Invited Paper

A Survey on Security Challenges in Next Generation Mobile Networks

Thomas Engel, Daniel Fischer, Thomas Scherer and Dagmara Spiewak

SECAN-Lab
University of Luxembourg
6, rue Coudenhove-Kalergi
L-1359 Luxembourg
{thomas.engel, daniel.fischer, thomas.scherer, dagmara.spiewak}@uni.lu

ABSTRACT

With the development of mobile next generation networks and their new topologies the challenges for security models are increasing drastically. The SECAN-Lab, the Interoperability Lab for Security in Ad Hoc Networks of the University of Luxembourg addresses those new challenges in several core areas of next generation networking such as MANETS, Mesh networks and satellite communication. New concepts like the introduction of trust as a computational value and disruption tolerance are essential. This paper presents an overview on those networks and the SECAN-Labs approach to secure them.

Keywords: MANET, Security, Peer-to-Peer, IPv6, Privacy

1 INTRODUCTION

Today wireless, mobile and non-static networks are getting more and more important and are triggering the development of next generation networks to support mobile devices and bridge the border to traditional, static networks such as the internet. Various forms of mobile and next generation networks must be able to operate under substantial environmental restrictions.Efforts to secure communication over spontaneous networks with non-permanent and opportunistic contacts must consider these specific constraints of the network topology. These can range from reduced power and limited computational power in networks of small devices to high propagation delays and asymmetric data channels in satellite networks. The absence of a central management instance in many mobile networks poses an additional challenge. All these restrictions make it hard to apply common systems to secure communication in static networks to be deployed in mobile networks. It becomes more and more clear that security in such networks means a tradeoff between ressource consumption and satisfied security requirements.

The Interoperability Laboratory for Security in Ad-Hoc Networks, SECAN-Lab develops suggestions and solutions to secure communication for next generation networks and their mobile devices ans form this point implements and evaluates prototypes. The relevance of point-to-point communication in networks with highly mobile topologies is considered in this laboratory as well as the borders between static and spontaneous created networks. An example for such a scenario is the combination of telephone, internet, satellite or mobile networks.

Desirable security requirements for applications in such networks are secured identities, integrity and confidentiality of data, privacy concerns and possibly anonymity. In the further development, liability or non-repudiation will become more and more important as well. In traditional networks Public Key Infrastructures (PKIs) and public key cryptography has been academically accepted but the high costs in running such systems and problems during the realization are strong reasons, not to introduce such systems. In the light of the special restrictions that apply to mobile next generation networks, this is especially true here. First approaches for self-organized public key infrastructures are discussed but are only at the beginning. In case of spontaneous communication, (i.e. where participants only communicate few times), the overhead that is introduced by such a security system is often too large. Moreover security does not guaranty the willingness to cooperate, nor does it guaranty the grade of cooperation. In these situations current security protocols cannot always fulfill the needs in digital communication and new approaches partially based on the factor of trust are needed.

With the transition of social interactions to the cyberspace, trust aspects are getting more and more the base of cooperation not only between human beings, but also as a means of communication of electronic devices. Trust has relevance in sociology, psychology and philosophy, but as a computable dimension, it will have strong influence in computer sciences and the way individuals and electronic devices interact. The trust aspect also touches basic device interaction like routing. Today routing in next generation networks is the focus of current research-teams to improve efficient and stable exchange of information. The mechanisms used expect a cooperative collective (e.g. Piconet and Scatternet in Bluetooth). New aspects like non-cooperative routing have to be investigated.IPSec, Secure Mobile IP, and Mobile PKI are settled in a higher level of the OSI-model and are not flexible in terms of adapting to a changing network topology. They cannot give an adequate solution for the first exchange of a secret.

The development of a reference platform to discuss security issues is one target of the lab. On this base, interoperability tests and security checks should take place. Security leaks should be analyzed. One request is the utilization of the knowledge from simulated attacks (hacking) and inner defense (e.g. intrusion detection) to identify and classify the trustworthiness of the participating clients. These results can be used for confidential routing or for the exchange of secrets and for the

creation of self-organizing public key infrastructures.
The contribution of this paper is to provide an overview on the various aspects on mobile next generation networks and to present approaches to address the security problems within those networks. The remainder of this paper addresses the various areas of research that are covered by the SECAN-Lab with special focus on Mesh and Satellite networks and the introduction of trust as a security aspect.

2 REQUIREMENTS AND EVALUATION FACTORS

From a user's point of view, mobility and roaming are important factors of communication systems, focusing on tailored and personalized services for Peer-to-Peer or group communications. Resulting demands aside others are end-user content creation, location based services and user profiling technologies.
Next Generation Networks are expected to do several transitions, covered by the term convergence (telecom and data, fixed and mobile). They also are required to operate in a non-unified environment. Scenarios like a student entering a foreign national research and academic network (NREN) and getting the credentials and access rights from his home university in another country are typical demands formulated in large European Research Projects like Gant2, where members of the SECAN-Lab participate in the Joint Research Activity JRA5 "Roaming, Access and Mobility" [38]. Service availability and context-induced services in converged, non-hierarchical topologies are key evolution factors for new security mechanisms and protocols.

3 BANDWIDTH AND QoS

The architecture of service oriented platforms as well as middlewares are subject to investigation in various recent research projects dealing with convergence issues. Most of them formulate tailored, ubiquitous services together with seamless access as one of the motivations for an architecture change. Convergence of telecommunication infrastructures and data (IP) networks keeps pace with the increase of bandwidth, leading to prioritization and Quality of Service (QoS) protocols for both worlds. Especially the high demands on the mobility side change question the established security concepts for fixed networks and require new approaches, for example for a fair distribution of bandwidth in a Wireless Mesh Network (WMN). Recent work of the SECAN-Lab [26] proved that it is possible to achieve fair Internet access in WMNs without producing bandwidth overhead. Unfortunately, this is not possible for WiFi WMNs [27]. If WiFi is used within a multi-hop WMN backbone bandwidth is always lost, as it is not possible to masquerate every performance loss produced by multi-hop communications by parallel transmissions. Hence, the horizontal convergence of technologies should include a vertical convergence of layered networking protocols allowing an adoption of protocol parameters to fulfill the overall requirements arising out of application, infrastructure and technology demands.

4 PEER-TO-PEER COMMUNICATION IS MORE THAN AN OVERLAY INFRASTRUCTURE

Convergence of Fixed and Mobile Networks makes the security situation more challenging. Well established fixed network concepts of hierarchical security management databases (e.g. PKI directories, network management etc.) face their limits, if esp. in highly mobile scenarios the central database is not accessible, because of a denial-of-service attack, a missing network link or a switched-off device. Therefore a lot of protocols for mobile ad hoc networks (MANETS) and sparse wireless networks have been designed and optimized for specific communication requirements. To overcome a weak reliability most of the protocols adaptively spread information among their neighbors in order to provide redundant and distributed routing and status information. Still a large majority of protocols uses a flooding approach for this distribution, which makes it not applicable for the intersection of fixed and mobile networks.
Peer-to-Peer (P2P) information systems show their practical strengths in daily use but are considered to be an overlay on top of the existing TCP/IP network, which nowadays most certainly is a fixed network. The SECAN-Lab tries to learn from P2P key distribution and look-up mechanisms to influence the adaptive design of new MANET protocols that are still applicable at the interface between fixed and mobile networks [33].
Besides the huge commercial success of different P2P systems in the last years, the idea of being able to share information and resources with people all around the world gained a huge interest in the research communities, as this is the ideology behind any academic research. A few years ago, a lot of research started in order to develop "pure" Peer-to-Peer information systems, not relying on central servers, like Chord [34], CAN [23], Pastry [25], Tapestry [40] or Kademlia [21]. The results lead to many possible current and new applications that could rely on distributed systems based on P2P networks. As an example, members of the Chord project published a work on supporting DNS upon Chord [5]. Another highly discussed topic is the use of decentralized P2P networks for web caching. P2P networks could also become the platform for many other network-based applications like telephony, videoconferencing or any other kind of streaming.
A fundamental problem in peer-to-peer applications is the provision of a decentralized storage place not being dependent on a centralized indexing system that represents a single point of failure. This is what for instance the Chord protocol is about. Given a key, it maps this key onto a node. The main issue of the Chord protocol is this keying problem. The data keys are distributed on the Chord Ring. To build up a Chord Ring, the consistent hash function assigns each node and each key an m-bit identifier using SHA-1. The value of m must be chosen large enough to make collisions improba-

ble. The SHA-1 hash of the key string returns a key Identifier. The SHA-1 hash of a node's IP-Address and its virtual node identifier returns the node Identifier in the flat key space. Note that both types of identifiers are placed on the same identifier space namely the Chord Ring.
The Chord Ring is an identifier circle modulo 2m. All identifiers are ordered on the Chord Ring according to the following rule. Key k is assigned to the first node whose identifier is equal or larger than k. This node is called the successor of k. The key location is done using a scalable key location algorithm that allows to find a given key within $O(\log N)$ requests (with N, the total number of nodes, currently in the network). This protocol also perfectly deals with frequent architecture changes, meaning many nodes joining and leaving continuously, which is the core idea of P2P networks.
Up to now P2P protocols are meant to exist as overlays on top of the existing network topology. In the design phase of new protocols and with respect to the convergence issues already mentioned, many of the above mechanisms in Chord may also be considered as intrinsic, not only as overlay.

5 ALL-IP NETWORKS AND THE ROLE OF IPv6

Standardization of network interfaces and not least the impact on the required design of more or less completely secure communication infrastructures induce very slow improvements. Once TCP/IP is installed on the network, there are highly sophisticated concepts for securing an infrastructure available. Tests and tools for intrusion detection/prevention are commercialized right now. TCP/IP and esp. IPv4 already offer concepts for many issues related to security or at least a platform for dedicated applications. There are a few drawbacks that could already be fixed in IPv6: the address range and "lower layer" security negotiation. But the impact is much deeper. Because of the sufficient increase of IP address range one now can imagine having a fixed IP address for every device or even purpose. This fully supports the user-induced change from client-server to a point-to-point behavior. It enables the global communication between sensor networks using the same IP addresses internally and externally. Car-to-Car and Satellite-to-Car communications define some application scenarios with a clear demand of security and reliability. MANETS and P2P infrastructures also are more "enabled" by IPv6.

6 CURRENT AND NEXT GENERATION SPACE NETWORKS

Special optimizations are needed for real or near-real time applications, if the round trip time of a data structure exceeds a certain range that makes it infeasible to use protocols with handshake sequences. The same applies, if the available bandwidth is limited and serious overhead reduction considerations are required. For instance such an infrastructure does not allow the exchange of large asymmetric keys and certificates for securing the communication. Both scenarios

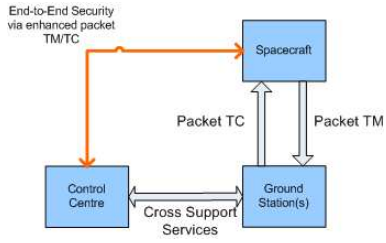

Figure 1: Packet TM/TC End-to-End Security

are common practice in ground and space segment infrastructures for satellites and space missions. Members of the SECAN-Lab participate in the security standardization effort of CCSDS, the Consultative Committee for Space Data Systems. This organization is responsible for developing standards in the area of space communication systems. The focus clearly lies on interoperability and cross support to enable the various space agencies to cooperate on missions, interchange data and use each others infrastructure. However, until now, security was not addressed very well in the CCSDS recommended standards. Many space agencies are realizing the growing importance of information security not only for military and governmental missions but also for purely scientific projects such as earth observation or planetary exploration. This development has led the agencies to formulate security requirements for many of their missions. Lack of appropriate standardization in the area of data security resulted in the development of proprietary solutions for every new mission. Increased development and maintenance costs were the results. It is therefore vital that a generic solution for enhancing security in the spacelink communication protocols is developed very quickly. Terrestrial protocols and security solutions do not perform very well in the space environment because of the above mentioned environmental properties.
CCSDS is already addressing the security issue in its newer protocol definitions such as the Space Communications Protocol Standards (SCPS) [28]–[30]. But as most mission infrastructure systems are based on well established standards such as the CCSDS Packet Telemetry (TM) & Telecommand (TC) protocol family [31], [35], [36], [4], a migration to these new standards is not a feasible option for the space industry. SCPS may be an adequate tool for future ground network systems and some projects are already ongoing in this context. For the space link, it represents just a step on the way from packet TM/TC to future space next generation protocols that may emerge from research projects like the Delay Tolerant Network approach (DTN) [10] and it will probably not become relevant because of the long implementation life cycles in the space business. In order to provide the urgently needed security enhanced standards, solutions for the inclusion of end-to-end data security features in the CCSDS Packet TM/TC standards in a transparent way are being developed on both theoretical [11] and application [12] side. Figure 1 gives a basic view on the space link infrastructure. One of the obstacles in packet TM/TC is that Quality of Service (QoS) is located very low in the protocol stack (at data link layer)

and some security functionalities (like authentication) benefit from direct access to those services. Following this, they need also to be located at this level. Confidentiality services may interfere with the availability of cross support services. Therefore the various possible security localizations have to be analyzed and the most fitting (least interfering) solution has to be chosen. Members of the SECAN-Lab work close together with the CCSDS security working group to archive this goal. This enables the space agencies to support end-to-end security and at the same time keep interoperability and cross support features. Another feature is the independence of the security enhanced packet TM/TC system from a specific set of algorithms or local standardization processes. Because of the transparent approach, the security enhanced version of the packet TM/TC protocol family can be implemented quickly and the agencies can respond to the urgent call for secure missions. This is especially important in the light of coming systems for security, environment control and navigation such as GALILEO [13], U-2010 [37] or the GMES [14] program.

However, the current approach has some limitations and might not withstand the requirements of future space communication networks. SCPS is a first approach that tries to adapt the successful IP protocol for the space environment and introduce the concept of a real network model for the space environment. Overhead is reduced compared to TCP/IP and other restrictions related to the space environment are handled as well. The result is an IP-like protocol for space with the drawback that many of its components are not compatible with terrestrial IP. However, still some of the properties of future space networks are not covered and therefore SCPS is not suitable for supporting next generation space networks.

In order to cope with the requirements of next generation space networks a protocol has to perform well under the restrictions of the space environment which are: very large signal propagation latencies, low and asymmetric data rates, intermittent scheduled and unscheduled connectivity. In addition such a protocol must be able to successfully bridge the border between terrestrial and space networks. This is a crucial requirement and is not met by any space protocol yet. The Delay Tolerant Networking (DTN) approach proposes a solution by introducing an overlay network on top of the transportation layer. As the underlying layers are kept flexible (e.g. TCP/IP for the internet, CCSDS packet TM/TC for space links) one does not have to worry about the nature of the underlying network. In order to cope with more challenging problems like intermittent connectivity and large delays, the network must have the ability to store data in at least some of its nodes during periods of non-availability of the next node on a route. In the DTN approach such nodes are called storage nodes. The whole concept is a bit based on the functionality of postal delivery services where mail deliveries are also stored in intermediate distribution points before being forwarded further. In order to realize the overlay network, an additional layer, the so called bundle layer, is introduced. It also introduces a new global addressing system in the form of endpoint identifiers. Those endpoints can contain one or more networks nodes realizing the concept of uni-, any-, multi- and broadcast. It is important to note that the DTN approach is not only applicable for space networks but also for MANETs, sensor networks and acoustic networks. In fact DTNs are able to bridge the border between these very different networks environments without the need for a translation gateway.

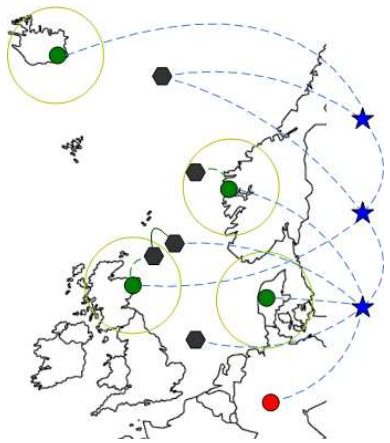

Figure 2: Ship Tracking System Application

A very simple example is the combination of a satellite network (for providing navigation and communication services) with a wireless network connecting cars. Such a combination could be used for predicting traffic jams, emergency services and communication. Realizing such a network using traditional protocols would require quite a translation effort between the two different types of network environments. A DTN could instead make use of the benefits of the underlying transport layers without the need for a translation node.

Another application is the tracking of ships that are moving too far offshore to be reached by radio communication. In the light of recent political developments, control of naval traffic is a desirable goal for many governments. Such a system could be realized by means of a DTN that allows the possibility of ship-to-ship and coast-to-ship communication and is backuped by a network of low earth orbit communication satellites. The security requirements however would exceed the current possibilities of the DTN development status and further research is required. Aspects like privacy and anonymity are important in order to prevent misuse of this system either by the ship owners or by intruders. Figure 2 shows an example for such an application in the north-west European region. The green circles represent coastal radio stations and their communication radius. The black items represent the ships and the blue stars passing low earth orbit satellites. The coastal stations are connected to the satellite network. In addition all ships maintain a low-bandwidth connection to a satellite. If accessible the connection via the coastal station is preferred over the direct link in order to save communication resources. The satellite network is controlled by a mission control center (red circle).

Within the DTN approach, there are a number of unresolved problems that are subject to ongoing research. Most of them are related to routing and security with the latter one being one of the research areas within the SECAN-Lab. The prob-

lems and challenges are almost identical with the ones described for MANETS. However, in space networks, the factor of trust may not play such an important role as all participants of a space network are most probably known prior to the communication attempt. Key management is one of the big open challenges. Lagging a central key distribution instance, a peer-to-peer approach seems like a promising endeavor. Another open area is connected to the routing problem. A secure DTN routing algorithm should be robust enough to withstand the active or passive attacks from hijacked or malicious nodes that may be discovered during the routing process. Finally, the problem of applying signatures to bundle data structures is not as trivial as it may sound. The DTN architecture supports reactive fragmentation of bundles to make also large bundles benefit from very small connectivity windows are alternate routes within the network. If a signed bundle gets fragmented, intermediate nodes are not able to check the integrity of the bundle fragment. Hop-to-hop integrity can be guaranteed by calculating a new signature for every hop depending on the fragment; however an end-to-end solution may be far more attractive as it would be able to counter malicious nodes in the network.
Another goal of the ongoing study is to discover how much of the security and trust research in the area of MANETS can be transferred to general DTN research and in which areas the space environment weakens the obstacles of security research.

7 OPEN SECURITY CHALLENGES IN NON-STATIC ENVIRONMENTS

The SECAN-Lab investigates new concepts leading to distributed mobile secure communication infrastructures that are also capable to serve at the interface between fixed and mobile networks. This helps to overcome the single point of failure characteristic of centralized control databases or costs for synchronizing well defined hosts. The change of paradigm from client-server to point-to-point implies the need of local mechanisms, not necessarily synchronized over large distances. Crisis Management Networks give excellent application scenarios for these reliable infrastructures and are investigated in the 6th framework of the European Commission in a project called U-2010 [37]. The idea is to combine and ”bridge” all existing and upcoming network technologies used by rescue teams in crises scenarios (like GSM, POTS, UMTS, WLAN, WMN, Satellite infrastructures, etc.) by using the Internet Protocol.

7.1 Trust and Dependability

Crucial data and applications transmitted within mobile wireless networks require a high degree of security. Principally, due to the absence of fixed base stations and pre-established infrastructure, these networks differ highly from traditional hierarchical networks. MANETs for instance, allow nodes to form and leave the network dynamically, sometimes even without leaving a trace. Even though, accepted securing techniques, like common public-key encryption and digital signatures are not accurate because of their dependability on continuously accessible entities for example managing reliable key-distribution, it is understandably very important to provide security services such as authentication, confidentiality, and privacy if required. As a consequence, recent research concentrates on *Trust-Metrics* for the purpose of preventing the weakness of having a centrally accessible Trusted Third Party organizing the network's security and simultaneously representing a dangerous bottleneck of the system. Although Trust is well known to everybody, the formal definition poses several challenges and differs depending on the application area. In [9] the notion of Trust in mobile wireless ad-hoc network settings is directly compared to *Trust* applied to the Internet, for instance while thinking of the *PayPal* Payment System. Due to the dynamical character and quick topology changes, *Trust* establishment in mobile wireless network settings should support among others a short, fast, online, flexible, uncertain and incomplete *Trust* evidence model and should be independent of pre-established *Trust* infrastructures. Additionally, the interdependency of *Trust* and *Security* is emphasized by the authors in [22], concluding that security is highly dependent on trusted key exchange and trusted key exchange on the other side can only take place with requisite security services.
In the following, we illustrate possible security attacks in mobile wireless ad-hoc networks before different *Trust* establishment methods are presented and their application to mobile wireless ad-hoc network settings is analyzed [32].

7.2 Attack Analysis

Generally, two kinds of security attacks can be launched against mobile wireless ad-hoc networks, *passive* and *active* attacks. The adversary rests unnoticed in the background while running a *passive* attack, even without disturbing the functions of the protocol, and eavesdrops worthwhile information about the network and the participating nodes. In *active* attacks, the attacker disturbs the correct functionality of the routing protocol by for example modifying routing information or launching Denial of Service attacks. Buchegger and Boudec [3] underline the importance of *Trust* in order to isolate malicious nodes and to establish reputation systems in all nodes that enable them to detect misbehavior of network participants. In the following, we discuss three different categories of *active* attacks in mobile wireless networks:

Integrity Attacks:
By launching an *Integrity Attack*, the malicious node drops messages, redirects traffic to a different destination, or computes longer routes in order to increase the communication delays. The most famous attack in this category is the setup of a *Blackhole* [24] where the attacker swallows all packets traversing its node. As an extension the active attacker might launch a *Greyhole* [16] attack allowing him to switch its cause of action from forwarding packets and discarding others. Even trickier is the establishment of a tunnel in the

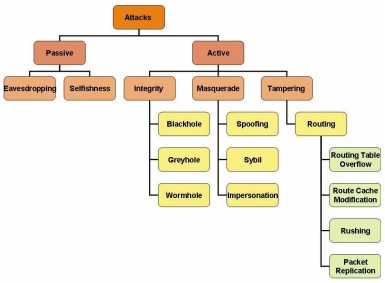

Figure 3: Classification of Attacks in Mobile Wireless Ad-hoc Networks

network between two or more cooperating and by the attacker compromised nodes that are linked through a private network connection, called *Wormhole* [17] allowing the attacker to short-cut the normal flow of packets. After *tunneling* the packets to another point in the mobile wireless ad-hoc network, the attacker replays them into the network. These three attacks can also be grouped as *Byzantine Attacks*. The following Figure 3 shows the classification of attacks in mobile wireless ad-hoc networks.

Masquerade Attacks:
By launching this type of attacks the adversary aims to adopt another identity in the network in order to appear as a good-natured node. Consequently, he may operate as a trustworthy node and for example advertise incorrect routing information. One dangerous attack is known as *Sybil Attack* [6] where the malicious node may not only impersonate one other node but multiple false identities. Especially mobile networks that apply a Recommendation-Based *Trust-Model* are vulnerable to *Sybil Attacks*. Here the malicious node can generate fake recommendations about the trustworthiness of a particular node in order to attract more network traffic to it offering an ideal staring point for *Wormhole Attacks*.

Tampering Attacks :
These attacks are based on the distribution of falsified routing messages and are difficult to identify and trace. The *Rushing Attack* [18] is one example for such an attack acting as an effective Denial of Service attack against all currently proposed on-demand ad-hoc network routing protocols. Launching this attack the adversary rapidly spreads routing messages all through the network, disabling authorized routing messages with the consequence that other nodes delete them as multiple copies. Obviously, also computational routes to a destination can be canceled by constructing routing error messages, asserting that the neighbor can not be reached. So, since flooding is the famous mechanism used by on-demand routing protocols to establish paths, disturbing flooding is an effective attack against these kinds of protocols.

7.3 Trust Models

Below, we discuss several famous *Trust Models* and analyze them towards their applicability to mobile wireless network settings.

7.3.1 PGP Trust Model

Pretty Good Privacy or *PGP* [43], is an important milestone in the history of cryptography, because for the first time cryptography is available to a wide community. It was principally created for encrypting or signing email messages and offers a hybrid cryptosystem. The basic idea is that all users operate as autonomous certification authorities and have the right to sign and verify keys of other entities. The absence of a central certification authority and the introduction of the so-called *Web of Trust* allow network entities to build a set of virtual interconnections of Trust. However, is it possible to *trust PGP* in mobile wireless and ad-hoc network settings? Subsequent to a detailed evaluation of the PGP model, we must unfortunately negate this question. Although no central certification authority is required, the distribution of keys is organized by a continuously accessible public-key directory that resides on a centrally managed server, which makes PGP inadequate for mobile wireless ad-hoc network settings, where nodes may join and leave the network spontaneously.

7.3.2 Adjusting PGP to mobile wireless network settings

In [19] *PGP* is extended by a public-key distribution system that better fits to the self-organized nature of mobile wireless ad-hoc networks. Similar to *PGP*, public-key certificates are issued, signed and verified by nodes in the network themselves. Additionally, each node maintains a *local certificate repository* that contains a subset of public-keys of network's entities. As a consequence, nodes may manage the distribution of public-key certificates also by themselves. However, the establishment as well as the update procedure of the *local certificate repository* is a computationally complex operation producing an extensive overhead while executed on resource constrained devices, like for instance PDAs. Moreover, the detailed analysis of the utilized algorithm demonstrates the high vulnerability to Sybil Attacks. Finally, the weaknesses in security paired with the high computational complexity make this *Trust Model* impractical for mobile wireless ad-hoc network settings.

7.3.3 Decentralized Trust Model

The *Decentralized Trust Model* [2] was the first system taking a comprehensive approach to *Trust* problems independent of any particular application or service. It extends the common identity-based certificates, which bind a public-key to a unique identity, by means of reliably mapping identities to the actions they are trusted to perform. The main achievement was the construction of a system called *PolicyMaker* in order to define policies and Trust relationship composed with the *PolicyMaker Language*. While this approach provides a basis for expressing and evaluating *Trust*, it does not consider the simultaneous problem of how to continuously control and manage *Trust* over a longer period of time.

7.3.4 Distributed Trust Model

The *Distributed Trust Model* [1] applies a recommendation protocol to exchange, revoke and refresh recommendations about other network entities. Therefore each entity needs its own *Trust Database* to store different categories of *Trust* values ranging form -1 (complete distrust) to 4 (complete trust). By executing a recommendation protocol, the network entity can determine the *Trust level* of the target node, while requesting for a certain service. The accordant *Trust level* for a single target is obtained by computing the average value for multiple recommendations. Although this model does not explicitly target mobile wireless ad-hoc networks it could be used to find the selfish, malicious, or faulty entities in order to isolate them so that misbehavior will result in isolation and thus cannot continue. Unfortunately, recommendation-based *Trust-Models* are very vulnerable to *Sybil Attacks*.

7.3.5 Distributed Public-Key Trust Model

The core of the *Distributed Public-Key Trust Model*, examined in [39] is the use of *Threshold Cryptography* in order to avoid the maintenance of a central Certification Authority (CA). *Threshold Cryptography* implicates sharing of a key by multiple entities. The system, as a whole, has a public-/private-key pair where the private-key is distributed over *n* of nodes. All nodes in the network know the public-key and trust any certificate signed by it. Additionally, each node has a pubic-/private-key pair and can submit requests to get the public-key of another node or requests to change their own public-key. The ingenious idea is that $(t+1)$ out of n *shareholders* have the ability to compute the private-key by combining their partial keys but not less then $(t+1)$. In order to obtain the private-key, $(t+1)$ nodes must be compromised. For the service of signing a certificate, each *shareholder* generates a partial signature for the certificate using its private key share and submits the partial signature to one arbitrary *shareholder*, called *combiner*. With $(t+1)$ correct partial signatures the *combiner* is able to compute the signature for the certificate. Although the model offers strong security, like *authentication* of communicating nodes, it has some factors that inhibit its deployment to mobile wireless ad-hoc networks. The pre-establishment of a distributed central authority requires a huge computational complexity. Furthermore, asymmetric cryptographic operations are also known to consume precious node battery power. Additionally, $(t+1)$ parts of the private-key may not be reachable to a node requiring authentication and following asymmetric cryptographic services. Finally, the distribution of signed certificates within the mobile wireless ad-hoc network settings is not sufficiently discussed and questionable. In [7] Levent Ertaul and Nitu Chavan visualize the potentialities and difficulties of *RSA*-based threshold cryptography in mobile wireless ad-hoc network settings and adapt their idea to *ECC*-based threshold cryptography in [8] for the purpose of higher efficiency.

7.3.6 Subjective Logic Trust Model

Josang emphasizes in [20] that public-key certificates alone do not assure authentication in mobile wireless ad-hoc networks, due to the missing reliable central certification. In this context, his solution introduces an algebra for the characterization of *Trust-relations* between entities. A statement such as: *"the key is authentic"* can only be either true or false but nothing in between. However, because of the *imperfect knowledge* about reality it is impossible to know with certainty wheatear such statements are true or false. Consequently, it is only feasible to have an *opinion* about the outcome of such statements. This leads to the notions of *belief (b), disbelief (d) and uncertainty (u)*. The relationship between these three attributes can be mathematically formulated as follows:

$$b + d + u = 1, \{b, d, u\} \in [0, 1]^3 \quad (1)$$

Triples $\omega = \{b, d, u\}$ that satisfy the above condition $b + d + u = 1$ are called *opinions* and are represented as a points in the Option Triangle.
Opinions of two different entities about the same subject may differ and are not automatically objective but subjective. The mathematical technique to characterize subjectivity is called *Subjective Logic*. By enhancing the traditional Logic with non-traditional operators such as *recommendation* and *consensus*, the *Subjective Logic* approach is able to deal with *opinions* that are based on other entities' recommendations. Furthermore, *Subjective Logic* can produce a single *opinion* about a statement in the presence of more then one recommendation. In the following scenario, node A receives the public-key of an unknown node B and starts to examine B's public-key certificate. The certificate contains opinions about the key authenticity as well as opinions about the recommendation trustworthiness assigned by other nodes. If multiple recommended certification paths to B's key exist, A has the capability to determine the authenticity of B's key by computing the *consensus* between the authenticities obtained for each path. By introducing *uncertainty* into *Trust-Metrics* it is possible to estimate the consequences of recommendation-based decisions. However, trustworthy authentication of B's public-key requires an unbroken chain of certificates and recommendations. This is a critical condition taking the characteristics of in mobile wireless ad-hoc networks into account, including the vulnerability to breakage of wireless links and the dynamically changing topology. Finally, we conclude that the *Subjective Logic Trust* approach is inadequate in mobile wireless ad-hoc network settings. Our concept of *Trust-based Identity Management* in mobile wireless ad-hoc network settings incorporates sufficient redundant information ensuring reliable authentication and authorization of participating network entities.

7.4 Identity and Privacy

In the following, we present *Privacy issues* in mobile wireless networks and discuss the difficulty of Identity-Management in such network settings.

7.4.1 Challenges of Privacy-Preservation in mobile wireless networks

In contrast to traditional networks with *a priori* determined network topology, mobile wireless networks, including MANETs, extend the concept of *Privacy* from *Identity-protection*, known as *sender-* and *receiver-anonymity*, to *Location-Privacy* and *Motions-Pattern-Privacy* of communicating entities [15]. In this context, *Mobility* implies additional threats to *Privacy* by uncovering the geographical location of nodes as well as their motion. In the following, threats on *Privacy* in mobile wireless network settings are itemized:

Sender and Receiver Identity Discovery Attack:
This attack targets to disclose either the identity of the sender, the receiver or even both for example by intercepting route request packets during the Route Discovery Phase of the communication protocol.

Motion Pattern inference Attack:
The aim of this attack [15] is to track the movement of nodes by *passively* monitoring nodes in listening range. However, by corrupting multiple nodes within the network the adversary may cover a wide listening rage and in the extreme case even the transmission area of the whole mobile wireless network. Consequently, the adversary may combine the gathered information and reconstruct the motion pattern of the observed node.

Location Privacy Attack:
Regarding the listening range of the adversary's node, the adversary may glean worthwhile information about:

- Active nodes within his listening range
- Size of the set of active nodes
- Active Communications

Route Tracing Attack:
The adversary tries to collect route information about a certain node within the mobile wireless network. He monitors the routing traffic in order to get details about routes to other network entities and to be able to identify the communicating nodes.
With above vulnerabilities in mind, we investigate in novel *Privacy-preserving* technologies applicable to All-IP networks as well as mobile scenarios. Anonymous routing strategies in combination to efficient *Trust-based Identity Management* techniques are developed, in order to assure an accurate level of efficiency and performance while providing *Privacy* of sensitive information and communicating identities.

7.4.2 Link Layer Association Identity Management

Determing a node's Identity in a wireless networks comprises problems appearing to be inherent in wireless environments. One of these problems arising in the wireless context are currently elaborated in the SECAN-Lab:
The **Monkey-Jack Attack** has its name from an existing software called "Monkey Jack" implementing the attack. The attack exploits the possibility to easily perform Man-in-the-Middle Attacks on the Link Layer of wireless networks. Even after successfully executing a cryptographic authentication procedure in a wireless network a station does not know if it is communicating immediately with the desired station. There might be arbitrary nodes in between although the communication on Link Layer is considered.
The common example presented in this context is a wireless Access Point (Real AP) offering services, like Internet Access to mobile clients. An attacker may situate another AP, the "Roque AP", near to the Real AP sensing and replaying all traffic produced by the Real AP. Wired networks provide natively a certain amount of protection as the attacker needs to be connected to the wire to perform Link Layer replays. It can not be guaranteed that a mobile client overhears both APs as this strongly depends on the environmental situation that may be influenced by the attacker. Considering a mobile node that only senses the traffic produced by the Roque AP will assume this as the Real AP and try to associate with it. If cryptographic authentication handshakes are performed the "Roque AP" may replay mobile client frames to the Real AP. So, authentication challenge replies produced by the Real AP or Mobile Client are replayed, too and the association can be successfully completed. Now, the attacker has the possibility to actively intervene the communication, maybe to perform other attacks or simply to produce Timing or Denial of Service failures.
The idea supplied by the SECAN-Lab is to solve this issue by finding points in time being unique for Real AP and mobile client as long as no attacker is in between them. Having more than one unique point in time both stations can negotiate durations between these unique events to estimate if an attacker performs the Monkey-Jack attack or not. Neglecting signal propagation a unique point in time is when a station starts transmitting a frame. As we consider the Link Layer this is possible in contrast to the Network Layer where packet delays are not visible. If Real AP and mobile client measure the beginning of two frame transmissions and calculate the time between these events they will obtain the same result although they are not synchronized with each other. On the other hand, if both station measure two different points in time they will obtain different result. This will happen if one station considers the transmission of a replay and the other station estimates the transmission of the original frame. Consider Figure 4, where two stations send a frame to each other. Both stations measure when transmissions start, as described above. After subtracting t_2 from t_1 both stations will achieve the same result. As link layer frame transmission where taken, the obtained difference is negligible. Figure 5 depicts the time measurement in case of an intermediate attacking node. Station 1 sends a message msg_1, which is replayed by the attacking node (msg'_1). Station 2 replies with msg_2, again replayed as msg'_2 by the attacker. Now, Station 1 will calculate $t_2 - t_1$ as

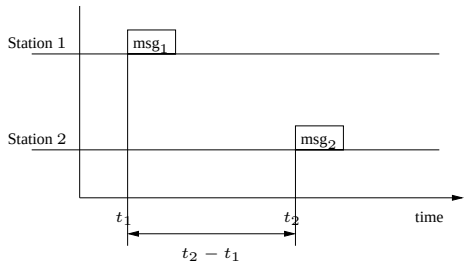

Figure 4: Time Measurement

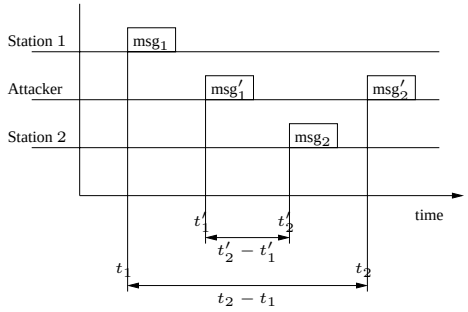

Figure 5: Time Measurement During Attack

the duration between the beginning of the two transmissions, namely its own and the attackers replay msg$'_2$. The two points in time estimated by Station 2 are t'_1 and t'_2. t'_1 is when the attacker starts transmitting msg$'_1$ and t'_2 is the beginning of Station 2's transmission.
The duration estimated by Station 1 is longer than the one estimated by Station 2. In fact, it contains the duration estimated by Station 2 and at least 2 more frame transmissions. In a first prototypic implementation the "Roque AP" produced a significant time variation whereas no time variation could be estimated (in microseconds) in the absence of an attacker.
To be able to detect the "Roque AP" the other stations need to exchange their estimations. This can be done by piggybacking them within subsequent frames encrypted together with the frame payload by using exiting protocols, like WPA.

8 Summary

In this paper we have presented most recent research of the SECAN-Lab project. While, today's communication systems get more and more mobile in such a way that communication services are required *anytime* and *anywhere*, the nature of mobile wireless networks makes them very susceptible to malicious attacks and selfish actions. For that reason, the SECAN-Lab project researches and develops reliable and efficient technologies enabling secure messaging in areas with no, less pre-installed, or destroyed communication infrastructure. This paper sketches SECAN-Lab's research activities starting with the discussion of the crucial issue "Bandwidth consumptions in Wireless Mesh Networks". Subsequently, the functionality of several peer-to-peer technologies is described, highlighting the achievement, strengths and weaknesses of peer-to-peer methodology. Security-enhancements in space communications represent one of the core research topics within the SECAN-Lab and are discussed in the subsequent section of this paper. The following chapter concentrates on difficulties associated with the maintenance of central entities within mobile wireless networks and outlines different *Trust* models essentially needed in order to establish reliable and high-performance communications. Finally, latest investigations in *Privacy-research* within mobile wireless network settings are presented, stressing the importance of *Data-protection* in combination to *Location-privacy* and *anonymity* of communicating entities within mobile wireless scenarios.

REFERENCES

[1] A.Abdul-Rahman, S. Hailes, A distributed trust model, In Proceedings of the 1997 workshop on New security paradigms, (1997).

[2] M. Blaze, J. Feigenbaum and Jack Lacy, Decentralized Trust Management, In Proceedings IEEE Conference on Security and Privacy, Oakland, 96-17, (May 1996).

[3] S. Buchegger and J. Le Boudec, Self-Policing Mobile Ad-Hoc Networks by Reputation, IEEE Communication Magazine, (2006).

[4] CCSDS. Command operations procedure-1. CCSDS 232.1-B-1, Blue Book, Issue 1, Washington, September 2003.

[5] R. Cox, A. Muthitacharoen, R. Morris. Serving DNS using Chord. First International Workshop on Peer-to-Peer Systems, Cambridge, MA, March, 2002.

[6] J. R. Douceur, The Sybil Attack. In Proceedings of the IPTP02, Cambridge, MA (USA), (March 2002).

[7] L. Ertaul, N. Chavan, Security of Ad Hoc Networks and Threshold Cryptography, Wirelesscom, (2005).

[8] L. Ertaul, W. Lu, ECC Based Threshold Cryptography for Secure Data Forwarding and Security Key Exchange in MANET (I), NETWORKING 2005, Waterloo, Canada, 2005 Proceedings, (May 2005).

[9] L. Eschenauer, V.D. Gligor, J. S. Baras, On trust establishment in mobile ad-hoc networks, ACM Conference on Computer and Communications Security 2002: 41-47, (2002).

[10] K. Fall. A delay tolerant network architecture for challenged internets, 2003 Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications

[11] D. Fischer, M. Merri, and T. Engel. Approach to the Integration of Data Security in the CCSDS Packet TM/TC Standards Presented at: Ninth International Conference on Space Operations (Spaceops 2006), Rome, June 2006.

[12] D. Fischer, M. Merri, T. Engel, and M.Pecchioli. Design of the data security system for scos-2000. Presented at: Ninth International Conference on Space Operations (Spaceops 2006), Rome, June 2006.

[13] G. Industries. Galileo industries web-

site. Online-Reference: http://www.galileo-industries.net.
[14] GMES. Global monitoring for environment and security. Online-Reference: http://gmes.info.
[15] X. Hong, J. Kong, M. Gerla, Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks, Special Issue on Wireless Network Security, Wiley Interscience Press (2006).
[16] Y.-C. Hu, A. Perrig, D. B. Johnson. Ariadne, A secure on-demand routing protocol for ad hoc networks. In Proceedings of the MobiCom '02, (September 2002).
[17] Y.-C. Hu, A. Perrig, D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Network, Technical Report TR01-384, (December 2001).
[18] Y.-C. Hu, A. Perrig, D. B. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network, WiSE 2003, San Diego, California, USA, (September 19 2003).
[19] J.-P. Hubaux, L. Buttyan, S. Capkun, The Quest for Security in Mobile Ad Hoc Networks, Proceeding of MobiHOC,(2001).
[20] A. Josang, An Algebra for Assessing Trust in Certification Chains, In Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium, (1999).
[21] P. Maymounkov and D. Mazieres. Kademlia: A peer-to-peer information system based on the XOR metric. In Proceedings of IPTPS02, Cambridge, USA, March, 2002.
[22] A.A. Pirzada, C. McDonald, Establishing trust in pure ad-hoc networks, CM International Conference Proceeding Series in Proceedings of the 27th conference on Australasian computer science,(2004).
[23] S. Ratnasamy, P. Francis, M. Handley, R. Karp, S. Shenker. A Scalable Content Addressable Network. TR-00-010, Berkeley, CA, 2000.
[24] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon K. Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, In Proceedings of the International Conference on Wireless Networks, Las Vegas, June, (2003).
[25] A. Rowstron, P. Druschel. Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems. Lecture Notes in Computer Science, 2218, 2001.
[26] T. Scherer and T. Engel. Bandwidth consumption for providing fair internet access in wireless mesh networks. In IEEE International Workshop on Wireless Ad Hoc & Sensor Networks, New York, USA, June 2006.
[27] T. Scherer and T. Engel. Bandwidth Overhead in WiFi Mesh Networks for Providing Fair Internet Access. ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks, Malaga, Spain, October 2006. 2006.
[28] CCSDS. Space communications protocol specification (scps) - network protocol. CCSDS 713.0-B-1 Blue Book, Issue 1, Newport Beach, May 1999.
[29] CCSDS. Space communications protocol specification (scps) - security protocol. CCSDS 713.5-B-1 Blue Book, Issue 1, Newport Beach, May 1999.
[30] CCSDS. Space communications protocol specification (scps) - transport protocol. CCSDS 714.0-B-1 Blue Book, Issue 1, Newport Beach, May 1999.
[31] CCSDS. Space packet protocol. CCSDS 133.0-B-1, Blue Book, Issue 1, Washington, September 2003.
[32] D. Spiewak, T. Engel. An Overview of Models applying Trust as a Component of Security Services in MANETs, In Proceedings of WSPWN, Miami Florida USA, (2006).
[33] M. Stocco, T. Engel, U. Roth. Trust Arrays: Allowing P2P nodes to "personally" evaluate trustworthiness of potential partners. Advances in Intelligent Systems - Theory and Applications (AISTA 2004). In cooperation with the IEEE Computer Society. Luxembourg, November 15-18, 2004.
[34] I. Stoica, R. Morris, D. Karger, F. Kaashoek, H. Balakrishnan. Chord: A Scalable Peer-To-Peer Lookup Service for Internet Applications. = Proceedings of the 2001 ACM SIGCOMM Conference, 149-160, 2001.
[35] CCSDS. Tc space data link protocol. CCSDS 232.0-B-1, Blue Book, Issue 1, Washington, September 2003.
[36] CCSDS. Tm space data link protocol. CCSDS 132.0-B-1, Blue Book, Issue 1, Washington, September 2003.
[37] U-2010. U-2010. Online-Reference: http://www.u-2010.eu.
[38] S. Winter, T. Engel: Location-Based Services for Scientists in NRENs. LoCA 2005: 341-349
[39] L. Zhou, Z. J. Haas, Securing Ad Hoc Networks, IEEE Network, (1999).
[40] B. Y. Zhao, J. D. Kubiatowicz, A. D. Joseph.
[41] apestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing.
[42] CB/CSD-01-1141, UC Berkeley, April, 2001.
[43] P. R. Zimmermann, The Official PGP User's Guide, Department of Computer Science, University of Helsinki, Finland, MIT Press, (1995).