FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Wireless Mesh Network Application

Manuel João Sampaio Martins

PREPRATION FOR THE MSC DISSERTATION

MASTER IN ELECTRICAL AND COMPUTERS ENGINEERING

Coordinator: PhD Professor Ana Cristina Costa Aguiar

February 16, 2013

Abstract

Wireless Mesh Networks (WMN) are presented as a low cost cooperative solution for wireless connectivity, having numerous applications in areas as businesses, homes, disaster, emergency or transport. Since the connectivity is provided as an overlay network, routing has been studied extensively, however security has been neglected by research, leaving vulnerabilities that can be exploited by malicious users. Consequently arming users with security mechanisms resistant to common types of wireless networks attack is critical. This way, confidential packet forwarding and secure routing are guaranteed.

From the few security models presented for WMN, most are centralized, resorting to key or certificate distribution. We propose to create and implement a fully distributed security protocol for wireless mesh applications, where mobile nodes are able to safely communicate without a server certification.

Using open source android we aim to develop and implement decentralized security procedures that will enable users to use safely a WMN application while maintaining a good performance level.

Contents

List of Figures

Abreviations and Simbols

WMN	Wireless Mesh Networks
App	Application
VoIP	Voice over IP
MANET	Mobile Ad Hoc Network
MAN	Metropolitan Area Network
AES	Advanced Encryption Standard
DES	Data Encryption Standard
DoS	Denial of Service
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PGP	Pretty Good Privacy
MAC	Message Authentication Code
IBC	ID Based Cryptography
OS	Operating System

Chapter 1

Introdution

This section aims to capture the reader's attention and introduce him the interesting subjects contemplated in the dissertation. In the following sections we will present context and motivation for the work, the objectives we aim to achieve and also the document's structure.

1.1 Context

Over the course of the Curricular Unit Preparation for the MSc Dissertation I proceeded to choose the Supervisor and theme for my master's final dissertation. The natural choice was Ph.D. Professor Ana Aguiar with the theme Wireless Mesh Networks Application.

Wireless Mesh Networks are a dynamic and cost effective solution for wireless device connectivity. As can be found on [**?**] Mesh networks are formed by a net of nodes enabled with ad hoc connectivity, therefore creating multipath solution for packet sending. This solution provides network infrastructure with some redundancy, increasing availability and resistance to failure or disconnection of nodes. The smart allocation of resources allows for the sharing of devices bandwidth with other nodes which increases the overall bandwidth and spectral efficiency. WMN implements an overlay network with self organising and addressing routing protocol. All these advantages do not come without a cost and so dynamic complex routing is required to execute the decentralized control. Multi hop communication together with decentralized control makes possible for a mesh network to operate without backbone or any other network connectivity within a significant range. Independence and autonomy make this topology ideal in big number of applications used in civil, military and business context.

Although the number of applications for WMN has experienced some growth, Security is still an unresolved issue for WMN.

1.2 Motivation

WMN has grown in recent years, the work done with a constantly increasing number of applications shows that users' motivation is high while operators stay sceptical due to the fact that they

Figure 1.1: Mesh Network

are unable to find a way to profitably charge this sort of service like stated in [**?**]. A increasing number of systems based on WMN from the most diverse areas such as emergency and disaster scenarios, tunnels, oil rigs, transportation systems, building automation, high speed video, VoIP Quality of Service, MANET, Metropolitan Area Networks, Enterprise networks as well as Health and Medical shows the versatility and adaptability of WMN. Security has been neglected from all this development, low security level will discourage users and operators from using the network, therefore we can consider security as an essential and also critical part of network planning. This has proven even more relevant because late attempts at security configuration are extremely expensive and a lot harder to implement.

1.3 Objectives

This dissertation project is done in the context of the MSc in Electrical and Computers Engineering. We aim at studying and implementing WMN security, developing application specific protocol. In order to achieve the intended goals we propose the specific partial objectives:

- Review known literature about security and cryptography
- Research models on key distribution and generation
- Develope and Implement security protocol for Android application
- Analyze results, draw conclusions of the implementation

1.4 Document Structure

Besides Introduction this report contains 3 more chapters. The next, Chapter 2, contains State of the art information about the theme, including models used for centralized and decentralized network management as well as key generation and sharing. On chapter 3, we elaborate on the methodology and plan designed to achieve the proposed goals. Lastly we draw some conclusions from the work already done.

Chapter 2

State of the Art

2.1 Introdution

In the following sections we will present a revision on relevant subjects to the dissertation and their respective bibliography, making the future work more educated and informed. We will provide a view of WMN specificities as well as a characterization of Network Security and Cryptography thought relevant. Lastly we will explore solutions to the Security in our specific work context, taking a glance at centralized algorithms and reviewing decentralized ones.

2.2 Wireless Mesh Network

We can found a detailed description about WMN and its characteristics in [**?**]. As the name states WMN enables wireless connectivity from a Ad Hoc type topology, where nodes form mesh connections - hops - assigned by techn independent routing. Compatible with most widespread wireless Technologies, WMN represent a very economical and scalable solution that allows user to communicate for a great range using multiple hops within the network. The economic advantage guaranteed by WMN has to do with the great resource maximization that made possible by the high bandwidth used and also spectral efficiency, where users can use the same portion of the bandwidth spectrum on different parts of the network by frequency hoping according to neighbours. All nodes have a dual functionality of server client that require them to forward other node messages while sending and receiving their own. Therefore there is a need for encouragement of cooperative behaviour. There is a cooperative compromise as every node depends on all the network if a node is misbehaving fairness is jeopardised.

WMN, unlike wired networks, possess unique characteristics that make it subject to channel and node vulnerabilities. As such a series of nontrivial problems are created for security design to solve and provide protected communication between nodes in a hostile environment as the shared wireless medium may become.

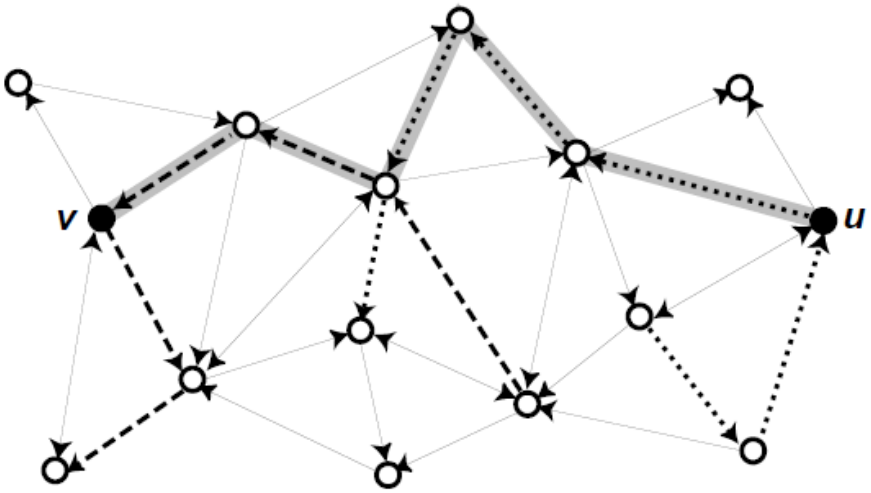

Figure 2.1: WMN Topology

Challenges in WMN like in MANETs are high node mobility and topology changes. This properties require sophisticated complex routing algorithms in protocols consequently increasing message exchange and network overhead.

The equality between nodes leads to a security weakness, no node can enforce security on other leaving algorithms to be easily broken.

2.3 Security and Cryptography

As a rule, Security is always the last concern, WMN is no exception. While no big problems or economical loss arises from security failures or vulnerabilities, researchers and companies will not be motivated towards it.

Encryption and cryptography protocols are used to protect information from undesired readers, this can be done relative to message content, confidentiality and integrity, or message source, authentication.

According to [**?**] there are 2 types of cryptography relevant in networking infrastructures, Symmetric and Asymmetric, also known as Public Key Cryptography. Detailed description is at this point out of the scope but an overview on characteristics and properties is relevant. We will start on Symmetric Cryptography has the advantage of simplicity and efficiency as the algorithms are much more simple to implement and less demanding in encryption and decryption in terms of time and processing. On the other hand authentication cannot be obtain with Symmetric algorithms, the same happens with message integrity where additional mechanisms, like hash functions, are required.

Requiring more processing as well as implementation effort we have PKC. PKC allows for message authentication, message encryption and also message integrity, when aided by hash function or Message Authentication Code. Public Key Cryptography is the most common due to its

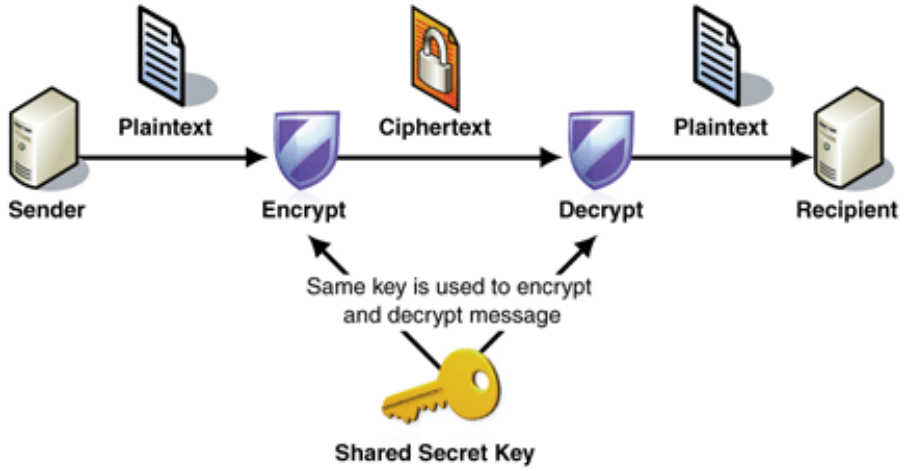

Figure 2.2: Symmetric Encryption Decryption

properties that allow for many security mechanisms. The basis of this Cryptography is a Key pair that are relational yet independent of each other. This keys decrypt each other but cannot be obtained from each other even if the user processes a message, encrypted or decrypted.

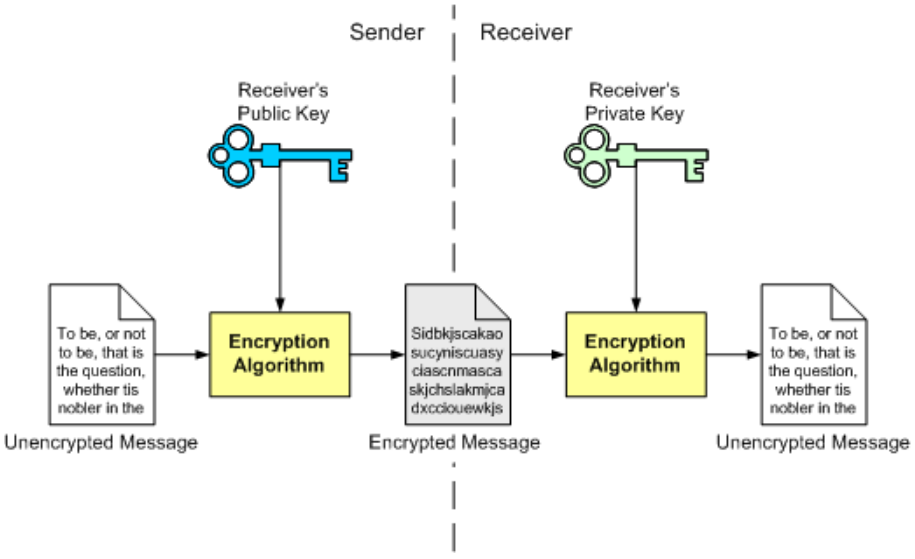

Figure 2.3: Asymmetric Encryption for End User Decryption

The most widely used algorithms in Symmetric key cryptology is Advanced Encryption Standard, Data Encryption Standard and triple DES. The most common public key algorithms for encryption and Decryption is RSA, it involves big prime integers which making them very heavy for devices.

2.3.1 Security and Vulnerabilities

Security should be one of the main concerns when planning any sort of network, and WMN are no exception. WMN have the specificity that part takers are very mobile, can enter and exit the network very frequently and also the reliability of the communication is not very high. Consequently a certain tolerance has to be conceded to the devices, failures in packet delivery tend to be normal and do not represent by itself malicious intent of the sender. Mobile Ad Hoc Networks, unlike wired networks, possess unique characteristics that make it subject to channel and node vulnerabilities. As such a series of nontrivial problems are created for security design to solve and provide protected communication between nodes in a hostile environment as the shared wireless medium may become.

According to [**?**], [**?**] there are two major security issues to ensure secure routing and secure data forwarding.

From [**?**] we can deduce that vulnerabilities of the physical layer are the most outstanding requiring mechanisms to maintain diversity. Major security vulnerabilities on a WMN according to [**?**] are related to key distribution, MAC and Control Secure. Since the nodes are extremely mobile and node failure, frequent updated tables are difficult to maintain. We can increase the frequency but there is a trade off between control messages and battery life as well as processing capacity forcing minimization of divulgation of keys or any other device's non essential information.

There is an inherent fragility of the link since nodes a limited level of physical protection. Node tampering prevention is an imperative in order to maintain network and communication integrity. Mechanisms should be embed on the nodes to guarantee incorruptibility. System imprinting is an important factor as minor vulnerabilities here may be exploited to compromise nodes.

Key distribution is one of the most critical aspects of a security protocol. The connectivity has a sporadic nature that makes throughput, delay levels very inconstant [**?**]. As such node tampering prevention is an imperative in order to maintain network and communication integrity.

Key distribution is one of the critical aspects of a security protocol it can be characterised in one of two ways as to the way keys are divulged centralized or decentralized. Centralized is the most common way to share a key using a third party server or management entity, on the other hand Decentralized key management is uncommon also poorly explored and researched.

Server dependence makes it a main target for attackers, due to the

2.3.2 Attacks

Attacks on a network can be classified with one of two categories - Active and Passive - depending on whether there are packet modification and node interaction, Passive attacks do none of the previous while active can do one or both. Passive attacks are those most difficult to detect, this is due to their remote non-interfering nature that they have. Eavesdropping is one of these attacks, a malicious user listens on the network packet exchange extracting confidential information from the packets, this sort of attack may be overcomed by using encryption. Traffic analysis is another of the attacks where the attacker listens on the packet flow and analyses it, hoping to get relevant

information from the frequency of communication. Lastly Tracking where rogue devices try to get the location of users, this can be done with messages with geolocalized data or by eye of sight maintaining target users within range. Active attacks take a more disruptive role on the network causing more damage on the different layers also being easier to detect because of their interactive nature. Denial of Service attempts to impede the normal function of a specific part of the network, this is usually done by overloading the target with a number of messages that he cannot manage. Channel jamming, similar to DoS, occurs when users interfere with signal emissions and reception blocking communication, can be done using the inherent network procedures like back off, to maintain congestion. Unauthorized access is related to non authenticated networks and the free access to resources or another attack - Impersonation - where malicious user impersonates another user in order to gain access to resources or private information. Message Replay affects both lower and upper layer, this attack consists in capturing messages and sending them in a later time, tries to replicate past circumstances or only confuse the network devices, usually related with control traffic, this attack is immune to message integrity check as the messages are always authentic. In a Battery exhaustion attack, the misbehaving user attempts to rapidly drain the battery of the aimed device. Wormhole is a specific attack to ad hoc network where a node does not forward the messages creating a "hole" in the network. All the previous attack can be generalized into Man In The Middle which refers to a strategically placed attacker that is within the network with capability of listening to messages and altering message content. Such an attack aims at the manipulation of communication in a way that favors the objectives rogue node, which can range from selfish interests in content to the arm of a specific user.

2.3.3 Centralized Models

Centralized Security Models have the advantage of maker user's work lighter while on the other hand there is a high server dependency. This translates into a one point vulnerability where a DoS or other server compromising attack can shut the network down or even compromise all user data.

Public Key Infrastructure

Kerberos is a centralized authentication service that grants access to resources within a network with a ticket based algorithm. The transparency of this service is guaranteed by the necessary authentication of both the user and the server on each access request. The simplicity of the authentication makes this an very efficient model for security.

The standard X.509 allows for the creation of certificate with stipulated parameters connecting a user to a public key. In this standard is also specified revocation certificates that disables user to public key connection. The principle behind certificates is the existence of a higher authority that guarantees the validity of a public key of certain user. The certificate formalises this connection with the authority's signature, which can be authenticated by all users. This has proven very useful in the world wide web environment.

A particular case for centralized security scheme in WMN is MobiSec [**?**]. This model uses the capabilities of routers to distribute key while maintaining independence from technology used in the communication, making security transparent from the user point of view. Besides user

independence MobiSec is able to maintain negligible impact on network performance without sacrificing security

2.3.4 Decentralized Models

There is not much work done in security decentralized models where main drawback is the absence of a authentication/certification authority able to provide an immune credible judgement on device credibility as well as revocation of certificates or black list insertion.

We will introduce, Pretty Good Privacy, a free ware security mechanism widely utilized in email and file storage applications. The combination of the algorithms and Cryptographic functions makes it one of the top choices due to the security resistance of its elements, ease of use and wide divulgation . PGP is a decentralized system users have several Private/Public key pair used to in distributed public key trust lists. The secure information are traded with session key, only used once for a single email, this key follows encrypted with the destination's public key. PGP also allows for message integrity check and message authentication. For each Public key entry a PGP computed key legitimacy field is assigned to it that evaluates the level of binding between the ID and the Public Key. Also an signature trusted field and a owner trust field are linked to the user, the first goes to the credibility of the user in signing public keys and the second shows how trustworthy is this user to certify others. Public key revocation is usually done by the key owner, when a key is compromised. Users issue a revocation certificate signed with the corresponding Private key. PGP introduces the concept of web of trust where every user keeps a Ring of public keys.

Self organization is one decentralized alternative proposed by Jean-pierre Hubaux in [**?**], where all nodes play equivalent roles and is fully decentralized. It is regarded as an adaptation of the well known PGP (Pretty Good Privacy), as the nodes can emit their own certificates and therefore self organize. Like in PGP publicly divulged and distributed trust list where every node includes its own set of trusted keys. And also like in PGP there is used a greatly balanced set of cryptographic functions that allow for a maximization of security while maintaining the efficiency and effectiveness of the network. This protocol has all the characteristics to be a good solution for the decentralized key sharing problem.

Key agreement is a proposal from N. Asokan and P. Ginzboorg in [**?**] for a distributed network system within a limited physical space or with another secure means to share simple key other than the WMN itself. Instead of the usual centralized mechanisms allowing for the sharing of a strong secure key, Key Agreement is based on the fact that a prior context share is available and therefore a authenticated key exchange is feasible. By using an authenticated exchange users are able to create a temporarily secure and authenticated user/ group channel. The great advantage of this model is to build a strong cryptography from a weak password share greatly significantly improving level of security.

Threshold Cryptography used in [**?**], another totally distributed protocol where PKI is used without certificates in a distributed fashion. The principle behind it is that only a certain percentage of user are malicious or misbehaving. In the algorithm User ID is linked to Public Key in a way that

resembles a ID Based Cryptography. Alternative mechanisms contemplate the use of Feldman's Verifiable Secret Sharing which allows users to check the validity of the keys functions by the . VSS is used to share the keys, as a secret. This security scheme claims to be more efficient than IBC fro a reasonably sized group with a low threshold. This central authority absence calls for a group judgement, in other words, since all the users or devices are regarded as equals a minimum of users must agree in a decision.

Another more recent model that provides decentralized anonymous communication is AP3 [**?**], that provide users with anonymity by a central mechanism keeping packet delivery to destination uncertain in every hop, this uncertainty is provided by a waged coin toss. To provide channelization of the communication users use a pseudo ID for them and the channel that is used for routing purposes. Necessary for frequent refreshment is obvious and with refreshing pseudonym creation. All nodes are assumed to be untrusted which leads to a more flexible infrastructure towards topology changes and new users.

2.4 Resume and Discussion

From the Security analyses done we could see that a decentralized security model may take some more implementation and user effort, but it grants security redundancies that prove important in the proposed work. Server dependancy is one of the drawbacks of centralized models, making it the biggest target of attacks.

Chapter 3

Methodology

In this chapter we present the methodology that will detail some aspects of the dissertation as well as a description of the steps to be taken during the development of this project. After reviewing the state of the art literature and studying security models for WMN communications, we will develop a security model fo WMN App. We intend to carry out with an implementation in order to apply the acquired knowledge and certify its applicability to the target audience.

WMN are very susceptible to insecurity as we described previously so we want to provide anonymous discovery as well as information confidentiality which should be built on top of an existing ad-hoc network creation software, already used on other projects by the Telecommunications Institute, and develop functionalities of either messaging or media exchange between peers.

The security protocol we propose to develop intends to be resistant to several known attacks therefore decreasing vulnerabilities against malicious users or devices. The objective is to keep interaction and information of users confidential, private and as safe as possible. At the same time maintaining network efficiency by balancing the trade off between security and overhead. Which will make us take into account performance aspects of the selected cryptography algorithms.

3.1 Hardware and Software

3.1.1 Software

Android is a Mobile Platform that proliferated through mobile phone and tablet devices. Thanks to the ease of access and use of development tools the Google owned operating system triggered an enormous enthusiasm among App developers which led more than 600 thousand Apps being currently available at Google Play. Together with the exponential growth in Apps also the number of devices sold that make it the leading mobile OS. For all this reasons our choice for implementation development is the android developers platform.

A already developed ad hoc network builder will be used to setup and maintain the connections between devices. Some restrictions are made by this application in terms of network configuration that needs to be manual but we do not concern this as a impediment.

3.1.2 Hardware

Android integrated mobile phones and tablets such as the models available at *Instituto de Telecomunicações* are the perfect fit for our project. Although encryption functions may take some processing effort from the phones, we aim at maintaining network performance and also hardware compatibility.

3.2 Analysis of Result

Through experiments conducted simulating malicious attacks we will ascertain that security is not compromised. The Analysis will include message origin and content by analysing traffic and captured packets. To accomplish this wireshark or droidshark application will be used.

Result analysis will also include network performance characteristics like throughput and delay, to certify that Users do not loose noticeable efficacy. This can also be obtained with the use of the previous mentioned tools.

Chapter 4

Workplan

Here we present the work distribution plan in order to achieve the proposed goals. The estimated start and finish dates followed by the projected weak duration.

- 18-02 to 03-03 - Protocol Research - 2 weeks
- 04-03 to 17-03 - Protocol Development - 2 weeks
- 18-03 to 04-04 - Protocol Implementation - 5 weeks
- 22-04 to 05-05 - Troubleshooting - 2 weeks
- 06-05 to 12-05 - Results Analysis - 1 week
- 13-05 to 30-06 - Writing the dissertation - 6 weeks

The Gantt Plan is outlined as follows:

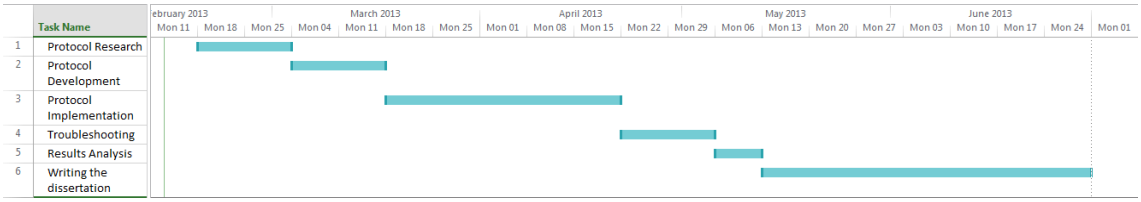

Figure 4.1: Gantt Chart

Chapter 5

Conclusion

We were able to get an overview of the security models properties and characteristics. This way we got familiarized with the several pieces of a security algorithms and how they are applied in different situations. From the Security analyses done we could see that a decentralized security model may take some more effort from implementation and user devices , but it grants security redundancies that prove important in the WMN system.

The enriching research research done will allow for the construction of a more secure and efficient Security Scheme that will give users a better image of applications and more security to use them.

References

[1] Ian F. Akyildiz and Xudong Wang. *Wireless Mesh Networks*. Open University Press, wiley edition, 2009. Cited on pages 1, 5, and 8.

[2] Jinyuan Sun, Chi Zhang, and Student Member. SAT : A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks. 8(2):295–307, 2011. Cited on page 2.

[3] William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson, 5th edition, 2010. Cited on page 6.

[4] UCLA Computer Science Department Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. Security in Mobile Ad Hoc Networks: Challenges and Solutions. 2004. Cited on page 8.

[5] D. Srikrishna and R. Krishnamoorthy. SocialMesh: Can networks of meshed smartphones ensure public access to twitter during an attack? *IEEE Communications Magazine*, 50(6):99–105, 2012. Cited on page 8.

[6] Jean pierre Hubaux. The Quest for Security in Mobile Ad Hoc Networks. Cited on page 10.

[7] P. Ginzboorg N. Asokan. Key agreement in ad hoc networks. Cited on page 10.

[8] Nitesh Saxena. Public Key Cryptography Sans Certicates in Ad Hoc Networks.pdf, 2006. Cited on page 10.

[9] Alan Mislove, Gaurav Oberoi, Ansley Post, Charles Reis, Peter Druschel, and Dan S. Wallach. AP3: Cooperative, decentralized anonymous communication. In *Proceedings of the 11th workshop on ACM SIGOPS European workshop: beyond the PC - EW11*, pages 30–es, New York, New York, USA, September 2004. ACM Press. doi:10.1145/1133572.1133578. Cited on page 11.