European Journal of Scientific Research
ISSN 1450-216X / 1450-202X Vol. 140 No 4 July, 2016, pp.458-463
http://www.europeanjournalofscientificresearch.com

Model of Secure Device Interaction Protocol in Mobile and Sensor Networks

Ali Jaber Tayh
College of Computer Science and Information Ttechnology
University of Al-Qadisiyah
E-mail: Ali.Jaber@qu.edu.iq

Abstract

Mobile devices are becoming truly ubiquitous, and mobile computing is making revolutionary changes in the computer world. Mobile devices can constitute heterogeneous networks that provide access to information in online mode from any point in the world. This leads to the issue of ensuring mobile network and information system security, which is quite a complex but relevant task. Such a security system should be easy to use and manage, and also ensure higher reliability. This article describes an approach to designing a security system and interaction protocols for protection of mobile and sensor networks by means of using cryptographic algorithms. In this work, a model of a distributed protocol for authentication in the wireless sensor networks is offered to enable devices to carry out the authentication procedure without using a conventional centralized authentication server

1. Introduction

In recent years, mobile computing systems have considerably changed the world. People can connect to the Internet and get access to data and information from virtually anywhere. Mobile devices, often called gadgets, such as smart-phones and tablets, can constitute distributed heterogeneous mobile networks that provide users with access to information in the on-line mode[3]. Mobile computing networks and sensor networks moved the world from the era of wireline networks and desktop computers to the era of widespread and global computerization[1] .Modern research works on computer network systems pay extra attention to ensuring computer security. Two lines are usually used to protect the network infrastructure. The first one is the IPS (intrusion prevention systems)[1][2]. Typical measures of intrusion prevention are, for example, authentication and ciphering, they can prevent the protected network from being affected by outside nodes. The second protection line is the intrusion detection systems (IDS) that can detect insider attacks performed using compromised nodes in the network[6]. If a network intrusion is detected, the countermeasures minimize the aftereffects of the attack. The intrusion prevention includes, as a rule, authentication and ciphering. Considering the distributed structure of sensor and mobile networks, many traditionally adopted methods of authentication and ciphering are either no longer effective or can't be used at all any longer. It is difficult to apply network intrusion detection methods of conventional wireline networks in mobile networks due to their architectural differences. Without centralized audit points, such as routers, commutators and gateways, mobile networks can collect audit data only locally, thus requiring a distributed and cooperative intrusion detection system[3]. Besides, devices used in the mobile networks and detectors in the sensor networks are quite tiny, therefore their computing capacity as well as power consumption are limited. Consequently, developing security protocols for mobile devices, it is necessary to design simple and power-efficient information security protocols.

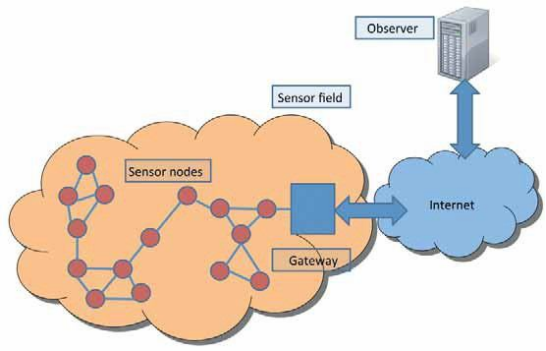
Secure data exchange between devices in the mobile and sensor networks opens a new area of research. Establishing trusted relations for secure data exchange between mobile devices requires information authentication and ciphering procedure for ensuring a controlled access[4].

Development of a distributed network interaction protocol for secure authentication, authorization and accounting by means of applying cryptographic algorithms is very relevant today. The purpose of the protocols is to reduce the network traffic and resource consumption for the network nodes. The existing protocols require, as a rule, reliable and centralized services and are very difficult to implement in the distributed network environment.

2. Characteristic features of wireless sensor network (WSN)

A WSN can generally be described as a network of nodes that cooperatively sense and control the environment, enabling interaction between persons or computers and the surrounding environment [1][2] [3] . WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or near the monitoring area (sensor field), form networks through self-organization. Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multihop routing, and finally reach the management node through the internet or satellite.

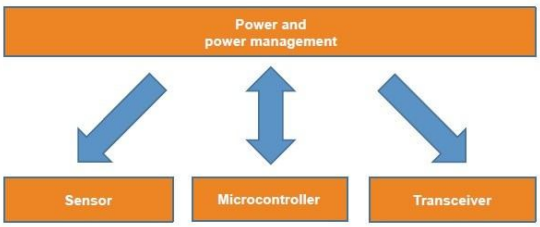
Figure 1: wireless sensor networks



3. Sensor Nodes

The sensor node is one of the main parts of a WSN. The hardware of a sensor node generally includes four parts: the power and power management module, a sensor, a microcontroller, and a wireless transceiver, see Figure(2). The power module offers the reliable power needed for the system. The sensor is the bond of a WSN node which can obtain the environmental and equipment status. A sensor is in charge of collecting and transforming the signals, such as light, vibration and chemical signals, into electrical signals and then transferring them to the microcontroller[1]. The microcontroller receives the data from the sensor and processes the data accordingly. The Wireless Transceiver (RF module) then transfers the data, so that the physical realization of communication can be achieved. It is important that the design of the all parts of a WSN node consider the WSN node features of tiny size and limited power.

Figure 2:



4. Modeling a System of the Distributed Authentication System in the Wireless Sensor Networks

As compared to wireline networks, wireless networks are difficult to make secure because of the nature of the node interaction. In the sensor and wireless networks, an intruder has much less problem bypassing the main intrusion detection system by connecting to the network and making attacks. If the intruder is identified and blocked out, he can disconnect from the network, change his identification data and then connect to the same network again at a different point[4].

Wireless sensor networks are extremely relevant to the modern world, for example, for military purposes, monitoring and alarm systems, etc. Security of the sensor networks in such applications is a priority. However, the limitations of memory capacity, battery capacity, communicative and computing capabilities in each device like that make the task of ensuring security extremely complex. Moreover, sensor networks often consist of a big number of small devices deployed in an uncontrollable external environment, which makes them vulnerable to a physical capture and compromising, which, in its turn, makes it more difficult to preserve the integrity of the device authentic software. Just one compromised device is enough to make the whole network insecure.

In order to protect a device from physical attacks, including software physical tampering and manipulations, it is offered to apply a program integrity check pattern in each device, called a program integrity check (PIC)[8].

Authentication between node-devices and network servers is another important issue. A node-device has to make sure that the messages sent are authentic and also prevent a data exchange with a malicious and fraudulent server.

To implement the PIC protocol, devices use the PIC-servers for checking the program integrity. Let's examine a distributed protocol of the PIC-authentication for secure data exchange between the devices without centralized infrastructure of the authentication servers. The PIC-authentication protocol's task is fully distributed authentication of the servers before a device addresses them. In this case, we consider the authentication as a pattern, according to which one device verifies the validity of another device before the communication starts. And consequently, the devices working under the PIC-authentication Protocol verify the validity of the PIC-servers[8].

It is also offered to use a pattern of the PIC-server status revocation when it is detected that the program integrity has been violated by the neighbouring PIC-servers. The PIC-authentication Protocol protects from both passive attacks (wire-tapping) and active attacks (replay, spoofing, data diddling). It also protects from masquerade attacks using ciphering based on pairwise keys between the interacting devices. Besides, the PIC-authentication is resistant to work of several compromised PIC-nodes based on the majority rule upon checking program integrity.

5. The PIC-Authentication Protocol has the Following Characteristics

1. Distributed authentication accreditation: the protocol enables neighboring PIC-devices to carry out the distributed PIC-authentication and warrant the authentication results, when there are no hacked PIC-devices.

2. Resistance to compromise of nodes: even if some PIC-nodes have been hacked, the probability that PIC-authentication protocol ensures a valid result of the authentication validation is very high.
3. Low computation overhead: the major computation load for the PIC-authentication Protocol mainly consists of computing pairwise keys and generating/ verifying MAC-addresses, which is a low-consuming procedure.
4. Low communication overhead: communication power consumption for the PIC-nodes is also extremely low – only two messages have to be exchanged to validate the authentication between the neighbouring PIC-nodes.
5. Low storage overhead: each sensor or PIC-node stores a specified type of polynomial for generating pair-wise keys with other nodes in the network, which occupies very little memory capacity[7].

6. PIC-Authentication Protocol

The PIC protocol checks the integrity of the program and data stored on the mobile device or sensor. The verification procedure itself occurs quite rarely, for instance, when the device has been off network for a long time or is trying to connect to the network at a minimum computing capacity used.

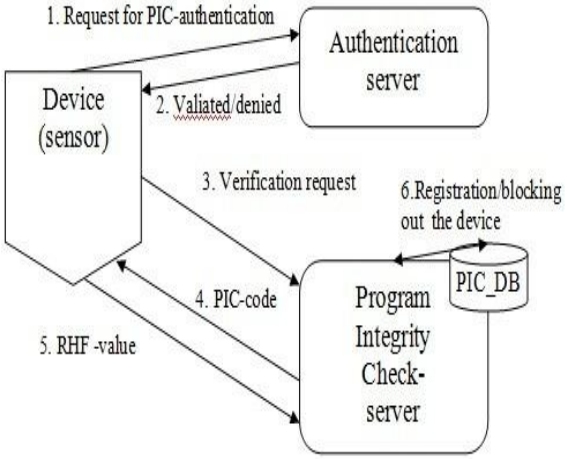
A mobile network consists of devices (sensors) and PIC-servers. The PIC-servers check the device program integrity and maintain the PIC-server original program image data base[10]. The randomized hash functions (RHF) are used for this purpose. While verifying devices, the PIC-server creates a new RHF and sends it to the device in PIC-code. Further, the PIC-server can check the validity of the mobile device software, receiving back the value of the PIC-code processed by the device.

Device security is also ensured by PIC-server authentication validation before communicating to them in order to protect the device from malicious and fraudulent PIC-servers. The devices validate the PIC-server authentication by communicating to a regular authentication server. The PIC Protocol fulfills three goals: (1) a centralized authentication validation of each PIC-server; 2) transmission and implementation of the PIC-code and (3) software check.

Any device that wants to get connected to the network first requests to validate the PIC-server authentication. In case of successful authentication, the device will request this PIC-server to validate the authentication of its own program. To validate the device program, the PIC-server sends the device a PIC-code with a new RHF, and then uses the same method to compute the hash-value of the device program image which is stored in the data base.

After the device receives the PIC-code from the PIC-server, it computes the hash-function value, which is further sent back to the PIC-server for a check. If the PIC-codes match upon the validation done by the PIC-server, the PIC-server registers the device in its PIC_DB data base, which contains all the validated identifiers of the devices. Otherwise, the device will be locked and its identifier is removed from the PIC_DB. The PIC protocol offers three ways to lock out a suspicious device: (1) the PIC-server informs the neighbouring devices not to respond to the service packs from suspicious devices; (2) the key manager generates a new cluster key excluding suspicious devices from it, and (3) with active network services, such as routing, the PIC_DB can be validated to determine valid devices. Figure 1 shows interaction between the centralized authentication server, PIC-servers and the device during the PIC-authentication.

Figure 3: Model of interaction in the PIC Protocol architecture



The main purpose of the PIC protocol is the countermeasure against the majority of physical attacks, i.e. it will extremely difficult for the intruder to reprogram the device or manipulate it (without adding new sensors), to say nothing of changing the sensor program without being detected. This protocol largely warrants the device program integrity as the device requests to check the integrity of its program before connecting to the network and after a long period of disconnection.

Sensor and mobile networks are often used for monitoring and collecting data for statistic processing. The majority of sensor networks have a basic station which acts as a gateway to an external network and it is usually a high-capacity computation node

The sensor networks can, as a rule, consist of hundreds or a couple of thousands node-sensors, nevertheless, their computation and communication structure is limited, there are also certain limits on the memory used or power consumed. As a consequence, such public key algorithms as Diffie-Hellman are not usually used in the sensor networks[9]. The algorithm of ciphering with the public key often requires considerable memory capacity, complex computations and processing and a long key, which leads to rapid battery exhaustion.

The main goal was to exclude the centralized authentication server in the PIC-infrastructure, to make the PIC a fully distributed protocol. Since the centralized authentication is required for the devices to verify the PIC-servers, it can easily become a bottle-neck for reliability, security and connection. This requirement is also incompatible with the nature of the distributed structure of sensor networks. What is more, the devices deployed near the centralized authentication node will consume more power for message routing to other sensors, which will lead to faster battery charge exhaustion in such devices. Thus, the centralized authentication server does not really fit large sensor networks.

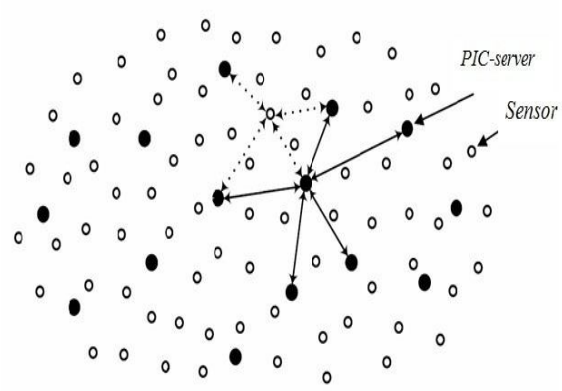
7. Conclusion

Model of secure sensor PIC-network: the structure of the secure sensor PIC-network is defined by the following

1. Sensors and PIC-servers a located randomly within the signal coverage, thus, we do not have any preliminary knowledge of the neighbors and location of each sensor before deployment.
2. The network includes maximum n sensors and s PIC-servers, each of them has the unique node identifier (NI).
3. The PIC-server has a higher capacity than a sensor
4. The PIC-server stores the programs of all the sensors in its memory before deployment and uses these programs for the verification of the sensors.
5. Each PIC-server has two radio-interfaces for communicating with the sensors and other servers, and the frequencies of these interfaces do not cross. Note that employment of several radio-channels for each node is a common thing.

6. For the majority of the network sensor systems, the sensors have to be time-synchronized. Consequently, PIC-servers are considered to be poorly time-synchronized.
7. Since the PIC-servers have a bigger transmission range than the sensors, each PIC-server has at least t neighbouring PIC-servers after deployment.

Figure 4: Plan of the network with the PIC-authentication



The PIC-servers interact with each other for mutual authentication. The full lines show the interaction between PIC-servers, the dotted lines show interaction between the sensors and PIC-servers.

Reference

[1] ASHTON, K. That 'Internet of Things' Thing. In the real world, things matter more than ideas. RFID Journal, 22 June 2009. Available from: http://www.rfi djournal.com/articles/view?4986
[2] BRORING, A. et al. New generation sensor web enablement. Sensors, 11, 2011
[3] Internet of Things: Wireless Sensor Networks White Paper IEC
[4] Yole Development SA. MEMS technology: World's smallest barometric pressure sensor. Micro News, 2009,78:1.
[5] 1. Jennifer Jabbusch ,"IDS vs. IPS: How to know when you need the technology", - 22 November 2010
[6] IDS AND IPS PLACEMENT FOR NETWORK PROTECTION By Robert Drum, CISSP 26 March 2006
[7] The Use of Software-Based Integrity Checks in Software Tamper ,Resistance Techniques, Ginger Myles IBM Almaden Research Center https://nsl.cs.usc.edu/Projects/PIC
[8] http://www.internet-computer-security.com/Firewall/IPS.html
[9] J. Yick, G. Pasternack, B. Mukherjee, D. Ghosal, Placement of network services in sensor networks, Self-Organization Routing and Information, Integration in Wireless Sensor Networks (Special Issue) in International Journal of Wireless and Mobile Computing (2006)
[10] K. Sohrabi, J. Gao, V. Ailawadhi, G.J. Pottie, Protocols for self-organization of a wireless sensor network, IEEE Personal Communications, October 2000