Routing Security in Mobile Ad-hoc Networks

Jonny Karlsson
The Open University, Milton Keynes, England, and
Arcada University of Applied Sciences, Helsinki Finland
jonny.karlsson@arcada.fi

Laurence S. Dooley
The Open University, Milton Keynes, England
l.s.dooley@open.ac.uk

Göran Pulkkis
Arcada University of Applied Sciences, Helsinki Finland
goran.pulkkis@arcada.fi

Abstract

The role of infrastructure-less mobile ad hoc networks (MANETs) in ubiquitous networks is outlined. In a MANET there are no dedicated routers and all network nodes must contribute to routing. Classification of routing protocols for MANET is based on how routing information is acquired and maintained by mobile nodes and/or on roles of network nodes in a routing. According to the first classification base, MANET routing protocols are proactive, reactive, or hybrid combinations of proactive and reactive protocols. According to the role-based classification, MANET routing protocols are either uniform when all network nodes have the same role or non-uniform when the roles are different and dedicated. A contemporary review of MANET routing protocols is briefly presented. Security attacks against MANET routing can be passive and or active. The purpose of the former is information retrieval, for example network traffic monitoring, while the latter is performed by malicious nodes with the express intention of disturbing, modifying or interrupting MANET routing. An overview of active attacks based on modification, impersonation/spoofing, fabrication, wormhole, and selfish behavior is presented. The importance of cryptography and trust in secure MANET routing is also outlined, with relevant security extensions of existing routing protocols for MANETs described and assessed. A comparison of existing secure routing protocols form the main contribution in this paper, while some future research challenges in secure MANET routing are discussed.

Keywords: MANET, routing protocol, routing security, mobile networks, network security, trusted routing, cryptography

Material published as part of this publication, either on-line or in print, is copyrighted by the Informing Science Institute. Permission to make digital or paper copy of part or all of these works for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage AND that copies 1) bear this notice in full and 2) give the full citation on the first page. It is permissible to abstract these works so long as credit is given. To copy in all other cases or to republish or to post on a server or to redistribute to lists requires specific permission and payment of a fee. Contact Publisher@InformingScience.org to request redistribution permission.

Introduction

A traditional wireless network has an infrastructure with fixed base stations for mobile network hosts and/or mobile networks. As computing devices are getting smaller and integrated into various systems, such as phones, vehicles, sensors, homes, health care systems, military equipment etc. the trend is mov-

ing towards ubiquitous, infrastructure-less and self-configuring wireless networks, such as *mobile ad hoc networks* (MANETs). In a MANET every network host is also a base station for other network hosts and therefore network communications can be established on demand without the need for fixed network equipment. While MANETs bring many attractive features for future network communications they also introduce many challenges related to (Taneja & Kush, 2010):

- unicast routing
- multicast routing
- dynamic network topology
- speed
- frequency of updates or network overhead
- scalability
- mobile agent based routing
- Quality of Service (QoS)
- energy efficient/power aware routing
- secure routing

Infrastructure-less networks are more vulnerable to routing attacks than their structured counterparts, since there are no dedicated routers and each network node takes part of the routing process. While routing packets can in theory be protected using cryptographic measures it must be taken into account that MANET nodes often consist of hardware restricted devices, such as small chips and sensors, where cryptography would incur a significant computational cost. Furthermore, in dynamic MANETs, where hosts are continuously joining and leaving the network, it is difficult to discern hosts with malicious intentions from legitimate hosts making cryptographic measures impossible to implement in practice. An alternative approach to cryptography is trust based security mechanisms where each node typically monitors the behaviour of its neighbor nodes with the intention to identify suspicious behavior. However, such solutions also typically impose a high load on the network making them challenging to implement in hardware restricted MANETs. Secure routing is therefore a very significant challenge in MANETs.

The main contributions in this paper are:

- a classification of current relevant routing protocols for MANETs and their security extensions, and
- a comparison of secure MANET routing protocols in regard to their protection and detection performance against several security attack types.

The remainder of this paper is organised as follows. In the next section, relevant MANET routing protocols and how these protocols can be classified is presented, while the following section describes security attacks against MANET routing protocols. This is followed by a survey of security extensions of MANET routing protocols, before some concluding comments and future research objectives are described.

Routing Protocols for MANETs

Research on MANETs has nearly 20 years focused on routing and this focus still remains. Several routing protocols for MANETs have been proposed and some surveys on these protocols have been published (Feeney, 1999; Qin & Kunz, 2004; Liu & Kaiser, 2005; Taneja & Kush, 2010) and an IETF Routing Area Working Group MANET (Mobile, 2011) has been active for a decade with six currently active Internet drafts.

Routing protocols for MANETs are usually classified into table driven/proactive protocols, on-demand/reactive protocols, and hybrid protocols based on how routing information is acquired and maintained by mobile nodes. Table driven/proactive protocols use a proactive routing

scheme, in which every network node maintains consistent up-to-date routing information from each node to all other nodes in the network. On-demand/reactive protocols are based on a reactive routing scheme, in which at least one route is established only when needed. A hybrid routing protocol is a combination of proactive and reactive schemes with the aim of exploiting the advantages of both types of protocols. (Qin & Kunz, 2004; Liu & Kaiser, 2005; Abusalah, Khokhar & Guizani, 2008; Singh, 2011)

Another classification into uniform and non-uniform routing protocols for MANETs is based on the network node roles in a routing scheme. In a uniform routing protocol all network nodes have the same role, importance and functionality. In a non-uniform routing protocol some network nodes carry out distinct management and/or routing functions. A uniform routing protocols is either reactive or proactive, while different classification schemes have been proposed for non-uniform routing protocol (Feeney, 1999; Liu & Kaiser, 2005)

In this section some relevant reactive, proactive, and hybrid routing protocols for MANETs are presented.

Table Driven/Proactive Protocols

Typical table driven protocols are *highly dynamic Destination-Sequenced Distance Vector Routing* (DSDV) (Perkins & Bhagwat, 1994) and *Optimized Link State Routing* (OLSR) (Clausen & Jacquet, 2003).

Table driven routing protocols have a low route acquisition delay because every node always has a fresh route to all other nodes in the network. However, the storage, bandwidth, and power requirements are high since each node must keep its routing table up-to date (with route information to all other nodes) which mandates periodic routing message exchanges (Mohseni et al., 2010).

On Demand/Reactive Protocols

On-demand protocols incur a much lower load on the network, compared to table driven, since each node does not need to constantly keep their routing tables up-to-date. However, route acquisition delay is high since routing messages must be exchanged every time before communication is possible over a new route (Mohseni et al., 2010). Two prominent MANET routing protocols, based on reactive routing schemes, are *Ad hoc On-demand Distance Vector* (AODV) (Perkins et al., 2003) and *Dynamic Source Routing* (DSR) (Johnson et al., 2007), which will now be respectively considered.

Ad hoc On-demand Distance Vector (AODV)

In AODV, when a node wants to communicate with another, the source node floods the network with *route request* (RREQ) messages. If a node that receives a RREQ packet is not the destination or doesn't have a fresh route to the destination it creates a reverse route to the source (a route back to source with the node from where the RREQ came from as next hop). If the receiver of a RREQ is the destination node, it sends a *route reply* (RREP) message back to the source as a unicast packet over the route it received the RREQ. The destination node only sends a RREP to the first RREQ message it receives. Every node receiving a RREP also creates a route to the destination in the routing table. As a result, when the RREP reaches the source, all nodes in the shortest route path will have a route both to the source and destination.

Dynamic Source Routing (DSR)

As with AODV, DSR floods the network with route request messages as a result of route discovery initiation. However, compared with AODV, the destination node returns a route reply for

each copy of route request message it receives. As a result, the source node will know more than one route to the destination node upon reception of all route replies. The addresses of all nodes through which both route request and route reply messages have traversed are added to the routing message headers, so a node knows not only the hop count values of all routes to a destination, but also all the intermediate nodes. Based on hop count and other route information, the source node finally selects the route with the lowest latency. Each data packet carries, in its header, the complete ordered list of intermediate nodes through which a packet is to be transmitted.

DSR has lower network overheads compared with AODV, mainly due to the multiple storage and source routing features. If a link fails, the source node does not need to re-initiate route discovery, as in AODV. Instead it selects another route from its routing table. Since the route information is included in all data packets, other nodes forwarding or overhearing any data packet can cache the routing information for future use, which also eliminates the need for route discovery if the route is still fresh.

Hybrid Protocols

A proactive scheme is used to discover routes to nearby nodes and reactive schemes are used to discover long distance nodes. An example of a hybrid routing protocol is *Zone Routing Protocol* (ZRP) (Haas et al., 2002). ZRP is also called a hierarchical routing protocol where the network can be grouped in clusters, trees, or zones where one node is chosen to be a leader that manages that particular routing area.

Hybrid protocols provide a lower route acquisition delay than reactive protocols and a lower overhead than proactive protocols. These protocols, however, are not suitable for highly dynamic MANET environments since in such network conditions it is simply infeasible to delegate roles to nodes and divide the network into zones.

Criteria for Routing Protocol Selection

The performance of a routing MANET protocol depends on a myriad of features, including for example, the MANET size defined by network node count and the geographical dimension, the rate of nodes joining and leaving the MANET, the distribution of existence times of available routes between network nodes, the mobility of the nodes, available network communication bandwidth, as well as processing and memory resources of the nodes. To define the best routing protocol for a specific MANET is therefore an intractable task, with the selection criteria requiring empirical research and experimentation with different MANET scenarios and different routing protocols.

Security Attacks against Routing in MANETs

Security attacks in MANET routing can be divided in two main types, passive attacks and active attacks. The intention of a passive attack is typically to listen and retrieve vital information inside data packets, for example by launching a traffic monitoring attack. In such an attack, a malicious node tries to identify communication parties and functionality which can provide information to launch further attacks. The attack type is called passive since the normal functionality of the network is not altered.

An active attack is performed by a malicious node with the intention to interrupt the routing functionality of a MANET. Examples include (Tomar et al., 2010; Goyal et al., 2010; Garg & Mahapatra, 2009; Wang, Hu & Zhi, 2008):

- Modification attacks
- Impersonation attacks
- Fabrication attacks

- Wormhole attacks
- Selfish behavior.

Modification Attacks

A modification attack is typically launched by a malicious node with the deliberate intention of redirecting routing packets, by for example modifying the hop count value of a routing packet to a smaller value. By decreasing the hop count value a malicious node can attract more network communication. A typical modification attack is the black hole attack where a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. As a result, the target node will send its packets through the malicious node when communicating with the destination node. The malicious node can choose to either drop the packets or place itself on the route as the first step in what is known popularly as either the *man-in-the-middle* (MITM) or a SYBIL attack**.**

A modification attack can also be a special kind of *denial-of-service* (DoS) attack. In this situation the intention is to destruct the entire routing function by altering the source routes in the header of the routing packet. A DoS attack however, is only effective on routing protocols where intermediate nodes are included in the packet header, such as DSR.

Impersonation/Spoofing Attacks

In this type of attack (also known as spoofing) a malicious node uses for example the IP or address of another node in outgoing routing packets. As a result, the malicious node can receive packets meant for the other node or even completely isolate it from the network.

Fabrication

The main purpose of fabrication attacks is to drain off limited resources in other MANET nodes, such as battery power and network connectivity by, for example, flooding a specific node with unnecessary routing messages. A malicious node can for example send out false route error messages. This kind of attack is more prominent in reactive routing protocols where path maintenance is used to recover broken links.

In a fabrication attack a malicious node can also attempt to create routes to nodes that do not exist. As a result, the routing table of a neighbor node can become full which prevents the registration of any new routes. This type of fabrication attack, which is a DoS attack, is only effective on table-driven routing protocols where each node in the network keeps an up-to-date route to all other nodes in the network.

A fabrication attack can also be launched by a selfish node that duplicates the transmission of packets to another node, just to make sure all packets will reach the destination node. This behavior may lead to an excessively high network traffic load.

Wormhole Attacks

A wormhole (Hu, Perrig, & Johnson, 2002; Liu et al. 2007; Sanzgiri et al., 2002) is a particularly severe attack on MANET routing. A malicious node captures packets from one location in a network and tunnels them to another malicious node, located several hops away, which forwards the packets to its neighboring nodes. This creates the illusion that two endpoints of a wormhole tunnel are neighbors even though they are located far away from each other in reality. A strategic placement of a wormhole causes most of the network traffic to pass through the malicious nodes which have formed the wormhole. Once the wormhole link has been successfully established,

further attacks can be launched by the malicious nodes such as selective packet drop to disrupt communication or data sniffing to capture confidential information for example.

There are two classes of wormhole attacks (Khabbazian et al., 2006): *hidden mode* (HM) and *participation mode* (PM). In the former, HM wormhole nodes are invisible from legitimate nodes as they do not process routing packets. They simply capture, tunnel and forward packets to each other and never appear in routing tables. In contrast, PM wormhole nodes are visible during the routing process since they process routing packets as any normal node. Aside from relaying routing packets to its neighbors, a PM wormhole node tunnels routing packets to the other PM node, giving it the opportunity to deleteriously control network performance**.**

A shortcut link between two HM or PM wormhole nodes can be established using either an *in-band* (I-B) or *out-of-band* (O-B) channel. An I-B channel is one where the wormhole nodes tunnel packets to each other through legitimate nodes in the network, while an O-B channel connects the two malicious nodes through an external communication link like a network cable or directional antenna.

Selfish Behavior

This refers to a node which does not cooperate in any routing. It may for example, be that it wishes to save energy and so switches to a “sleep mode” whenever it is not taking part in any network communication. While such an attack may not be launched with explicitly bad intentions, it can lead to serious disruptions in network communications such as high route discovery delays and dropped data packets. If the selfish node also happens to be the only communication link between two MANET endpoints, communications between these endpoints will become unavailable.

Secure Routing Protocols for MANETs

Most routing protocols have been designed without taking security into account. It has been assumed that all nodes in a MANET are trusted. However, this is not the case in a large scale and dynamic MANET and if the routing protocol is unprotected, the whole MANET can be liable to several different types of security attacks. Much research has been done in the area of routing security in MANETs and several surveys on this research have been published (Abusalah, Khokhar & Guizani, 2008; Wang, Hu & Zhi, 2008; Djenouri & Badache, 2010; Singh, 2011). Due to the dominant status of reactive routing protocols for MANETs, most security research has tended to give attention to these protocols.

Secure routing protocols for MANETs are usually derived as extensions of existing routing protocols, see Table 1. Security extensions are cryptographic and/or trust-based. Trust and security are closely interrelated concept. Using trust can result in considerable security enhancement in a network. The main features of trust within a MANET are defined as (Ramana, Chari & Kasiviswanth, 2010):

1. A decision method to determine trust against an entity should be fully distributed since the existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed.
2. Trust should be determined in a highly customizable manner without excessive computation and communication load, while also capturing the complexities of the trust relationship.
3. A trust decision framework for MANETs should not assume that all nodes are cooperative. In resource-restricted environments, selfishness is likely to be prevalent over cooperation, for example, in order to save battery life or computational power.
4. Trust is dynamic, not static.
5. Trust is subjective.

6. Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C.
7. Trust is asymmetric and not necessarily reciprocal.
8. Trust is context-dependent. A may trust B as a wine expert but not as a car fixer. Similarly, in MANETs, if a given task requires high computational power, a node with high computational power is regarded as trusted while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

Table 1: Security extensions of some MANET routing protocols.

Reactive Protocols	Proactive Protocols	Hybrid Protocols
DSR • *SQoS Route Discovery* • *Ariadne* • *Confidant*	DSDV • *SEAD*	ZRP • *SRP*
AODV • *CORE* • *SAODV* • *TAODV* • *SAR*	OLSR • *SLSP*	
Others • *SPREAD* • *ARAN*		

The security extensions of the existing MANET routing protocols in Table 1 are cryptographic except QoS Route Discovery (Maltz, 1999), Confidant (Buchegger & Boudec, 2002), and TAODV (Li, Lyu & Liu, 2004; Pushpa, 2009), which are trust-based. An experimental comparison of two security extensions of AODV (Perkins et al., 2003) – the cryptographic security extension SAODV and the trust-based security extension TAODV – is provided in (Cordasco & Wetzel, 2007). Many secure proposals for secure routing in MANETs have concentrated on protecting MANETs from specific routing attacks, especially the wormhole attack. A recent proposal for trust-based routing decisions in MANETs has been shown to provide complete protection against all type of wormhole attacks in realistic network deployment situations (Karlsson, Dooley & Pulkkis, 2011). The purpose of this section is to provide an overview of the relevant security extensions of the existing MANET routing protocols summarised in Table 1.

Trust Based Secure Routing

In this subsection, the three trust-based MANET routing protocols: QoS Route Discovery, Confidant and TAODV are reviewed. An overview of trust-based routing schemes in MANETs is provided in (Patmaik & Gore, 2011).

Cooperation of nodes: Fairness in dynamic ad hoc networks (Confidant)

The main idea of Confidant (Buchegger & Boudec, 2002) is to make non cooperative nodes unattractive for other nodes to communicate with. A node chooses a route based on trust relationships built up from experienced, observed or reported routing and forwarding behavior of other nodes. Each node observes the behavior of all nodes located within the radio range. When a node discovers a misbehaving node, it informs all other nodes in the network by flooding an alarm mes-

sage. As a result, all nodes in the network can avoid the detected misbehaving node when choosing a route.

Thus Confidant effectively detects non cooperative nodes such as selfish nodes and PM wormhole nodes that drop data packets. HM wormhole nodes and PM wormhole nodes that do not drop packets are, however, not detected. Moreover, a major weakness of Confidant is that an attacker is able to send false alarm messages, and as a consequence the attacker can claim that a node is misbehaving even if that is not true.

Trusted AODV (TAODV)

In TAODV route selection is based on quantitative Route Trust and Node Trust values (Pushpa, 2009; Pirzada & McDonald, 2004).

Route Trust from a source node to a destination node is defined as the difference between the number of packets sent from the source node and the number of related packets received by the destination node. Route Trust is thus 0 for a perfect route and trustworthiness decreases for growing Route Trust values.

For calculation of Node Trust each node monitors the behavior of all neighbor nodes by counting both successes and failures of events such as Control Packets Received, Control Packets Forwarded, Data Packets Received, Data Packets Forwarded, Route Established etc. Node Trust value for a certain monitored event type is $(R_s\text{-}R_f)/(R_s+R_f)$, where R_s and R_f are the number of successful and failed events respectively. This value will lie between +1 (complete trust) and -1 (complete mistrust). Node Trust for a neighbor node is weighted sum of the trust values for all monitored event types. The weights are dynamically assigned values between 0 and 1based on circumstances and chosen criteria.

For route selection RT = 0.4 * (Hop Count) + 0.6 * (Route Trust) and the 3 neighbor nodes are selected from which the routes with lowest RT values start. For each selected node an average Node Trust is calculated from the monitored Trust Values of neighbor nodes. The route starting from the node with the highest average Node Trust is selected.

QoS route discovery

In (Maltz, 1999) a QoS-Guided route discovery protocol for MANETs is presented. In this protocol a node specifies route trust by traditional QoS metrics, bandwidth, latency and jitter that must be satisfied by a discovered route.

Cryptography Based Secure Routing

In this subsection the cryptography-based secure routing protocols in Table 1 are presented.

Securing QoS route discovery (SQoS route discovery)

SQoS Route Discovery (Hu & Johnson, 2004) is a cryptographically protected version of QoS Route Discovery. SQoS Route Discovery relies entirely on symmetric cryptography.

Ariadne

Ariadne (Hu, Johnson, & Perrig, 2002a) is a secure reactive (on-demand) routing protocol based on DSR that provides authentication of routing messages. Authentication can be performed by using shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures. Ariadne is based on the *Timed Efficient Stream Loss-tolerant Authentication* (TESLA) protocol (Perrig et al., 2005) which is a

broadcast authentication procedure requiring relaxed time synchronization. It consists of two steps:

1. authentication of routing messages
2. verification that there is no node missing in the routing message headers

In step 1, if shared secrets are used, a node sending a routing request message indicates a *message authentication code* (MAC) which is computed with a shared secret key over a time stamp (or other unique data). The receiver of the message can then authenticate the message by using its own shared secret key.

In step 2, per-hop hashing is used to verify that no hop was omitted. Authentication of routing messages is not enough since an attacker could still remove a node from the list of intermediate nodes in a routing message. Ariadne though uses a one-way hash function to prevent this.

Ariadne provides good defense against modification, fabrication, and spoofing due to its message authentication and routing message header verification features. Ariadne can also provide protection from HM wormhole attacks, when used together with the TESLA Instant Key disclosure (TIK) protocol for precise time synchronization between neighbouring nodes, and PM wormhole attacks if the wormhole nodes do not have valid shared secrets.

Secure AODV (SAODV)

SAODV (Zapata & Asokan, 2002) was introduced to protect the routing messages of the original AODV protocol. In SAODV, digital signatures are used to authenticate RREQ and RREP messages and hash chains are used to authenticate the hop-count fields within the RREQ and RREP messages.

The source node selects a random seed number in the beginning of the route discovery process and sets a *maximum hop count* (MHC) value. The source node then computes a hash value by using a hash function as *h(seed)* and *Top_Hash* as $h^{MHC}(seed)$. An intermediate node checks, after reception of a RREQ, whether the *Top_Hash* value equals $h^{MHC\text{-}Hop\_Count}(Hash)$. If it does, the intermediate node assumes the hop count value has not been altered. The intermediate node then increments the hop-count value in the RREQ header and computes a new hash value by hashing the old value (*h(Hash)*), before rebroadcasting the RREQ messages to its neighbors.

Since all other fields of the RREQ message are non-mutable they can be authenticated by verifying the signature in the RREQ. The RREQ message is signed by the private key of the source node and the RREP message is signed by the private key of the destination node. By doing this, both the source and the destination can identify its communication partner and avoid impersonation attacks. The intermediate nodes are verifying the signatures in both the RREQ and RREP messages as well and only store a forward or reverse route entry in their routing tables if the signature in the routing message can be verified.

Security aware ad hoc routing (SAR)

The SAR protocol (Yi et al., 2001) incorporates security attributes as parameters into ad hoc route discovery. It enables the use of security as a negotiable metric with the intention to improve the relevance of the discovered routes. While AODV discovers the shortest path between two nodes, SAR can discover a path with desired security attributes. For instance, the criteria for a valid route can be that every node in the route must own a particular shared key. In such a case, routing messages would be encrypted with the source node's shared key and only the nodes with the correct key can read the header and forward that routing message. As a result, if a routing message reaches the destination, it must have been traveled through nodes having the same trust level as

the source node. It is then for the node initiating the route discovery to decide upon the desired security level for that route.

SAR has been presented as an extension to AODV but it can also be extended to any existing routing protocol. Due to strong cryptographic protection of routing messages, attacks such as modification, impersonation, and fabrication are effectively eliminated. A major problem with SAR, however, is that it involves significant encryption overhead since each intermediate node has to perform both encryption and decryption operations.

Authenticated routing for ad hoc networks (ARAN)

The purpose of the ARAN protocol (Sanzgiri et al., 2002) is to detect and protect against malicious actions by third parties and peers. It provides authentication, message integrity, and non-repudiation. ARAN can be used in two different security stages: a simple mode which is mandatory and an optional stage which provides stronger security but also more overhead and is not suitable on mobile devices with very low processing or battery capacity. ARAN uses cryptographic certificates for authentication and non-repudiation. Each routing message is signed by the source node and broadcasted to all neighbors. An intermediate node removes the certificate and signature of the previous hop and replaces them with its own.

Due to strong authentication, message integrity, and non –repudiation ARAN provides effective protection from modification, impersonation, and fabrication attacks. However, due to heavy asymmetric cryptographic operations and large routing packets, ARAN has a high computational cost for route discovery. ARAN is also vulnerable against selfish nodes that e.g. drop routing packets. In particular, if the selfish node is an authenticated node, then ARAN is unable to detect this type of attack.

Secure efficient ad hoc networks (SEAD)

SEAD (Hu, Johnson, & Perrig, 2002b) is a proactive routing protocol based on DSDV. SEAD uses a hash chain method for checking the authenticity of data packets and the hash chain value is used for transmitting routing updates. The authentication of each entry of a routing update message is verified by a receiving node. Looping is removed by using a sequence number and authentication of the source of routing update message. Authentication of the source can be done for example by providing a shared secret key between each pair of nodes in the MANET which is then used for MAC calculations between the nodes for the authentication of a routing update message.

SEAD provides strong protection against attackers trying to create incorrect routing state in other nodes by for example modifying the sequence number in the routing packet. However, SEAD does not protect against an attacker tampering the next hop or the destination field of a routing update packet.

Secure link state routing protocol (SLSP)

The main functionality of SLSP (Papadimitratos &Haas, 2003) is to secure the discovery and the distribution of link state information by using asymmetric keys. SLSP consists of three major steps: public key distribution, neighbor discovery, and link state updates. Public keys are distributed between a node and all its neighbors. A central server for key distribution is thus not needed. Periodic hello messages, used in neighbor discovery, are signed using the private key of the sender. Signed link state update messages are identified by the IP address of the initiating node and include a sequence number. A node receiving a link update messages verifies the attached signature using the public key it received earlier during the public key distribution phase. The hop count field in the update message is protected by using a one-way hash chain.

DoS attacks are also avoided in SLSP since each node maintains a priority ranking of their neighbor nodes based on the rate of control traffic they have observed. Neighbor nodes that generate update packets with the lowest rate are given highest priorities. Thus, malicious neighbors generating a huge amount of unnecessary update packets will get the lowest priority which limits the effectiveness of a DoS attack.

Secure routing protocol (SRP)

SRP (Sanzgiri, 2002) is a protocol designed to secure ZRP but can also be used with pure reactive routing protocols. A *security association* (SA) is required between a source node and a destination node. It is assumed that the SA can be established by using a shared key between the two communicating nodes. SRP uses an additional header to the underlying on-demand routing protocol packet. The header contains a sequence number QSEC, an ID number QID, and a MAC field where the output of a key hashed functions is inserted. A route request messages is discarded by intermediate nodes if the SRP header is missing.

When the route request message has reached the destination node it verifies if it has a SA with the source node. The route request packet is dropped if QSEC is greater or equal to a QMAX value since it is then considered to be replayed. If the QSEC value is valid, the destination calculates the keyed hash of the request fields and compares the output with the MAC field of the SRP header. If they match the authenticity of the sender and the integrity of the request message are verified and the destination generates a route reply message where it includes the path information from source to destination, QID, and QSEC.

The source node validates QSEC and the MAC field in the same way as the destination node. The source node also compares the source route (path information) included in the reply message with the reverse of the route carried in the reply packet. If they match it can be ensured that the route information in the routing packets has not been altered.

Summary and Discussion

Table 2 provides a comparative summary of the features of some relevant secure routing protocols, from which the general conclusion can be made that no single routing protocol provides protection against all forms of routing attacks. It is also notable that the achievable security level is highly dependent on both the underlying assumptions and network scenarios employed.

Table 2: Comparison of the best known secure routing protocols.

Protocol	Based on/type	Provides protection from attacks:				
		Modification	Impersonation	Fabrication	Wormhole	Selfish
Ariadne	DSR/reactive	Yes	Yes	Yes	Yes	No
Confidant	DSR/reactive	No	No	No	No	Yes
SAODV	AODV/reactive	Yes	Yes	Yes	No	No
TAODV	AODV/reactive	Yes	No	Yes	No	Yes
SAR	AODV/reactive	Yes	Yes	Yes	No	No
ARAN	Others/reactive	Yes	Yes	Yes	No	No
SEAD	DSDV/proactive	Weak	Yes	Yes	No	No
SLSP	OLSR/proactive	Yes	Yes	Yes	No	No
SRP	ZRP/hybrid	Yes	Yes	Yes	No	No

Conclusions

Routing security in infrastructure-less and self-configuring mobile networks, such as MANETs, has been highlighted as one of the most challenging security issues in current and future ubiquitous networks. Since there are a number of potential MANET security threats and many possible network environments (small, scalable, fixed, dynamic, homogeneous, heterogeneous, etc.) it is difficult to design a secure routing protocol providing protection from all types of attacks while at the same time being suitable for all types of MANET scenarios. A comparison of established secure routing protocols based on the classification is the main contribution in this paper. Further research needs to be undertaken both in in order to provide protection from all possible MANET routing attacks and for formulating recommendations on the selection of a secure routing protocol for a specific MANET, since no single currently proposed routing protocol provides protection against all forms of routing attacks in MANETs.

In some secure routing protocols based on cryptography different symmetric cryptographic keys must be generated for and distributed to all possible pairs of MANET nodes and/or trust in public keys of MANET nodes is provided by certification. Research is needed on how generation, distribution and certification of cryptographic keys for nodes entering a MANET can be implemented by services, which are distributed among all already accepted MANET nodes. Improvements of existing security protocols, intrusion detection systems and security mechanisms for detecting specific types of attacks are relevant topics for future research. Use of simulated networks and virtual network infrastructures in cloud computing can maintain the expenditure on MANET security research to a reasonable level.

Secure routing protocols based on cryptography impose additional computational load on all network nodes and are vulnerable to some types of DoS attacks. Trust-based secure routing protocols are computationally more light-weight and less vulnerable to DoS attacks but can consume much communication bandwidth, since each MANET node monitors continuously the behavior of a set of other MANET nodes. Search of computationally efficient combinations of cryptography and trust-based solutions with low communication bandwidth consumption is therefore an important research topic in the development of secure routing protocols for MANETs

References

Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. *IEEE Communications Surveys & Tutorial, 10*(4), 78-93.

Buchegger, S., & Boudec, J.-Y.L. (2002). Cooperation of nodes fairness in dynamic ad-hoc networks. *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC).*

Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR).* IETF, Request for Comments (RFC) 3626.

Cordasco, J., & Wetzel, S. (2007). Cryptographic vs. trust-based methods for MANET routing security. *Electronic Notes in Theoretical Computer Science, Elsevier, 197*(2), 131-140. Retrieved December 11, 2011 from http://www.cse.msstate.edu/~ramkumar/cryptvstrust.pdf

Djenouri, D., & Badache, N. (2010). *Security in mobile ad hoc networks.* Germany: LAP Lampert Academic Publishing.

Garg, N., & Mahapatra, R. P. (2009). MANET security issues. *IJCSNS International Journal of Computer Science and Network Security, 9*(8).

Goyal, T., Batra, S., & Singh, A. (2010). A literature review of security attack in mobile ad-hoc networks. *International Journal of Computer Applications, 9*(12), 11-15.

Haas, Z. J., Pearlman, M. R., & Samar, P. (2002). *The zone routing protocol (ZRP) for ad hoc networks.* Internet draft, IETF.

Hu, Y., & Johnson, D. B. (2004). Securing quality-of-service route discovery in on-demand routing for ad hoc networks. *Proceedings of ACM SASN'04*.

Hu, Y.-C., Johnson, D. B., & Perrig, A. (2002a). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Proceedings of Mobicom'02*.

Hu, Y.-C., Johnson, D. B., & Perrig, A. (2002b). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Proceedings of Fourth IEEE Workshop on Mobile Computing Systems and Applications (WM-CSA'02*).

Hu, Y., Perrig, A., & Johnson, D. (2002). Packet leashes: A defense against wormhole attacks in wireless networks. *Proceedings of INFOCOM, IEEE*.

Johnson, D., Hu, Y., & Malz, D. (2007). *The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4*. IETF, Request for Comments (RFC) 4728.

Karlsson, J., Dooley, L.S., & Pulkkis, G. (2011). A new MANET wormhole detection algorithm based on traversal time and hop count analysis. *Sensors, 11* (12), 11122-11140. Retrieved December 11, 2011 from http://www.mdpi.com/1424-8220/11/12/11122/pdf

Khabbazian, M., Mercier, H., & Bhargava, V.K. (2006). Wormhole attack in wireless ad hoc networks: Analysis and countermeasure. *Proceedings of Global Telecommunications Conference, GLOBECOM'06, IEEE.*

Li, X., Lyu, M. R., & Liu, J. (2004). A trust model based routing protocol for secure ad hoc networks. *Proceedings of Aerospace Conference, Vol. 2, USA*: IEEE Press. 1286-1295, ISBN 0-7803-8155-6.

Liu, C., & Kaiser, J. (2005). *A survey of mobile ad hoc network routing protocols*. MINEMA (Middleware for Network Eccentric and Mobile Applications) Scientific Programme Report TR-4, University of Magdeburg, Germany. Retrieved December 7, 2011 from http://www.minema.di.fc.ul.pt/reports/report_routing-protocols-survey-final.pdf

Liu, J., Fu, F., Xiao, J., & Lu, Y. (2007). Secure routing for mobile ad hoc networks. *Proceedings of Eight ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing.*

Maltz, D. A. (1999). *Resource management in multi-hop ad hoc networks*. Carnegie-Mellon University, School of Computer Science, Technical Report CMU-CS-00-150.

Mobile Ad-hoc Networks (MANET). (2011). IETF Routing Area Working Group. Retrieved December 7, 2011 from http://datatracker.ietf.org/wg/manet/charter

Mohseni, S.,Hassan, R., Patel, A., & Razali, R. (2010). Comparative review study of reactive and proactive routing protocols in MANETs. *Proceedings of 4th IEEE International Conference on Digital Ecosystems and Technologies,* Abu Dhabi, United Arab Emirates.

Papadimitratos, P., & Haas, Z. (2003). Secure link state routing for mobile ad hoc networks. *Proceedings of IEEE Workshop on Security and Assurance in Ad Hoc Networks*.

Patmaik, G. K., & Gore, M. M. (2011). Trustworthy path discovery in MANET – A message oriented cross-correlation approach. *Proceedings of 2011 Workshops of International Conference on Advanced Information Networking and Applications (WAINA).* USA: IEEE Press, 170-177.

Perkins, C., Beldin-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing*. IETF, Request for Comments (RFC) 3561.

Perkins, C.E. & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications,* ACM, New Youk, USA.

Perrig, A., Song, D., Canetti, R, Tygar, J. D., & Briscoe, B. (2005). *Timed efficient streamless-tolerant authentication*. IETF, Request for Comments (RFC) 4082.

Pirzada, A. A., & McDonald, C. (2004). Establishing trust in pure ad-hoc networks. *Proceedings of 27th Australasian Computer Science Conference.* Retrieved December 11, 2011 from http://crpit.com/confpapers/CRPITV26Pirzada1.pdf

Pushpa, A. M. (2009). Trust based secure routing in AODV routing protocol. *Proceedings of 2009 International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, USA: IEEE Press, 1-6 .

Qin, L., & Kunz, T. (2004). *Survey on mobile ad hoc network routing protocols and cross-layer design.* Technical report SCE-04-14, Systems and Computer Engineering, Carleton University, Canada. Retrieved December 7, 2011 from http://kunz-pc.sce.carleton.ca/Thesis/RoutingSurvey.pdf

Ramana, K. S., Chari, A. A., & Kasiviswanth, N. (2010). A survey on trust management for mobile ad hoc networks. *International Journal of Network Security & Its Application (IJNSA), 2*(2), 75-85. Retrieved December 10, 2011 from http://airccse.org/journal/nsa/0410ijnsa6.pdf

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks. *Proceedings of the 10th International Conference on Network Protocols (ICNP'02).*

Singh, U. (2011). Secure routing protocol in mobile ad hoc networks – A survey and taxonomy. *International Journal of Reviews in Computing, 7*(2), 9-17. Retrieved December 10, 2011 from http://www.ijric.org/volumes/Vol7/Vol7No2.pdf

Taneja S., & Kush, A. (2010). A survey of routing protocols in mobile ad hoc network. *International Journal of Innovation, Management and Technology, 1*(3), 279-285.

Tomar, P., Suri, P. K., & Soni, M. K. (2010). A comparative study for secure routing in MANET. *International Journal of Computer Applications, 4*(5), 17-22.

Wang, D., Hu, M., & Zhi, H. (2008). A survey of secure routing in ad hoc networks. *Proceedings of the Ninth International Conference on Web-Age Information Management WAIM '08*, USA: IEEE Press, 482-486.

Yi, S, Naldurg, P., & Kravets, R. (2001). Security-aware ad hoc routing for wireless networks. *Second ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'01)*, 2001.

Zapata, M. G. & Asokan, N. (2002). Secure ad hoc on-demand distance vector (SAODV) routing. *ACM Mobile Computing and Communications Review, 3*(6), 106-107.

Biographies

Jonny KARLSSON received his Bachelor of Science degree in Information Technology and is since May 2002 research assistant and teacher at Arcada University of Applied Sciences, Helsinki, Finland. In January 2009 he started PhD studies in security of future networks at the Open University, Milton Keynes, UK. His current research interests include security of wireless and mobile networks.

Laurence Sean DOOLEY was awarded his B.Sc. (Hons), M.Sc. and Ph.D. degrees in Electrical and Electronic Engineering from the University of Wales/Cymru (Swansea) in 1981, 1983 and 1987 respectively. He is *Chair of Information and Communication Technologies* in the Department of Communication and Systems at The Open University, UK, where his research interests include: cognitive radio systems, distributed source coding, multimodal medical imaging, MANET and LTE/4G security, educational technologies and SME technology/knowledge transfer. He has co-edited one book and published 220 peer-reviewed scientific journals, book chapters, monographs and conference papers, with 3 papers being awarded international research prizes/nominations. He received the 2010 *IEEE Certificate of Award* for promoting international exchange in recognition of his services to the IEEE international conference series on signal processing. He has supervised 18 PhD/MPhil students to completion together with being a recipient of significant public and private sector funding to support his multifaceted research. He is a Chartered Engineer, a Fellow of the British Computer Society and a Senior Member of the IEEE, as well as being a Vice President of the Crawshays Rugby Football Club.

Göran PULKKIS received in 1983 his doctoral degree at Helsinki University of Technology and is presently senior lecturer and researcher in computer science and engineering at Arcada University of Applied Sciences, Helsinki, Finland. His current research interests include network security and applied cryptography.