Chapter 8

CONCLUSION

8.1 SUMMARY OF THE WORK

The purpose of this dissertation was to show whether smart cards could be used to secure field area network. A literature study provided background on field area networks, the requirements of information security and what smart cards could offer. The system that had to be secured was defined and possible threats were identified. Functional requirements were determined and a risk analysis done to see how the threats could have an impact on the system. Safeguards were selected to provide the security services and two security policy schemes, using different mechanisms, were formulated. Both schemes were evaluated to determine whether security could be assured. Performance was also evaluated to determine whether it is feasible to implement these schemes in a field area network.

8.2 SUMMARY OF THE RESULTS

8.2.1 Effectiveness of Security Policies

8.2.1.1 Scheme 1

Scheme 1 has a major advantage when it comes to key management. Master keys do not need to be kept as session keys can be exchanged at will using RSA. RSA digital signatures also provide better repudiation. This scheme has two major problems:

- Performance: The nodes and the smart cards cannot efficiently implement the PKI functionality. Mutual authentication and key exchanges taking over $4s$ are not feasible. If the system requires the extra security this scheme can be implemented.
- RSA: Many countries do not allow public key cryptography for the purpose of data encryption (as required by the X.511 protocol) but only as a means to perform digital signatures. Therefore many smart cards cannot recover data encrypted using RSA. The digital signature basically uses RSA decryption for signing and encryption for verification. Verify signature commands implemented in smart cards do not return any data.

8.2.1.2 Scheme 2

Scheme 2 has a slightly more intricate key management system, as nodes, gateways and owners need to keep updated symmetric keys. The key management suggested never allows the master key shared between the owner and the node to be revealed (it is never send over a data link). Therefore owner to node communication should be very secure.

The other master keys are also distributed using secure channels. If a node's master key with its owner should be compromised it can be revoked and only a new smart card is needed to restore functionality. This system also places fewer burdens on the node's processing and storage resources. This scheme has one major problem:

- Non-repudiation: The symmetric nature of the signature does not allow for non-repudiation as both the receiver and the sender can generate the signature. The transaction must therefore be recorded by an independent arbiter. This is however only an issue with node-to-node communication. The way the key management is done requires the node to contact the gateway or its owner to gain a key. These entities can record the nature of the transaction and settle later disputes.

8.2.2 Comparison of Security Policies

Both the proposed schemes adequately provide the necessary security functions. Although scheme 2 does not have such a high security assurance as scheme one it definitely performs better using low-resource hardware. It is suggested that scheme 1 is utilized in advanced field area networks where nodes have sufficient resources to implement PKI efficiently e.g. factory and industrial automation. Scheme 2 should be used to secure simple field area networks in less intensive environments, e.g. remote data loggers or power measurement.

8.3 CONCLUSIONS

Finally, the following important conclusions can be made:

- It is possible to formulate a policy which could be implemented successfully into a field area network using the security mechanisms provided by a smart card while maintaining reasonable system performance, despite the resource limitations of the field area network.

- The performance of the security operations, as implemented using smart cards, is adequate but application specific considerations must still be taken into account regarding the scheme to be applied. Both schemes assures security, but scheme 1 has the major advantage of easier key management at the cost of performance, while scheme 2 performs better at the cost of a more intricate key management system. Which scheme to use is up to the implementer and application constraints.

- The performance measures of field area networks are fairly predictable. This enables the designer to determine the time to perform security operations in advance and then make a suitable policy choice accordingly.

8.4 SUGGESTIONS FOR FUTURE WORK

Future work should include the following:

- Evaluation and verification of the proposed security policies using cryptanalysis and formal methods.
- Algorithm design for smart cards. Faster digital signatures and key exchange using public key cryptography.