Security Mechanisms in Resource-Constrained Computer Systems

Erman Döser Abdul Jamal
*Email: {*ermdo912*, abdja944}@student.liu.se*
Supervisor: Christian Vestlund, {christian.vestlund@*.liu.se*}
Project Report for Information Security Course
Linköpings Universitetet, Sweden

Abstract

In this report, we present a brief description of how the need of security mechanisms will impact and reduce the performance of the different dedicated embedded systems. We provide a brief look to two types of networks -Ad hoc and sensor-, which have challenges in deploying security mechanisms on embedded systems due to the limited resource constraints. We also discuss various design limitations such as processing gap, battery gap, flexibility, tamper resistance, and assurance gap. In addition, we empower our study with the solutions to these limitations, which are represented in various articles.

1. Introduction

Security in embedded systems becomes an important concern due to the need for a safe communication channel in terms of integrity and confidentiality of the information when they are used for military purposes.

Nowadays, security is not an additional future of a system, and should be included in the design and implementation phases of the development. Moreover, security in software and hardware are developed as a unit. Thus vulnerabilities in embedded systems can be obtained in both software and hardware level. In case of a failure in the implementation of security measures in the hardware level, the cost that is needed to fix such an issue would be high [25].

Limited capabilities of embedded systems lead designers to the consideration of the important measurements such as cost, performance and also power. Due to the fact that cryptographic functions are expensive to compute, designers are subject to develop new approaches in order to cover performance issues. In addition, the increasing need for energy in the security mechanisms, and the need of the execution of different security mechanisms on the same embedded system in order to provide multi-featured devices (e.g. the connectivity through both 3G and wireless network on a mobile device, called Flexibility) are examples of other challenges in designing a security mechanism for embedded systems [24].

The sensitivity of the security in ad-hoc networks and sensor network depends on the purpose for which they are used. For instance, a network that is established for military purposes, is supposed to require a solid security.

Security in Ad hoc networks mostly suffers from the absence of a base for defense according to its most distinguishing property: self-organization [26]. The lack of traffic monitoring and the unprotected environment leave these networks vulnerable to the various attacks. Thus, security becomes a challenging issue in ad-hoc networks and sensor network.

We will discuss some of the limitations of the Ad hoc / Sensor networks and consequences of them from the security perspectives.

2. Background

One of the key design problems in the embedded systems is the security mechanism implementation based on cryptographic algorithms and security protocols [24].

Our literature survey is focused on efficient security mechanisms in wireless ad-hoc and sensor networks, design challenges, possible attacks, various solutions, and tradeoffs between these challenges.

3. Design Challenges and Problems

Security is an important concern in the network embedded systems due to the increasingly sensitive data exchanged.

Limited resource constraints such as power, energy, processing capacity, size, and memory are another concerns of embedded systems.

In order to deploy security mechanism in the ad hoc and sensor networks on embedded systems, designers must know the unique traits of the embedded devices, which makes it challenging.

In this section, we point out the design problems and challenges, which cause difficulty for the designer to implement an effective security mechanism in the ad hoc and sensor networks on embedded systems.

- **Processing gap**

Current limited resource ad hoc and sensor devices are hardly capable of keeping up the computational and processing power demands of the security mechanisms. Cryptographic functions are expensive to compute, designers are subject to develop new approaches in order to cover performance issues [1][2].

- **Battery gap**

Power and energy consumption overhead of supporting the security mechanism on the battery constrained ad hoc and a sensor network device is very high [1][2].

- **Tamper Resistance**

Sensor and ad hoc devices are facing an increasing number of threat and attacks from the physical hardware and software attacks [1][2].

- **Assurance gap**

It should the possibly hard that the ad hoc and sensor device should continue to operate reliable even if it is attacked [1][2].

In order to analyze these challenges, we will investigate the security mechanisms, how they are affected by resource constraints, which challenges they are related to, and which solutions have been found against those challenges, in three different network mechanisms, which are designed for embedded systems.

4. Method

Our method of work is a literature survey. The aim of our study is to have an in-depth understanding of how resource constraints affect the deployment of security mechanisms.

We chose two types of networks, which are usually structured on embedded systems, in order to investigate the effects of resource constraints in security designs and exemplify proposed solutions.

5. Resource Constraints and Security Issues in Ad hoc and Sensor Embedded system

Maintaining routing security in a critical network system for military concerns, or in the case of a catastrophe by using low-powered nodes with limited computational capacity is a challenging issue. The mobile devices that are being used in such a network are vulnerable for various attacks. Thus, in such a network system, it is not possible to implement a public key infrastructure based on a reliable Certificate Authority, due to the missing implementation of an infrastructure [17].

The most effective resource constraints on ad-hoc networks are energy, computational power and bandwidth limitations. In addition, wireless channels, which provides lower capabilities compared to wired channels, are inconsistent because of high power consumption and unstable signal quality [28]. Resource aware security mechanisms are focused on obtaining the optimal tradeoff between the reasonable security level and the network performance. On the contrary, conventional security mechanisms are subject to cause overheads on bandwidth, energy consumptions [18].

Characteristics of Wireless Ad-hoc Networks (WANET's) and the capabilities of mobile nodes require efficient security mechanisms. For instance, there is still a challenge between the symmetric and the asymmetric approaches. Even though symmetric approach uses one key for both encryption and decryption, and it needs less computational power, scalability with symmetric approach is poor compared to the asymmetric approach. Also, symmetric approach requires more bandwidth usage in order to establish a secret key. On the other hand, asymmetric approach has its disadvantages such as, leading to Denial of Service (DoS) attacks and difficult public key management.

There are possible threats on basic mechanisms and security mechanisms in ad-hoc networks. The former generally is focused on routing protocols and the latter is focused on key management. The basic mechanisms (e.g. routing) are extremely vulnerable in ad-hoc networks because every node routes packages. In case of a hijacked node, an attacker can affect the whole network unlike conventional networks [25]. In addition, the characteristics of WANET's, such as dynamic topology, the absence of an infrastructure, limited capabilities, and open medium, become the skeleton of vulnerability to the various attacks for routing routines [17].

In order to provide robust security mechanisms, the possible attacks and threats have to be addressed correctly. Hence, these attacks are defined in two

categories called as passive and active. The passive attacks, which aim to gather information from the network, are hard to detect. The active attacks usually focus on data modification and manipulating the packet transmission, thus violating integrity, and are classified in two categories: external and internal [17].

In order to stay in the scope, this part of the paper concerns the routing attacks, which directly threatens the network layer in the protocol stack. The routing protocols in ad-hoc networks such as Ad Hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are based on an assumption of trusted environment. Moreover, this vulnerability allows attackers to capture devices and make them behave maliciously to capture information from the network or manipulate the routing tables with improper information such as wrong distance values or deleting a node from the list.

It is also possible for attackers to direct the network traffic to the nodes, which they have captured, by manipulating routing tables. For instance, a node without fresh route information to the destination node can be malicious and claim the information in order to crash the whole network or a part of it. This attack is also known as “black hole” [20].

Wireless sensor devices, which are highly distributed networks of devices, are deployed in large numbers to sensing, processing and communications to monitor the modern world environment. However, sensing devices have critical, limited resource constraints due to their lack of computation power, power supply, memory and effective low cost. They are also constrained by their physical size.

One of the key design problems in embedded systems is the security mechanism implementation based on cryptographic algorithms and security protocols [1][2][4].

Limited bandwidth and transmission power constraints are affected by security mechanisms. Key distribution techniques allow small chunks of data, so it is not efficient to send large amount of data on the limited bandwidth [3]. For example, UC Berkeley Mica platform transmitter has a bandwidth of 10 Kbps and low transmission reliability makes communication of large blocks of data expensive [3].

Limited memory and processor capacity are extremely low in typical sensor devices. SmartDust, as an example, has 8bit, 4 MHz CPU, 512 RAM [9].

All embedded wireless devices are vulnerable to security attack, and sensor has additional security attack because of physically not safe. We present a list of attacks, which can be addressed in sensor networks.

Physical Attacks: Sensor devices operate in hostile outdoor environments, which is highly susceptible to physical attacks. Node destructions, revealing secret cryptographic information, tamper with associated circuitry; modify programming in sensors [1][4][13].

Node Replication Attacks: Attacker adds a node to an existing sensor network and copy the ID of the node. This attack makes the network performance worst, disconnected, false read and reveals the secret keys [1][4][13][14].

Denial of Service Attacks: To cause degradation in network capacity, make out of order, consumes their energy and affect the resource to perform its expected functions. Defense against DOS attacks require high processing overhead and hence not suitable for resource constrained sensor network and very costly [1][4][13].

Sybil Attack: In this case the one node presents more than one identity or node has more addresses. Similarly it also affects the routing mechanism, multiple routes through a single malicious node [13].

These attacks cannot allow the sensor to go in sleep mode if there is not data for processing and attacks sends message. This will affect the performance of the battery [14].

6. Solution and Analysis

6.1 Effects of Resource Constraints and Security Issues in Ad hoc networks

There are two approaches listed as proactive and reactive. The proactive approaches aim to protect the system against attacks by using cryptographic functions. On the other hand, the reactive approaches aim to detect attacks then defuse them accordingly.

In order to prevent the threats, which we stated in the previous section, against the routing protocols in ad hoc networks, prevention, detection, and reaction should be implemented as a whole by combining reactive and proactive approaches [3].

The common message authentication primitives, which are used in most security solutions, are Message Authentication Codes (HMAC), Digital Signature, and One-way HMAC key chain. HMAC uses pair wise shared keys, which are obtained by "n" nodes in order to verify a message between two nodes by using a hash function. This one-way hash function can produce the output efficiently, thus nodes do not suffer from processing gaps.

On the contrary to this "symmetric" approach, Digital Signature uses asymmetric approach and can be approved by any node, which can reach the public key of the signing node. This approach needs more computational power and is less secure against DoS. In other words, the attacker can drain the batter power of a node by enforcing it to verify bunch of signatures [4].

In the third approach, a chain of a cryptographic hash function is used to authenticate a message. The computation involved does not cause processing gaps, however, for immediate authentication; the internal clocks of the nodes need to be synced. In order to point out the practical applications of these approaches to routing protocols, SEAD [5] and Ariadne [6] can be reviewed.

The absence of a systematic approach in the design of a security mechanism can lead high network loads and DoS attacks [2]. For a whole security provisioning, Chigan, Li and Ye proposed a framework in order to apply the sufficient security measures on the necessary network layers in order to provide a complete coverage of security. The approach consists of two parts named as "the offline optimal cross-layer secure protocol set selection" and "the online self-adaptive security control module". [18]

Implementing a secure protocol at every layer of the network protocol causes a large overhead on system resources. In that sense, applying security mechanisms on the most suitable layer is reasonable due to the fact that high security provisioning is not necessary for some systems and the data coming from a higher level is always perceived as payload data.

In order to determine the most suitable layer set, Chigan, Li and Ye presented two quantities: security index (SI) and performance index (PI). SI is a value assigned for the contribution of the layer to the security level of the system, and PI represents the effect of implementing the security mechanism at the related level with respect to the QoS measures.

The offline optimal cross-layer secure protocol set selection part of their approach constructs different protocol sets according to their security level (high, medium, low) with their performance costs. The higher SI results better security, the lower PI results better performance. According to this, the protocol set which have the highest SI and the lowest PI is the most efficient set. During this selection, the minimum SI of a protocol set has to be higher than the security expectation of the network. In addition the highest PI in a protocol set has to be lower than the minimum QoS expectations. This procedure is done offline.

Since the offline optimal secure protocol selection mode offers a set of protocols, which are categorized according to their SI and PI values, there is an availability of adapting the security level according to the malicious activity in the network environment. The online self-adaptive security control module is a response to that gap in the security provisioning. Every node applies "online peer trust evaluation model" in order to determine if there is a malicious activity in the network. According to the negotiation between the nodes, the necessary security level can be obtained and the protocol set, at which security mechanisms are applied, can be changed with another set. Therefore, the required security can be covered while the performance costs are degraded [18].

6.2 Effects of Resource Constraints and Security Issues in Sensor networks

We presented various types of attacks, which threaten wireless sensor devices, above. These attacks impact on the processing power, energy capacity, memory and cost.

The main objective should be to find simple solutions that allow the low power consumption, little energy, less memory and minimum cost.

In the sensor network various security mechanisms solution have been point out (Hardware and Software approaches) for the wireless sensor embedded devices. In order to design the security mechanisms for Wireless Sensor system, it is necessary to be aware about the constraints and limitation of sensor nodes.

It is possible to deploy security mechanisms both in hardware and software levels. Although implementing security via software running on programmable processor, gives good flexibility and fast implementation, it affects performance of the processor and energy consumption on the embedded device [1][4].

Another solution is implementing a specific hardware to perform cryptographic functions, which has high performance and lower energy consumption regarding to processing gap, limited flexibility. However, deploying security mechanisms on the entire network in the hardware level is quite extensive and challenging [1][4].

Alternative hardware solution in sensor networks is designing separate cryptographic processors, which reduce the computation workload on the main processor and provides high performance, low energy consumption. On the contrary, due to the extensive number of nodes in a network, there will be a high cost of producing such hardware for each node [7].

6.2.1 Appropriate Cryptographic Method for Sensor Network

Although many researchers noted that the public key cryptography is not suitable for sensor networks, the papers, we have studied, states that it is feasible to apply public key cryptography with ECC and RSA algorithms on the sensor devices [15][16].

Elliptic curve cryptography (ECC) is suitable for resource constrained sensor networks. It provides more security per bit than other asymmetric cryptographic approaches. It also offers efficient authenticated key transfer mechanism, encryption and decryption [29]. Even smaller key size provides better level of security thereby reducing processing and communication overhead [29].

As an example, RSA with 1024 bit key size, which equivalent in strength of ECC with 160 bit keys, RSA key size for most application is 2048 bit while equivalent to ECC key size 224 bits [30].

This means ECC provides the same level of security with RSA by using less resource. It can be used to create smaller, faster and more efficient cryptographic keys. In conclusion, ECC has benefits of low computing power need, less memory need, less energy consumption.

Piotrowski, Langendoerfer, and Peter also stated that RSA is not the best choice for wireless sensor networks. Their results for the time needed for SSL/TLS handshake on different hardware shows that calculations and the data has to be transmitted while RSA is being used, causes higher time results compared to ECC. Results are listed below [31].

Sensor node	RSA-1024 handshake	Performance ratio (RSA)
MICA2DOT	22.00 s	1.00
MICA2/MICAz	12.00 s	1.83
TelosB	5.70 s	3.86
Sensor node	ECC-160 handshake	Performance ratio (ECC)
MICA2DOT	1.60 s	1.00
MICA2/MICAz	0.87 s	1.85
TelosB	0.50 s	3.20

6.2.1.1 Symmetric Key Cryptography

In many of the sensor networks, symmetric key cryptographic algorithms are used. The challenge to deploy this approach in sensor networks is to take care of the single share key. The encryption schemes AES, RC4, RC5, SHA-1 and MD5 have uniform cost for six different processors Atmet AVR, Mitsubishi M16C but the hashing algorithm MD-5, SHA-1 increase the higher overhead than encryption algorithm [4].

This method is more efficient than public key method in terms of speed, low energy and cost [4].

Effective key distribution mechanism in the symmetric key cryptography is needed.

6.2.1.2 Key Management

Global key: This key encrypt and decrypted the information with the same key and entire network has one key shared and it increase the energy efficiency, but attacks can be easily come [14].

Pair wise key node: Different keys shared with the n number of neighbors, which increase the security but limit the energy and calculation time [14].

Pair wise key Group: Cluster based key share between the nodes, but problem is cluster head not consume all the energy [14].

7. Evaluation and Comparison

Cryptographic hardware provides support to increase the efficiency but also it will increase the cost of the whole device. On the other hand, in recent researches, it is stated that a reasonable security level can be obtained by only cryptographic software. For example, TinySec implementation, which uses only software methods for cryptographic calculations, by University of California, Berkley, discloses 5%-10% overhead on packet size. If it is considered that hardware implementations cannot reduce packet size, there is a limit for the enhancement that can be obtained by hardware [12].

Hardware mechanisms will make a sensor device tamper-resistant is very high cost while the low cost, low power sensor devices in hostile environments are vulnerable to physical capture by an attacker [10].

Low computing power cannot be process the complex cryptographic algorithms for sensor networks as Public

key cryptography, for example MicaZ sensor 16MHz of frequency and 128k of memory [14].

Selecting appropriate cryptographic methods depends on the processing capability, energy and cost of the sensor node and ad hoc, there is no unified solution for all sensor and ad-hoc devices. Security mechanism are highly application specific [4].

8. Conclusions

This paper summarizes how security mechanisms are affected by limited resource constraints of nodes in sensor and ad hoc networks, and also explores the attacks, which are handled by the security mechanisms.

References

[1] Jian Qin Hardware mechanisms and their implementations for secure embedded systems, Linköping University 2005

[2] Lyes K, Yacine C, Abdelmadjid B, Nadjib B, "On Security Issues in Embedded Systems: Challenges and Solutions." 2009

[3] Yang Xiao, Venkata Krishna Rayi, Bo Sun "A Survey of Key Management Schemes in WirelessSensor Networks" 2007

[4] Jaydip Sen "A Survey on Wireless Sensor Network Security" Vol. 1, No. 2, August 2009

[5] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley and Sons, 1996

[6] S. K. Miller, "Facing the Challenges of Wireless Security," *IEEE Computer*,vol. 34, pp. 46–48, July 2001.

[7] Guy G,Tilman W,Wayne B"Reconfigurable Security Support for Embedded Systems" 2006

[9] A. Perrig, R.Szewczyk,V.Wen,D.culler "Security protocols for sensor network" 1998 pp163-168

[10] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway. A survey of key management schemes in wireless sensor networks. 2007

[11] Jaydip Sen A Survey on Wireless Sensor Network Security Vol. 1, No. 2, August 2009

[12] Adrian P, John S, David W, "Security In Wireless Sensor Networks"2004

[13] John P, Zhengqiang, L,Weisong S, and Vipin "Wireless Sensor Network Security: A Survey" 2006 chtp 17

[14] David M Hervé G "Wireless Sensor Network Attacks and SecurityMechanisms : A Short Survey"

[15] N. Gura et al., "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," Aug. 2004.

[16] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public Key Cryptography in Sensor Networks-Revisited,", 2004.

[17] Routing Security in Wireless Ad Hoc Networks, Hongmei Deng, Wei Li, Agrawal, D.P., Cincinnati Univ., OH, USA

[18] Resource-aware Self-Adaptive Security Provisioning in Mobile Ad Hoc Networks, Chunxiao Chigan, Leiyuan Li, Yinghua Ye

[19] Security in Ad-hoc Networks Arun Kumar Bayya, Siddhartha Gupte ,Yogesh Kumar Shukla, Anil Garikapati

[20] Hao Yang, Haiyung Luo, Fan Ye, Songwu Lu, "Security In Mobile Ad-Hoc Networks: Challenges and Solutions"

[21] Y. Hu, D. Johnson, and A. Perrig, "Sead: Secure Effi- cient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," IEEE WMCSA, 2002.

[22] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A SecureOn-demand Routing Protocol for Ad Hoc Networks,"ACM MOBICOM, 2002.

[23] Lyes Khelladi, Yacine Challal," On Security Issues in Embedded Systems: Challenges and Solutions "

[24] Srivaths Ravi, Anand Raghunathan, Paul Kocher, and S. Hattangady. Security in embedded systems: Design challenges. ACM Transactions on Embedded Computing Systems

[25] Tsutomu Matsumoto. Security Issues in Networked Embedded Systems and InformationAppliances. Network, (October):13{14, 2009.

[26] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in Mobile Ad-hoc Networks: Challenges and Solutions. Wireless Communication 2005

[27] J.P. Hubaux, L. Butty_an, and S. Capkun. The Quest for Security in Mobile Ad Hoc Network 2001

[28] Yuguang Fang, Xiaoyan Zhu, and Yanchao Zhang. Securing resource-constrained wireless ad hoc networks2009

[29] An Elliptic Curve Cryptography (ECC) Primer www.deviceforge.com/articles/AT4234154468.html Jul. 20, 2004

[30] Elliptic Curve Cryptography, SECG Std. SEC1, 2000, available at www.secg.org/collateral/sec1.pdf

[31] How Public Key Cryptography Influences Wireless Sensor Node Lifetime, K.Piotrowski, P.Langendoerfer, S. Peter, SASN '06 Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. 2006