An Adaptive Protocol for Efficient and Secure Multicasting in IEEE 802.11 based Wireless LANs

Sandeep K S Gupta and Sriram Cherukuri
Department of Computer Science and Engineering
Arizona State University, Tempe, AZ.
sandeep.gupta@asu.edu

Abstract— **Multicast refers to the technique of sending data to a group of receivers. The use of multicast paradigm in wireless LANs brings significant advantages like savings in channel bandwidth and energy. Considerable research has been done with regard to issues like reliability, but they have not taken into consideration the operation in an insecure environment. We present schemes for secure multicast in wireless LANs, based on the notion of *location based access control*, wherein only a user present in specific locations can access the services provided. Location based access control is a significant requirement in the pervasive computing environments. These schemes make use of the broadcast nature of the medium for sending encrypted data to a group and for key management. Those schemes which are adaptive to the dynamics of the multicast group perform better than static schemes. Three schemes are presented in this paper. The three schemes, vary according to whether, the base station shares the same session key with all the members of its cell(*SSK*) or different session key for each one of the members(*SSK*), or a combination of the two schemes for efficient key management(*Hybrid*). The comparative performance of the three schemes based on the results of simulations are presented.**

Index Terms— **multicasting, security, key management, batching, location based access, adapative protocol.**

I. Introduction

Wireless LANs based on IEEE 802.11 are proliferating at a very fast rate. Unlike conventional networks, wireless LANs offer increased mobility to users. In some cases it may not be economical or even possible to install a wired network. In such situations, wireless LANs can be installed with greater ease. The overall cost of installation and operation can be significantly lower as compared to fixed networks.

As the technology and popularity of the Internet grows, applications such as video conferencing will become more widespread. In such applications, the multicast paradigm plays an important role. In multicast a sender of multicast data sends data to a group of nodes. The broadcast nature of the wireless medium may be used to conserve energy and bandwidth and reduce latency, instead of sending the same data to each receiver one at a time. Multicast protocols used in static networks do not perform well in wireless LANs, because multicast network structures are fragile due to their dynamic nature and must be readjusted as the nodes move and connectivity changes.

There are many applications for multicast in wireless LANs. In hospitals, staff working on certain sections need to send patient information. It may be used in Warehouses, to give instructions to a group of employees. Students on a campus may also be connected to a wireless LAN and access specialized services. Different applications have different security requirements. For instance, scenarios like campuses and conferences, the students or the delegates keep moving in and out of the wireless LAN. It should not be possible for an illegitimate node, which has physical access to the range of a base station to receive multicast data in a useful form, by exploiting the dynamic behavior of the members of the group. If the communication is not secured, it may lead to economic loss to the service providers, as most of the participants may end up not paying. But, we must also ensure that legitimate users are not denied both the service as well as their mobility.

When we try to come up with a scheme for secure multicasting in wireless LANs, two issues are of utmost significance; the *basic security primitives* and *efficient performance* in terms of resource consumption. A secure multicast protocol must ensure that only legitimate users are able to receive the data in useful form. To all others, even if they receive it, it should be unintelligible. Cryptographic techniques are used in order to achieve requirements of security like availability, confidentiality, integrity, authentication, and non-repudiation [6]. Many of the available solutions are not suitable, as they are computation and bandwidth intensive. Our endeavor is to minimize the cost incurred in terms of communication and computation, for implementing the security mechanism. In order to achieve a higher performance, the security scheme has to make use of the fact that all the group members receive the same data and it can be transmitted simultaneously, making use of the broadcast nature of the medium.

Securing multicast communication, in addition to those stated earlier should provide the following functionalities [3]:

- **Forward Message Secrecy** – A node should not be able to read multicast communication after it leaves the multicast group.
- **Backward Message Secrecy** – A node should not be able to

read multicast communication exchanged prior to its joining the multicast group.

Schemes based on unicast communication have been proposed for secure communication in wireless LANs [4]. However, if they are extended to multicast, then they do not take advantage of the broadcast medium. Therefore even though they may be secure, they would not be efficient in terms of energy consumed at the receiving end, because the packets sent will be received at the physical layer of all the nodes within the range of the sender. Also they are based on expensive public key cryptography like digital certificates.

Multicasting schemes currently exist for wireless LANs, however none of these address the problem of secure multicast communication. The objectives of existing protocols for multicast communication are reliable message delivery [2] and energy efficiency. However, operation in a hostile environment has not been considered. Secure multicast protocols are difficult to implement efficiently, due to the dynamic nature of the multicast group and the scarcity of energy at the receiving end. Hence, the security mechanisms need to be studied and those which are compatible to existing multicast protocols need to be implemented.

Relatively little research has been done in this area in the past. The research presented in this paper makes use of the shared group key mechanism, thereby taking advantage of the multicast paradigm. The schemes presented in this paper provide a security architecture for -existing multicast protocols with reliable message delivery like [2]. Three schemes are presented in this paper. In the *Single Session Key(SSK)* and *Different Session Key(DSK)* schemes, the base-station shares the same session key and different session key with the members of the cell respectively. The dynamic nature of the multicast group, causes a static solution to provide sub-optimal performance. Adaptive schemes that respond to current conditions perform better than static ones. In the adaptive *Hybrid* scheme the base station shares a single session key with a set of the relatively less mobile receivers and separate session keys with the remainder. As the multicast groups are highly unpredictable, it is shown that each scheme performs differently depending on the mobility patterns of the members of the multicast group. In this paper, our main objective is to achieve the basic security requirements in an efficient manner for multicasting in wireless LANs.

The remainder of this paper is organized as follows. Section II describes the notion of the multicast group, Section III presents the system model and the assumptions, Section IV describes the key exchange protocol, Section V, VI, and VII describes the three key management schemes for secure multicast and certain optimizations. In Section VIII we describe the results of simulation. In section IX, the conclusions are presented.

II. The Notion of the Multicast Group

In this section, we describe the group membership and the semantics associated with it. In our model, we adopt the location of the mobile host as the criterion to define the group. The services and the data accessed by the mobile host is dependent on its location. The location of the mobile host with respect to a base station, determines whether it is part of that group or not. This model is similar to the Pervasive computing environment model. In Pervasive computing environments, *location based access* is used for granting permission for accessing resources to users. For instance, only people assembled inside a hall may get streaming music and not people in the adjacent room, even if they are in the range of the base station. The knowledge of the user location is used to grant access to resources, but it is equally important to protect the privacy of his location. In our schemes, the user's privacy of location is not violated because the system does not possess the knowledge of the exact location, nor is his movement monitored continuously as history of exact location is not maintained. This is tune with privacy requirements of the pervasive computing environments [10].

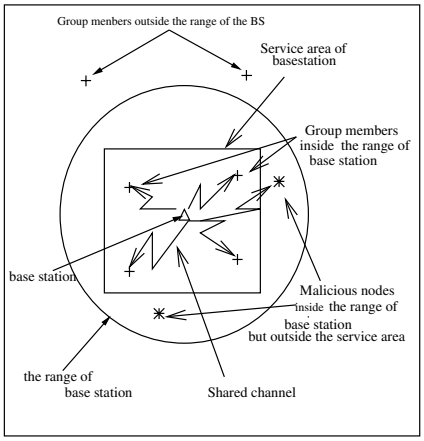

Fig. 1. System Model

III. Assumptions and System Model

A. Basic Assumptions

- The base-station is the only sender of multicast data.
- All the legitimate members of the multicast group share a ***weak key***. A weak key may be an alphanumeric password readily available to all members of the group. The weak key acquisition depends on the application.
- A suitable mechanism for reliable multicast communication [2] and unicast message delivery [1] is assumed.
- Appropriate MAC level protocols are assumed to assure contention free channel access for communication [1].

B. System Model

Our system consists of a group of nodes, which constitute the multicast group. Each of these nodes attaches itself to a base station depending on its location. The group members keep moving

in and out of a cell in random patterns. Each base station caters to a cell like a floor of a building. The cell is a part of the transmission range of the base-station. There exist areas in the range, which are not part of the cell. The base station keeps track of the membership of the cell. The members of the group periodically inform the base station of their presence. Whenever the base station detects a change in the membership of its cell, keys are distributed, depending on the protocol that is followed. The topology at a random instant of time is as shown in figure 1. With regard to the multicast data the base station multicasts it to all the members which share the same session key, while it unicasts it to members with whom it shares unique keys. The base station expects the legitimate group members to move in and out of the cell. It also expects malicious nodes to be present in the transmission range. The security model is based on the shared key encryption.

IV. Key Agreement and Set Up

A node X which wants to join the multicast group, needs to obtain the session key to ensure secure communication. This involves two stages. In the first stage a unique key is established. Then the session key for the multicast is then encrypted using the corresponding unique key and is sent to all the nodes which need to get it depending on the protocol at hand. The establishment of the unique key is done by the following protocol. The two nodes X and Y share a weak secret P. The goal of the protocol is to enable X and Y to mutually authenticate each other based on P, and agree on a strong individual key K, in such a way that an attacker watching the traffic will not be able to learn K or mount a dictionary attack on P. During the protocol, X generates random string S_x. Y generates two random strings: R, and S_y. A suitable symmetric key encryption scheme, which are freely available [9] and which can be used with the unique key is considered. The lengths of the other random strings could be specified in the specific implementation of the protocol. The protocol proceeds as follows:

1) X→ Y: X Hi I am X
2) Y→ X: R Prove it
3) X→ Y: E_P(hash(R),S_x)
4) Y→ X: E_P(hash(S_x),S_y)

E_P(x) refers to the encryption of x using P as the key. In the first step the entering node X sends a message requesting a key. Upon receiving the request the base station Y generates a random number R and sends it to X in the second step asking X to authenticate itself. In the third step, in order to authenticate itself X encrypts R along with a random nonce S_x using P(a weak shared secret). On receiving it, Y decrypts it with P and if it results in R then X is authenticated to Y. Y also extracts S_x. Here S_x serves two purposes. One is that X does not have to encrypt a random number which is not generated by it. This prevents resend attack [6]. Secondly S_x is used as a parameter to the function used to generate the unique key. In the last step Y encrypts with P the combination hash of S_x and S_y, which is a random nonce generated by Y. Now X can obtain S_y. S_x and S_y, which are known to both X and Y are used as parameters for the generation of the unique key. Since both the parties contribute the input material for key generation it is not possible for one of the parties to act maliciously (i.e.) select a weak key.

It may be seen that unless an adversary knows the initial shared secret it is not possible for him to attack the above key sharing protocol. If a malicious node say M tries to masquerade as X then it will fail in the third step of the protocol, since it will not be able to encrypt R correctly as it does not have knowledge of weak shared secret P(only those nodes that are legitimate members of the multicast group have knowledge of P). On the other hand if some node gets hold of the key request message from X of the first step and may try to masquerade as Y. In such a scenario the protocol would fail in step four, since the malicious node cannot encrypt S_x generated by X correctly as it does not have knowledge of weak secret P.

V. Group Communication for the Key Distribution

Session keys have to changed after every leave and join, to achieve forward and backward message secrecy. Changing a session key may be done in two ways. After a join or leave the new session key is computed and it is encrypted with unique keys of all the members and it is unicasted to the members of the group. Another way would be as follows. After a join the new session key is encrypted with the newly established unique key of the new member and sent to it. The new session key is encrypted with the old session key and is multicasted to the older members of the cell. For the leave the new session key has to be encrypted with the unique keys and sent.The old session key cannot be used, as the node with has left has knowledge of the old session key. We have performed experiments for both above methods. They are presented in section VIII.

VI. Algorithms

In this section we present the algorithms for each of the proposed schemes.

A. Single Session Key

The scheme with the Single Session Key (SSK) for all members of a cell works as follows:

1) The sender of the multicast data sets up the initial multicast group.
2) After the receiver joins a base station, the session keys are set up between them.
3) The base station establishes the same session key with all the members in the cell, as explained earlier.
4) When a receiver node leaves the cell, the base station establishes a new session key with the remaining members in the cell. This ensures forward message secrecy.

5) When a new receiver node attaches to a base station, the base station establishes a new session key with all the members of the cell. This ensures backward message secrecy. Here multicasting may be used as explained in the previous section.

B. Different Session Keys

The scheme with Different Session Keys (DSK) for all members of a cell works as follows:

1) The sender of the multicast data sets up the initial multicast group.
2) After the receiver joins a base station, the session keys are set up between them.
3) The base station establishes individual session keys with each member node using the protocol explained earlier.
4) When a member leaves the cell, no key exchange is required. The key the base station shared with the departed member is invalidated
5) When a new member attaches to a base station, the base station establishes a new session key with it.

C. Hybrid Scheme

The hybrid scheme uses the concept of *Stable* and *Unstable* nodes to determine the kind of session key shared by the mobile host and base station. A member is classified as *Stable* or *Unstable* depending on whether it has been a member of the group for more than a given period of time. This period of time serves as parameter for adaptation. The base station shares the same session key with all the *Stable* members of the cell, while it shares a separate session key with each individual *Unstable* member.

Initially all the members are classified as *Unstable* upon entering a cell. In this scenario the base station shares different session keys with each member, making this similar to *DSK*. If the node stays in the cell for a predefined time interval, then the node is classified as *Stable*. A node remains *Stable* until it moves out of the cell. All the *Stable* members share the same session key with the base station.

The hybrid scheme is made adaptable by the parameter t_s. This parameter determines whether a member will be reclassified or not. If the ratio of time for which the mobile host has been in the service area to the *batch interval* is greater than t_s, then the mobile host can be reclassified. The parameter t_s is determined from the mobility rate of the nodes and prior history. t_s is not constant for the entire network, but each base station in the network can dynamically configure the value of t_s. We have conducted experiments to determine the optimum value of t_s, the results of which are presented in section VIII. , adapative The hybrid scheme requires maintaining a record of position of each member node. The history maintenance starts as soon as the member enters the cell when it is classified as an *Unstable* member. Thus whenever the member enters, a counter is started for that member. If the member remains in the cell for time greater than t_s times the beacon interval then it is classified as stable. However, if the member moves out before that time interval elapses then the timer is reset (i.e.) the history is erased. If the value of t_s were higher then the memory required for maintaining the history would increase. However, choosing a small value for t_s may result in nodes that are not totally stable being classified as *Stable*. Thus the value for t_s should be such that the memory requirement is minimized and appropriate reclassification is performed.

VII. Periodic Batch Re-keying

In the algorithms described above, we have mentioned that the base station responds to the events of members entering and leaving the cell as they happen. But such individual rekeying would be inefficient. Suppose a series of events, which require rekeying occur in a small interval of time, then using individual rekeying requires that we rekey for each of the events. *Periodic batch rekeying* can be used to solve these problems to a large extent. In periodic batch rekeying the events requiring rekeying are collected over a period of time called batch interval and handled together at the end of the interval. This reduces the number of rekeyings. But this procedure increases the delay to access the data, because a new user has to wait longer to be accepted by multicast group and departed user stays longer. A balance is maintained by choosing the right value for the *batch interval* (i.e.) it should not be too large [7].

VIII. Simulations and Results

In this section we present the simulations performed in order to study the performance of the schemes for secure multicast described above. We describe the properties of the nodes, their mobility patterns and the performance metrics that have been used to evaluate the proposed schemes. Then we present the comparison of the performance of the proposed schemes based on the results of the simulations. The performance of the Hybrid scheme at various mobilities for different values of t_s, the factor of adaptation is also presented.

A. Simulation Environment

The schemes for secure multicast described above have been simulated using the NS-2 simulator [8]. The schemes have been implemented at the Medium Access(MAC) layer of the protocol stack. In the simulations, a multicast subgroup consisting of 25 nodes is taken into consideration. This subgroup represents a base-station in the multicast group and its service area. Each node has a transmission range of 250 meters and a bandwidth of 2Mbps. The "scengen" tool with random way point model available for NS was used to generate random movement of the mobile hosts.

Parameter	Value used
Batch Interval	0.1 secs
Beacon interval	0.01 secs
No. of Packets	1000
Simulation time	70.00 secs

Fig. 2. Parameters used in the simulations

The communication cost at any speed is the average of communication costs of 10 sets of mobility patterns generated for that speed using "scengen".

In the simulations, data packets are generated at a continuous rate. For each of the schemes the simulations are run for a fixed duration of 70s. The time taken by the system, for the multicast of 1000 packets is measured. This communication time includes both the time consumed for multicasting the data packets as well as the time consumed for performing the key distribution. The base-station checks its table after a specific period of time over which the joining and leavings of members are batched. If it finds that rekeying has to be performed then the data is stopped and the rekeying process is started. This time is also included in the communication cost. The need for rekeying may arise or may not arise depending upon the scheme which is being simulated.

B. Comparison of DSK and SSK

For low mobility rates the communication time for *SSK* scheme is lower as compared to *DSK*. This due to the fact that the number of rekeyings are less and hence the key management part of the total cost is lower than the data communication time. Since *SSK* multicasts data while DSK unicasts it after encrypting it with different keys the data communication cost of *DSK* is more than that of *SSK*. But in case of high mobilities the key management cost of *SSK* dominates over the data communication cost. Hence the total communication cost increases rapidly in case of *SSK*. Whereas in case of *DSK* even at high mobilities the data communication cost prevails. Hence it performs better than *SSK*.

C. Comparison of SSK and the Hybrid Scheme

The hybrid scheme perform better than SSK depending on the mobility rate of the nodes. If the nodes are highly mobile, then frequent change of session keys would be required. This is overcome in the hybrid approach since a node does not share the same session key until it becomes stable. However, if the nodes are pretty static with respect to the base-station after joining the multicast, then an overhead is incurred in the hybrid scheme to move those nodes from the *Unstable* group to the *Stable* group.

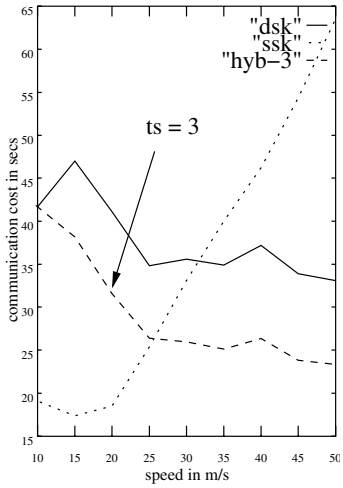

Fig. 3. Comparison of the three schemes

D. Comparison of DSK and the Hybrid Scheme

In *DSK* all the nodes have a different session key even though nodes that are fairly immobile with respect to the base-station could share the same session key. The hybrid scheme moves such nodes into the *Stable* group thereby reducing the communication overhead. This brings in an element of the multicast paradigm. The communication cost required to send the data to all the nodes is reduced for the *HYBRID* scheme since the data is multicasted for a subset of the mobile nodes.

E. Performance with Batching

Figure 4a shows the performance of the Hybrid scheme when the join/leave events are batched and when they are not batched. From the figure it may be observed that the scheme performs better when the events are batched at high mobilities. This improvement in performance may be attributed to the fact that the rekeying which are required in a batch interval are merged into one in batched scheme, while this is not the case when batching is not done.

F. Performance with Multicasting for key distribution

Figures 4b shows the performance of the HYBRID scheme when multicasting is used for key distribution as explained in section V and when it is not used . Performance improves with multicasting due to reduction in number of transmissions by base-station.

G. Adaptability of Hybrid scheme

Results of experiments performed to determine the optimal value of t_s for Hybrid scheme are shown in figure 5. As mobility increases the communication cost varies significantly and the scheme performs better with higher values of t_s. But this trend

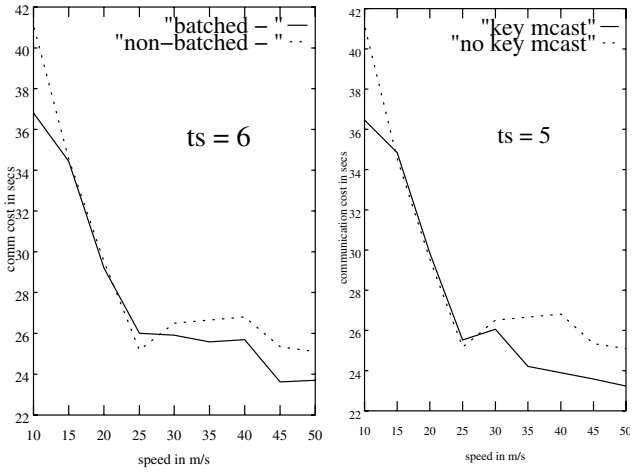

Fig. 4. Performance of Hybrid scheme with and without (a) Batching and, (b) key-multicast

reverses after a certain point (t_s = 8). This is because at high mobility, the probability that a node moves out after a particular time is high. So it is desirable that we wait for longer time before we classify the mobile host as stable because of the overhead involved in rekeying, if a stable node leaves is high. But if we wait for too long, mobile hosts which are eligible for classification as stable remain as unstable for longer time. Hence data is unicasted them instead of including them in the multicast group. This overhead exceeds the overhead of rekeying. Thus a value of t_s which balances both overheads is to be chosen.

IX. Conclusions

In this paper, we have examined three schemes for secure multicasting in wireless LANs and discussed their relative performance. It has been observed that for wireless LANs which are prone to moderate to high dynamic behavior, the Hybrid scheme performs better than the other two schemes due the introduction of multicast paradigm in data transmission and the reduction in the number of key setups. We have also used the concepts of batch processing and multicasting in key management to optimize the cost. Within the Hybrid scheme we are able to adapt to the mobility, thereby reducing the cost further. The optimal value of adaptability factor has been determined.

Acknowledgemets

The author would like to thank the anonymous refrees for their helpful suggestions which helped to improve the quality of the paper. This research is supported in part by National Science Foundation Grants ANI-0086020 and ANI-0196156.

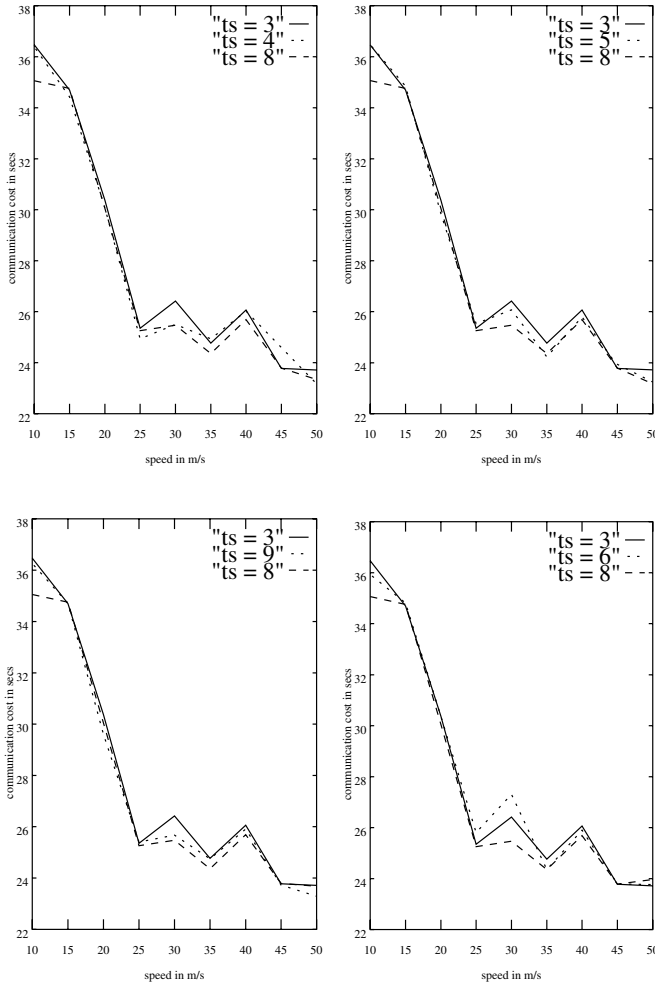

Fig. 5. Performance of Hybrid scheme with variation in t_s

References

[1] ANSI/IEEE Standard 802.11, In 1999 Edition,

[2] J.Kuri and S.K.Kasera, Reliable Multicast in Multi access Wireless LANs, In IEEE INFOCOM '99, 1999,

[3] L.R.Dondeti, S.Mukherjee, A.Samal, Scalable secure one to many communication using dual encryption, In Computer Communications, Volume 23, Issue 17, Pages 1581-1723 (November 2000)

[4] V.Bharghavan, Secure Wireless LANs, In ACM Conference on Computers and Communications Security '94,; Fairfax, VA.

[5] D. Bruschi and E. Rosti, Secure Multicast in Wireless Networks of Mobile Hosts:Protocols and Issues http://citeseer.nj.nec.com/295645.html.

[6] B.Schneier Applied Cryptography,Protocols,Algorithms and source code in C Second Edition.John Wiley & Sons

[7] X.S.Li, Y.R.Yang, M.G.Gouda,S.S.Lam Batch Rekeying for Secure Group Communications Tenth international World Wide Web Conference,Hong Kong,China May 2001

[8] http://www.isi.edu/nsnam/ns

[9] J.B. Lacy, D. P. Mitchell, and W. M. Schell CryptoLib: Cryptography in software Proc USEN1X4th UN1XSecurity Symp., Oct. 1993.

[10] Marc Langheinrich Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems Proceedings of Ubicomp 2001, September 30 - October 2, 2001, Atlanta, GA.