

ROUTING SECURITY - an overview

Heikki Ollikainen
Helsinki University of Technology
heikki.ollikainen@hut.fi

Abstract

Routing has an extensive role in Internet communication. Traditional interior and exterior routing protocols do not provide adequate security mechanisms for current needs of Internet communication, and they do not consider any mobility requirements. Routing requirements, methods and protocols vary between fixed and mobile network architectures even most routing protocols are designed to forward packets along the shortest way. The goal of routing security is to provide efficient, secure and robust way for routing. This paper introduces some common security problems and solutions for routing security from overall point of view

1 Introduction

Internet has globally spread out fast during past decade. Moreover, it has become an information gateway between people all around the world. Therefore, security has raised as an important issue when different participants - e.g. operators, other ISPs - are concerned and they are providing services that requires security, encryption, reliability and integrity among clients and servers. Further, IP convergence is also setting new requirements and challenges for secure routing when different types of networks are working seamlessly together over IP protocol. Therefore, some security improvements have to be made for traditional routing protocols in the terms of routing security and new design mechanisms and approaches have to be defined for MANET (Mobile and Ad-hoc Network) type of communication networks.

This paper provides an overview to routing and routing security. Some typical requirements, problems and solutions are discussed and the routing security is concerned from both point of views: traditional and MANET type of network. However, this paper focuses mostly to the routing security problems in fixed networks or the problems related routing protocols that are working rather static routing environment. MANET routing protocols are still strongly evolving and the role of ad hoc networks is unclear for example in the scope of 4G networks. Some security problems (see chapter 4) and solutions (see chapter 5) are also described. Finally, most important issues are emphasized, summarized and conclusions are expressed at the end of the paper.

2 Overview of Routing

2.1 Network Characteristics

A computer network is a set of computers that are connected and able to exchange messages. Traditional networks forms a communication network over certain area, and depending on the size of area network, it is defined as LAN, WAN, MAN or PAN. Each node is connected to network according to certain network topology, routing is carried out over IP and different area networks are connected to each other with different network components (e.g. bridges, switches). Internet - as we understand the existence of it at the moment - is mostly build in such way over TCP/IP stack.

Mobile and wireless networks are currently understood as cellular routing architecture. Moreover, there is some basic concepts that are relating to cellular telephony are such as multiple access techniques, frequency reuse, speech coding, mobility, ciphering, authentication and network planning [6]. Wireless networks are evolving fast toward IP convergence, which means that MN (Mobile Node) is able to use seamlessly and access independently different IP services between radio access and core network. Static base stations (3GPP R4) or IP backbone (All IP in 3GPP R5) in offers routing for MN when it is accessing into network.

Ad-hoc network characteristics are defined purpose-specific, autonomous, dynamic and transient [5]. Ad-hoc networks differ significantly from traditional networks, since there is no fixed base stations or routers - a mobile node functions as host and router. Therefore, this creates very dynamical nature of ad-hoc network in general - host neighbor relationships and domain memberships may vary fast. Ad-hoc network supports mobility and other MANET properties such as dynamic topologies, bandwidth-constrained variable capacity links, power-constrained and limited physical security [5]. Therefore, security requirements are usually higher since transmission media is shared. In addition, ad-hoc network may have unidirectional links, which is a difference compared to fixed networks that rely on bi-directional links on routing.

An ad-hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. The primary goal of such an ad hoc network routing protocol is correct and efficient route

establishment between a pair of nodes so that messages may be delivered in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption.

There are currently two variations of mobile wireless networks. The classification can be done roughly in two main categories: infrastructured and non-infrastructured network. Moreover, the first option is known as a network that includes fixed and wired gateways. The bridges are known as base stations. Therefore, a MN (mobile node) within these networks connects to - and communicates with it - the nearest base station that is within the communication radius. When mobile travels through the network, hand-off occur when MN arrives in the area of new base station. Typical application of this network exploits for example WLAN. The second type of mobile wireless network is the non-infrastructured mobile network, commonly known as ad hoc network. Ad hoc networks have no fixed base station or routers. All nodes in the ad hoc network are capable of movement and can be connected dynamically in the in an arbitrary manner. Moreover, nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Routing protocols are the key factor for providing connectivity. Furthermore, wireless, mobile and ad hoc networks require own routing protocols that will be able notify these mobility requirements, and dynamical nature of the network to carry out the routing and connectivity tasks. Therefore, the routing protocols that are working in traditional, fixed/wired or rather static environment are not suitable for routing task in these wireless and mobile networks such as mobile and ad hoc networks. Each routing environment (wired/wireless) requires its own protocols or modification to existing routing protocols.

2.2 Routing Protocols

Routing protocols are providing the routing of IP datagrams over the Internet. Routers [16] and switches are responsible for making decisions how the destination is chosen along the optimal path. The basic problem of routing is to find low-cost path between any two nodes of the network [6]. There are many static and dynamic routing protocols available for fixed network in Internet. In general, these are categorized into two main categories: Interior (RIP [1], OSPF [10]) and exterior [9] routing protocols (BGP [8], EGP [13]). The difference of interior and exterior protocols is depending on whether they are used within or between autonomous systems that can be viewed as a logical portion of much larger IP network [6].

However, the traditional routing protocols are not mostly suitable for MANET type of dynamic, mobile and secure-sensitive networks, for example they do not consider the mobility requirements at all. MANET routing protocols can be divided into distance-vector, link-state and hybrid protocols. Current routing security is based mainly into improvements of these base protocols, such as distance-vector proto-

col RIPv2 [2] and link-stated protocol OSPFv2 [7], [11].

Ad-hoc routing protocols can be divided into two main categories: table driven (DSDW, WRP, STAR) and on-demand (AODV [14], TORA, DSR [19], ABR, TBRTF [20]). Table driven protocols resemble fixed network routing protocols in respect of that hosts build a routing table of the whole network. Therefore, if network topology experiences a change, information is updated through the network. On the contrary, on-demand protocols do not require maintaining complete structure of routing table - host establishes route when it is required on-demand base [14].

MANET routing protocols can be divided into three main categories: table driven or proactive, source-initiated on-demand or reactive and hybrid routing protocols [5]. Table driven or proactive routing protocols require the periodical refreshing or updating of the routing information. Moreover, this way each node can operate with consistent and up-to-date routing tables. When using proactive routing protocol and the route is established, the uses of it is efficient. Proactive routing protocols are not suitable for ad hoc network, since the requirements for constant and heavy routing information exchange. On the contrary, source-initiated on-demand or reactive routing protocols do not require periodical update of the routing information. Moreover, the routing data is updated to the necessary nodes only when required. Therefore, many of the MANET routing protocols are on-demand driven for the optimization purposes. This means that the routing traffic is only generated when the routing fabric must really be changed. However, source-initiated on-demand or reactive routing protocols create a lot of overhead when the route identity being determined, since the routes are not necessarily up to date when required. Hybrid routing protocols combine both approaches, and can be used under certain conditions, for example table-driven protocols can be used between the networks and on-demand protocols can be used inside the the network [5].

2.3 Traditional Networks

Security aspects that are relevant for computer security in general apply also for routing security in fixed and MANET networks: confidentiality, integrity, authentication, and non-denial [5].

As notified, traditional routing protocols functions in rather static fabrics in fixed network, and typically apply very limited methods for security. Original routing protocols define usually simple security mechanisms or there is no security means at all, for example RIPv1 (Routing Information Protocol), that is one of the most widely used routing protocols in Internet, defines authentication scheme [1]. RIPv2 provides authentication of routing information with clear-text password (2-octet). The method does not provide security required in current Internet, since the passwords are not protected and it is possible to capture and modify them easily [2]. RIPv2 provides also an extension that defines MD5 authentication that includes secret key generation, negotiation and storage protection [2]. The result of the authentication is

confirmed with unique 4-octet sequence number. However, the protocol leaves out from scope the protection of secret keys and their management.

OSPFv2 routing exchanges can also be authenticated. The OSPFv2 packet header includes an authentication type field, and 64-bits of data for use by the appropriate authentication scheme. The authentication type is configurable on a per-interface basis. Additionally, authentication data is also configurable per-interface basis. OSPFv2 provides 3 types for authentication: NULL authentication, simple password and cryptographic authentication. NULL authentication means that routing exchanges are not authenticated and 64-bit authentication field can contain anything, data included to it is not processed in message parser [2]. Simple password authentication type is configured per-network basis. All packets sent on a particular network must have this configured value in their OSPFv2 header 64-bit authentication field. This serves as clear-text 64-bit password. In addition, the whole contents of OSPF packet are checksummed in order to detect the data corruption [2]. Cryptographic authentication type requires a shared secret key is configured in all routers attached to a common network. For each OSPF protocol packet, the key is used to generate and verify a "message digest" that is appended to the end of the OSPF packet. The message digest is a result of one-way function of the OSPF protocol packet and the secret key. Since the secret key is never sent over the network in the clear, protection is provided against passive attacks [2]. The OSPFv2 protocol specification specifies the use of cryptographic authentication type implicitly only with MD5 algorithm.

2.4 MANET networks

Security considerations in MANET routing protocols are still evolving. Routing protocols are expected to work under dynamically changing conditions of the networks. Protocol security is an extension when core protocols are completed and tested to be reliable and robust enough. Most MANET network routing protocols does not have RFC numbers, even the current drafts are relatively old. Though, MANET working group has specified routing protocols and some security issues are discussed.

For example, OLSR (Optimized Link Stated Routing Protocol) does not currently specify any security means [21]. However, it is a target for various attacks that are related to confidentiality, integrity, node identification and interaction with external routing domains. OLSR is a proactive routing protocol that means that it diffuses topology information periodically. Moreover, if used unprotected, network topology is revealed to anyone who is interested of OLSR control messages. In OLSR, each node is transmitting topology information through the network with HELLO messages. If a node get malfunction, transmits invalid information, network integrity may be compromised. Therefore, authentication is needed. Moreover, when OLSR is operating with external routing domains, it must not allow potentially insecure and unreliable information to be transmitted from host OLSR domain to external routing domains, if the routing protocol

governing that domain permits. Finally, OLSR makes assumption that each node has unique IP address.

AODV (Ad Hoc On-Demand Distance Vector) security consideration states that AODV does not specify any special security measures at the moment [14]. Route protocols, however, are prime targets for impersonation attacks. In the case, when network membership is known and there is a danger of impersonation attacks, AODV control messages must be protected with authentication techniques [14]. Moreover, specification does not introduce such authentication mechanism, but the use of IPSEC AH (Authentication Header) is appropriate choice for the cases where the nodes share an appropriate secure association that enables the use of AH [15].

Use of IPSEC is more clear in IPv6 networks. In the case of OSPFv3, it relies on the IP AH and IP encapsulating security payload to ensure integrity, authentication and confidentiality of routing exchanges. However, when IPSEC is used to protect OSPFv3 packets, it is important for the implementation to check the IPSEC SA (Secure Association), and local SA database to make sure that the packet originates from a source that is trusted for OSPFv3 purposes [12].

3 Routing security requirements and challenges

ISA (Internet Security Association) has proposed an architecture for the inclusion of security facilities in the design of protocols to be used in the Internet. ISA lists four fundamental rules for security [18]: vulnerability, threat, security service and countermeasures.

Moreover, vulnerability is a weakness in security system, a threat is a possibly violation of security and it requires an attacker that is able to exploit this vulnerability. Threats can be classified into two main categories disclosure and disruption:

- Disclosure is an event that in which an entity gains access to data that results in an authorized entity to receive.
- Disruption is an event that interrupts or prevents the correct operation of system to function.

Further, security services are security measures how to minimized or prevent threats and vulnerabilities. In general, security services includes confidentiality, integrity, authentication, non-repudiation, availability and countermeasures of routing data. Therefore, these security requirements should be notified when designing a routing security mechanism for routing protocol. Countermeasures are mechanisms or features of routing protocol that provides a security service. For example of countermeasures can include authentication scheme and encryption of network traffic to provide confidentiality using for example challenge-response authentication scheme.

Current routing security challenges are related to security requirements and protocol specification discussed above. Ex-

isting traditional routing (e.g. OSPFv2, RIPv2) protocols require more detailed specification of routing security options (e.g. encryption and authentication option), and how to use them in network as defined in RIPv2 MD5 authentication extension [29]. In general, MANET routing protocol design does not consider the fundamental security aspects defined by ISA. Moreover, routing protocol design is clearly aiming for core protocol design excluding the routing security features. For example, OLSRP [21] protocol specification does not specify any security measures. Nonetheless, when security is not considered as part of core protocol design, notifying of routing security fundamentals in protocol expansion is more difficult, if not impossible. However, effective security services can be specified after completing the core protocol design. Further, for example, secure border gateway protocol [25] propose encryption of all BGP messages between peers using session keys exchanged at BGP link establishment time. In general, this improvement offers integrity and authenticity of all path attributes whose values are valid for at most hops, and confidentiality of all routing exchanges.

Another challenge is to improve computational cost of using different encryption methods in routing. Moreover, it means that routing security requires improvement of different authentication and encryption algorithms. Therefore, it is expected that future routing security solutions are able to overcome the deficiencies identified in previous researches, such as time consuming, limited applications, high storage and cryptographic computational costs for volatile environments. Nonetheless, for example, the digital signature size and computational cost of routing protocols are fixed irrespective of the size or content of message to be signed.

In general, there has been research from routing security area. However, most security solutions have been ignored by standardization and working groups. As an opinion, most hardest challenge is to propose a routing security solutions that would be accepted by IETF or other well-known standardization organization. Further, another solution or a challenge is to develop a solution that would satisfy the current security needs of Internet and introduce them into existing traditional routing protocols or MANET routing protocols, that are mostly missing security measures and requiring the design of security mechanisms.

4 Security Problems

Routing protocols are a target for several types of attacks in general. The following section presents possible routing problems.

4.1 Routing information confidentiality

Routing information is basically local information about the local host. The main task of routing security is to ensure routing information exchange. Moreover, this means the correctness of routing information base. Definition for correct routing information means the dynamically updated location information. For example, MANET networks deploy binding mechanism. Moreover, the location of MNs can be main-

tained and exchanged between the nodes correctly. Maintaining the location information correctness is crucial in dynamically changing routing network. For example, binding updates must be authenticated in Mobile IP. If not authenticated, it may lead to situation, where opponent can eavesdrop and redirect the traffic between MN (Mobile Node), FA (Foreign Agent) and/or FA, HA (Home Agent). Therefore, it is vulnerable to distortion of binding update [23].

In MANET, integrity threats usually involve tampering with the routing information. Therefore, the integrity of the routing message is crucial for maintaining the the routing routes of the dynamic MANET network. In general, the result of these attacks may propagate to the whole MANET network, if routing protocol does not define a robust scheme for recovering from this kind of badly functioning action [4].

4.2 Faulty source

Source routing provides a massive security hole for Internet, moreover, its not very good feature in Internet. Loose source routing has been an IP option for a long time. Main security problem with this option (LSR) is that several IP stacks reverse a source route when responding to a source-routed packet. Therefore, it would be trivial for an attacker to spoof a packet as coming from a trusted IP address that is source routed through an IP address that attacker is sniffing. As a result, victim sends return traffic to the spoofed source, but loose source routing it through the attacker. Attacker can carry on whole TCP sessions in this way without worrying about attacking weaknesses in TCP sequence numbers or lost packets [22].

However, some of the current MANET routing protocols apply source routing - DSRP (Dynamic Source Routing Protocol). Moreover, to improve routing security most routers in traditional networks are configured to deny service from all source routing requests to prevent spoofing and redirection.

For example, if router is compromised, it is possible that only the links or subnets directly being connected to the evil router are affected. However, it is more likely the case that all erroneous information is flooded to all routers within the autonomous system - for example in link-state routing. Further, it is fairly easy to detect such problems when router is sending false router advertisements. For example, if router A and router B are on the same link, and both routers are sending router advertisements, eventually it will detected the conflicting router advertisements.

4.3 Denial-Of-Service

Usually denial of service attack means forging the source address for IP datagrams. Denial of service attack is also known as DOS attack. As a result server is fooled, and it might cause unwanted behavior. First action is to forge the source address of your target machine and send packets to other machines. Moreover, it responses back to the forged address. The target experiences enormous traffic, if there are many senders. Second action is to forge an illegal

source address - various broadcast addresses are common ones. Moreover, when target machine receives these datagrams, it replies to the forged broadcast address. As a result, all machines in the same network with target machine replies to these broadcast packets, flooding the network with traffic as one initial packet triggers dozens or hundreds of replies.

Therefore, from the routing security point of view, might be dangerous to make any assumptions that each node has unique IP address and routing domain must be very careful when interacting with external routing domains. Moreover, redundancies in communication increase the possibility that each node receives proper routing information. Redundancies allow compromised nodes to be detected and prevented performing malicious actions [5].

There are a number of a vulnerabilities that allow strategically placed intruder to fabricate, modify, replay or delete routing information. Further, an intruder can compromise the network in a number of a ways using these capabilities. In general, the modification of routing updates allows an intruder to reconfigure the logical routing structure of an Internet, potentially resulting in the denial of service, the disclosure of network traffic, and inaccurate accounting of network resources. Further, replay and deletion of routing updates blocks the evolution of subsets of the logical routing structure. Moreover, it might reset it to an earlier configuration. Nonetheless, in the case of BGP, specific attacks include [25]:

- An intruder subverts an authorized BGP host.
- An unauthorized BGP host established a BGP link with an authorized BGP host.
- An intruder subverts a link through which BGP links pass.

Moreover, in the case of BGP, these attacks exploit vulnerabilities that reflect the lack of access control, authentication and integrity of routing messages.

Intruder might try to modify, replay and delete data packets. The effectiveness of these attacks at deceiving or disrupting the source and destination process depends on the end-to-end protocols in use at the transport layer and above, and its not a routing protocol issue. However, the effectiveness of these attacks at deceiving the intermediate routing nodes is not an end-to-end protocol issue. Countermeasures to these vulnerabilities depends on mechanisms in the network or lower layers of the protocol hierarchy. The appropriateness and effectiveness of end-to-end versus link-layer security measures is a fundamental issue in the design of the Internet protocols. While in general the issue do not involve routing protocol mechanisms, two exceptions include the ability to use multiple paths to a single destination, and the inclusion of authentication and process control mechanisms in the packet forwarding function [25].

There is some attack types (e.g. impersonation) that can not be specific categorized. Moreover, threats can be divide mostly in three groups specified by [3]. As presented above

the denial of service threats involve the exhaustion of explicitly or arbitrarily. However, there exist more worse versions from DOS nowadays. DDOS (Distributed Denial Of Service) threats involve a large amount of distributed hosts attacking the systems in the same time. This kind of attack is probably impossible to prevent. The best alternative is to disconnect the node off the network for a while or block the incoming traffic from certain address.

The problem with MANET networks is that the network addresses are not fixed. Therefore, the blocking of the traffic against DOS or DDOS attack from specific address is not working with MANET networks. However, within any system the denial of service attacks will not likely to be targeted at any centralized resource. Therefore, there should be only distributed services in MANET system.

4.4 Disclosure of Routing Message

It is more or less easy for an intruder to gain access to routing traffic. In general, routing traffic includes information about the appropriate next hop to reach a destination, and the path taken by traffic to different destinations. Therefore, next hop information is available from sources such as monitoring authorized traffic to the desired destination for the next hop it uses, and therefore cannot be protected solely by measures directed at the routing traffic. However, under some specific circumstances, the path used to reach different destinations may be considered confidential. In the case of BGP specific attacks to obtain this path information include [25]:

- An intruder subverts an authorized BGP host.
- An intruder subverts a link through which BGP links pass

However, the vulnerabilities these attacks use are the lack of confidentiality of peer links. Further, it considers also the level of trust placed in BGP host.

4.5 Intrusions in routing

In general, intrusion detection mechanism is related to the area of network security management. Intrusion detection is a common issue when most network events are unobserved. Moreover, it might become very difficult to detect certain network infrastructure attacks. Further, for example, mostly link-state protocols (e.g OSPF) assume that all participating routers are always trusted. This is the case if a link state advertisement is sent from router A to router B and advertisement contains router A's valid authentication. Moreover, router B will trust to the received link state advertisement and update its routing table properly. However, this assumption is working only when handling with attacks from outside of network, but it is unrealistic if there is possibility for internal attacks too.[28]

Link state routing protocols are flooding the link state information through the network. Moreover, it means that eventually every router in the network will have identical topology information about the network. In general, there might

be a situation when link state advertisement visits in every node before reaching its destination. Nonetheless, an evil router may cause much more damage than the source router. For example, if link state advertisements come from many different source routers and advertisements will be flooded through intermediate router, and then compromising one single router implies tampering the network status for many different network segments in worst case scenario. Therefore, preventing intermediate routers to modify the link state advertisements is an important goal in developing secure link-state routing protocols.[34]

For example, if we would try to solve the faulty intermediate router problem in the OSPF protocol, it would cause us to be responsible for the cost of RSA/MD5 in software. Moreover, in general it would mean $2 \cdot 10^6$ usec per link-state advertisement [34]. Therefore, it kind of explains why this solution is not supported by major standardization organizations like IETF. In fact, unless we can develop a secure and more efficient public-key system, the faulty intermediate router problem can not be prevented by the standard link-state protocol such as OSPF.

In MANET, compromised nodes are one of the most centralized security threats, since the whole routing fabric is being generated and maintained by the nodes themselves without any help from base stations and routers. Therefore, the security of the whole system may be broken with an attack on a single point of the system [4]. For example, in MANET there can be a node that performs certification with its private key. If the attacking this node, the MANET network may be compromised. Therefore, distributed security services are needed to prevent such a problems [5].

5 Routing security solutions

5.1 Securing Border gateway Protocol

Routing protocols dynamically configure the packet forwarding function in Internet that allows for the continued delivery of packets in spite of changes in network topology. Therefore, these changes typically occur due ongoing introduction, failure and repair of network links and routing nodes, which protocols have been designed to accommodate [25]. The compromise of the routing function in the global Internet can lead to denial of the network service, the disclosure or modification of sensitive routing information or the diversion of network traffic to an attacker. Further, it is caused by the reconfiguration of the logical routing structure. Current, routing protocols contain few measures, if any mechanisms to provide for the security of their operation.

Secure BGP [25] proposes several countermeasures for improving routing security. Encryption of routing messages between peers in the network, add sequence number to protect against replayed and deleted messages, use an UPDATE sequence number or timestamp to protect against replayed UPDATE messages. Further, secure BGP proposes to add PREDECESSOR path attribute to indicate autonomous system prior to the destination autonomous system for the current

route. Moreover, it allows the verification of the path information in a manner similar to path-finding algorithms to detect loops. Nonetheless, digitally sign all unchanging UPDATE fields whose values are fixed on creation by the BGP host originating or most recently aggregating the route. This provides for the integrity and authenticity for the full route from source to destination.

Peer-to-peer encryption is based to the establishment of each BGP link, a session key is exchanged by the peers for use in encrypting each BGP message transmitted over that link. Moreover, the purpose is to provide confidentiality of the messages. The other purpose is to provide authentic and integrity of KEEPALIVE and NOTIFICATION messages. Further, it involves distribution of some path attributes - for example next hop - carried in UPDATE messages. These attributes can be modified in autonomous system. Nonetheless, two important issues is worth mentioning when using peer-to-peer encryption for authenticity and integrity of these path attributes: recipient of these path attributes receives them from either the most recent modifier, or via single relay that is an internal peer, and the assumption that internal peers are trusted [25].

When sequence number is added into each messages, it is initialized to zero on establishment of BGP link. Moreover, it is incremented with each message. On detection of a skipped or repeated sequence number, the BGP link is terminated with NOTIFICATION message. However, the size of the sequence number is made large enough to minimize the change of it cycling back to zero. Further, sequence number is reset when link is terminated and new link established that also means the establishment of a new session key [25].

BGP provides specifically peer-to-peer encryption and peer-to-peer sequence number that provides corruption detection, sequencing, acknowledgement, and retransmission mechanisms that are redundant to those provided by TCP. Moreover, these improvements are to be considered effective countermeasures that provide secure transport services, that is not available in many other current transport protocols. Further, it is a sign of insecurity of TCP mechanisms. However, the secure measures BGP provides is not enough if a secure network or transport protocol is not used.

5.2 Use of digital signature

Currently, many Internet routing protocols (e.g OSPF and RIP) introduce authentication schemes for improving routing security. Moreover, it means reservation of fields in the format for authentication use. However, the authentication schemes in these protocols are based to clear-text password. Therefore, cleartext passwords are not strong enough against for example sniffing attacks. Further, as noted cryptographic protection (e.g peer-to-peer encryption) of source authenticity and message integrity provides stronger protection. In general, considerable work has been done with various routing protocols, for example [31], [30], [33] and [32].

Further, many of these protocols use public-key digital sig-

nature for ensuring authenticity and integrity of routing messages. Moreover, using digital signatures by itself does not protect against the internal threat of a default router. However, digital signature does protect routing information against faulty intermediate routers as well as external intruders. Further, using digital signature can be achieved data robustness to faults in non-routing nodes in Internet, robustness to faults in routing nodes concerning links and simple robustness of all other faults in routing nodes. However, public-key digital signatures can be costly that means generating and verifying public-key digital are quite time consuming. Moreover, in routing context in means that context switching happens frequently and digital signatures have to be generated and verified in real time. In general, use of digital signatures with link-state routing protocols can be a problem. Moreover, it means that signature is verified by a large number of routers. [26]

Previous research [33] has identified the high costs of using public-key digital signature in securing link-state protocols. Two methods has been proposed secure processing of link-state updates. Therefore, first technique (SLS) proposes the use of single chain of hashes as authentication tokens. Moreover, what can be achieved by that is each hash can be seen as a one-time signature for one bit of information that means no link-adjacent to the signing router changes state. Further, the seminar paper [33] proposes another solution (FLS) in order to sign more than one bit of information. The main purpose of FLS is to use set of hash chains with every pair of them represent the status, for example UP and DOWN considering of a single link. Therefore, hash chains can be seen as one-time signatures of the status of each link.

Murphy [30] has proposed a public key signature scheme to protect the integrity of link state advertisements flooded through the network. Moreover, the public-key infrastructure is exploited when the source router uses its private-key to sign the MD5 value for link state advertisement created. Nonetheless, since the intermediate routers do not know the private key of the source router, it is impossible for them to tamper the advertisements without being detected. However, every receiver of link state advertisements must use the source routers public key to verify its integrity. Therefore, the scheme is very secure against compromised intermediate routers. However, as noted in chapter 3, it is very expensive to use create, implement and use the public-key systems.

5.3 A link state routing update

Routers exchange routing messages. In general, it means that routers exchange control packages to be able to construct routing tables and smoothly forward packages from source to destination. Routing security has to provide security measures for securing routing traffic from different possible threats [34]:

- Packet generation that means masquerading as a particular router sends bogus control packages to other routers.
- Packet alteration that means modifying control or data

packets in transit.

- Packet removal that means removing control packets to prevent information about network changes from propagating to other routers.
- Missrouting that means routing control or data packets so they will not reach correct destination.
- Sniffing that means eavesdropping the routing data and performing traffic analysis.

Further, routing security solutions has to consider protection mechanisms such as data authenticity, ordering and correctness of control packets have been proposed [27] that introduces an efficient authentication scheme for protecting control packets in link state routing. Cheung and Levit [34] has done some earlier research how to use cooperative intrusion detection. Cheung and Levit's research focusses on protecting routing infrastructures from routers that incorrectly drop and misroute packets. Authentication scheme presented in [27] goals for minimizing the cost of performing link state update authentication when the network components are working normally. Moreover, that is the case most of the times. Further, the efficient authentication scheme assumes, that router uses a key and another symmetric-key based data authentication scheme to sign a link state update. Nonetheless, the link state update and the signature are disseminated to all other routers. Therefore, receiving router accepts the routing update as if it were authenticated.

However, there might be a situation when the key arrives and the receiving router verifies the authenticity of the key using a secure and efficient method. Moreover, the verified key will be used to verify the authenticity of link state update using the symmetric-key based data authentication scheme. However, still the signature generation and verification can be done very efficiently using a symmetric-key based data authentication scheme.

Therefore, if false routing updates are detected, a distributed diagnosis protocol will be invoked to locate the malicious router. Further, the network reconfiguration will be carried out and disconnect those routers to restore the operational status of the network.[27]

5.4 Traffic analysis in intrusion detection

In intrusion detection, it is interesting to analyze how the evil router will be detected in the network or can unpreventable security problem, such as faulty intermediate router, be possibly detected or isolated by distributed intrusion detection system. A typical solution includes the action where each router log all the router advertisements it receives and forwards over some specific period of time. Further, analyzing the received data its possible to identify the trusted routers in forwarding the advertisements. However, this intrusion detection mechanism includes some problems [28]:

- The amount of data in the log files might get intolerable form that analysis and correlation will take a fairly long time to detect faulty routers. However, most likely the evil routers will be detected in the end.

- The network bandwidth needed for transferring the analysis data between detection modules can be very high.

6 Consideration and Conclusions

How is the routing security concept understood at the moment? Currently, standards are presenting some extensions (e.g. OSPFv2, OSPFv3, RIPv2) to routing protocols how to improve routing security. Moreover, this means authentication schemes, authentication options in the terms of traditional, fixed and/or wired networks. Current interior and exterior routing protocols are capable to improve routing security by identifying the routing information with simple clear-text password and checksum (e.g MD5). However, as concluded earlier, current methods are not efficient enough for the Internet. Therefore, some possible attacks can be prevented by using loose source routing option in IP header. Therefore, routers should deny services for all source routing requests to prevent spoofing and redirection. In general point of view of routing security, security considerations have been ignored, and improvements are retrofitted into existing routing protocols.

There exists several proposals how to improve routing security, for example with digital signatures, new authentication schemes, traffic analysis and intrusion detection mechanisms. However, most researchers agrees with the issues related to the cost of using encryption algorithms and control data. Further, it means that the systems using for example public-key method for securing routing messages between peers is quite expensive and time consuming. This means that new and more efficient algorithms are required. In fact, it is fairly possible that standard and commonly accepted routing protocols can not include this kind of security mechanism into core protocol. The large amount of control data may cause a problem if it is required to do reliable traffic analysis for intrusion detection purposes.

Mobile and MANET network routing protocols are strongly evolving. This has been effecting into routing security so that security consideration are mostly ignored at all, since the focus is in core protocol design. However, MANET routing protocols (e.g. OLSR, and AODV) standards have been identifying some possible threats that are obvious routing in MANET environment. In MANET, the possibility of compromised nodes can potentially cause the corruption of the whole MANET network. Therefore, distributed security services are required to prevent such problems.

Mobile wireless networks are generally more flexible to physical security threats than fixed networks. This means that existing link-level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats. Link-level encryption at the network layer is one of the most pressing issues and inter-router authentication prior to the exchange of network control information. Several levels of authentication ranging from no security and simple shared-key approaches, to full public key infrastructure-based authentication mechanisms will be explored by the

MANET group [24].

Mobile IP itself does not provide much security or privacy protection mechanism for routing information. Further, the security issues have to be handled with outside services (e.g. link-layer encryption) or using IPSEC that may provide solutions for the use of mobile IP. A major issue in the Mobile IP is securing the critical information such as locations of MNs.

References

- [1] Routing Information Protocol version 1 RFC 1058, IETF Network working Group, June 1988
- [2] Routing Information Protocol version 2 RFC 2453, IETF Network working Group, November 1998
- [3] E. Amoroso Fundamentals of computer security technology Prentice-Hall, Englewood, USA, 1994
- [4] L. Zhou, Haas Securing Ad Hoc Networks [referred 29.03.2004] <http://www.ee.cornell.edu/haas/Publications/network99.ps>
- [5] V. Karpijoki. Signalling and Routing Security in Mobile and Ad-hoc Network In *Department of Computer Science*, Espoo, Finland, May 2000, Helsinki University of Technology
- [6] B. Patil, Y. Saifullah, S. Faccin, S. Sreemanthula, L. Aravamudhan, S. Sharma, R. Mononen *IP in Wireless Networks*. Pearson Education Inc. 2003.
- [7] Open Shortest Path first version 2 RFC 1850, IETF Network working Group, November 1998
- [8] Border Gateway Protocol RFC 1105, IETF Network working Group, June 1989
- [9] Exterior routing protocol formal defition RFC 904, IETF Network working Group, November 1984
- [10] Open Shortest Path first version 1 RFC 1058, IETF Network working Group
- [11] Open Shortest Path first version 2 RFC 2328, IETF Network working Group, April 1998
- [12] Open Shortest Path first version 3 RFC 2740, IETF Network working Group, December 1999
- [13] Exterior Gateway Protocol RFC 0827, IETF Network working Group, October 1982
- [14] Ad hoc On-Deman distance Vector RFC 3561, Network working Group, July 2003
- [15] Internet Protocol Security RFC 2401, IETF Network working Group, November 1998
- [16] Requirements for IP Version 4 Routers RFC 1812, IETF Network working Group, November 1998
- [17] Routing Protocol Security Requirements Internet Draft, IETF Network working Group, June 1995

- [18] Routing security requirements Internet Draft, IETF Network working Group, November 1998
- [19] Dynamic Source Routing Protocol Internet Draft, MANET working Group, November 1998
- [20] TBRTF Internet Draft, MANET working Group, November 1998
- [21] OLSR RFC 3626, MANET working Group, October 2003
- [22] Richard Stevens and Gary Wright *TCP/IP Illustrated, Volume 2*. Pearson Education Inc. 2003.
- [23] Reverse tunneling for mobile IP RFC 1058, IETF Network working Group, May 1998
- [24] MANET RFC 2501, MANET working Group, January 1999
- [25] S. Kent, C. Lynn, J. Mikkelsen, K. Seo Securing Border Gateway Protocol In *BBN Technologies*, USA, California, 2001, University of California
- [26] K. Zang Efficient Protocols for signing Routing Messages In *Cambridge University Computer Laboratory*, UK, Cambridge, 2001, University of Cambridge.
- [27] S.Cheung An Efficient Message Authentication Scheme for Link State Routing In *Department of Computer Science*, USA, California, 2001, University of California
- [28] F. Shytsun, Fei Wang, M. Brian, W. Rance II Intrusion Detection for Link-State Routing Protocols In *Computer Science Department*, USA, North Carolina, 2001, North Carolina State University
- [29] RIP-II authentication RFC 2082, Networking working Group, January 1997
- [30] Murphy Digital signature protection of OSPF routing protocol In *Internet society symposium on network and distributed system security*, USA, San Diego, February 1996
- [31] Inter-Domain Policy Routing protocol specification RFC 1479, Networking working Group, July 1993
- [32] Smith Securing Distance Vector routing protocols In *Internet society symposium on network and distributed system security*, USA, San Diego, February 1997
- [33] Hauser Reducing the cost of Security on Link-State routing In *Internet society symposium on network and distributed system security*, USA, San Diego, February 1994
- [34] Murphy, Levitt Protecting routing infrastructures from denial of service using cooperative intrusion detection. In *Proceedings of the new security paradigm workshop*, September 1997

7 FURTHER INFORMATION

References

- [1] *IETF Routing area* <http://www.rtg.ietf.org/>
- [2] *IETF Security area* <http://sec.ietf.org/>
- [3] *IETF MANET* <http://www.ietf.org/html.charters/manet-charter.html>