TikiriAC: Node-Level Equally Distributed Access Control for Shared Sensor Networks

Nayanajith M. Laxaman, M.D.J.S. Goonatillake, and Kasun De Zoysa

University of Colombo School of Computing
No. 35, Reid avenue, Colombo 7, Sri Lanka
{nml,jsg,kasun}@ucsc.cmb.ac.lk
http://www.ucsc.cmb.ac.lk/wasn

Abstract. In this paper, we propose an access control mechanism that can be used to overcome challenges and problems related to access controlling in a shared Wireless Sensor Network (WSN) databases with complex connectivity topologies.

Keywords: Distributed Access Control, Shared Wireless Sensor Networks, Privilege Management Infrastructure, Public Key Infrastructure.

1 Introduction

Researchers and organizations from various disciplines are interested in using WSN for their research and applications. Deploying a sensor network of their own is a time consuming, infeasible, and a complicated task for companies and organizations such as universities, research groups, small business groups, and other interested individuals due to high cost of the devices, not authorized to deploy, etc. Therefore, the concept of Shared Wireless Sensor Networks (SWSN) is getting popular among these communities [1]. However, providing shared access for WSN has given rise to a different set of problems. An important issue which we consider in this paper is controlling access among SWSN users.

A considerable amount of research has been carried out in the area of controlling access of users within a SWSN. There have been mainly four approaches found in related research literature for authentication and authorization of users for SWSNs. 1) Centralized, 2) Selectively distributed within SWSN, 3) Equally distributed within SWSN, 4) Client side [2], [3], [4]. However, there are pros and cons of each of these approaches depending on the topology used to access the SWSN. For example, access controlling measures of a SWSN with single entry point would be different from the measures considered in a SWSN with multiple entry points. Therefore, it is challenging to come up with a solution that can address the issues which would arise in any SWSN topology. In this paper we propose a solution which addresses all these SWASN topologies. TikiriDB is a database abstraction which enables sharing sensor network whilst supporting all these topologies of user connectivity [1]. Therefore, we developed our solution as a module to the TikiriDB.

P.J. Marron et al. (Eds.): REALWSN 2010, LNCS 6511, pp. 202–205, 2010.

2 Our Approach

Since, a particular user may have the total control over the client application, client side authentication and authorization would be the least preference when giving a solution to the mentioned problem. Centralized approach has the limitation of single point of failure. Therefore, a distributed access controlling mechanism is preferable where the failure of several SWSN nodes may have a limited impact on total access controlling system. However, if access controlling has been distributed to handle individually by the nodes themselves, probability of failure can further be reduced. Therefore, in our proposed access controlling solution for SWSN, we opted to handle access controlling at node level, individually. In our approach, we opted to use public key certificates and attribute certificates to implement authentication and authorization in SWSN. Researchers have successfully implemented public key infrastructures on top of WSN using Elliptic Curve Cryptography (ECC) [5]. ECC scheme provides 1024 bit RSA equivalent security only by using 160 bit certificates. Therefore, many researchers in sensor network discipline have opted ECC as their primary cryptographic system [5], [6], [2]. Public key cryptography is used for initial secure communication and a shared key is exchanged between source and destination nodes to continue further communication using symmetric key cryptography.

2.1 TikririAC Module for TikiriDB

TikiriAC is developed as a module for TikiriDB. TikiriAC module has two main components where one is at the node and other is with the user. Enabling TikiriAC in TikiriDB pass the optimized query generated by TikiriDB client to TikiriAC. Then, TikiriAC handles authentication and authorization of users. The result of successful authorization process passes requested query to TikiriDB query processor at nodes. TikiriAC also ensures the security of the query results when they transferred back to the user.

2.2 TikiriAC Public Key Infrastructure

Figure 1 illustrates proposed public key infrastructure in TikiriAC. Public key certificates are issued by a Certification Authority (CA) and attribute certificates are issued by an Attribute Authority (AA). However, considering the resource limitation in sensor nodes we propose using common certificates for both AA and CA by forming a Hybrid Authority (HA). Furthermore, since network communication consumes a considerable amount of power of a sensor node, we further reduced the size of attribute certificate and public key certificate by removing several attributes from the certificates to reduce number of data packets propagated in WSN when initializing the security algorithm. Therefore, it should be mentioned that the certificates used in TikiriAC are not fully compliant with X.509 standard. In addition to that, for the time being, certificate revocation protocols have not been incorporated. Hence, the user certificate expiration time has been set to a very short period to make sure users renew their

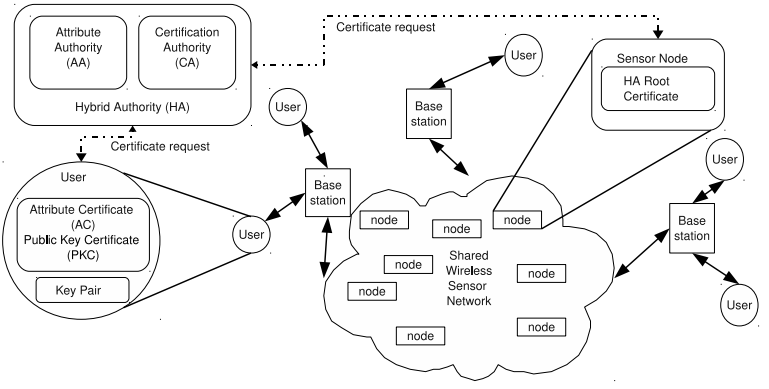

Fig. 1. TikiriAC public key infrastructure

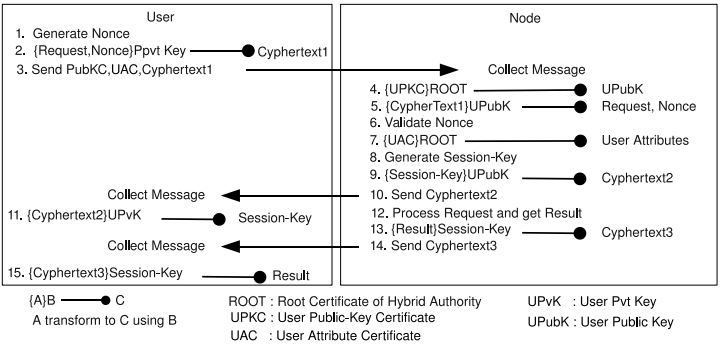

Fig. 2. TikiriAC Protocol

certificates frequently. Public key certificates are used to authenticate the users and to share a symmetric key between data requesting user and destined sensor nodes. Attribute certificates are to manage authorization of the users [7]. Every authenticated user of the SWSN has a public key certificate and an attribute certificate issued by the owner of the SWSN or a trusted coordination party. The public key certificate of the hybrid authority (HA root certificate) is burned in to each node at the time of deployment.

2.3 TikiriAC Protocol

Figure 2 illustrates TikiriAC protocol. First, the user who accesses the SWSN generates a nonce (a time stamp) for the current message to be sent with the message (1). The query and nonce is signed using requesters private key (2). The content is then sends to the destination node with the signature, and requesters public key certificate and attribute certificate (3). At the destination node, to verify the authenticity of the requester, node use ECC algorithms to verify requesters public key certificate using HA's root certificate (4). Then the public

key certificate of the user is used to decrypt the encrypted content and reveals nonce and the query (5). Newly received nonce is used to prevent replay attacks (6). If the message possess a valid nonce, the attribute certificate is verified using the HA's root certificate (7). A valid attribute certificate is providing the accessibility constrain information for a particular user such as; which sensors the user can access, how long he can execute a query, what is the maximum frequency that the user can obtain information, etc. Within the TikiriAC protocol, if the message fails at any step of verification or validation, the request is discarded. After successfully completing the above process, node generates a session key to be used for the communication between the user and node itself (8). The session key is then encrypted with users public key and sends back to the user (9). Then the user decrypts the encrypted session key by using his/her private key and keeps the session key until this query execution finishes (10). Any further communication or new session key exchange is done through an encrypted channel between the user and the node. It should also be mentioned that it is required to encrypt the messages in certain situations such as for in-network aggregation of sensor data. For example, calculating the average temperature of given set of nodes. A group key generation and manipulation algorithm is introduced to overcome this issue.

3 Conclusions

Here, we have introduced a solid architecture to overcome the access control problem arising in shared sensor networks with complex topologies. High security was guaranteed in the use public key cryptography. We considered several measures to reduce the resource consumption caused due to public key cryptography in the sensor network. Finally we explained the appropriate architecture and technologies to implement our design as a module for TikiriDB.

References

1. Laxaman, N.M., Goonatillake, M.D.J.S., Zoysa, K.D.: Tikiridb: Shared wireless sensor network database for multi-user data access (2010)
2. Wang, H., Sheng, B., Li, Q.: Elliptic curve cryptography-based access control in sensor networks. Int. J. Security and Networks
3. Benenson, Z.: Authenticated queries in sensor networks. In: Molva, R., Tsudik, G., Westhoff, D. (eds.) ESAS 2005. LNCS, vol. 3813, pp. 54–67. Springer, Heidelberg (2005)
4. Networks, W.S., Karlof, C.: Tinysec: A link layer security architecture for wireless sensor networks
5. Liu, A., Ning, P.: Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks
6. Gupta, V., Wurm, M., Zhu, Y., Millard, M., Fung, S., Gura, N., Eberle, H., Shantz, S.C.: Sizzle: A standards-based end-to-end security architecture for the embedded internet. Technical report (2005)
7. Johnston, W.: Authorization and attribute certificates for widely distributed access control (1998)