SECURITY ISSUES IN WIRELESS SENSOR NETWORKS FOR ENVIRONMENTAL MONITORING

VIDES PĀRRAUDZĪBAS PAREDZĒTO BEZVADU SENSORU TIKLU DROŠĪBAS PROBLĒMAS

D.Bliznyk

Wireless networks, security, SunSPOT, environment monitoring, performance evaluation

The use of wireless sensor networks for environmental monitoring demands that their functioning is fully secured. This paper discloses aspects for securing sensor networks within five use cases of European Union Seventh Framework Programme project - "ProSense". Security threats are examined from four aspects: privacy, authentication, confidentiality and continuity. Every use case is examined on specific security issues and for each use case own ways of overcoming possible problems are proposed. The paper describes practical realization of secure data communication on the SunSPOT hardware platform using lightweight elliptic curve cryptography (ECC) ciphers suite. Finally results of practical testing and influence of secure data communication usage on low-processing sensor nodes are represented. Tests examine wireless sensors' communication delay at initialization phase and during usual message sending in secured and plain transmission modes. Also energy consumptions are compared in secured data transmission mode and plain data communication mode.

Introduction

Developers of the wireless sensors networks for environmental monitoring are confronted with a lot of tasks to solve: choosing hardware, communication protocols, high level application programming and others. And after completing all of mentioned steps there is still a work to do for making the network be applicable in real life. Despite the fact that network is working perfectly in ideal laboratory conditions it might be not ready for harsh real life, that is full with natural and even intentional threats. Therefore wireless sensor networks should be resistant to external influences, especially when this networks are used for environmental monitoring, that is gained data might be important or vital. Some of the applications might involve private data sending over the network. In this case it is important that this data cannot be seen by unauthorized persons. As appears from the above, wireless sensor network should be secured and security issues must be taken into consideration at the beginning of network development.

This papers points out primary security issues for wireless sensor networks intended for environmental monitoring. Since the research was carried out in the limits of EU "Seventh Framework Programme" (FP7) project named "ProSense" [2], the paper indicates specific security issues for every use case of this project and possible ways of overcoming them.

Significant part of securing wireless network is secure data communications establishment. That will allow overcoming most of security problems. Since the hardware platform is predefined, the task was to determine the scope of available "SunSPOT" [3] hardware platform and realizing secure data communication according to security requirements. The chapter *Current sunSPOT security situation* contains survey of secure data communications on SunSPOT nodes and possibilities of the secure data communication protocol – SSL (Secure Sockets Layer) [4] implementation. Since secure data communication protocols will increase communication data overhead and CPU load it is essential to obtain numerical results of the influence on environmental monitoring sensor network's performance. The chapter *Performance tests* contains the results of these tests and drawn.

Security issues

As it was already mentioned there are many security threats in wireless sensor networks intended for environmental monitoring. In this paper security issues are divided in four following groups [1]:

- Privacy. Ability to hide personal information (identity).
- Authentication. Ability to prove personal identity.

- Confidentiality (encryption). Ability to protect information from unauthorized access and change.
- Continuity. Ability to maintain permanent availability of service.

For better understanding how to deal with security threats it is important to find out at what OSI layers threats are acting.

Since security aspects are defined, it is possible to determine which of them are most important for each of five use cases and propose defense strategies.

Fire detection

Goal - protection in a case of natural or human-made disasters (specifically forest fires) using attached smoke and temperature sensors on sunSPOT nodes in a forest.

Continuity. Since the goal of service in this use case is to report if dangerous situation (fire) arises, therefore temperature and smoke detection nodes must be robust to attacks tended to disable node ability to operate or communicate.

Proposal:

- Use of node reservation - increase number of nodes per unit of area.
- Use of protection from physical attacks – making nodes hardly visible, safe node's shell.
- Tuning communication algorithms (lower OSI layer) to be immune to popular denial of service attacks.

Authentication. System must be protected from fake alarms, therefore all nodes must be able to prove their genuine.

Proposal - use of authentication by digital signatures (asymmetric data encryption) and signing every data containing alarm message.

Possible attack types: physical access, jamming [6], Link Layer attack [5].

Smart building

Goal - automated recognition of people's location in buildings for providing advances services.

Synopsis: Every employee has a badge holder ID with an active tag. When Person X comes at work, the system notices his presence, the RFID tag communicates with the RFID reader and the information about the persons ID and location is stored in the server. Depending on the time interval, different information is presented on the monitor.

Privacy & Encryption. System must be able to hide personal information (location) at any moment of time.

Proposal:

- All data transmissions must be encrypted.
- All nodes should periodically transmit data. To increase complexity of determining user's first identification moment.
- Messages must always be the same size (no adding zeros at the end!), to make impossible to distinguish message containing location or presence information from any other usual request message.

Authentication ("Protected room scenario"). Ability to prove identity with digital signature.

Proposal - use of digital signatures for RFID devices.

Possible attack types: physical access, tampering.

RFID item reminder

Goal - item Reminder allows users to detect missing items and to ensure that they have everything they need when leaving a location.

Privacy & Encryption. Ability to hide information about forgotten items and relation between item and owner.

Proposal - use of encryption.

Possible attack types: physical access, tampering.

Railroad

Goal - monitoring the containers condition and providing effective and in time prevention activities. Measuring environmental parameters (temperature, humidity…), high-level sounds, vibrations and tilt changes.

Continuity. Similar to fire detection use case, all nodes must provide permanent and failsafe operation, therefore nodes must be robust to attacks tended to disable node ability to operate or to communicate.

Proposal:

- Use of node reservation - increase number of nodes per unit of area.

- Use of protection from physical attacks – making nodes hardly visible, safe node's shell.
- Tuning communication algorithms to be immune to popular denial of service attacks.

Authentication. System must be protected from fake alarms, therefore all nodes must be able to prove their genuine.

Proposal - use of digital signatures (asymmetric data encryption) and signing every data containing alarm message.

Possible attack types: physical access.

Smart road monitoring

Goal - improving traffic safety by efficient use of road regulations. Real time road regulations monitoring and violations reporting using inside vehicle placed sensors and roadside nodes. Driver notification of possible rule changes. Creating infrastructure for future use. Gathering statistical data for traffic analysis.

No need for special security measures, due to absence of private and crucial data. Only informational types of messages are sent. To increase trustworthiness of statistical information, when obtaining traffic data, vehicle unique identifiers could be used. This safety measure could avoid flooding with false statistical messages. In case of special functions usage for service personal, authentication and data encryption should be used. Possible attack types: physical access.

Summary

To prevent private information leakage it is advised to encrypt all data transmissions. All nodes should periodically transmit data. To increase complexity of determining user's first identification moment. Messages must always be the same size (no adding zeros at the end!), to make impossible to distinguish location or presence information from any other service request. To prevent message replaying, when attacker captures packet and retransmits it, nodes should include counter in every message, therefore message with same number will be discarded and would not affect reliability of data.

For encryption and authentication only "lightweight" algorithm types should be chosen, due to limited processing power and throughput.

To provide continuity of service it is advised to use of node reservation - increasing number of nodes per unit of area. Use of protection from physical attacks – making nodes hardly visible, safe node's shell. Not only attacker can cause damage to nodes, but they can be affected by environment itself. Sensors and circuit boards should be well protected from moisture. If it is possible nodes should be enclosed in ready made shells with certified dust and liquids protection ratings (>IP65 or >NEMA 4x) [7,8]. To prolong wireless nodes operation time on batteries all diagnostic light emitters (e.g. LED) should be turned off, because their energy consumption is relatively high comparing to node's low power mode. Since nodes usually are placed at hardly accessible places, they should collect diagnostic data, to let diagnose problem distantly.

Sensor position should be chosen wisely to obtain correct data. E.g. temperature sensor should be protected from direct sun rays, environmental temperature should be measured only in shade.

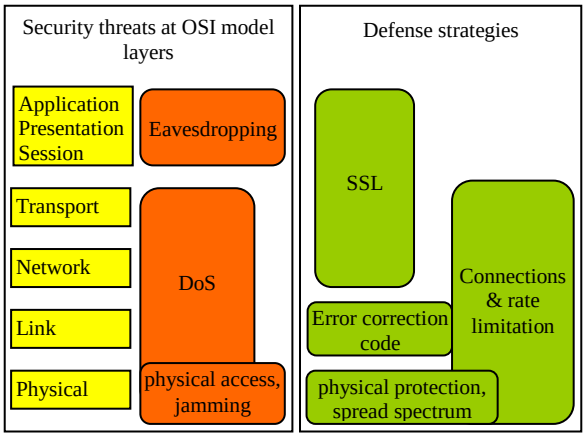

Fig.1 Security threat from OSI model aspect

Symmetric key deployment taking into account received signal strength indication (RSSI), e.g. only nodes that are placed physically close, are able to obtain the key.

Figure 1 summarizes security threats from Open Systems Interconnection (OSI) model aspect.

Current sunSPOT security situation

The SunSPOT SDK already supports code authentication using digital signatures. SSL support for encrypted communication between several SunSPOT nodes or SunSPOTs and

Internet server is available as a technology preview, but is not officially included in the SunSPOT SDK.

SSL library for the Sun SPOT is based on the SSL implementation in Sun's reference implementation of Java ME MIDP (the Java ME profile used for cell phones) but includes several enhancements:

- support for TLS 1.0,
- support for server-side SSL/TLS,
- support for Elliptic Curve Cryptography cipher suites (for now, only ECDH-ECDSA-RC4-SHA and secp160r1 are supported).

SPOT applications built using this library have access to new GCFconnection type "sradiostream" (this is to radiostream what HTTPS is to HTTP) for secure stream oriented communication between two SPOTs. This uses ECC ciphers only because running the server side on a SPOT using RSA would be much slower.

In typical end-user/browser usage, TLS authentication is unilateral: only the server is authenticated (the client knows the server's identity), but not vice versa (the client remains unauthenticated or anonymous).

TLS also supports the more secure bilateral connection mode (typically used in enterprise applications), in which both ends of the "conversation" can be assured with whom they are communicating (provided they diligently scrutinize the identity information in the other party's certificate). This is known as mutual authentication. Mutual authentication requires that the TLS client-side also hold a certificate (which is not usually the case in the end-user/browser scenario).

TLS communication establishes in following steps:

- check communication partner's supported algorithms,
- choose most secured algorithm,
- exchange keys,
- authentication,
- use of symmetric message encryption and authentication.

ECC - cryptographic schemes based relying on scalar multiplication of elliptic curve points. For elliptic curves, the problem assumed to be intractable is finding the discrete logarithm of an element. [9] Key in elliptic curve cryptography can be shorter, but still offering same security as RSA. For example, a 160-bit ECC key provides the same level of security as a 1024-bit RSA key, and a 224-bit ECC key provides the same security as a 2048-bit RSA key. Smaller keys mean faster computation, lower power consumption, and memory and bandwidth savings. [10]

Performance tests

After the task of implementing SSL protocol in given SunSPOT nodes is completed and transferred data is secured, performance influence should be measured. Since secure communication requires extra memory, processing power and communication overhead, there is a need to check the level of an impact on network and node's performance characteristics. Knowing requirements of the use cases there is no need in obtaining precise tests values, main idea is to check if there exists strong impact on some performance characteristics or impact can be neglected in terms of current use cases.

The aim of the first test is to check communication delays. Even none of current use cases demands real time communication, very long communication delays can impact network stability. To test communication initialization delay the time from launching application till first received message was measured in plain and secured scenarios. In both scenarios two SunSPOT nodes were used. One of them was configured to listen for incoming packets, other node was initiating communication and sending messages. The results are as following: in plain scenario maximal initialization delay was 1 second, in secured scenario maximal delay increased significantly - up to 8 seconds. Even if impact is so significant it should not affect network's performance, because it is delay of the initialization, which is performed only at the beginning of communication session.

Next test is aimed to find communication delays in normal operating mode, i.e. after initialization. Given hardware and software tools don't have ready made delay measuring mechanisms, therefore to minimize the time for obtaining the results, visual delay check was used. SunSPOT nodes have ready made demo application for communication testing called "BouncingBall". Each SunSPOT node has eight LEDs in a row, application creates virtual connection between two SunSPOT LED rows and after that there is one 16 position virtual row

for displaying moving virtual ball that is imitated by blinking LED. The ball is able to "jump" from one node to another when it reaches last LED in a physical row. Replacing plain text data transfer for secure in this ready made demo application and looking at working application if there is delays between "jumps" could save a lot of time, comparing it with own delay measuring application creation. When modified application was launched and the ball was bouncing from one node to another, no delay could be seen. Therefore delay is not significant in aspect of project's use cases.

Delay test prove that SunSPOT nodes are able to use SSL technique in project's use cases. Test shows that there is no delay in message transfer after initialization phase and it means that there is enough node's processing power and throughput of wireless channel to encrypt and send message data with encryption and hash function overhead. Still it is unknown how big is increase in node's CPU load and message data size. There are no functions to measure CPU load in SunSPOT nodes and indirect techniques, like evaluating the number of active process threads, cannot give precise results. It is possible to evaluate CPU load theoretically looking on the algorithms used in data encryption and hashing. Briefly looking on RC4 and SHA1 [11] algorithms it is clear that there is no complex and long lasting mathematical operations, therefore encryption and hashing would not significantly affect node's primary objective realization, still additional tests are required to prove this statement.

Increase in CPU load due to SSL technique usage couldn't be measured directly, but there is possibility to measure communication data overhead. It could be done using wireless sniffer, a program that is able to capture all wireless transmissions that are sent from SunSPOT nodes. SunSPOT SDK contains ready made application for sniffing. Using this program nodes' transferred data were captured in SSL and plain communication modes. After capturing data packets it is possible to see transferred data and therefore obtain message size. The results of this test confirm that data encryption using RC4 algorithm adds no overhead and SHA (SHA1 - 160 bits) hash produces 20 bytes of overhead. Overhead is not big in absolute scale (transferring 20 bytes will take less than 1ms). In practice wireless sensors send small data amounts and effective data size is comparable with overhead, therefore efficiency of data transfer will be only half from maximal. To increase efficiency data could be buffered and sent by big blocks using all available packet size (~2K bytes at most). In this case efficiency could be >99%.

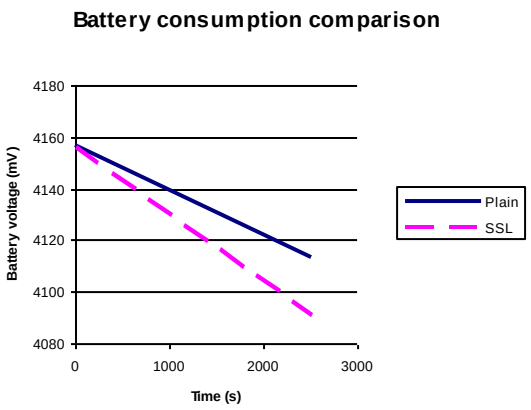

Fig.2 Wireless node battery consumption comparison in secured and plain transmission modes

To test the influence of increase in CPU load and sent data overhead, battery consumption was measured in SSL and plain text transmission modes. SunSPOT SDK contain tools to measure battery voltage, therefore it is possible to determine if there is increase in energy consumption between two above mentioned modes. Figure 2 shows that in SSL mode voltage drop is bigger than without encryption for 48%. For the test same nodes were used, both modes testing started at full battery and were performed for 2500 seconds.

Each second 20 bytes of actual data were sent. In SSL mode total packet size was 45 bytes, due to overhead. As it could be seen, SSL usage increases node battery consumption, main reasons for that are sent data overhead and increase in CPU load for encrypting and hashing of the data. It should be mentioned that this test cannot be perfectly accurate, because voltage drop is not linear, but it prove that there is noticeable increase in energy consumption.

Literatūras saraksts (piemērs)

1. Bing B. Emerging Technologies in Wireless LANs. Theory, Design and Deployment. – New York, Cambridge University Press, 2008, 853

2. ProSense project homepage [Electronic resource] - http://www.prosense-project.eu – Resource reported at 2009, 19'th of October
3. SunSPOT wireless sensors developers homepage [Electronic resource] - http://www.sunspotworld.com - Resource reported at 2009, 19'th of October
4. RFC 65454 standard description [Electronic resource] – http://tools.ietf.org/html/rfc5246 – Resource reported at 2009, 19'th of October
5. Energy efficient link-layer jamming attacks against three wireless sensor network MAC protocols. 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), 2005 November. – New York: ACM, 2005 pp. 76-88
6. Raymond D.R., Midkiff S.F. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. IEEE Pervasive Computing vol.7 no.1 – Washington: IEEE Computer Society, 2008, pp. 74-81
7. IEC 60529 standard [Electronic resource] – http://www.iec.ch – Resource reported at 2009, 19'th of October
8. NEMA Standards Publication 250-2003 [Electronic resource] – http://www.nema.org – Resource reported at 2009, 19'th of October
9. SEC1: Elliptic Curve Cryptography [Electronic resource] – http://www.secg.org/download/aid-385/sec1_final.pdf – Resource reported at 2009, 19'th of October
10. Huge Advance for Tiny Devices [Electronic resource] – http://research.sun.com /spotlight/2005_02_10.tiny_devices.html – Resource reported at 2009, 19'th of October
11. RFC 3174 standard Devices [Electronic resource] – http://tools.ietf.org/html/rfc3174 – Resource reported at 2009, 19'th of October

Dmitry Bliznyk Mg.sc.ing.
Researcher at Riga Technical University
Faculty of Computer Science and Information Technology
Department of Computer Network and System Technology
Address: Meza str.1, LV-1048, Riga, Latvia
E-mail: dmitrijs.bliznuks@rtu.lv

Bļizņuks D. Vides pārraudzības paredzēto bezvadu sensoru tiklu drošības problēmas

Bezvadu sensoru tīklu izmantošana vides pārraudzībai prasa pilnīgo aizsardzību. Raksts atspoguļo tīkla drošības pasākumus ES „Seventh Framework Programme" ProSense projekta piecu pielietojumu ietvaros. Drošības problēmas ir apskatītas no četrām pozīcijām: privātums, autentificēšana, konfidencialitāte un nepārtrauktība. Katram pielietojumam tiek aprakstītas to specifiskas drošības problēmas un to pārvarēšanas iespējas. Rakstā tiek atspoguļota drošas bezvadu komunikācijas praktiskā realizācija uz SunSPOT platformas izmantojot mezgla resursu nepieticīgu eliptisko līkņu kriptogrāfijas šifru komplektu. Nobeigumā ir parādīti tīkla testēšanas rezultāti, kā arī drošas datu pārraides mehānisma ietekme uz izmantotiem mazas skaitļošanas jaudas sensoru funkcionāliem parametriem. Testi apskata bezvadu sensoru komunikācijas aizkavi inicializācijas fāzē un normālā darbībā, drošā un atvērtā pārraides režīmā. Kā arī enerģijas patēriņš tika salīdzināts drošā datu pārraides režīmā un nešifrētā teksta sūtīšanas gadījumā.

Близнюк Д. Проблемы безопасности в беспроводных сенсорных сетях, предназначенных для слежения за окружающей средой

Использование беспроводных сенсорных сетей для слежения за окружающей средой требует полной уверенности в надежности полученных данных. Данная статья описывает способы обеспечения безопасности сети в пяти практических применениях реализованных в рамках проекта ProSense Европейской программы „Seventh Framework Programme". Проблемы безопасности рассмотрены с точки зрения четырех аспектов: приватность, аутентификация, конфиденциальность и безотказность. Были исследованы специфические проблемы безопасности для каждого из применений и указаны пути преодоления этих проблем. В статье описывается практическая реализация безопасной передачи данных, реализованная на элементной базе «SunSPOT» с использованием нетребовательного к ресурсам комплекта шифров на базе эллиптических кривых. Также отражены результаты практических испытаний безопасной передачи данных и ее влияния на функциональные характеристики сенсоров с малой вычислительной мощностью. В тестах были оценены задержки коммуникации на этапе инициализации и обычном обмене данными, в защищенном и открытом режимах посылки данных.