Requirements to Mobile Telemetry Application Protocol

Elitsa Gospodinova[1], Ivaylo Atanasov[1], Evelina Pencheva[1]

Abstract – **In this paper an analysis on functional requirements to application protocol for mobile telemetry is presented. The protocol is used for communication between mobile agents and a central control unit. It relies on Internet protocol connectivity and is access network independent. Along with the domain specific functionality, security issues are discussed such as authentication, ciphering and integrity check at application level.**

Keywords – **Mobile agents, Internet protocol connectivity, Reliable transport, Authentication, Ciphering, Integrity check.**

I. Introduction

The mobile telemetry uses mobile data for remote information measurement and reporting. Special mobile agents containing modules for data transfer and positioning combined with sensors can be used to implement a wide variety of outdoor and indoor applications. Some example applications of mobile telemetry include traffic monitoring, resource distribution, medicine, home security, energy monitoring etc. Care needs to be taken when assessing requirements to monitoring data and data costs. Furthermore, possible external attacks have to be taken into account, especially when mobile agents use internet for data transmission.

Security aspects of mobile telemetry are subject of intensive research. The proposed security mechanisms include authorization through digital certificates in virtual private networks [1], security policy assigning new identification numbers [2], location privacy and pseudo-direct communication, which can be incorporated into the distributed authentication protocol [3], authentication and privacy by using public keys to certify the identity of parties [4] and other. Different aspects of telemetry functions and their implementation in mobile agents are discussed in [5], [6] and [7].

The proposed solutions are applicable to mobile hosts like personal computers having relatively high computational power and onboard energy supply. Smart solutions require reduction of energy budget and autonomous operation with battery powered.

In this paper, we study the requirements to application layer protocol that can be used for mobile telemetry. The protocol is based on Internet protocol (IP) connectivity that may be obtained by means of any cellular or wireless network. The protocol has to be access-independent so that the data transfers may take place over Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Wideband Code Division Multiple Access (WCDMA), Enhanced Data Rates for Global Evolution (EDGE), Wireless Local Area Networks (WLAN), WiMAX and cdma2000 networks. The application layer protocol follows the pattern of requests going from client to server, and responses sent back from server to client.

The paper is structured as follows. In Section II, services that have to be provided by mobile telemetry application protocol are investigated. The security issues at application level are discussed in Section III. Section IV describes a mathematical model for evaluation of protocol efficiency. Before concluding the paper some remarks on future work ate outlined.

II. Common Protocol Requirements

The main requirements to application layer mobile telemetry protocol include access independency which calls for IP connectivity, operation with low energy consumption, and secure data transfer.

A mobile telemetry system consists of a central control unit that handles information gathering from multiple mobile sources and a set of mobile agents capable of domain data monitoring and measurement reporting.

The control unit plays an important role in registration of mobile agents. It is responsible for configuration of the operation modes of mobile agents regarding measurements and reports transmission. The control unit has to store all mobile agent and operation-related data of the telemetry system. The main data stored in the control unit include identities of the mobile agents, registration information and parameters related to the monitoring and reporting modes. It also stores a secret key for each mobile agent used to generate dynamic security data for each mobile agent. In addition to functions related to security, the control unit needs to store the measurement database or to provide interfaces to a measurement data repository if standalone solution is chosen.

The mobile agent is an embedded device equipped with sensor(s), positioning module, data transmission module and power supply module. The main requirement to mobile agent is to operate using as low energy as possible which calls for usage of energy efficient transmission methods [8].

Being an application layer protocol, the mobile telemetry protocol makes use of transport-layer protocols such as User Datagram Protocol (UDP) or Transmission Communication Protocol (TCP) in order to send and receive messages. UDP as a transport does not offer a reliable message-delivery service. Therefore, the mobile telemetry protocol, when forwarding a message to the UDP layer for transmission, has to expect that the message may not reach the destination. In order to cope with this limitation when using UDP, the mobile telemetry protocol must implement, as part of itself logic that guarantees the reliable delivery of messages. This logic basically utilizes retransmissions of messages upon expiry of timers in order to

[1]The authors are with the Faculty of Telecommunications, Technical University of Sofia, Kliment Ohridski 8, 1000 Sofia, Bulgaria, E-mails: ed_gospodinova@tu-sofia.bg; iia@tu-sofia.bg; enp@tu-sofia.bg

increase the probability of successful message delivery. The mechanism that may be used in order to implement this reliability at application layer is like the transaction concept defined for Session Initiation Protocol (SIP).

SIP possesses all required functionality for registration and management of sessions but it is not as suitable as one for mobile telemetry proposes. The main reasons are: the SIP session is a complex process, including many messages exchange; SIP messages are text-based which means considerable number of bytes; implementation of SIP compression in the mobile is undesirable because of the limited power budget. In order to decrease communication overhead, the mobile telemetry protocol must be binary.

Registration is performed after the mobile agent is switched on. The aim is to bind the IP address that is currently used by the mobile agent and mobile agent identity. Prior to registration which allows the mobile agent to operate in the telemetry system e.g. to perform measurements and send reports, the mobile agent must obtain IP connectivity. The registration contains two phases: first, the control unit challenges the mobile agent and then the mobile agent responds to the challenge and completes the registration as shown in Fig.1. In case of successful authentication, a new temporary identity is assigned to the mobile agent to avoid exposure of the unique mobile identity during transmission.

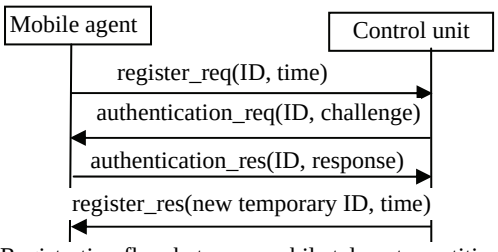

Fig.1 Registration flow between mobile telemetry entities

If the registration fails, for example, due to unsuccessful authorization, the control unit rejects the mobile agent's registration. It is the mobile agent's responsibility to keep its registration active by refreshing it periodically. If the mobile agent does not refresh its registration, then the control unit will silently remove the registration when the registration timer expires. The time for active registration may depend on the application domain. If the mobile agent is switched off, it performs de-registration setting the registration timer to zero. Sometimes the control unit needs to deregister the user, e.g. for administrative reasons. In this case, the control unit sends notification request to the mobile agent indicating that mobile agent has been deregistered as shown in Fig.2. If the mobile agent is unable to recognize the notification request it reports an error condition. Authentication procedure is directly coupled to registration and configuration of operation modes.

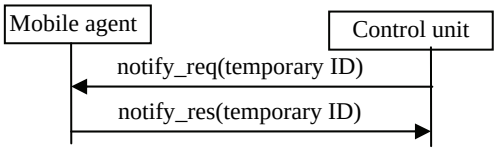

Fig.2 Control unit initiated de-registration of a mobile agent

The mobile agent may be configured to operate in different operation modes. Periodic monitoring and reporting require the mobile agent to make measurements and send reports at given rates. The measurement periods for the domain-related sensor function, the periods of gathering positioning data, and the periods for sending reports via the communication network may differ. This requires the mobile agent to possess functions for local data storage and processing. The frequency of reports is application dependent. The control unit requests for periodic reports after successful authentication as shown in Fig.3. The parameters of the request to start periodic reporting include the following: current time, needed for synchronization with the mobile agent, mobile agent temporary ID, dialogue ID, period of report transmissions, period of domain measurements, period of location measurements, accuracy of domain measurements, and accuracy of location measurements.

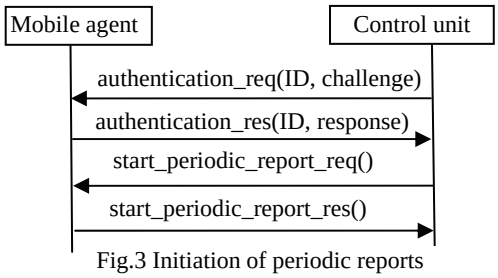

Fig.3 Initiation of periodic reports

In case of intensive reporting e.g. every minute, no mobile agent authentication may be required with each report but the first. The signaling flow for periodic reports is shown in Fig.4.

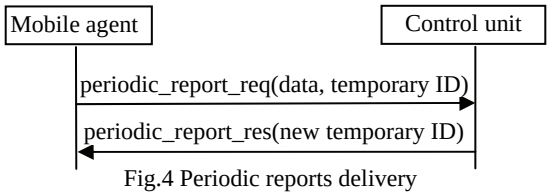

Fig.4 Periodic reports delivery

At any time the control unit may request for modification of the periodic reports. Any modifications of the reporting should take place after successful authorization. It is the responsibility of the control unit to stop the periodic reports which is also bound by authentication as shown in Fig.5.

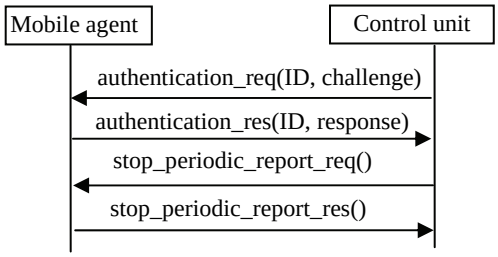

Fig.5 End of periodic reporting

Triggered reporting operation mode requires monitoring for certain criteria and submitting reports on their occurrence. The control unit starts the triggered reports by setting the reporting criteria. The parameters of the start trigger reporting request include current time, new temporary ID of the mobile agent, dialogue ID, trigger type (location or data values), location data (longitude, latitude, radius), threshold values of the measured data. The control unit may modify the trigger criteria after successful authentication as shown in Fig.6.

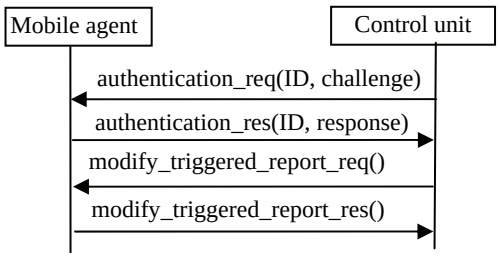

Fig.6 Modification of trigger criteria

When the criteria for triggered reporting are met, the mobile agent sends reports as shown in Fig.7.

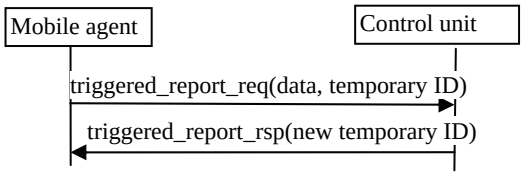

Fig.7 Triggered reporting

The termination of the triggered reporting is initiated by the control unit and it is also bound by authentication.

The third mode of operation is reports upon request. The control unit induced reporting requires mobile agent to perform measurements and to send reports on demand as to Fig.8. The mobile agent response in Fig.8 just acknowledges that the request is accepted. Fig.9 shows the signaling flow for reporting the measurement data upon requests.

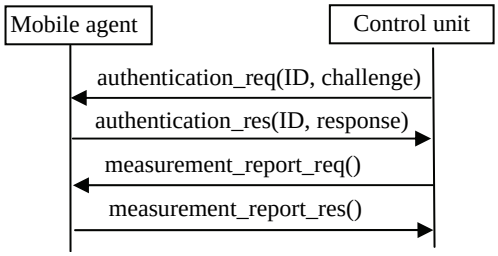

Fig.8 Measurement on demand

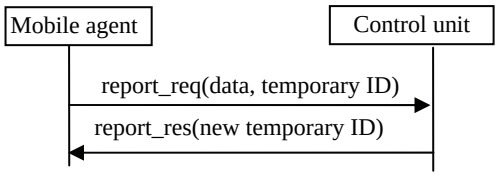

Fig.9 Delivering report on request

Any errors concerning problems in configuration or modifications of the operation modes are reported. In case of error, the mobile agent indicates the error type. The possible error types include: unsuccessful request for start/ modification/stop of periodic reports, unsuccessful request for start/modification/stop of triggered reports, unsuccessful request for report on demand. Receiving report the control unit also may response by indicating an error. Possible reasons for request rejection may be format error, invalid identification, invalid parameter values etc. Fig.10 shows an error case when the mobile agent responses to a start request for periodic reports caused by wrong message code. Fig.11 shows the signaling flow when the control unit indicates that the triggered report fails.

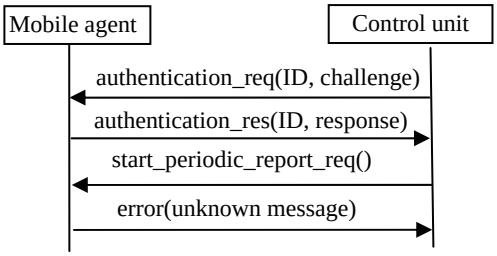

Fig.10 Rejection of request to start periodic reports

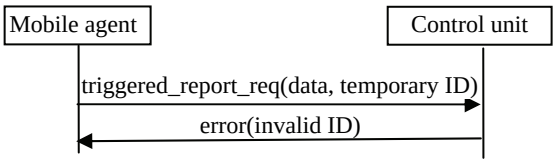

Fig.11 Rejection of triggered report

III. Requirements to Security

The access security is responsibility of the network that provides IP connectivity. In addition to access security, the security mechanisms at upper layers are mandatory.

The basic tool used for protection of IP network traffic is the IP Security (IPSec) protocol suite. It provides confidentiality and integrity of communication in the IP layer. Communicating parties can also authenticate each other using IPsec [9]. The critical issue is key management: how to generate, exchange and distribute the various keys needed in algorithms that are used to provide confidentiality and integrity protection. This security mechanism is unsuitable for low class embedded mobile devices.

At application layer, the security mechanisms for mobile telemetry need to include the following:

- mutual authentication;
- integrity check;
- temporary identifications;
- optional ciphering.

The authentication is required on registration, configuration and modification of operation modes. The aim of authentication is twofold: the control unit needs to authenticate the mobile agent and the mobile agent needs to verify if the control unit is authorized to request authentication. The authentication procedure relies on shared secret stored in the mobile agent and in the control unit. Each time an authentication is required the control unit computes an authentication token and sends it in the authentication request together with the challenge. The mobile agent uses the authentication token to check the authority of the request. If the authentication token does not coincide with the mobile agent's expectation the authentication request is rejected. If the control unit is authorized to request authentication the mobile agent computes its response using the challenge and the shared secret.

The integrity check has to be mandatory for all requests and responses. Messages are checked to ensure they have been received intact.

The ciphering is optional. The control unit may decide to activate the ciphering mode as shown in Fig.12. The control unit also decides when to stop ciphering.

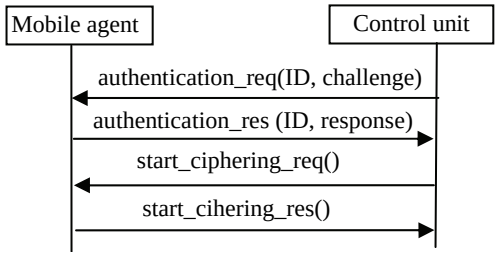

Fig.12 Activation of ciphering mode

The mobile agent has a unique identity (ID). This identity is used for authentication and registration. Temporary identity is used to protect the unique ID from disclosure. New temporary ID is assigned on registration, configuration or modification of operation modes.

IV. Protocol Mathematical Model

To evaluate efficiency of the mobile telemetry protocol, the metric used is message arrival delay. The mathematical model is characterized by the following assumptions. The message loss rate is α. The number of maximum message transmissions is N. The initial timeout before the first re-transmission is T. We assume that the timeout between re-transmissions increases exponentially.

The probability of message arrival exact after i-th retransmission is:

$$P_i = \alpha^{i-1}(1-\alpha) \quad (1)$$

Then the probability of message arrival within N retransmissions is:

$$P_N = \sum_{i=1}^{N} \alpha^{i-1}(1-\alpha) \quad (2)$$

The overall message loss probability is:

$$Q_N = 1 - P_N \quad (3)$$

In exponential back off case, the expected protocol delay for message arrival at the corresponding entity (mobile agent or control unit) is expressed by:

$$W = (1-\alpha).T.\sum_{i=1}^{N}(\alpha^{i-1}(2^{i-1}-1)). \quad (4)$$

Having $\alpha = 10^{-3}$, $N = 4$ and $T = 500$ *ms*, the expected message arrival delay is $W = 0.501$ *ms*.

V. Conclusion

In this paper we study the requirements to application level mobile telemetry protocol. We argue that the protocol needs to be based on IP connectivity to provide access independency and define the basic protocol functions. In order to be transport independent, the main protocol requirement is to provide a mechanism for reliable message delivery. The requirements to security functions include mutual authentication, integrity check to protect against any manipulation, and confidentiality. Our future work will be focused on different schemes for message re-transmission in order to decrease the protocol latency considering message processing time. At the protocol design phase, we will evaluate the protocol overhead.

Acknowledgement

The work is funded by the project grant 112pd004-7/2011 at Research and Development Sector, TU-Sofia, Bulgaria.

References

[1] M. Huerta, T. Viva, R. Clotet, R. Gonzalez, R. Alvizu, A. Perez, D. Rizas, F. Lara, and R. Esclante, "Implementation of a Open Source Security Software Platform in a Telemedicine Network Advances in E-Activities", *Information Security and Privacy*, pp. 72-76, 2009.

[2] V. Sanjeevi, Veluchandhar, S. Sakthivel, and M. Supriya, "Security Policy for Deducting Unauthorized IP Based Mobile Host Inside the Network", *7th WSEAS Int. Conf. on Electronics*, Hardware, Wireless and Optical Communications, Cambridge, UK, pp. 177-181, 2008.

[3] A. Georgiades, Y. Luo, A. Lasebay, and R. Comley, "Location Privacy in Mobile IPv6 Distributed Authentication Protocol Using Mobile Home Agents", *8th WSEAS Int. Conf. on Electronics*, Hardware, Wireless and Optical Communications, Cambridge, UK, pp.243-248, 2009.

[4] M. Worris, "Single-chip ZigBee for Indoor Mobile Telemetry", *IEE Seminar on Telemetry and Telematics 2005*, (Refl No 2005/11009), pp.10/1-10/4, 2005.

[5] S. Carrellas, "Mobile Telemetry as a Data Gathering Tool for the Advanced Mobile Phone Service Field Trial", *32nd IEEE Vehicular Technology Conference*, pp. 327-330, 2006.

[6] G. Horler, S. Hindle, and D. McGorman, "Including Coupled Telemetry and Actuation", *IEE Seminar on Telemetry and Telematics 2005*, (Refl No 2005/11009), pp.5/1-5/6, 2005.

[7] H. Nassar, H. Al-Mahdi, M. El-Gabali, and S. Aziz, "Design and Analysis of a One-Step Addressing Protocol for a Ad Hoc Networks", *7th WSEAS Int. Conf. on Electronics*, Hardware, Wireless and Optical Communications, Cambridge, UK, pp. 140-145, 2008.

[8] H. Gochev, V. Poulkov, and G. Iliev, "Uplink Power Control for LTE Improving Cell Edge Throughput", *Int. Conference on Telecommunications and Signal Processing, TSP 2010*, Baden near Vienna, Austria, pp. 465-467, 2010.

[9] C. Wu, S. Wu, and R. Narayan, "IPsec/PHIL (packet header information list): Design, Implementation and Evaluation", *10th International Conference on Computer Communications and Networks*, Scottsdale, AZ, USA, pp. 206-211, 2001.