Secure Aggregation in Wireless Sensor Networks

Julia Albath

1 Introduction

In-network aggregation in wireless sensor networks (WSNs) is an approach that allows for a large savings of energy.Most wireless sensor network applications are deployed in environments which can affect the motes. An attacker may be able to gain physical access to some motes, introduce motes into the network or simply inject messages into the communication channel. Such corrupted or spurious motes may fail to participate in the common tasks of a sensor network. Security in WSNs includes confidentiality, integrity and availability. Any useful sensor network protocol needs to ensure that the generated data is available the user in a timely manner. Unfortunately, many existing security primitives cannot be used in sensor networks, either because the computing power of the motes is too limited or the additional work created by the protocols causes excessive network traffic [1].

We propose to contribute to the characterization of and protocols for secure aggregation in wireless sensor networks. Security is even more of a challenge in WSNs when in-network aggregation is utilized. Hence in order to secure data aggregation in a sensor network, we must not only provide protection against eavesdroppers, but we must also prevent intermediate motes from interfering with the data.

2 Prevention of Attacks on Aggregation in Clustered Environments

We propose a protocol that achieves secure and private aggregation. The Secure and Private (SePri) protocol has three phases. Our protocol is a threshold protocol. In phase one, each mote generates a random number, which becomes its private key. Each mote makes available the corresponding public key. After the private keys have been generated, the next phase of the SePri protocol securely and privately calculates the aggregate. Motes participate in a secure multi-party computation protocol (SMC) to calculate the aggregate. At the end of the protocol, motes will have calculated the aggregate. Motes then use their secret key to sign the aggregate. The mote sends its signature to the cluster-head. The cluster-head combines the partial signatures into a full signature. The cluster-head sends the aggregate reading, a list of non-contributing motes and the full signature to the base station for verification. The base station uses the list of missing contributors to generate the appropriate public key and verifies the signature.

2.1 Secure Multi-Party Computation (SMC) for WSN

General SMC offers the ability to securely and privately compute most functions in a distributed fashion [2]. Each participant, generally referred to as Player P_i, executes the same steps. At the end of the protocol each player knows the result of the function applied to all inputs, without having learned anything about the inputs of the other players. To execute the SMC protocol, each player choses a random polynomial $f_i(x)$ of degree $t-1$. The zero-term of the polynomial is the current input of the player. Each player then computes and distributes one share for each participating player using the polynomial. Next, each player calculate its local aggregate using the received shares. The players communicate their local aggregate with all other players. Each player can now calculate the final aggregate using interpolation. Only t of the distinct shares are required to calculate the aggregate.

The one thing that makes a straightforward use of a SMC protocol difficult in sensor networks is the number of messages which need to be exchanged [3]. After each player generates its shares, one set of messages for every pair of players needs to be exchanged. After the local aggregate has been calculated, one message from each player for the entire network needs to be broadcasted. Especially in the case of a multi-hop network, the communication cost encountered for such a broadcast can become very large. In sensor networks, an SMC protocol should only be applied in a cluster. In order to reap the benefits of SMC within the constraints of wireless sensor networks some changes need to be made. We propose two simplifications to the general SMC protocol:

- Any mote which is not able to directly communicate with its cluster-head shares its reading with its parent, the next hop toward the cluster-head. This simplification is acceptable because in WSNs a sensor generates readings which are similar to its neighbors. Additionally, a leaf mote has no choice but to trust that its parent honestly participates in all

protocols. Only the gray motes would participate in the SMC protocol, this would reduce the number of players from 20 to five and thus result in communications savings.

- In a highly connected cluster, such as depicted in, m motes would randomly be selected to act as the players in the SMC protocol. We show the selected motes in gray. The other motes would send their reading to one of those m motes for further processing. In either case, this first step reduces the number of players in the SMC protocol from n to m. The process of selecting which m motes participate as players in the protocol should be randomized. This would also make it harder for motes to collude, as colluding motes will have to be players at the same time. An attacker which has gained access to several motes with the intend to overcome the protocol by controlling t motes, needs to make sure that those t motes participate in the protocol as players during the same execution. If the selection of player-motes is randomized, then an attacker will have to control more than t in order to be sure that the protocol can be overcome. Requiring an attacker to control more motes makes it less plausible that the attacker will be able to overcome the protocol.

There are some open questions regarding the use of SMC in sensor networks that this study will be answering:

- To what degree will a missing share affect the aggregate?
- When shares are not received from motes, could estimation be used to substitute the missing value? What effect would estimation have on the accuracy of the result?
- How much will different threshold values t affect the accuracy of the aggregate if there are missing shares?

3 Summary

The proposed research will further the security of aggregation in sensor networks. Possible attacks and behavior of corrupted motes will be classified. The possibility of using a SMC type protocol in sensor networks will be explored in great detail. At the end of the proposed research, guidelines will be available which will define the effect of various strategies for securing aggregation in sensor networks.

References

[1] J. Albath and S. Madria. Practical algorithm for data security (PADS) in wireless sensor networks. In *MobiDE '07: Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access*, pages 9–16, New York, NY, USA, 2007. ACM Press.

[2] R. Cramer, I. Damgard, and R. de Haan. Atomic Secure Multi-Party Multiplication with Low Communication. *LECTURE NOTES IN COMPUTER SCIENCE*, 4515:329, 2007.

[3] I. Damgard and J.B. Nielsen. Scalable and Unconditionally Secure Multiparty Computation. *LECTURE NOTES IN COMPUTER SCIENCE*, 4622:572, 2007.