Group, Internet Draft (September 2005)
32. Zapata, M.G.: Key Management and Delayed Verification for Ad Hoc Networks. Journal of High Speed Networks 15(1), 93–109 (2006)